

Міністерство освіти і науки України,
ДНУ «Інститут модернізації змісту освіти»,
Національний технічний університет України «Київський політехнічний інститут ім.
Ігоря Сікорського»,
Інститут кібернетики ім. В.М. Глушкова НАН України,
Інститут телекомунікацій і глобального інформаційного простору НАН України,
Інститут цифровізації освіти НАПН України,
Житомирський державний університет імені Івана Франка,
Житомирський військовий інститут імені С.П. Корольова,
Черкаський державний технологічний університет,
Вінницький національний технічний університет,
Опольська політехніка (Республіка Польща),
Варшавський технологічний університет (Республіка Польща),
Технологічний університет Лулео (Королівство Швеція),
Технічний університет (Чеська Республіка),
Технічний університет (Республіка Болгарія),
Університет країни Басків (Королівство Іспанія),
Віденський технічний університет (Республіка Австрія),
ADA University (Азербайджан)

ТЕЗИ ДОПОВІДЕЙ

*XVI Міжнародна
науково-технічна конференція*

Інформаційно-комп'ютерні технології

м. Житомир, 02-03 квітня 2026 р.

Житомир

2026

УДК 004
Т11

*Рекомендовано до друку Вченою радою Державного університету
«Житомирська політехніка» (протокол № 7 від 27.04.2026 р.)*

Тези XVI Міжнародної науково-технічної конференції
Т11 «Інформаційно-комп'ютерні технології», м. Житомир, 02-03 квітня
2026 р. – Житомир: Житомирська політехніка, 2026. – 742 с.
ISBN 978-966-683-734-2

Представлено доповіді учасників XVI Міжнародної науково-технічної конференції. Наведено аналіз та результати досліджень сучасних проблем інформаційних технологій, математичного моделювання та розробки програмного забезпечення, інформаційних систем, комп'ютерної інженерії та кібербезпеки, цифрової обробки сигналів та зображень, комп'ютерно-інтегрованих технологій, робототехніки та приладобудування, інформаційних технологій в телекомунікаціях та біомедицині, інформаційно-комунікаційних технологій в освіті.

УДК 004

Наукове видання

Тези XVI Міжнародної науково-технічної
конференції «Інформаційно-комп'ютерні
технології»,
Житомир, 02-03 квітня 2026 р.

Відповідальний за випуск

Ю.В. Венгловська

Свідцтво про внесення до Державного реєстру суб'єктів видавничої справи ДК № 7177 ВІД 04.11.2021 р.

Адреса редакції: Державний університет «Житомирська політехніка»,
вул. Чуднівська, 103, м.Житомир, 10005

© Житомирська політехніка, 2026

Секція 1 **МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА** **ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

УДК 004.421.2

Заїка Д.В., здобувач
Кобилін І.О., асистент

Харківський національний університет радіоелектроніки

ОПТИМІЗАЦІЯ АЛГОРИТМІВ КОДУ У ВІДЕОІГРАХ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ПРОБЛЕМИ ЕФЕКТИВНОСТІ

Сьогодні ігрова індустрія є дуже популярною, і системи на яких запускаються ігрові застосунки досягли вражаючих рівнів. Попри це, їх продуктивність зменшилась. Це можна пояснити тим що через дедлайни, стрімку конкуренцію та заради більшого охоплення аудиторії, розробникам залишається все менше часу на оптимізацію алгоритмів, змушуючи їх зосереджуватись переважно на графіці та швидкому виробництві контенту.

Оптимізація алгоритмів – це важливий процес спрямований на підвищення ефективності та продуктивності із використанням меншої кількості обчислювальних ресурсів. Це стосується механізмів обчислення фізики, поведінки штучного інтелекту, рендерингу графіки та управління даними.

У минулому розробники були вимушені працювати із мінімальними ресурсами для створення ігор, тож їм доводилося оптимізувати кожен рядок коду. З 1990-х до початку 2000-х років було написано такі ігри як half-life, deus ex, morrovind, gta 3 які демонструють, наскільки майстерно було реалізовано ефективність програмних рішень. Вони залишалися технологічно передовими, водночас маючи мінімальні вимоги до апаратного забезпечення.

Сучасне нехтування оптимізацією частково пов'язано із тим що ігрові рушії спрощують написання коду, роблячи його універсальним, але це призводить до зниження його швидкодії. Також із появою все кращого апаратного забезпечення створюється ілюзія що оптимізація ігор може залишатися в минулому. В тому числі варто згадати про популяризацію нейронних мереж що генерують готові алгоритми для розробників, але які не завжди роблять їх оптимальними, або навпаки роблячи їх дуже неефективним.

Через нехтування оптимізацією з'являється своєрідне коло: розробники створюють неоптимізовані програми вважаючи що

користувач придбає нове апаратне забезпечення яке буде здатно їх запускати. Як наслідок, користувачам доводиться обирати між відмовою від продукту або купівлею нового апаратного забезпечення, хоча, теоретично, із оптимізацією програм, навіть системи що вважаються застарілими могли б запускати сучасні ігри.

Таблиця 1 – Роки, з яких вимоги апаратного забезпечення стрімко зросли

	ОЗП			VRAM		
Рік	2014	2015	2016	2014	2015	2016
Рекомендована кількість	4 GB	8 GB	16 GB	1 GB	3 GB	4 GB

Оптимізація алгоритмів коду у відеоіграх не має бути застарілою практикою, вона повинна бути умовою сталого розвитку ігрової індустрії. Ігри повинні не тільки мати вражаючі візуальні ефекти чи цікаві механіки, а й бути здатними запускатися не виключно на найсучасніших системах. Справжня майстерність програміста полягає не у використанні найновішого обладнання, а у здатності досягати високої якості на обмежених ресурсах. Тож, якщо сучасні розробники повернуться до принципів оптимального програмування, користувачі зможуть насолоджуватися іграми без зайвих витрат на постійне оновлення техніки, а індустрія – розвиватись без технічної марнотратності.

Список використаних джерел:

1. Game Engine Black Book: Doom. CreateSpace Independent Publishing Platform, 2019. 432 p.
2. Alan C. The Inmates Are Running the Asylum: Why High Tech Products Drive Us Crazy and How to Restore the Sanity. Upper Saddle River : Pearson Education, 2008.
3. Bentley J. Programming pearls. Communications of the ACM. 1986.
4. Nystrom R. Game Programming Patterns. Apress, 2011. 300 p.

УДК 004.4:004.85

*Сосновська Є.Р., здобувач,
Осипова О.І., к.е.н., доцент*

*Київський національний економічний університет імені Вадима
Гетьмана*

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМАТИЗОВАНОГО ЗБОРУ ТА АНАЛІЗУ ДАНИХ РИНКУ НЕРУХОМОСТІ

Актуальність дослідження ринку нерухомості зумовлена постійною динамікою цін та величезним обсягом неструктурованих пропозицій на профільних веб-ресурсах. Для ефективного моніторингу та прийняття обґрунтованих рішень критично необхідною є автоматизація збору інформації та побудова надійних математичних моделей для оцінки вартості майна.

Метою даної роботи є розробка програмного забезпечення для автоматизованого збору даних з ринку нерухомості та створення на їх основі прогностичних моделей для оцінки вартості житла. Для досягнення цієї мети було реалізовано таку послідовність етапів дослідження: спочатку було розроблено програмний модуль для автоматизованого збору даних (парсер), далі сформовано та збережено набір даних з характеристиками об'єктів нерухомості, після цього виконано попередню обробку та аналіз даних, і на завершальному етапі побудовано та оцінено моделі машинного навчання для прогнозування вартості квартир.

Ядром розробленого програмного забезпечення є модуль автоматизованого збору даних з сайту lup.ua [1], реалізований мовою Python виключно за допомогою інструменту автоматизації браузерів Selenium [2]. Архітектура парсера побудована на механізмах явного очікування - скрипт синхронізується з роботою веб-ресурсу і ініціює вилучення даних лише після повної появи та рендерингу цільових об'єктів у DOM-структурі сторінки. Це гарантує стабільний збір інформації без необхідності застосування алгоритмів імітації поведінки користувача.

Парсер налаштований на вилучення строго визначеного набору характеристик кожного об'єкта:

- кількість кімнат;
- загальна площа, житлова площа та площа кухні;
- поверх та загальна поверховість будинку;
- рік будівництва;

- ціна за квадратний метр.

На етапі первинної обробки зібрана ціна за квадратний метр алгоритмічно перетворюється у підсумкову вартість квартири, яка виступає цільовою змінною для подальшого аналізу [3].

Перед навчанням моделей "сирі" дані пройшли етап глибокої обробки за допомогою бібліотеки Pandas [4]. Процес включав очищення датасету, трансформацію ознак та важливий крок - усунення мультиколінеарності шляхом аналізу та відкидання певних взаємозалежних змінних (ознак), що дозволило підвищити стабільність та інтерпретованість моделей.

Враховуючи суттєві економічні розбіжності у ціноутворенні, очищений датасет був концептуально розділений на дві незалежні групи: квартири в місті Києві та квартири в інших обласних центрах. На основі сформованих вибірок було побудовано окремі регресійні моделі з використанням алгоритмів машинного навчання бібліотеки Scikit-learn [5], зокрема Random Forest Regressor, k-Nearest Neighbors Regressor та Decision Tree Regressor. Розділення даних за географічною ознакою (Київ та інші міста) дозволило врахувати регіональні особливості формування цін на ринку нерухомості, що сприяє підвищенню точності прогнозування вартості квартир.

Розроблений програмний комплекс забезпечує повний цикл роботи з даними ринку нерухомості. Застосований підхід - від стабільного автоматизованого збору цільових метрик за допомогою Selenium до географічного кластеризації даних та очищення ознак від мультиколінеарності - доводить свою ефективність у створенні точних прогностичних інструментів для сфери PropTech.

Список використаних джерел:

1. ЛУН – пошук нерухомості в Україні. URL: <https://lun.ua/> (дата звернення: 06.03.2026).
2. Selenium Documentation. URL: <https://www.selenium.dev/documentation/> (дата звернення: 06.03.2026).
3. VanderPlas J. Python Data Science Handbook: Essential Tools for Working with Data. O'Reilly Media, 2016. 546 p.
4. pandas - Python Data Analysis Library. URL: <https://pandas.pydata.org/docs/> (дата звернення: 06.03.2026).
5. Scikit-learn: Machine Learning in Python. URL: https://scikit-learn.org/stable/user_guide.html (дата звернення: 06.03.2026).

УДК 004.076.2

Царева О.С., асистент,

Цап Д. І., здобувач

Івано-Франківський національний технічний університет нафти і газу

ЕНЕРГОЕФЕКТИВНІСТЬ ПРОГРАМНОГО КОДУ: АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ

Енергоефективність програмного коду сьогодні виходить на передній план серед глобальних викликів ІТ-індустрії, перетворюючись із глибокої концепції на критичну необхідність. Із значним зростанням обсягів даних та обчислювальних потужностей екологічний слід цифрових технологій стає дедалі відчутнішим. Екологічне програмування — це екологічно стійка обчислювальна практика, яка прагне мінімізувати енергію, задіяну в обробці рядків коду, і, у свою чергу, допомогти організаціям зменшити загальне споживання енергії.[1] Ця тенденція зумовлює появу нового напрямку, мета якого полягає у мінімізації вуглецевого сліду на всіх етапах розробки. Оптимізація коду здатна не лише знизити навантаження на довкілля, а й суттєво зменшити операційні витрати компаній на утримання хмарної інфраструктури.

Однією з ключових сучасних тенденцій є свідомий вибір інструментів розробки та архітектурних шаблонів з огляду на їхнє енергоспоживання. Дослідження доводять, що компільовані мови програмування є більш енергоефективними за інтерпретовані, що змушує інженерів шукати баланс між швидкістю написання коду та ресурсомісткістю готового продукту. В середньому програми на C і Rust є найбільш енергоефективними. Програми на Java споживають приблизно в 2 рази більше енергії, ніж програми на C. Програми на JavaScript/TypeScript споживають від 4 до 20 разів більше енергії, ніж програми на C. Нарешті, програми на Python є чорними вівцями з енергоспоживанням у 75 разів більшим, ніж програми на C.[2] Це означає перехід від традиційного підходу, орієнтованого виключно на швидкість виконання функцій, до архітектури, яка ретельно враховує показники використання процесора та оперативної пам'яті.

На рівні безпосереднього написання коду тенденції зводяться до суворого усунення надмірності та ефективного використання апаратних ресурсів. Важливим аспектом стає мінімізація передачі даних через мережу, агрегація запитів та продумане кешування на клієнтському боці. Оптимізація програмного коду є ключовим кроком у досягненні енергоефективності, високої продуктивності та цілей сталого розвитку. Екологічний вплив виконання неефективного коду, хоча і не завжди очевидний, збільшує вуглецевий слід компанії, яка розробляє

неефективний код.[3] Видалення неактивного (мертвого) коду, зниження алгоритмічної складності для уникнення непотрібних вкладених циклів та відмова від постійного опитування серверів стають фундаментальною основою екологічного програмування. Таким чином, енергоефективність сьогодні формує нове розуміння чистого коду, вимагаючи від фахівців усвідомлення того, як програмні рішення впливають на фізичний світ.

Окрему увагу варто приділити ролі центрів обробки даних (data centers), які є основою сучасної цифрової інфраструктури. За оцінками міжнародних досліджень, дата-центри споживають значну частку світової електроенергії, а їхній внесок у глобальні викиди CO₂ постійно зростає. Неефективний програмний код прямо впливає на навантаження серверів, збільшуючи потребу в охолодженні, електроенергії та додатковому обладнанні. Таким чином, навіть незначна оптимізація програм може мати масштабний екологічний ефект у глобальному вимірі.

Таким чином, енергоефективність сьогодні формує нове розуміння чистого коду, вимагаючи від фахівців усвідомлення того, як програмні рішення впливають на фізичний світ. З огляду на це, екологічне програмування стає не просто технічною перевагою, а професійною етикою. Впровадження інструментів моніторингу енергоспоживання у CI/CD процеси та вибір алгоритмів з меншою обчислювальною складністю дозволяють розробникам створювати продукти, які є економічно вигідними для бізнесу та безпечними для навколишнього середовища. Врешті-решт, справжня якість коду в епоху кліматичних викликів вимірюється не лише відсутністю помилок, а й мінімальною кількістю ват-годин, витрачених на його виконання.

Список використаних джерел:

1. Ibm Cloud Education Team. How environmentally friendly organizations can use green coding to drive long-term success. *IBM. Topics*. URL: <https://www.ibm.com/think/topics/green-coding> (дата звернення: 07.03.2026).
2. Julien Richard-Foy, Wojciech Mazur. Sustainable Scala. *Scala. Blog*. URL: <https://www.scala-lang.org/blog/2021/12/14/sustainable-scala.html> (дата звернення: 07.03.2026).
3. CGI IT UK Ltd, University of Leicester. Green software guide. URL: https://www.cgi.com/sites/default/files/2025-02/green_software_guide.pdf (дата звернення: 07.03.2026).

ЗАСТОСУВАННЯ АЛГОРИТМУ IDA* З ВИКОРИСТАННЯМ PATTERN DATABASE ДЛЯ ОПТИМАЛЬНОГО РОЗВ'ЯЗАННЯ КУБИКА РУБІКА

Кубик Рубіка є однією з найвідоміших комбінаторних задач, що належить до класу задач пошуку в просторі станів. Кількість можливих конфігурацій кубика становить приблизно 43 квінтільйони ($4,3 \times 10^{19}$), що робить повний перебір неможливим. Відомо, що будь-який стан кубика можна розв'язати максимум за 20 ходів у метриці FTM (Face Turn Metric) – це так зване «число Бога» (God's Number), доведене у 2010 році. Традиційні методи пошуку в ширину чи A* потребують величезного обсягу оперативної пам'яті, тому для пошуку оптимальних розв'язків на звичайних комп'ютерах використовують комбінацію алгоритму IDA* (Iterative Deepening A*) та евристичних баз даних шаблонів (Pattern Databases).

Розроблено повноцінну програму мовою Go під назвою «RubikSolver», що складається з трьох основних модулів: генерація та серіалізація Pattern Database; високошвидкісний рушій виконання ходів та координатного представлення стану; розв'язувач на основі IDA*.

Технічна реалізація «RubikSolver» базується на переході від фізичного представлення кубика (колір кожної грані) до математичного координатного рівня, що дозволяє оперувати індексами в межах Pattern Database. Оскільки повний простір станів у 43 квінтільйони комбінацій неможливо прорахувати прямим перебором, стан кубика розбивається на окремі координати: орієнтацію кутів, орієнтацію ребер та їхні перестановки. Це дозволяє використовувати алгоритм IDA*, який поєднує переваги пошуку в глибину з евристичною оцінкою відстані до розв'язаного стану, що зберігається в попередньо згенерованих базах шаблонів. Ключовою особливістю розробки на мові Go є використання моделі пам'яті та примітивів паралельності для прискорення обчислень. Генерація баз шаблонів відбувається за допомогою горутин (goroutines), які паралельно заповнюють таблиці відстаней, значно скорочуючи час підготовки програми до роботи. Завдяки ефективній серіалізації, ці бази зберігаються у бінарному форматі, що дозволяє програмі швидко завантажувати їх у RAM і знаходити оптимальний розв'язок (до 20 ходів) менш ніж за 15 секунд. Такий підхід забезпечує продуктивність на рівні мов C/C++, зберігаючи при цьому високу читабельність коду та кросплатформність.

Використання симетрій кубика Рубіка є ключовим методом радикального скорочення обсягу даних у Pattern Database. Оскільки куб має 48 власних симетрій (включаючи повороти та віддзеркалення), багато станів є еквівалентними з точки зору кількості ходів до розв'язку. Замість зберігання окремого значення для кожної конфігурації, програма обчислює «канонічний» стан для групи симетричних позицій. Це дозволяє зменшити розмір таблиць у 8–16 разів без втрати точності евристики, що критично для роботи програми на звичайних ноутбуках з обмеженим обсягом оперативної пам'яті.

У процесі пошуку за алгоритмом IDA* симетрія також допомагає уникати зайвих обчислень. Під час генерації баз шаблонів мовою Go, використання симетрій дозволяє швидше заповнювати координатні таблиці, оскільки знаходження відстані для одного стану автоматично визначає відстані для всіх його симетричних копій. Це забезпечує високу швидкість роботи рушія та дозволяє знаходити оптимальний результат у межах 20 ходів за мінімальний час.

Загальний обсяг баз дозволяє запускати програму на звичайному ноутбукі без значних вимог до ресурсів. Середня швидкість розв'язання випадкових позицій є достатньо високою для практичного використання, з середньою довжиною розв'язку, близькою до теоретичного оптимуму. Для позицій, що вимагають максимальної кількості ходів (так званих «суперфліп» та інші екстремальні конфігурації), розв'язок знаходиться в розумні строки. Проведено порівняння з оригінальною реалізацією Kociemba (C) – розроблена програма працює з продуктивністю, близькою до референсної, при значно більшій читабельності та безпеці коду.

Дослідження підтвердило, що використання алгоритму IDA* з базами шаблонів на мові Go дозволяє ефективно знаходити оптимальні розв'язки кубика Рубіка (до 20 ходів) менш ніж за 15 секунд. Завдяки високій продуктивності коду та двофазному підходу програма демонструє стабільну роботу на сучасному обладнанні, залишаючи простір для прискорення через адитивні бази даних та паралельні обчислення.

Список використаних джерел:

1. Kociemba H. Two-Phase-Algorithm and God's Algorithm: God's number is 20. URL: <https://kociemba.org/cube.htm> (дата звернення: 28.11.2025).
2. Rokicki T., Kociemba H., Davidson M., Dethridge J. The Diameter of the Rubik's Cube Group Is Twenty // SIAM Journal on Discrete Mathematics. 2013. Vol. 27, No. 2. P. 1082–1105.

УДК 004.85

*Кльонов А.С., здобувач,
Колосовський А.С., здобувач*

Харківський національний університет радіоелектроніки

ЗАСТОСУВАННЯ МЕТОДУ ГРАДІЄНТНОГО СПУСКУ У ВИБОРІ ШВИДКОСТІ В МОДЕЛІ МАШИННОГО НАВЧАННЯ

Широке використання інструментів машинного навчання стикається з проблемою мінімізації функції втрат та підвищення точності моделей прогнозування. Одним із алгоритмів оптимізації в розв'язанні таких задач є метод градієнтного спуску. За цим методом виконується коригування параметрів моделі в ітеративному режимі в напрямку, протилежному градієнту функції втрат. Це забезпечує поступове зменшення похибки. Алгоритм продовжує виконувати послідовні оновлення параметрів до досягнення мінімального значення функції або до виконання заданого критерію зупинки.

У спрощеному розумінні градієнтний спуск є механізмом навчання моделі, який полягає у багаторазовому уточненні її внутрішніх параметрів з метою покращення прогнозу. На кожній ітерації здійснюється обчислення помилки між фактичними та прогнозованими значеннями, після чого визначається напрям зміни параметрів, що дозволяє зменшити цю помилку. Таким чином відбувається поступове наближення до оптимального розв'язку [1].

Існують різні модифікації алгоритму градієнтного спуску, серед яких стохастичний градієнтний спуск (SGD), що здійснює оновлення параметрів на основі одного випадкового прикладу; mini-batch gradient descent, який використовує невеликі підмножини навчальних даних; метод спряжених градієнтів, спрямований на покращення апроксимації мінімуму; квазі-ньютонівський метод BFGS, що застосовує апроксимацію матриці Гессе; а також алгоритм Adam, який адаптивно змінює швидкість навчання на основі ковзних середніх градієнтів.

Важливим аспектом застосування градієнтного спуску є вибір швидкості навчання – гіперпараметра, що визначає розмір кроку оновлення. Надмірно велике значення може призвести до нестійкості та «перестрибування» мінімуму, тоді як занадто мале – до повільної збіжності алгоритму.

Регуляризація L1 (Lasso) передбачає додавання до функції втрат суми абсолютних значень параметрів моделі. Це стимулює занулення частини коефіцієнтів, що сприяє автоматичному відбору ознак та формуванню розріджених моделей.

Регуляризація L2 (Ridge) додає до функції втрат суму квадратів параметрів. Такий підхід не занулює ваги, але зменшує їхні значення, що дозволяє знизити варіативність моделі та підвищити її узагальнювальну здатність [2].

Крім того, існує ризик потрапляння в локальний мінімум і перенавчання моделі, що потребує застосування методів регуляризації, зокрема L1 або L2. З обчислювальної точки зору алгоритм може бути ресурсомістким, особливо при роботі з великими наборами даних або складними моделями, тому для підвищення ефективності використовуються методи векторизації та паралельних обчислень.

Гرادієнтний спуск – це математичний метод, що ітераційно знаходить ваги й зсув, які дають змогу створити модель із найменшими втратами. Градієнтний спуск знаходить найкращі ваги й зсув, повторюючи процес, описаний нижче, протягом кількох ітерацій, які визначає користувач[1]. Модель починає навчання з рандомізованими вагами і зсувом, близькими до нуля, а потім повторює такі кроки: обчислення втрат із поточною вагою і зсувом; визначення напрямку, у якому переміщувати ваги й зсув, що зменшують втрати; незначне переміщення значень ваги й зсуву в напрямку, що зменшує втрати; повернення до першого кроку й повторення процесу, доки модель не зможе більше зменшувати втрати.

Отже, градієнтний спуск є фундаментальним інструментом сучасного машинного навчання, який забезпечує систематичне та обґрунтоване зменшення функції втрат шляхом ітеративного оновлення параметрів моделі. Розуміння принципів його роботи є необхідною передумовою для подальшого вивчення методів оптимізації та побудови ефективних інтелектуальних систем.

Список використаних джерел:

1. Gradient descent [Електронний ресурс] // Google Developers. Machine Learning Crash Course. URL: <https://developers.google.com/machine-learning/crash-course/linear-regression/gradient-descent?hl=uk> (дата звернення: 26.02.2026).
2. Gradient Descent and Stochastic Gradient Descent in Machine Learning [Електронний ресурс] // Codelabs Academy. URL: <https://codelabsacademy.com/uk/blog/gradient-descent-and-stochastic-gradient-descent-in-machine-learning> (дата звернення: 26.02.2026).

УДК 004.8

*Глинчук Л.Я., к.ф.-м.н., доцент
Волинський національний університет імені Лесі Українки*

ЗАСТОСУВАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ АВТОМАТИЧНОЇ ГЕНЕРАЦІЇ ТЕХНІЧНОЇ ДОКУМЕНТАЦІЇ ПІД ЧАС РЕІНЖИНІРИНГУ ІНФОРМАЦІЙНИХ СИСТЕМ

Технології штучного інтелекту активно впроваджуються у процеси розроблення та модернізації програмного забезпечення. Особливе місце серед таких технологій займають великі мовні моделі (LLM), які демонструють високу ефективність у задачах генерації, аналізу та узагальнення текстової інформації. LLM дедалі частіше використовуються у сфері програмної інженерії, зокрема для автоматизації процесів створення програмної та технічної документації [5].

Використання великих мовних моделей у процесі реінжинірингу інформаційних систем розглядається як перспективний підхід до автоматизації процесу формування технічної документації на основі аналізу вихідного коду та інших джерел інформації [1; 2].

Використання підходів, зокрема Retrieval-Augmented Generation, дозволяє підвищити точність і релевантність згенерованих матеріалів, що є важливим для створення якісної технічної документації [3; 4]. У зв'язку з цим і є актуальною тема дослідження.

Дослідження показують, що великі мовні моделі (LLM) можуть ефективно застосовуватися для автоматичної генерації технічної документації на різних етапах реінжинірингу інформаційних систем. Зокрема, LLM здатні:

1. Генерувати пояснення до програмного коду та опис функціональних модулів системи [1].
2. Формувати структуровані технічні матеріали на основі аналізу існуючих документів, коментарів у коді та зовнішніх джерел [2].
3. Підтримувати процес управління знаннями в організації, інтегруючи згенеровану документацію у корпоративні бази даних та системи управління проектами [3].

Використання **Retrieval-Augmented Generation (RAG)** дозволяє LLM комбінувати внутрішні знання моделі з релевантними даними з баз знань або сховищ документації, що підвищує точність і повноту автоматично згенерованих матеріалів [4]. Крім того, застосування технік **prompt engineering** дає змогу налаштовувати моделі під специфічні завдання, наприклад: створення інструкцій користувача,

технічних описів програмних компонентів або звітів про зміни у системі [3; 5].

У практичному застосуванні було виділено три ключові етапи інтеграції LLM у процес реінжинірингу систем:

- ✓ Аналіз наявної документації – оцінка стану технічних матеріалів і визначення прогалів.
- ✓ Генерація та узагальнення тексту – формування пояснень, описів і інструкцій.
- ✓ Верифікація та інтеграція – перевірка точності згенерованого тексту та його впровадження у корпоративні системи.

Результати дослідження свідчать, що інтеграція LLM у процес реінжинірингу дозволяє:

- ✓ значно скоротити час на підготовку документації;
- ✓ забезпечити узгодженість і структурованість матеріалів;
- ✓ підвищити якість управління знаннями в організації.

Використання таких моделей особливо ефективно у великих інформаційних системах, де ручне оновлення документації є трудомістким і схильним до помилок.

Список використаних джерел:

1. Dvivedi S. S., Vijay V., Pujari S. L. R., Lodh S., Kumar D. A comparative analysis of large language models for code documentation generation. 2023. URL: <https://arxiv.org/abs/2312.10349> (дата звернення: 02.03.2026).

2. Laitinen T. Applications of large language models for technical documentation. 2025. URL: <https://urn.fi/URN:NBN:fi:aalto-202508186196> (дата звернення: 02.03.2026).

3. Kim H., Park J., Lee S., Choi Y. In-house knowledge management using a large language model: focusing on technical specification documents review // *Applied Sciences*. 2024. Vol. 14, No. 5. DOI: <https://doi.org/10.3390/app14052096>.

4. **De Oliveira R. S., Nascimento E. G. S.** Transformer-based large language foundation models for text generation: a comprehensive literature review for different languages and application domains // *Information Processing & Management*. 2026. Vol. 63, No. 2. DOI: <https://doi.org/10.1016/j.ipm.2025.104477>.

5. Олійник Б. О., Чичкарьов Є. А. Методи реалізації Retrieval-Augmented Generation у поєднанні з сучасними великими мовними моделями // *Наукові записки Державного університету інформаційно-комунікаційних технологій*. 2025. DOI: <https://doi.org/10.31673/2786-8362.2025.012843>.

УДК 004.415.3:005.8

Иценко Д. Г., магістрант

Харківський національний університет радіоелектроніки

ІНТЕГРАЦІЯ ПРАКТИК DEVOPS В УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ СИСТЕМИ СКЛАДСЬКОЇ ЛОГІСТИКИ

This work focuses on DevOps integration within the IT project lifecycle management for warehouse automation systems. The main problem is the operational disconnect between development, testing, and deployment stages, which leads to prolonged release cycles and critical bugs in production environments. Existing siloed lifecycle approaches are highly manual and prone to human errors, limiting the system's adaptability. The specific task of this research is to design an automated continuous delivery lifecycle model optimized for WMS. The results present an engineered CI/CD management pipeline that acts as a structural methodology to govern software releases. This lifecycle management method ensures systematic quality control, automated database migrations, and a significantly reduced time-to-market.

Основною проблемою дослідження управління ІТ-проєктами є розрив між етапами розробки, тестування та експлуатації в життєвому циклі програмного забезпечення. Для критичних систем, якими є системи автоматизації складських операцій (WMS), будь-які затримки в процесі випуску оновлень або дефекти, допущені на етапі розгортання, миттєво призводять до зупинки реальних фізичних процесів обробки вантажів та незворотних фінансових втрат логістичного підприємства.

Розглядаючи існуючі підходи та моделі вирішення цієї проблеми, в інженерії програмного забезпечення виділяють традиційні ізольовані моделі управління життєвим циклом [1]. У таких моделях фази написання коду, контролю якості (QA) та системного адміністрування суворо розділені між різними відділами. Стислий опис їх недоліків зводиться до того, що передача артефактів проєкту між етапами відбувається здебільшого в ручному режимі. Це створює концептуальні "вузькі місця" в управлінні проєктом, суттєво збільшує тривалість зворотного зв'язку та кардинально підвищує ризик людської помилки під час міграції баз даних та налаштування цільових серверних оточень. У масштабах безперервної складської логістики такі архітектурні недоліки стають критичними [2].

З огляду на це, формулюється конкретна задача дослідження: розробити та обґрунтувати модель управління життєвим циклом WMS-системи на основі інтеграції управлінських та інженерних практик DevOps, яка б повністю автоматизувала перехід програмного продукту

між усіма стадіями життєвого циклу, забезпечивши синергію між командами розробки та експлуатації [1, 3].

Результати дослідження полягають у розробці концептуальної моделі безперервного життєвого циклу для ІТ-проєкту WMS. У межах дослідження автоматизація розглядається не просто як технічний інструмент, а як повноцінний управлінський метод контролю випусків[3]. Відповідно до розробленої моделі, перехід артефактів між фазами життєвого циклу управляється системою автоматичних шлюзів якості. Замість повільного ручного контролю менеджерами, програмний код автоматично проходить стадії модульного тестування. Лише у разі стовідсоткового успішного проходження встановлених метрик якості, життєвий цикл переходить до етапу автоматизованого розгортання [2].

Розроблений метод управління життєвим циклом передбачає глибоку автоматизацію не лише процесів оновлення клієнтських та серверних застосунків, а й управління версіями та міграціями реляційної бази даних. Дослідження показує, що впровадження такої багаторівневої моделі в управління проєктом трансформує життєвий цикл з жорсткого лінійного процесу у гнучкий безперервний цикл постачання цінності, радикально зменшуючи загальну тривалість етапу випуску оновлень з декількох днів до лічених хвилин [3].

Інтеграція методології DevOps у процеси управління життєвим циклом розробки ІТ-проєкту успішно вирішує фундаментальну проблему технологічної та організаційної ізольованості етапів життєвого циклу [1]. Розроблена модель безперервного постачання дозволяє менеджерам проєктів практично повністю мінімізувати вплив людського фактора на критичних етапах релізу та суттєво пришвидшити процеси автоматизації складських операцій, забезпечуючи високу відмовостійкість програмного забезпечення підприємства [2, 3].

Список використаних джерел:

1. Кім Д., Хамбл Д., Дебуа П. Довідник DevOps. Як створити гнучку, надійну та безпечну ІТ-компанію / пер. з англ. Київ : Наш Формат, 2020. 424 с.
2. Forsgren N., Humble J., Kim G. Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations. IT Revolution Press, 2018. 288 p.
3. Бабіч О. В. Моделі управління життєвим циклом програмного забезпечення в умовах Continuous Delivery. *Програмна інженерія*. 2023. № 4. С. 45–52.

УДК 004.942

*Бондарчук М. Ю., здобувач,
Горобець С.М., к.пед.н., доцент
Житомирський державний університет імені Івана Франка*

МОДЕЛЮВАННЯ ПРОЦЕСУ РОЗПОВСЮДЖЕННЯ ЗАБРУДНЮЮЧИХ РЕЧОВИН В АТМОСФЕРІ

Атмосферне повітря в промислових регіонах України зазнає значного антропогенного навантаження через викиди підприємств і транспорту [4]. Моделювання розповсюдження забруднюючих речовин є важливим для прогнозування концентрацій та оцінки їх впливу на довкілля. Метою роботи є дослідження та програмна реалізація математичної моделі розповсюдження забруднювачів в атмосфері.

Для моделювання концентрації забруднюючої речовини у шлейфі обрано Гаусову модель (Gaussian plume model), яка широко застосовується для викидів з точкових джерел на локальних масштабах [2, 3]. Моделювання базується на припущенні нормального розподілу концентрації під час горизонтального перенесення повітряних мас (адвекції) та турбулентної дифузії шарів повітря.

Основне рівняння для розрахунку концентрації забруднюючої речовини $C(x, y, z)$ на висоті z , відстані по напрямку вітру (вісь x) та поперечному відхиленні (вісь y) [4]:

$$C(x, y, z) = \frac{Q}{2\pi u \sigma_y \sigma_z} e^{-\frac{y^2}{2\sigma_y^2}} \left[e^{-\frac{(z-H)^2}{2\sigma_z^2}} + e^{-\frac{(z+H)^2}{2\sigma_z^2}} \right] \quad (1)$$

де Q – потужність викиду; u – швидкість вітру; σ_y, σ_z – коефіцієнти розсіювання, що залежать від відстані та класу стійкості атмосфери; H – висота джерела забруднення над поверхнею ґрунту.

Модель реалізовано за допомогою мови Python із використанням бібліотек NumPy та Matplotlib. Обчислено коефіцієнти розсіювання σ_y та σ_z залежно від відстані, після чого виконано чисельний розрахунок приземної концентрації ($z = 0$) на двовимірній сітці координат із урахуванням проєкції шлейфу на поверхню ґрунту.

Результати моделювання представлено у вигляді двовимірної карти розподілу приземної концентрації забруднювача від джерела, розташованого на заданій висоті. Це дозволяє оцінити просторову структуру поширення забруднення на рівні ґрунту (рис. 1).

Для моделювання використано параметри: $Q = 50$ г/с, $u = 4$ м/с, $H = 30$ м. Координати в межах 1000 м по вісі x та ± 200 м по вісі y .

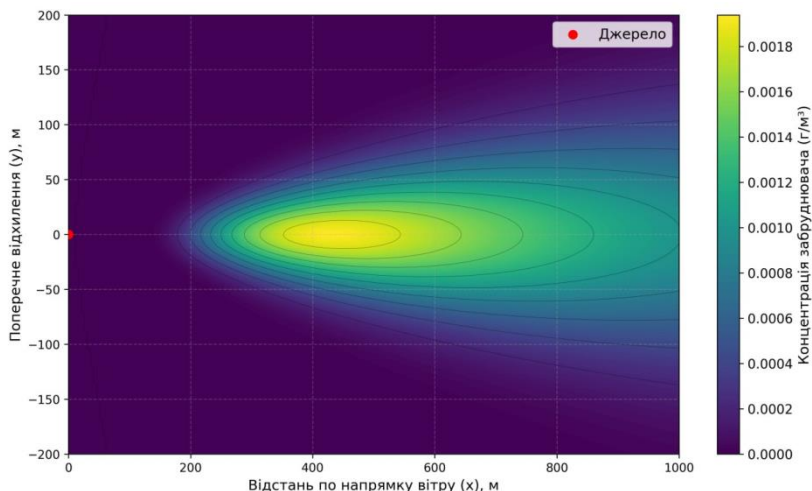


Рис. 1. Карта моделювання розподілу концентрації забруднюючої речовини в атмосферному повітрі на рівні ґрунту ($Q = 50$ г/с, $u = 4$ м/с, $H = 30$ м)

Отже, нами розглянуто застосування математичної моделі оцінки розподілу приземної концентрації забруднювача. Розрахунки проведені з використанням бібліотек NumPy та Matplotlib мови Python. Побудована карта розподілу концентрації забруднюючої речовини демонструє характер поширення та області підвищеного забруднення. Отримані результати можуть бути використані для попередньої оцінки впливу промислових викидів на якість повітря.

Список використаних джерел:

1. Air Quality in Europe – 2023 Report / European Environment Agency. Luxembourg : Publications Office of the European Union, 2023. 18 с.
2. Seinfeld J. H., Pandis S. N. Atmospheric Chemistry and Physics: From Air Pollution to Climate Change. 3rd ed. Hoboken : John Wiley & Sons, 2016. 1051 с.
3. Air Dispersion Modelling Guidance Note (AG4) / Environmental Protection Agency. Dublin : EPA, 2020. 80 с.
4. Holnicki P., Nahorski Z., Kałuszko A. Air Quality Modeling in Urban Regions. Cham : Springer, 2017. 348 с.

УДК 004.8:001.895

*Єрмаков В.А., здобувач,
Косенко С.І., к.т.н., доцент
Національний університет «Одеська політехніка»*

ОГЛЯД СУЧАСНИХ МЕТОДІВ СТАТИСТИЧНОГО АНАЛІЗУ МЕДИЧНИХ ДАНИХ

У контексті розвитку цифрової медицини та біоінформатики значення статистичного аналізу медичних даних постійно зростає. Результати медичних досліджень, електронні медичні записи, дані проспективних спостережень, а також великі обсяги геномних та протеомних даних створюють значні обсяги інформації, що вимагає застосування ефективних методів опрацювання та інтерпретації [1]. Статистичні методи відіграють ключову роль у виділенні значущих закономірностей, оцінюванні взаємозв'язків між факторами ризику та клінічними результатами, а також у побудові прогностичних моделей. Актуальність огляду сучасних підходів до статистичного аналізу медичних даних обумовлена не лише зростанням обсягів даних, але й потребою у виборі адекватних методів для підвищення точності висновків та клінічних рекомендацій [2].

Одним із базових підходів до обробки медичних даних є регресійний аналіз. Лінійна регресія традиційно застосовується для оцінювання зв'язку між кількісними предикторами та безперервними результатами. При цьому важливо перевіряти відповідність даних припущенням моделі щодо нормальності розподілу залишків і гомоскедастичності.

Логістична регресія є стандартним методом для аналізу бінарних результатів. Вона дозволяє моделювати ймовірність настання певної події залежно від множини факторів ризику. Однією з переваг цього методу є інтерпретованість отриманих коефіцієнтів у вигляді відношення шансів. Однак для великих наборів предикторів з високою мультиколінеарністю застосовують регуляризацію, зокрема LASSO та Ridge-регресії, що дозволяють зменшувати надмірну варіацію оцінок та підвищувати стабільність моделей.

У випадку високовимірних даних, наприклад даних генетичних асоціацій, застосовують методи багатовимірного аналізу, зокрема аналіз головних компонент, факторний аналіз та множинний кластерний аналіз. Ці підходи дозволяють виявити латентні структури в даних, зменшити їхню розмірність і здійснювати візуалізацію складних взаємозв'язків між ознаками [1]. Аналіз головних компонент

особливо корисний при роботі з даними високого виміру, де пряма інтерпретація частинної кореляційної структури є складною.

Методи машинного навчання, такі як випадкові ліси, метод опорних векторів та градієнтний бустинг, набули поширення у медичному аналізі даних. У клінічних задачах вони ефективні для класифікації станів пацієнтів, прогнозування ускладнень та оцінювання ризику. Важливою перевагою є їх здатність автоматично обробляти великі набори ознак, однак інтерпретованість таких моделей часто нижча порівняно з класичними статистичними підходами.

Для оцінювання якості класифікаційних моделей у медицині використовують різні метрики, включно з площею під кривою ROC, показниками чутливості та специфічності, що дозволяє повноцінно оцінювати прогностичну здатність моделі на тестових даних [2].

Методи багатовимірною узагальнення параметрів, наприклад байєсівські підходи, активно використовуються в тих випадках, коли дані мають складну структуру або коли необхідно включити апіорні знання експертів у модель. Серед непараметричних підходів варто зазначити методи, що не роблять жорстких припущень про форму розподілу даних [1]. Наприклад, методи ядерної оцінки щільності та сплайн-регресії широко застосовуються для виявлення нелінійних трендів у наборах медичних даних. Непараметричні тести, такі як критерії Манна–Уїтні та Краскела–Уолліса, використовуються для порівняння розподілів між групами у випадках, коли дані не відповідають припущенням нормальності [2].

В результаті проведених досліджень слід зазначити, що лінійні та логістичні моделі залишаються основою для багатьох медичних досліджень завдяки своїй простоті та інтерпретованості, тоді як сучасні алгоритми машинного навчання дозволяють працювати зі складнішими даними та виявляти нелінійні залежності. Методи обробки пропущених даних, непараметричні підходи та часові моделі доповнюють арсенал інструментів, що дозволяють ефективно аналізувати великі та гетерогенні набори медичних даних.

Список використаних джерел:

1. Harrell F.E. Regression Modeling Strategies: With Applications to Linear Models, Logistic and Ordinal Regression, and Survival Analysis. Statistics in Medicine. 2015. Vol. 34, No 7. P. 1151–1152.
2. Obermeyer Z., Emanuel E.J. Predicting the Future — Big Data, Machine Learning, and Clinical Medicine. New England Journal of Medicine. 2016. Vol. 375, No 13. P. 1216–1219.

УДК 629.5:004.8

*Шибасєва Н.О., к.т.н., доцент,
Рудніченко М.Д., к.т.н., доцент,
Шведов Д.В., аспірант*

Національний університет «Одеська політехніка»

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ УПРАВЛІННЯ ОБРОБКОЮ НЕКОНВЕНЦІЙНИХ ДАНИХ У ТРАНСПОРТНИХ СИСТЕМАХ

Неконвенційні дані, що включають геопросторові, часові, поведінкові, соціальні та мультимодальні сигнали, створюють виклики щодо їх інтеграції, адаптивної обробки, фільтрації шуму та забезпечення релевантності інформації для прийняття оперативних рішень. Управління обробкою таких неконвенційних даних у транспортних системах вимагає гнучких архітектурних рішень, що забезпечують адаптивність до варіативності джерел даних, обчислювальну ефективність, масштабованість та інтеграцію з IoT-інфраструктурою. Актуальність аналізу сучасних підходів ґрунтується на зростанні вимог до точності прогнозів, безпеки руху та оптимізації потоків у складних міських середовищах.

Одним із широко застосовуваних підходів є побудова багаторівневих архітектур даних, де на нижньому рівні здійснюється безпосередня обробка сировинних сенсорних сигналів. На цьому рівні реалізуються методи попередньої фільтрації шуму, нормалізації, часової синхронізації та базового розпізнавання шаблонів. Ці базові операції дозволяють підготувати дані для передачі на більш високі рівні обробки, де вони можуть бути агреговані й узагальнені для подальшого аналізу. Серед сучасних архітектурних підходів значну увагу приділяють концепціям edge-обчислень, що передбачають розподілену обробку даних безпосередньо на транспортних вузлах чи сенсорних платформах. Такий підхід дозволяє зменшити затримки та зменшити обсяг переданих у центральні системи даних, особливо у випадках, коли обробка в режимі реального часу є критичною.

На центральному рівні обробки створюються платформи для агрегації та аналітики, що інтегрують дані з різних джерел. Ці рішення часто базуються на хмарних архітектурах із підтримкою масштабованих сховищ та обчислень, що дозволяють виконувати складні аналітичні задачі, прогнозування навантажень, виявлення закономірностей у часових рядах та побудову моделей поведінки учасників руху.

Для ефективного управління обробкою неконвенційних даних дослідники пропонують гібридні підходи, що поєднують символічні

моделі, машинне навчання та статистичну інтерпретацію. Ці підходи передбачають адаптивні механізми, що визначають спосіб обробки даних залежно від їхньої природи, якості чи рівня сигнал-шум. Наприклад, дані з відео можуть попередньо оброблятися алгоритмами для виділення об'єктів і подій, тоді як GPS-треки — через часові моделі та кластерні алгоритми для виявлення патернів руху.

Методи машинного навчання відіграють важливу роль у сучасних транспортних системах для прогнозування поведінки транспортної мережі. Глибокі нейронні мережі та рекурентні архітектури, зокрема LSTM та Transformer-подібні моделі, дозволяють навчатися на великих масивах часових даних для прогнозування навантажень, виявлення аномалій чи адаптації маршрутів залежно від зміни трафіку. При цьому важлива увага приділяється інтеграції цих моделей у реальному часі через edge-сервери або гібридні обчислювальні платформи, що поєднують локальні та централізовані компоненти.

Іншим напрямом є використання технологій stream-обробки, що дозволяють оперативно обробляти потоки даних із датчиків та сенсорних мереж без потреби збереження всієї історичної інформації. Stream-обробка поєднується з event-driven архітектурами, де певні події дорожнього руху чи транспортні аномалії стають тригерами для запуску специфічних аналітичних або управлінських процесів.

Висновки. Слід зазначити, що сучасні підходи до управління обробкою неконвенційних даних у транспортних системах демонструють широкий спектр архітектурних рішень: від edge-обчислень та stream-обробки до хмарної аналітики з гібридними алгоритмами машинного навчання. Ефективне поєднання цих підходів дозволяє забезпечити оперативність, масштабованість та адаптивність систем при обробці складних і різномірних джерел даних. Подальші дослідження можуть бути спрямовані на підвищення інтеграції між компонентами обробки.

Список використаних джерел:

1. Zhao L., Chen J., Hassan M.M. Edge-Cloud Collaborative Processing for Intelligent Transportation Systems: A Survey. *IEEE Transactions on Industrial Informatics*. 2024. Vol. 20. P. 5128–5141.
2. Li H., Zhang X., Tian Z., Zhang Y. Multimodal Data Fusion for Traffic Flow Prediction: A Comprehensive Review. *Transportation Research Part C: Emerging Technologies*. 2025. Vol. 140. P. 104531.
3. Gao Y., Song J., Wang H., Liu Q. Real-Time Anomaly Detection in Transportation Systems Using Streaming Data Analytics. *IEEE Access*. 2023. Vol. 11. P. 156309–156321.

УДК 004.7

Закусило В.В., здобувач

Житомирський державний університет імені Івана Франка

РОЗРОБКА СИСТЕМИ ТРЕНУВАННЯ ШВИДКОГО НАБОРУ ТЕКСТУ З АВТОМАТИЧНИМ АНАЛІЗОМ ПОМИЛОК НА ОСНОВІ ЛІНГВІСТИЧНИХ МЕТРИК ПОДІБНОСТІ

У сучасному інформаційному суспільстві швидкість та точність набору тексту є критичними навичками, що безпосередньо впливають на ефективність професійної діяльності. Проте більшість існуючих тренажерів обмежуються поверхневою перевіркою символів, не враховуючи глибинну структуру помилок. Використання лінгвістичних метрик подібності, таких як відстань Левенштейна або коефіцієнт Жаккара, дозволяє системі не просто фіксувати хибодруки, а проводити інтелектуальний аналіз паттернів помилок користувача. Це відкриває шлях до створення адаптивних алгоритмів навчання, які підлаштовуються під індивідуальні когнітивні особливості людини, перетворюючи механічне тренування на науково обґрунтований процес вдосконалення когнітивно-моторних навичок.

Метою дослідження є розробка та програмна реалізація комплексної десктопної системи тренування навичок швидкого набору тексту на базі ігрового рушія Unity, яка поєднає методи гейміфікації з поглибленим аналізом помилок на основі лінгвістичних метрик подібності. Проєкт спрямований на створення адаптивного навчального середовища, де за допомогою алгоритмів відстані Левенштейна, Дамерау-Левенштейна та Джаро-Вінклера здійснюється ідентифікація специфічних паттернів друкарських помилок (замін, пропусків та перестановок сусідніх символів) у реальному часі. Використання 18 рівнів складності з поступовим обмеженням часових та кількісних ресурсів у поєднанні з візуалізацією теплової карти помилок дозволяє не лише підвищити швидкість друку, а й забезпечити цілеспрямовану корекцію когнітивно-моторних навичок користувача, трансформуючи процес навчання у динамічний та інтелектуально керований ігровий процес.

Головним результатом роботи стала розробка функціональної десктопної гри на рушії Unity, яка успішно інтегрує механіки швидкого набору тексту з глибоким лінгвістичним аналізом. Завдяки використанню компонентів TextMeshPro, вдалося досягти високої чіткості візуалізації тексту та миттєвого оновлення кольорового фідбеку (зелений/червоний) без втрати продуктивності. Система стабільно обробляє введення через `Input.inputString`, що забезпечує

точну синхронізацію дій користувача з ігровою логікою в усіх 6 режимах складності.

Особливу увагу приділено ефективності алгоритмів порівняння рядків. Впровадження відстані Дамерау-Левенштейна дозволило системі ідентифікувати не просто помилкові символи, а специфічні типи помилок, зокрема транспозиції (перестановку сусідніх клавіш), які складають значну частку дефектів при швидкому друці. Порівняльний аналіз показав, що поєднання цієї метрики з коефіцієнтом Джаро-Вінклера забезпечує більш гуманну та точну оцінку прогресу гравця на складних рівнях, де слова залишаються впізнаваними навіть при незначних хибодруках.

Апробація розробленої системи рівнів (від 120 до 40 секунд) підтвердила гіпотезу про стимулюючий вплив часового тиску на концентрацію користувача. Встановлено, що жорсткий режим, який блокує подальший ввід до виправлення помилки, сприяє швидшому формуванню м'язової пам'яті порівняно зі звичайним режимом. Гейміфікація процесу через систему рекордів у ResultsUI створила сталий мотиваційний цикл, спонукаючи користувачів до багаторазового проходження рівнів для покращення власних результатів.

Найбільш значущим аналітичним компонентом стала теплова карта помилок, інтегрована в інтерфейс статистики. Вона дозволила наочно продемонструвати кореляцію між швидкістю набору та конкретними "проблемними" зонами клавіатури для кожного окремого користувача. Це підтвердило практичну цінність системи як діагностичного інструменту: на основі отриманих даних було закладено фундамент для майбутнього алгоритму адаптивної генерації тексту, який автоматично збільшуватиме кількість слів із символами, що викликають найбільші труднощі.

У підсумку, створений прототип довів, що поєднання лінгвістичного аналізу та ігрових технологій є ефективним методом навчання. Система не лише фіксує кількісні показники (кількість слів за хвилину), а й надає якісну оцінку помилок, що робить процес тренування свідомим та персоналізованим.

Список використаних джерел:

1. Бивойно П. Г., Кореновська С. М. Методи та алгоритми визначення подібності текстових об'єктів : монографія. Київ : НТУУ «КПІ ім. Ігоря Сікорського», 2019. 156 с.
2. Трофименко О. Г., Прокоп Ю. В., Букацела О. В. Програмування ігор на платформі Unity : навч. посіб. Одеса : Фенікс, 2021. 240 с.

УДК 004.032.26:622.73

*Аблець А.В., аспірант,
Тронь В.В., к.т.н., доцент
Криворізький національний університет*

ГІБРИДНА ФІЗИЧНО-ІНФОРМОВАНА НЕЙРОМЕРЕЖА ДЛЯ ПРОГНОЗУ СПОЖИВАНОЇ ПОТУЖНОСТІ МЛИНА НАПІВСАМОПОДРІБНЕННЯ НА ГОДИНУ ВПЕРЕД

Млин напівсамоподрібнення (SAG-млин) є одним із найбільших споживачів електроенергії на збагачувальній фабриці. Тому прогноз його споживаної потужності на годину вперед має цілком прикладне значення: він дає змогу коригувати режим роботи, вирівнювати енергетичне навантаження та раніше виявляти відхилення в процесі.

Підходи до такого прогнозування помітно різняться. Фізичні моделі добре відображають закономірності процесу, але потребують параметрів, яких у SCADA-архівах часто немає або які оцінюються з великою невизначеністю [1]. Моделі, що спираються лише на дані, зазвичай дають меншу похибку, проте їх важче інтерпретувати, а при зміні технологічного режиму вони не завжди залишаються достатньо стійкими [2].

У роботі розглянуто гібридну модель Elastic Physics-Informed Neural Network (Elastic-PINN), у якій нейромережева частина поєднується з фізичним регуляризатором [3, 4]. Термін «elastic» означає, що фізичне обмеження вводиться м'яко через зважений компонент функції втрат, а коефіцієнти фізичної моделі адаптуються під час навчання. Фізична гілка не замінює основний прогнозувач, а лише стримує модель від фізично неправдоподібних рішень.

Спираючись на відому залежність потужності від швидкості обертання [1], у фізичній гілці використано спрощену апроксимацію:

$$P = kS^n + aF + b_0$$

Тут S - частота обертання млина, F - витрата руди; коефіцієнти k , n , a та b_0 спершу оцінюються методом найменших квадратів, а далі оптимізуються разом із параметрами мережі. Абляційний аналіз показав, що саме коефіцієнти, що навчаються, дають найбільший внесок у підсумкову точність моделі.

Нейромережеву складову реалізовано на основі Temporal Convolutional Network (TCN) із каузальними розширеними згортками [5]. Окремий LSTM-модуль прогнозує частоту обертання та витрату руди на горизонті 60 хвилин. У підсумку модель враховує часову динаміку процесу і водночас зберігає фізичну інтерпретованість.

Модель оцінено на промисловому масиві SCADA-даних тривалістю 117 діб із дискретністю 1 хвилина. У нормальному режимі роботи отримано $RMSE = 0,633$ МВт та $MAE = 0,490$ МВт, що відповідає приблизно 4,7 % від середньої тестової потужності 13,56 МВт. Перевага над найкращою моделлю без фізичної складової невелика, але простежується стабільно.

Абляційний аналіз дав змогу з'ясувати, за рахунок чого саме працює модель. Фіксація коефіцієнтів, оцінених методом найменших квадратів, погіршує $RMSE$ на 30,2 %, а вилучення фізичного компонента з функції втрат - на 14,8 %. Якщо ж замінити прогнозовані екзогенні змінні їхніми істинними майбутніми значеннями, похибка зменшується ще приблизно на 13 %. Це свідчить, що головне обмеження точності пов'язане насамперед із прогнозом екзогенних змінних, а не з архітектурою моделі потужності.

Загалом гібридна архітектура поєднує прийнятну точність короткострокового прогнозування з інтерпретованістю. Наукова новизна полягає у поєднанні коефіцієнтів фізичної моделі, що навчаються, з м'якою регуляризациєю в архітектурі PINN для прогнозування потужності SAG-млина з урахуванням прогнозу екзогенних змінних. Навчувані фізичні коефіцієнти можна аналізувати окремо, а сам підхід придатний для подальшого використання в системах підтримки прийняття рішень на збагачувальній фабриці.

Список використаних джерел:

1. Silva M., Casali A. Modelling SAG milling power and specific energy consumption including the feed percentage of intermediate size particles // Minerals Engineering. 2015. Vol. 70. P. 156-161.
2. Zhang D., Xiong X., Shao C., Zeng Y., Ma J. Semi-autogenous mill power consumption prediction based on CACN-LSTM // Applied Sciences. 2025. Vol. 15, No. 1. Article 2.
3. Karniadakis G. E., Kevrekidis I. G., Lu L., Perdikaris P., Wang S., Yang L. Physics-informed machine learning // Nature Reviews Physics. 2021. Vol. 3. P. 422-440.
4. Raissi M., Perdikaris P., Karniadakis G. E. Physics-informed neural networks: a deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations // Journal of Computational Physics. 2019. Vol. 378. P. 686-707.
5. Bai S., Kolter J. Z., Koltun V. An empirical evaluation of generic convolutional and recurrent networks for sequence modeling // arXiv. 2018. URL: <https://arxiv.org/abs/1803.01271> (дата звернення: 10.01.2026).

УДК 517.938:004.94

*Лунаренко О.В., к.т.н., доцент
ДВНЗ «Приазовський державний технічний університет»*

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ТА АНАЛІЗ ДИНАМІЧНИХ РЕЖИМІВ НЕЛІНІЙНИХ СИСТЕМ У СЕРЕДОВИЩІ MATLAB

Нелінійні динамічні системи широко використовуються для математичного моделювання складних процесів у фізиці, біології, технічних та інформаційних системах. Такі системи можуть демонструвати різні режими поведінки – стаціонарні стани, періодичні коливання, квазіперіодичну динаміку та хаотичні режими. Для багатьох моделей аналітичне дослідження глобальної структури фазового простору є складним або неможливим, тому важливу роль відіграють методи комп'ютерного моделювання та чисельного експерименту. Сучасні програмні засоби дозволяють досліджувати динаміку широкого класу нелінійних систем, зокрема моделей Лоренца, Росслера та Чуа.

Нелінійні динамічні системи, що розглядаються у роботі, описуються системами автономних звичайних диференціальних рівнянь першого порядку:

$$\dot{x} = f(x, y, z), \quad \dot{y} = g(x, y, z), \quad \dot{z} = h(x, y, z),$$

де x, y, z – змінні стану системи, а функції f, g, h визначають її динамічну поведінку. Для дослідження еволюції систем у фазовому просторі використовується чисельне інтегрування рівнянь у середовищі MATLAB. Чисельний розв'язок отримано за допомогою вбудованих методів Рунге–Кутти з адаптивним кроком (зокрема солвера **ode45**), що дозволяє аналізувати часові реалізації змінних стану та структуру фазових траєкторій при різних початкових умовах і значеннях параметрів.

Для дослідження динамічних режимів використано розроблений програмний комплекс у середовищі **MATLAB**, який забезпечує автоматизоване проведення чисельного експерименту та візуальний аналіз результатів моделювання. Програмний засіб реалізовано у вигляді інтерактивного додатку з графічним інтерфейсом користувача, що дозволяє виконувати комплексний аналіз нелінійних динамічних систем. Користувач має можливість обрати досліджувану математичну модель із набору реалізованих систем, задати початкові умови та параметри інтегрування, а також змінювати керуючі параметри моделі.

Програмний комплекс забезпечує побудову фазових портретів та їх проєкцій на координатні площини і реалізує графічні методи аналізу динаміки, зокрема перерізи Пуанкаре, карти повернення та рекурентні

діаграми. Інтерактивні елементи керування (бігунки) дозволяють у режимі реального часу змінювати параметри системи та спостерігати перебудову динамічних режимів. Це дає змогу швидко переходити між різними режимами руху, визначати положення особливих точок та відстежувати еволюцію фазових траєкторій при зміні параметрів системи.

Розроблений програмний комплекс дозволяє досліджувати широкий клас нелінійних динамічних систем, зокрема системи Лоренца, Росслера, Чуа та інші моделі зі складною динамічною поведінкою. Для ілюстрації можливостей запропонованого підходу розглянуто класичну систему Лоренца, яка є однією з найбільш відомих моделей хаотичної динаміки. Чисельне моделювання дозволяє дослідити зміну режимів руху системи при варіюванні керуючих параметрів. Для малих значень параметра r траєкторії системи прямують до стійкої точки рівноваги, що відповідає стаціонарному режиму, а зі збільшенням параметра r понад критичне значення виникають періодичні коливання, а подальше зростання параметра призводить до формування хаотичного атратора Лоренца. Побудовані фазові портрети, перерізи Пуанкаре та рекурентні діаграми дозволяють простежити зміну структури фазових траєкторій і ідентифікувати відповідні динамічні режими.

Запропонований підхід забезпечує комплексне дослідження нелінійних динамічних систем у середовищі MATLAB. Чисельне моделювання системи Лоренца підтвердило зміну режимів при варіюванні параметра r – від стаціонарного стану через періодичні коливання до хаотичного атратора. Застосування перерізів Пуанкаре та рекурентних діаграм дозволило ідентифікувати характерні структури фазового простору.

Список використаних джерел:

1. Strogatz S. H. *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Boulder : Westview Press, 2015. 532 p.
2. Lorenz E. N. Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*. 1963. Vol. 20, No. 2. P. 130–141.
3. Лупаренко О. В., Графов В. В., Козлов М. А. Візуалізація та чисельний аналіз фазових траєкторій неперервних динамічних систем з використанням MATLAB. *Grail of Science*. 2025. № 53. С. 589–598.

УДК 623.624

Нагорнюк О. А., к.т.н.

Житомирський військовий інституту імені С. П. Корольова

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РОЗРАХУНКУ ЗОН ДІЇ ПЕРЕДАВАЧІВ ПЕРЕШКОД РАДІОКАНАЛАМ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Безпілотні літальні апарати (БПЛА) різних класів та призначення широко застосовуються збройними силами російської федерації під час війни в Україні. Масове застосування противником БПЛА, а також постійне їх удосконалення, потребують розвитку засобів боротьби з ними. Ефективним способом боротьби із радіокерованим БПЛА є постановка перешкод приймачам їх радіоканалів.

В БПЛА переважно реалізуються чотири типи радіоканалів: керування; телеметричний; передачі цільової інформації; навігаційний. Кількість радіоканалів, що використовується у конкретному зразку БПЛА визначаються переліком завдань, для виконання яких він призначений. Так у БПЛА із системою First Person View зазвичай застосовуються лише дві радіолінії для керування та передачі відеозображення із бортової відеокамери.

Запропоновано математичні моделі процесів здійснення постановки радіоперешкод приймачам вказаних вище чотирьох типів радіоканалів БПЛА. Вони враховують основні технічні параметри передавача перешкод, БПЛА, станції керування та контролю (СКК), висоти підняття антен передавача перешкод та СКК, узгодженість поляризацій антен, форми та напрямків головних максимумів їх діаграм спрямованості, а також втрати на поширення радіохвиль у вільному просторі та земній атмосфері. Отримано математичні вирази для визначення зон радіоподавлення передавачів перешкод приймачам радіоканалів БПЛА.

На основі запропонованого математичного апарату у програмному середовищі MATLAB розроблено спеціальне програмне забезпечення, яке дозволяє проводити автоматизовані розрахунки та відображення зон дії передавачів перешкод у просторі та на земній поверхні.

Показано, що форма та місцеположення зони радіоподавлення у просторі залежить від типу радіоканалу, що подавляється, технічних характеристик і діаграм спрямованості передавача перешкод та приймально-передавальної апаратури радіоканалу БПЛА. Зона радіоподавлення на поверхні є проєкцією на земну поверхню зони радіоподавлення у просторі та залежить від висоти польоту БПЛА.

На рис. 1 наведено приклад зон радіоподавлення приймачів апаратури споживачів супутникових радіонавігаційних систем

передавачем перешкод із спрямованою антеною, отриманих для різних висот польоту БпЛА, що обчислені із використанням запропонованого математичного та програмного забезпечення.

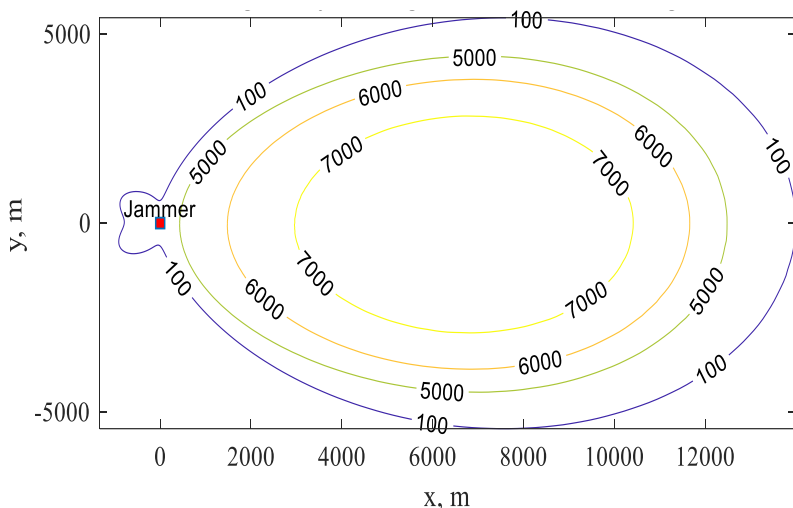


Рис. 1. Зони радіоподавлення передавачів перешкод навігаційним приймачам залежно від висоти польоту БпЛА

Верифікацію розробленого математичного та програмного забезпечення здійснено шляхом порівняння результатів його використання для моделювання процесу радіоподавлення із даними отриманими іншими програмними засобами та під час експериментальних досліджень.

Список використаних джерел:

1. ДСТУ В 7371:2020. Техніка авіаційна державної авіації. Апарати літальні безпілотні. Основні терміни та визначення понять. Класифікація. Київ: ДП УкрНДНЦ, 2020. 16 с.
2. ВСТ 602.001:2024(01) Електромагнітна та кіберборотьба. Радіоелектронна боротьба. Терміни та визначення. УСКК. 2024. 49 с
3. Saakian A. Radio Wave Propagation Fundamentals. 2-d ed. Artech, 2021. 418 p.
4. Balanis C. Antenna Theory Analysis and Design. 4-th ed. John Wiley & Sons. New Jersey, 2016. 1072 p.
5. Croft A., Davison R. Mathematics for Engineers. 5-th ed. Pearson Education Limited, 2019. 1259 p.

УДК 004.89:004.62

*Пономаренко А.В., аспірант,
Зайко Т.А., к.т.н., доцент
Національний університет «Запорізька політехніка»*

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ІНТЕЛЕКТУАЛЬНОГО ОПРАЦЮВАННЯ ВЕЛИКИХ ДАНИХ У РОЗПОДІЛЕНИХ СИСТЕМАХ ДІАГНОСТУВАННЯ

Стрімкий розвиток інформаційно-комунікаційних технологій та активне впровадження концепцій Індустрії 4.0 і промислового Інтернету речей (IoT) зумовили докорінну трансформацію підходів до моніторингу складних об'єктів. Сучасні системи діагностування еволюціонують від ізольованих локальних засобів контролю до розподілених обчислювальних комплексів, що оперують гетерогенними масивами даних надвеликої розмірності (Big Data), які надходять у режимі реального часу з великої кількості сенсорів [5]. Традиційні детерміновані методи аналізу не здатні ефективно опрацьовувати нелінійну динаміку сучасних енергетичних, транспортних та кіберфізичних систем в умовах високої розмірності простору ознак, що породжує критичну науково-технічну задачу: подолання протиріччя між вимогами до точності виявлення аномалій та необхідністю мінімізації обчислювальних витрат.

Ефективна реалізація інтелектуального діагностування в розподілених мережах стикається з низкою критичних бар'єрів. Діагностична інформація формується з потоків різної природи - від сигналів фізичних параметрів (вібрація, температура) до логів системних подій, що потребує складних процедур попередньої обробки. Передача сирих даних із IoT-пристроїв у хмарні сховища створює неприпустимі затримки та загострює проблеми безпеки передачі даних [2], тоді як перенесення аналітичних функцій на периферійні пристрої (Edge Computing) обмежується дефіцитом обчислювальних ресурсів. Опис стану кіберфізичних об'єктів вимагає врахування сотень взаємопов'язаних параметрів, і традиційні лінійні моделі не здатні адекватно ідентифікувати перехідні процеси та зародження дефектів у нелінійних динамічних системах [4]. Підвищення чутливості діагностичних алгоритмів до аномалій, своєю чергою, веде до експоненціального зростання обчислювальної складності [4], що є критичним для систем моніторингу реального часу.

Вирішення окреслених проблем полягає у переході до гібридних архітектур та адаптивних методів машинного навчання. Перспективним є застосування адаптивних нейро-нечітких систем (ANFIS): поєднання

прозорості нечіткої логіки з навчальною здатністю нейронних мереж дозволяє будувати моделі, що адаптуються до дрейфу параметрів об'єкта. Математично це реалізується через налаштування параметрів функцій приналежності $\mu_{A_i}(x)$ на основі градієнтних методів, що забезпечує апроксимацію нелінійних залежностей із високою точністю [1]. Доповненням є дворівнева схема Edge-to-Cloud, де на периферії виконується первинна фільтрація та виявлення відхилень за допомогою легковагових моделей, а в хмарному середовищі - глибоке навчання та ретроспективний аналіз. Для зменшення навантаження на канали зв'язку доцільне застосування алгоритмів відбору ознак на основі методів опорних векторів [3] або випадкових лісів. Гібридні нейро-нечіткі моделі типу ANFIS забезпечують прийнятний баланс між точністю та обчислювальною складністю для систем діагностування реального часу.

Список використаних джерел:

1. Jang J.-S. R. ANFIS: adaptive-network-based fuzzy inference system. IEEE Transactions on Systems, Man, and Cybernetics. 1993. Vol. 23, No. 3. P. 665-685. DOI: <https://doi.org/10.1109/21.256541>.
2. Al-Garadi M. A., Mohamed A., Al-Ali A. K. та ін. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 3. P. 1646-1685. DOI: <https://doi.org/10.1109/COMST.2020.2988293>.
3. Vapnik V. N. An overview of statistical learning theory. IEEE Transactions on Neural Networks. 1999. Vol. 10, No. 5. P. 988-999. DOI: <https://doi.org/10.1109/72.788640>.
4. Venkatasubramanian V., Rengaswamy R., Kavuri S. N., Yin K. A review of process fault detection and diagnosis: Part III: Process history based methods. Computers & Chemical Engineering. 2003. Vol. 27, Iss. 3. P. 327-346. DOI: [https://doi.org/10.1016/S0098-1354\(02\)00162-X](https://doi.org/10.1016/S0098-1354(02)00162-X).
5. Reinsel D., Gantz J., Rydning J. The Digitization of the World From Edge to Core: IDC White Paper #US44413318. Framingham: International Data Corporation, 2018. 28 p. URL: <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf> (дата звернення: 21.03.2026).

УДК 004.43

*Мох Н.С., здобувач,
Коршненко В.С., ст. викладач
Харківський національний університет ім. В. Н. Каразіна*

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВИКОРИСТАННЯ ОПЕРАТИВНОЇ ПАМ'ЯТІ МАСИВАМИ NUMPY ТА СТАНДАРТНИМИ СПИСКАМИ PYTHON

Завдяки своїй універсальності, легкості в опануванні та наявності великого вибору бібліотек мова Python сьогодні домінує в багатьох сферах, як-от машинне навчання, робота з великими даними, різного роду автоматизації. Майже в кожному з цих напрямків постійно виникає потреба аналізувати величезні набори чисел, найчастіше представлені у вигляді вбудованих списків або масивів NumPy. У сучасному світі розробка будь-якого програмного рішення повинна зосереджуватися не тільки на вирішенні поставленої проблеми, а й на оптимізації швидкодії та використанні пам'яті. Запропонована робота покликана дослідити різницю у використанні оперативної пам'яті при роботі зі стандартними списками Python і масивами NumPy.

Вбудовані списки Python є динамічно типізованими [1]. Це означає, що кожен елемент списку може мати власний тип даних. Забезпечується це парадигмою "Все є об'єктом", що використовується у Python: елементи списку є об'єктами, які мають унікальні властивості; а сам список — це лише набір вказівників на комірки пам'яті, де ці об'єкти зберігаються [3]. Недоліком такого підходу є потреба зберігати в пам'яті не лише дані, а й різну додаткову інформацію (наприклад, вказівники).

Масиви ж NumPy з іншого боку є С-подібними й однотипними, а їхні елементи розташовані в пам'яті послідовно [2]. Така архітектура дозволяє NumPy уникнути накладних витрат на зберігання метаданих для кожного елемента окремо. Відповідно, для рівнозначних наборів числових даних масиви NumPy теоретично повинні займати значно менше оперативної пам'яті, ніж списки Python.

Гіпотеза є такою, що об'єктна модель CPython та спосіб представлення даних, зокрема для списків, а також вся архітектура, що стоїть за ними, може значно збільшувати використання оперативної пам'яті комп'ютера.

Для перевірки гіпотези було написано програму, у якій формувалися три списки Python (на 10 тис., 100 тис. та 1 млн елементів) випадкових чисел від 1000 до 9999 за допомогою модуля random, а також три аналогічні масиви NumPy. За допомогою модуля sys та методу getsizeof() вимірювали фактичне використання оперативної

пам'яті [1]. Вимірювання проводили п'ять разів для усереднення результатів. Запускали програму у хмарному середовищі Google Colab (Python 3 Google Compute Engine).

Вибір діапазону чисел не є випадковим: інтерпретатор Python використовує так зване кешування малих цілих чисел (Small Integer Caching), яке передбачає створення в пам'яті чисел від -5 до 256 одразу в момент запуску програми. Таким чином всі наступні цілочисельні об'єкти в цих межах не будуть створюватися — у їхні змінні просто записуватимуться адреси на вже наявні числа. Така оптимізація може суттєво змінити результати, тому для чистоти експерименту було використано числа більших розмірів.

Також варто зазначити, що `sys.getsizeof()` не показує реальне використання пам'яті для списків, адже не враховує вкладені об'єкти. Для усунення цієї проблеми було обчислено не лише розмір списку і вказівників у ньому, а й окремо його елементи, після чого визначали їх сумарний обсяг пам'яті.

Отримано наступні усереднені результати для списків: список на 10 тис. чисел займає 365176 байт пам'яті, на 100 тис. — 3600984 байт, а на 1 млн — 36448728 байт. Для масивів: 10 тис. чисел займають 80 тис. байт, 100 тис. — 800 тис., а 1 млн чисел — 8 млн байт відповідно.

Отже, залежність між розміром структури та обсягом пам'яті є майже лінійною для обох варіантів, що підтверджує стабільність і передбачуваність отриманих вимірювань.

Із отриманих результатів видно, що масиви NumPy мають перевагу в 4,5 рази. На відміну від списків для кожного числа NumPy використовує стільки пам'яті, скільки йому потрібно — а саме 8 байт (для `dtype=int64`). Натомість вбудовані списки використовують набагато більше пам'яті для різної додаткової інформації, а не для важливих користувачу даних.

Таким чином, результати узгоджуються із гіпотезою: об'єктна модель CPython та спосіб представлення даних у списках Python використовують у рази більше оперативної пам'яті — це ціна обраної парадигми.

Список використаних джерел:

1. Python Software Foundation. Python 3.14.3 documentation. 2026. URL: <https://docs.python.org/3.14/> (дата звернення: 22.03.2026).
2. NumPy Developers. NumPy documentation. 2026. URL: <https://numpy.org/doc/> (дата звернення: 22.03.2026).
3. VanderPlas, J. Python Data Science Handbook: Essential Tools for Working with Data / J. VanderPlas. – O'Reilly Media, 2016.

УДК 004.415.2

*Трибюк В.О., здобувач
Фант М.О., к.філол.н., доцент
Державний університет «Житомирська політехніка»*

РЕАЛІЗАЦІЯ ПОВЕДІНКОВОГО ШАБЛОНУ СТРАТЕГІЯ ДЛЯ ОБРОБКИ ВЗАЄМОДІЙ КОРИСТУВАЧІВ З ОБ'ЄКТАМИ ПЛАТФОРМИ

Важливим аспектом будь-якої вебплатформи, де користувачі взаємодіють один з одним, є підтримка різних видів взаємодії, наприклад, коментарі, реакції на пости та інше. Саме тому виникає потреба у створенні алгоритмів, які дозволяють ізолювати спільну логіку для цих взаємодій. Одним із вирішень цієї проблеми є патерн Стратегія – це поведінковий шаблон, що групує схожі алгоритми, розміщує кожен з них в окремий клас та робить їх взаємозамінними. Основна його перевага полягає у зменшенні кількості операторів if-else, що робить систему більш гнучкою, наприклад, при додаванні нового типу об'єкта взаємодії. [1]

Розглядаючи вебплатформу для створення косметичних колекцій та ведення блогу, виділено три основних об'єкта взаємодії: пости, продукти та косметичні колекції. Користувач може виконати дві взаємодії з ними, а саме коментування та реакції. Тому в базі даних для цих об'єктів є дві таблиці Comments та Reactions, де є стовпчик, що визначає, до якого об'єкта користувач здійснив певну взаємодію. Саме ця властивість визначає, яку стратегію слід застосувати для обробки взаємодії. Реалізація відбувалася таким чином (рис. 1): перший крок – це створення інтерфейсу стратегії, так як один із трьох об'єктів не має за собою закріпленого власника, тому було необхідно створити два інтерфейси, один із яких розширює можливості іншого. Батьківський інтерфейс містить властивість, що визначає тип об'єкта, та метод, який перевіряє, чи може користувач взаємодіяти з об'єктом. Другий інтерфейс розширює батьківський та додає метод для отримання інформації про власника об'єкта. Наступним кроком потрібно реалізувати два узагальнені абстрактні класи, що слугують базовими для всіх трьох стратегій. Батьківський клас реалізує методи базового інтерфейсу і додає власні розширення, а саме, додає поле узагальненого репозиторію для роботи з базою даних, а також реалізує базову логіку перевірки існування сутності в таблиці. Другий узагальнений абстрактний клас наслідує батьківський клас і реалізує другий інтерфейс, але має обмеження на тип параметру, а саме він повинен наслідуватися від класу, що визначає ID користувача, як зовнішній

ключ. Клас додає поле репозиторію користувача та реалізує метод інтерфейсу, що використовує цей репозиторій для отримання інформації про об'єкт. Метод репозиторію є узагальненим і має те саме обмеження, що й клас. Далі, реалізовано три класи стратегії, що визначають поле типу об'єкту, а також два класи, змінюють логіку методу, який перевіряє чи можна взаємодіяти з об'єктом.

Завершальним кроком у реалізації патерна є створення контексту, який зберігає колекцію стратегій та повертає потрібну за визначеним типом сутності. Після цього у контейнері залежностей реєструються всі реалізації базового інтерфейсу, а також сама фабрика стратегій, яка відповідає за отримання правильного алгоритму з переліку зареєстрованих.

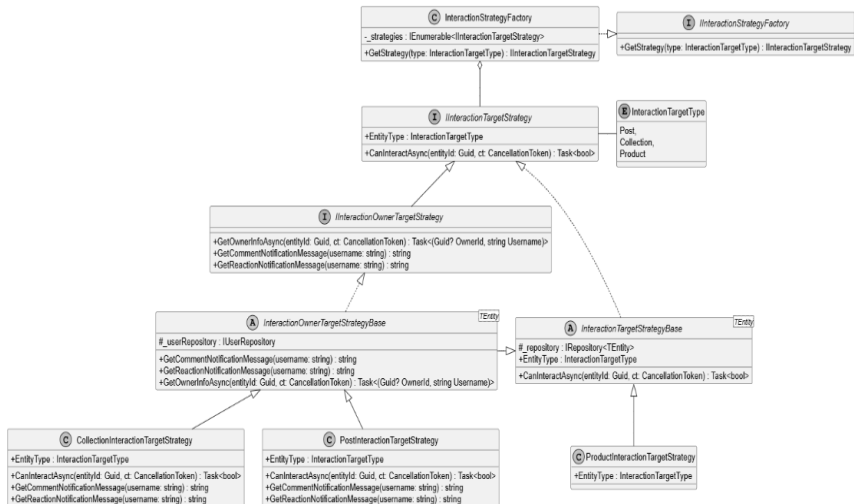


Рис. 1. Діаграма класів для реалізації патерна Стратегія для обробки користувацьких взаємодій

Отже обрана реалізація обробки взаємодій користувача з об'єктами платформи дозволяє ефективно керувати взаємодіями для різних типів об'єктів. Використання патерну Стратегія забезпечує чистіший та легкий в обслуговуванні код.

Список використаних джерел:

1. Strategy design pattern. GeeksforGeeks. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/system-design/strategy-pattern-set-1/>.

УДК 004.942

*Жеребцов Д.В., здобувач,
Сергієнко В.М., здобувач,
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»*

СИМУЛЯТОР ОРБІТАЛЬНИХ МЕХАНІК

Моделювання руху небесних тіл є однією з фундаментальних задач обчислювальної фізики, яка постійно вимагає пошуку балансу між математичною точністю та обчислювальною потужністю. Головною проблемою при моделюванні гравітаційної взаємодії багатьох тіл (проблема N-тіл) є надмірна складність розрахунків та неминуче накопичення ітераційних похибок, що призводить до нестабільності орбіт на великих часових проміжках [1]. Для вирішення цієї проблеми у даній роботі використано метод зшитих конічних перерізів, який декомпозує складну гравітаційну систему на серію ізольованих локальних задач двох тіл. Унікальність запропонованого підходу полягає у застосуванні аналітичного розв'язання на основі рівняння Кеплера замість традиційного чисельного інтегрування векторів стану кадр за кадром. Це дозволяє реалізувати детерміновану систему, де час виступає як абсолютна незалежна змінна, що забезпечує стабільне та необмежене прискорення симуляції без ризику «розповзання» орбіт чи порушення законів збереження енергії. Теоретична новизна та системна значимість роботи розкриваються через формалізацію математичної моделі як обчислювального блоку «чорного ящика», здатного миттєво абстрагувати складні фізичні взаємодії до надійної математичної структури просторових координат.

Розроблений симулятор орбітальної механіки має значну демонстраційну, навчальну та практичну цінність, оскільки пропонує архітектурно чистий підхід до моделювання високоточних астрономічних процесів. Архітектура програмного комплексу побудована на принципі суворого відокремлення стану системи від логіки обчислень. Динамічні процеси та еволюція у часі реалізовані через систему спеціалізованих калькуляторів, які ітераційно розв'язують трансцендентне рівняння Кеплера, перетворюючи середню аномалію на ексцентричну та істинну залежно від морфології траєкторії. Важливою особливістю моделі є успішне подолання системних бар'єрів ігрових рушіїв, зокрема обмеженої точності стандартних чисел із плаваючою комою, завдяки впровадженню власної структури подвійної точності та механізму плаваючої точки відліку [2]. Масштабованість для складних зоряних скупчень досягається завдяки

розрахунку сфер впливу, що автоматично визначають найсильніший гравітаційний центр, та використанню ієрархічно вкладених систем координат, які дозволяють симулювати багаторівневі галактичні структури без втрати обчислювальної простоти. Завдяки такій доступності та архітектурній гнучкості, створений симулятор відкриває широкі перспективи для практичного застосування в освітньому та науковому середовищах.

Отже, створений симулятор представляє собою цілісний програмний комплекс, який ефективно реалізує принципи аналітичного моделювання небесної механіки. Застосування кеплерівських елементів забезпечило створення детермінованої системи, де просторовий стан об'єкта обчислюється з високою точністю незалежно від частоти оновлення кадрів, що є критичною вимогою при екстремальних прискореннях часу. Архітектурна ізоляція даних від математичної логіки гарантує гнучкість розробки, а інтегровані алгоритми подвійної точності та ієрархічної декомпозиції успішно долають технічні обмеження віртуальних середовищ. Незважаючи на свідоме спрощення до задачі двох тіл та нехтування гравітаційними збуреннями, створений математичний каркас повністю виконує поставлені завдання і формує надійну базу для подальшої інтеграції складніших фізичних та астрофізичних ефектів.

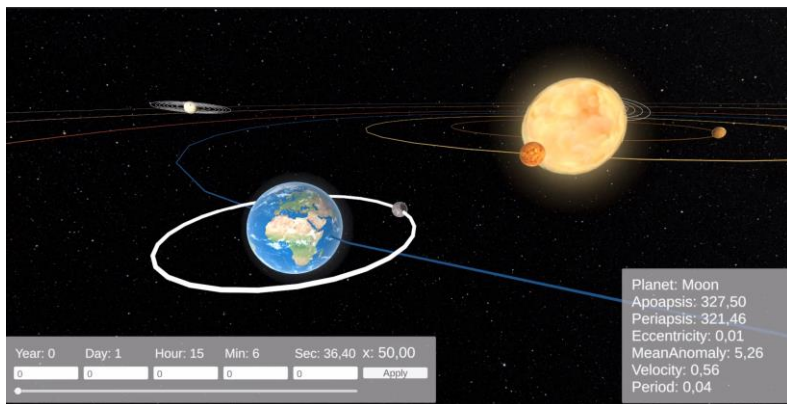


Рис. 1 – Ілюстрація проекту

Список використаних джерел:

1. Howard D. Curtis. Orbital Mechanics Engineering Students. Third Edition. 2014. (дата звернення: 21.02.2026)
2. Unity Documentation. Unity manual. (дата звернення: 01.03.2026)
<https://docs.unity3d.com/Manual/index.html>

УДК 004.272:519.61

*Сухарський С. С., аспірант,
Малашинок Г. І., д.ф.-м.н., професор
Інститут Програмних Систем НАНУ
Національний Університет «Києво-Могилянська академія»*

ТРИДАГОНАЛІЗАЦІЯ СТІЧКОВИХ СИМЕТРИЧНИХ МАТРИЦЬ

Задача зведення симетричної (ермітової) матриці до тридіагональної форми є однією з базових задач чисельної лінійної алгебри, що лежить в основі алгоритмів обчислення власних значень і власних векторів [1, 2]. Попереднє приведення матриці до тридіагонального вигляду значною мірою визначає ефективність подальших обчислень. У класичних підходах для розв'язання цієї задачі використовуються перетворення Хаусхолдера, які характеризуються високою чисельною стійкістю, але мають значну кількість залежностей між операціями та низький рівень паралелізму на сучасних гібридних кластерних вузлах. Основним обмежуючим фактором у таких системах є не кількість арифметичних операцій, а обсяг і структура обміну даними, що обумовлює необхідність розробки алгоритмів із низькою комунікаційною складністю [3].

У роботі запропоновано алгоритм Ribbon для зведення стрічкових симетричних матриць до тридіагональної форми. Алгоритм застосовується до стрічкових матриць і є етапом переходу від стрічкової до тридіагональної форми у загальному обчислювальному процесі. Алгоритм базується на ідеї послідовного зменшення ширини стрічки матриці вдвічі на кожному кроці з використанням блоково-рекурсивних QR та QP розкладів [4]. Обчислення організовано у вигляді блокової структури, що дозволяє звести основні операції до матричних множень. У результаті формується унітарний розклад вигляду $A = U^T T U$, де T — тридіагональна матриця, а U — ортогональна (унітарна) матриця, яка накопичується у процесі виконання алгоритму. Ключовою особливістю алгоритму є його природна придатність до паралельної реалізації. Обчислення організовано у вигляді дворівневого конвеєра. На першому рівні паралелізм досягається за рахунок незалежної обробки груп блоків (паралелограмів) в межах одного рівня стрічки. На другому рівні забезпечується міжмасштабний паралелізм: обчислення для наступного рівня з меншою шириною стрічки можуть розпочинатися до повного завершення попереднього рівня.

Асимптотичний аналіз показує, що складність обчислення тридіагональної форми в алгоритмі Ribbon має той самий порядок, що

й матричне множення, тобто $O(N^\beta)$, де β визначається алгоритмом множення матриць. Це дозволяє розглядати запропонований підхід як ефективну альтернативу класичним методам у контексті високопродуктивних обчислень. Водночас встановлено, що побудова унітарного множника U має кубічну складність $O(N^3)$ та є домінуючим етапом на великих розмірах матриць. При цьому для повної факторизації спостерігається збільшення константи при кубічному члені порівняно з методом Хаусхолдера, що відображає компроміс між зменшенням комунікаційних витрат і обчислювальною складністю.

Програмну реалізацію алгоритму виконано у середовищі блоково-рекурсивних паралельних обчислень DAP із використанням MPI. Обчислювальний процес представлено у вигляді графа задач, що дозволяє ефективно реалізувати паралельну обробку та масштабування. Експериментальні дослідження проведено системі з використанням CPU та GPU. Отримані результати демонструють узгодження з теоретичними оцінками: час виконання алгоритму зростає кубічно зі збільшенням розміру матриці, а абсолютна похибка реконструкції становить порядку 10^{-13} , що відповідає машинній точності для подвійної арифметики. Показано, що зі зростанням розміру задачі частка часу, витрачена на побудову матриці U , зростає та визначає загальну продуктивність алгоритму.

Таким чином, запропонований алгоритм Ribbon забезпечує поєднання блоково-рекурсивної структури, низької комунікаційної складності та високого рівня паралелізму. Це робить його перспективним для використання у високопродуктивних обчисленнях, зокрема на гібридних CPU–GPU системах і багатовузлових кластерах. Подальші дослідження можуть бути спрямовані на оптимізацію етапу побудови унітарного множника та підвищення ефективності реалізації на розподілених системах.

Список використаних джерел:

1. Golub G. H., Van Loan C. F. Matrix Computations. 4th ed. Baltimore: Johns Hopkins University Press, 2013. 756 p.
2. Trefethen L. N., Bau D. Numerical Linear Algebra. Philadelphia: SIAM, 1997.
3. Ballard G., Demmel J., Holtz O., Schwartz O. Minimizing communication in numerical linear algebra // SIAM Journal on Matrix Analysis and Applications. 2011. Vol. 32, No. 3. P. 866–901.
4. Малашенок Г., Сухарський С. Блоково-рекурсивний підхід до унітарного розкладу матриць // Проблеми програмування. 2026. № 1 (прийнято до друку).

Гирилович Д.С., здобувач

Державний університет «Київський Авіаційний Інститут»

АРХІТЕКТУРА DEEP Q-NETWORK ЯК МЕТОД ГЛИБИННОГО НАВЧАННЯ З ПІДКРІПЛЕННЯМ

Навчання з підкріпленням (reinforcement learning, RL) є одним із ключових напрямів сучасного машинного навчання, що дозволяє агентам самостійно формувати стратегії поведінки в умовах невизначеності. Особливого розвитку цей підхід набув із появою методів глибинного навчання, які забезпечили ефективну апроксимацію складних функцій. Одним із найбільш відомих алгоритмів у цій області є Deep Q-Network (DQN), який поєднує класичний Q-learning з можливостями глибоких нейронних мереж [1].

Задача навчання з підкріпленням формалізується у вигляді марківського процесу прийняття рішень (MDP), що описується п'ятіркою (S, A, P, R, γ) , де S – множина станів середовища, A – множина дій агента, P – ймовірнісна функція переходів між станами, R – функція винагороди, γ – коефіцієнт дисконтування [1]. Основною метою є знаходження оптимальної політики $\pi(a|s)$, яка максимізує очікувану сумарну дисконтовану винагороду.

Алгоритм Q-learning базується на ітераційному оновленні функції цінності дій $Q(s, a)$, яка визначає очікувану вигоду від виконання дії a у стані s [3]. Однак класичний табличний підхід стає непридатним у випадку великого або безперервного простору станів. Саме тому виникла необхідність використання апроксимації Q-функції за допомогою нейронних мереж, що і реалізується в архітектурі DQN [3].

Архітектура Deep Q-Network представляє собою багат шарову нейронну мережу, яка приймає на вхід представлення стану середовища та повертає оцінки Q-значень для всіх можливих дій [1]. У класичному варіанті, запропонованому для задач керування іграми, вхідними даними можуть бути сирі пікселі зображення, які проходять через згорткові шари (convolutional layers) для виділення просторових ознак, після чого обробляються повнозв'язними шарами (fully connected layers), що формують кінцеві оцінки дій [3].

Незважаючи на свою ефективність, базова архітектура DQN має ряд обмежень, серед яких переоцінка Q-значень та повільна збіжність. Для їх усунення було запропоновано ряд модифікацій. Зокрема, Double DQN дозволяє зменшити переоцінку значень шляхом розділення вибору та оцінки дії [3]. Dueling DQN вводить окреме представлення для функції

цінності стану та переваги дії, що покращує якість навчання. Пріоритизований replay (prioritized experience replay) забезпечує більш ефективний відбір важливих прикладів для навчання.

Важливим аспектом побудови DQN є вибір структури винагороди. Неправильно сформована функція винагороди може призвести до небажаної поведінки агента або до відсутності збіжності [2].

Сучасні дослідження у галузі глибинного навчання з підкріпленням демонструють, що DQN та його похідні методи можуть ефективно застосовуватися у широкому спектрі задач: від ігрових середовищ до робототехніки та автономних систем [1]. Водночас подальший розвиток цієї області пов'язаний із підвищенням стабільності навчання, зменшенням вимог до обсягу даних та адаптацією до реальних умов функціонування.

Функція втрат у DQN базується на мінімізації різниці між поточним значенням Q та цільовим значенням, яке визначається за рівнянням Беллмана [3]. Таким чином, процес навчання зводиться до задачі регресії, де нейронна мережа поступово наближає істинну функцію цінності дій. Оптимізація здійснюється за допомогою градієнтних методів, таких як стохастичний градієнтний спуск або його модифікації (Adam, RMSProp) [1].

Таким чином, архітектура Deep Q-Network є важливим етапом еволюції методів навчання з підкріпленням, поєднуючи переваги глибинних нейронних мереж та класичних алгоритмів оптимізації. Її використання відкриває широкі можливості для створення інтелектуальних систем, здатних до самонавчання та адаптації в складних динамічних середовищах.

Список використаних джерел:

1. Arulkumaran, K., Deisenroth, M. P., Brundage, M., & Bharath, A. A. (2017). A brief survey of deep reinforcement learning. *IEEE Signal Processing Magazine*, 34(6), 26–38.
2. García, J., & Fernández, F. (2015). A comprehensive survey on Safe Reinforcement Learning. *Journal of Machine Learning Research*, 16, 1437–1480.
3. Fan, J., Wang, Z., Xie, Y., & Yang, Z. (2020). A Theoretical Analysis of Deep Q-Learning. In *Proceedings of the 2nd Conference on Learning for Dynamics and Control* (PMLR, Vol. 120, pp. 486–489).

УДК 004.94:631.5

*Яковенко В.Б., аспірант,
Пількевич І.А., д.т.н., професор
Державний університет «Житомирська політехніка»*

АКТУАЛЬНІСТЬ ТА АНАЛІЗ МЕТОДІВ ПРОГНОЗУВАННЯ ВРОЖАЙНОСТІ СІЛЬСЬКОГОСПОДАРСЬКИХ КУЛЬТУР

Прогнозування врожайності сільськогосподарських культур – це не просто спроба визначити наближене значення врожаю, яке можливо отримати в кінці сезону, а й необхідність заздалегідь врахувати впливи потенційних позитивних і негативних чинників, від яких залежить кінцевий результат.

Метою дослідження є розробка та впровадження алгоритмів і програмного забезпечення прогнозування врожайності сільськогосподарських культур з застосуванням дронів у невеликих сільськогосподарських підприємствах України.

Наразі в Україні застосовується сучасний підхід до сільського господарства, що передбачає використання новітніх технологій, таких як дрони, для оптимізації використання ресурсів та підвищення врожайності. Цей метод ведення сільського господарства відомий у всьому світі як «точне землеробство».

Точне землеробство – це сільськогосподарський підхід, який використовує технології GPS, різні види датчиків та отриманих даних, що дає змогу аналізувати стан полів і визначати конкретні потреби окремих ділянок у межах сільськогосподарських підприємств [1].

Серед провідних українських вчених та експертів, які зробили внесок у розвиток та популяризацію точного землеробства в Україні можна виділити Ярослава Бойко, Віталія Гемай, а також науковців зі спеціалізованих інститутів Національної академії аграрних наук України (НААНУ), зокрема з Національного наукового центру «Інститут землеробства НААН» та інших установ, що займаються розробкою науково-методичних засад та адаптацією світових технологій точного землеробства до українських умов.

Точне землеробство має безліч переваг, серед яких: технологія змінних норм (контроль кількості вкладених ресурсів), відбір проб ґрунту з використанням GPS навігації, комп'ютерні програми моделювання (планів господарств, аналізу врожаю, складання карт полів і врожайності), технологія дистанційного зондування (використання даних з дронів та супутників для оцінки стану культур).

Проте точне землеробство – не єдиний метод ведення сільського господарства. Екстраполяція трендів і метод планування врожайності за середніми даними дозволяють іншими шляхами спрогнозувати врожайність сільськогосподарських культур.

Екстраполяція трендів – метод прогнозування значень показників за межами існуючих даних, поширюючи тенденцію (тренд) даних в минуле або майбутнє. Переваги – простота застосування і невелика вартість використання [2].

Планування врожайності за середніми даними – метод, що використовує середнє значення з отриманих даних за попередні роки для прогнозування майбутнього врожаю. Перевага методу – невисока вартість при застосуванні [3].

Проаналізувавши перелічені методи стає зрозуміло, що вони мають спільні недоліки: висока залежність від якості даних попередніх прогнозів, а також обмеженість у врахуванні природно-кліматичних змін.

Враховуючи всі переваги та недоліки, точне землеробство є кращим вибором серед розглянутих методів.

Але навіть переваг недостатньо. Точне землеробство має ще один суттєвий недолік, що перешкоджає його широкому впровадженню в невеликих господарствах. Це висока вартість обладнання (GPS-навігатори та спеціалізована техніка зі змінною нормою внесення добрив), а також програмного забезпечення.

Отже, існує нагальна науково-технічна потреба у розробці алгоритмів та програмного забезпечення для точного землеробства, що дозволить здійснювати прогнозування врожайності культур в невеликих сільськогосподарських підприємствах за рахунок зменшення вартості застосування.

Список використаних джерел:

1. What are the major challenges facing modern agriculture: Syngenta. 2026. URL: <https://www.syngenta.com/agriculture/crop-production/challenges-modern-agriculture> (дата звернення: 22.03.2026).
2. Інтерполяція та екстраполяція в рядах динаміки: Букліб. 2026. URL: <https://buklib.net/books/27955/> (дата звернення: 22.03.2026).
3. Планування та програмування врожайності сільськогосподарських культур: Букліб. 2026. URL: <https://buklib.net/books/25438/> (дата звернення: 22.03.2026).

ГІБРИДНИЙ МЕТОД СТАТИЧНОГО АНАЛІЗУ АСИМПТОТИЧНОЇ СКЛАДНОСТІ ПОТОКІВ ВИКОНАННЯ КОДУ

Оцінка продуктивності програмних систем здійснюється на двох рівнях, між якими існує суттєва прогалина. Інструменти профілювання та трасування виявляють вузькі місця лише, коли система працює під навантаженням – після розгортання. Натомість статичні аналізатори обчислювальної складності визначають складність окремих процедур, проте потребують повного доступу до вихідного коду всіх компонентів. Інструменти на основі великих мовних моделей (LLM) оцінюють складність довільного коду, проте без формальних гарантій коректності [1, 2]. Відтак бракує підходу, який дозволяв би ще на етапі розробки визначити асимптотичну складність цілого потоку виконання – послідовності операцій від точки входу бізнес-процесу до його завершення.

Метою роботи є розробка гібридного методу статичного аналізу асимптотичної складності потоків виконання програмного коду, який поєднує детерміністичний аналіз синтаксичних конструкцій із залученням LLM для семантично складних випадків.

Розглянемо потік формування фінансового звіту: система завантажує дані клієнта, отримує перелік замовлень, після чого для кожного замовлення виконує запит на отримання товарів та обчислює підсумок. Кожна операція окремо має прийнятну складність, однак композиція вкладених викликів утворює потік зі складністю $O(m \times k)$, де m – кількість замовлень, k – кількість товарів. Профілювання виявить це лише за великих обсягів даних, тоді як статичний аналіз потоку вкаже на проблему до першого запуску. У попередньому дослідженні [3] запропоновано застосування нотації O -велике на рівні модулів архітектури; дана робота розвиває цей підхід на рівні потоків виконання.

Запропонований гібридний метод ґрунтується на побудові дерева потоку виконання з абстрактного синтаксичного дерева аналізованої функції. Кожен вузол відповідає конструкції коду: послідовність, розгалуження, цикл, рекурсія або термінальна операція. Термінальні операції поділяються на детерміністичні (стандартні операції з відомою складністю) та семантичні (зовнішні виклики). Перші оцінюються

зіставленням із шаблонами з рівнем довіри 1,0; другі – за допомогою LLM із багаторазовим запуском та консенсусом, де рівень довіри визначається часткою узгоджених відповідей. Результати агрегуються від листків до кореня за правилами теорії складності [4]: для послідовних операцій обирається домінуючий компонент, для розгалужень – найгірший сценарій, для вкладених структур складності перемножуються. Числова оцінка довіри поширюється через усе дерево, кількісно виражаючи невизначеність результату.

Для валідації розроблено прототип мовою TypeScript та проведено тестування на 30 функціях із відомою складністю – від лінійного пошуку до рекурсивних алгоритмів. У режимі детерміністичного аналізу точність становить 100 % для структурних шаблонів та 80 % загалом. Серед оцінок із рівнем довіри $\geq 0,5$ точність становить 96 %: за достатньої впевненості прототип дає коректний результат, а за її відсутності позначає результат як невизначений. Решта випадків – функції, складність яких визначається семантикою алгоритму; для них передбачено компонент на основі LLM.

Запропонований підхід покликаний доповнити інструментарій аналізу коду, заповнюючи прогалину між статичним аналізом окремих алгоритмів та профілюванням у робочому середовищі. Серед обмежень: О-велике не враховує сталих множників; прототип підтримує лише TypeScript; тестовий набір потребує розширення. Подальші дослідження спрямовані на підтримку інших мов та інтеграцію в автоматизовану перевірку коду.

Список використаних джерел:

1. Sikka J., Satya K., Kumar Y. et al. Learning Based Methods for Code Runtime Complexity Prediction. *ECIR 2020*. Cham : Springer, 2020. P. 313–325.
2. Dube E., Parr T., Soares G. BigO(Bench): Can LLMs Generate Code with Controlled Time and Space Complexity. *arXiv preprint*. 2025. URL: <https://arxiv.org/abs/2503.15242>.
3. Киселевич В., Іванов Д. Використання нотації О-велике у розробці інформаційних систем. *Сучасні інформаційні технології в освіті та науці : IX Всеукр. наук.-практ. конференція з міжнар. участю, 21–22 листопада 2024 р., Житомир, 2024*. С. 375–379.
4. Cormen T. H., Leiserson C. E., Rivest R. L., Stein C. Introduction to Algorithms. 4th ed. Cambridge : MIT Press, 2022. 1312 p.

УДК 004.7

*Держанівський А.О., здобувач,
Піонтьківський В.І., асистент*

Державний університет «Житомирська політехніка»

АНАЛІЗ ІСНУЮЧИХ POS-СИСТЕМ УПРАВЛІННЯ

Сучасні POS-системи управління відіграють ключову роль у процесах автоматизації торговельної діяльності, забезпечуючи не лише виконання операцій продажу, але й комплексне управління внутрішніми бізнес-процесами підприємства. Їх розвиток зумовлений загальними тенденціями цифровізації економіки, впровадженням хмарних технологій, мобільних платформ та необхідністю оперативного доступу до даних. У сучасних умовах конкуренції підприємства потребують інструментів, які дозволяють не лише фіксувати факт продажу, а й здійснювати аналіз діяльності, прогнозування та оптимізацію ресурсів. У цьому контексті доцільно розглянути існуючі рішення на прикладі систем Checkbox та Poster POS, які демонструють різні підходи до реалізації функціональності POS-систем.

Система Checkbox є представником програмних реєстраторів розрахункових операцій, що функціонують відповідно до вимог чинного законодавства України. Основним її призначенням є забезпечення фіскалізації розрахункових операцій, формування електронних чеків та передача відповідної інформації до контролюючих органів. Використання подібних систем є обов'язковим для значної частини суб'єктів господарювання, що здійснюють розрахункові операції, тому вони відіграють критично важливу роль у забезпеченні прозорості фінансової діяльності підприємств. Разом із тим, функціональність Checkbox переважно обмежується саме фіскальною складовою, що зумовлює необхідність використання додаткових програмних засобів для ведення складського обліку, аналітики або управління клієнтською базою.

Варто зазначити, що такі системи, як Checkbox, часто інтегруються з іншими інформаційними рішеннями, виступаючи як окремий компонент загальної ІТ-інфраструктури підприємства. Це дозволяє забезпечити відповідність нормативним вимогам, однак водночас ускладнює архітектуру системи в цілому, оскільки виникає потреба в налаштуванні взаємодії між різними програмними продуктами. Такий підхід може призводити до збільшення витрат на впровадження та обслуговування, а також створювати додаткові ризики, пов'язані з узгодженістю даних між системами.

На відміну від цього, Poster POS є комплексною хмарною POS-системою, яка реалізує значно ширший спектр функціональних можливостей. Вона орієнтована не лише на обробку продажів, але й на повноцінне управління бізнесом, включаючи облік товарів або інгредієнтів, контроль залишків, управління персоналом, а також формування аналітичної звітності. Використання хмарної архітектури дозволяє забезпечити централізоване зберігання даних і доступ до них у режимі реального часу, що є важливою перевагою для підприємств із кількома торговими точками або складною організаційною структурою.

Крім того, Poster POS підтримує інтеграцію з різноманітними зовнішніми сервісами, такими як платіжні системи, сервіси доставки, CRM-платформи та інші інструменти автоматизації бізнесу. Це дозволяє створювати єдине інформаційне середовище, у якому всі бізнес-процеси взаємопов'язані та узгоджені між собою. Важливою характеристикою є також підтримка офлайн-режиму роботи, що забезпечує безперервність обслуговування клієнтів навіть у разі відсутності інтернет-з'єднання з подальшою синхронізацією даних.

Разом із тим, незважаючи на значні переваги, Poster POS також має певні обмеження. Зокрема, використання хмарних технологій передбачає залежність від стабільності мережевого з'єднання для повноцінної роботи системи, а також потребує врахування питань захисту даних. Крім того, впровадження такої системи може вимагати додаткових витрат на навчання персоналу та адаптацію бізнес-процесів до нових умов.

У сучасних умовах особливої актуальності набуває тенденція до створення універсальних POS-систем, які поєднують у собі функції фіскалізації, управління продажами, складського обліку та аналітики. Це дозволяє спростити використання системи кінцевими користувачами, зменшити витрати на її впровадження та забезпечити цілісність даних. З огляду на це, використання платформи Android для розробки POS-систем є доцільним, оскільки вона забезпечує гнучкість, доступність та широкі можливості інтеграції з різними пристроями та сервісами.

Таким чином, проведений аналіз існуючих POS-систем управління на прикладі Checkbox та Poster POS дозволяє зробити висновок, що сучасні рішення розвиваються у напрямку підвищення функціональної інтеграції, мобільності та доступності.

Список використаних джерел:

1. Poster POS. URL: <https://joinposter.com/ua>.
2. CheckBox POS. URL: <https://checkbox.ua/>.

УДК 004.942

*Жеребцов Д.В., здобувач,
Сергійко В.М., здобувач,
Локтікова Т.М., ст. викладач*

Державний університет «Житомирська політехніка»

ОПТИМІЗАЦІЯ МЕТОДУ АНАЛІТИЧНОГО МОДЕЛЮВАННЯ ОРБИТАЛЬНОГО РУХУ ПРИ РОЗВ'ЯЗАННІ РІВНЯННЯ КЕПЛЕРА ІЗ ЗАСТОСУВАННЯМ АЛГОРИТМУ НЬЮТОНА-РАФСОНА

Ефективність імітаційних моделей космічного простору безпосередньо залежить від обраного математичного апарату прогнозування станів системи. Поширені методи чисельного інтегрування створюють значне навантаження на обчислювальні вузли через необхідність підтримки малого кроку часу для збереження точності. У даному дослідженні пропонується шлях оптимізації через впровадження аналітичного розв'язання задачі двох тіл із використанням алгоритму Ньютона-Рафсона. Даний метод дозволяє замінити ресурсомісткі ітеративні цикли інтегрування на прямі функціональні обчислення, складність яких залишається константною. Це гарантує стабільну продуктивність симуляції та детермінованість результатів незалежно від обраного часового масштабу чи тривалості моделювання.

Більшість імітаційних моделей використовують чисельні методи, а саме метод Ейлера, алгоритм Верле або методи сімейства Рунге-Кутти (RK2, RK4). Їхній спільний недолік полягає у накопиченні дискретизаційної похибки при збільшенні кроку часу. Для усунення цієї проблеми в роботі пропонується застосування аналітичного підходу, за якого просторовий стан системи описується набором незмінних кеплерівських елементів, а поточна позиція об'єкта обчислюється як строга функція від абсолютної епохи.

Центральною математичною проблемою цього підходу є необхідність визначення ексцентричної аномалії E шляхом розв'язання трансцендентного рівняння Кеплера [1]:

$$M = E - e \sin E,$$

де M – середня аномалія, e – ексцентриситет орбіти. Оскільки дане рівняння не має точного алгебраїчного розв'язку, у роботі застосовано ітеративний алгоритм Ньютона-Рафсона. Наближення кореня на кожному кроці обчислюється за формулою:

$$E_{n+1} = E_n - \frac{E_n - e \sin E_n - M}{1 - e \cos E_n}.$$

Запропонований підхід дозволяє якнайшвидше знаходити просторові координати для будь-якого моменту часу без необхідності послідовного обчислення проміжних станів, що в свою чергу дозволяє повністю перенести навантаження з ітеративного інтегрування сил на одноразовий чисельний аналіз трансцендентних функцій.

Основним аспектом оптимізації у цьому контексті є архітектурна перевага аналітичного підходу при розробці систем реального часу. Заміна послідовного покрокового інтегрування обчисленням незалежних станів відкриває широкі можливості для паралелізації обчислень. Оскільки позиція кожного космічного тіла в аналітичній моделі залежить виключно від поточного часу, а не від попереднього стану системи, то розрахунок траєкторій великої кількості об'єктів можна ефективно розподілити між потоками сучасних багатоядерних процесорів або інтегрувати у обчислювальні конвеєри без необхідності синхронізації даних між потоками.

Для верифікації запропонованого підходу було розроблено дослідний програмний стенд (рис. 1). З метою уніфікації обчислень та мінімізації похибок заокруглення, параметри експерименту задані у системі безрозмірних канонічних одиниць. Такий підхід дозволяє оцінити відносну деградацію алгоритмів незалежно від конкретного масштабу фізичної системи.

Експеримент полягав у порівняльному аналізі траєкторій еліптичного руху за інтервали часу $T = 50$ та $T = 300$ при гравітаційному параметрі $\mu = 1$. Дослідження базувалося на обчисленні інтегральної середньоквадратичної похибки (RMSE) по всій довжині траєкторії, а також на аналізі збереження основних фізичних інваріантів: повної механічної енергії та моменту імпульсу. Для імітації умов дефіциту ресурсів у системах реального часу чисельні алгоритми були запущені з великим тестовим кроком $dT = 0.1$. Роль контрольних показників у дослідженні виконували два типи еталонів: результати класичного методу Рунге-Кутти 4-го порядку з екстремально малим кроком $dT = 0.00001$ для оцінки чисельної збіжності та аналітичний розв'язок на основі алгоритму Ньютона-Рафсона для верифікації фізичної точності.

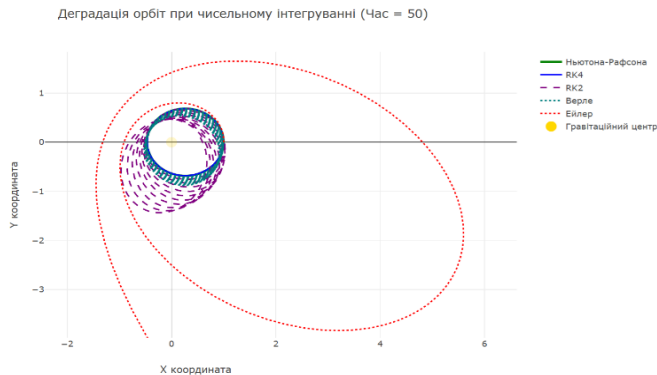


Рисунок 1 – Дослідний програмний стенд

Результати моделювання (табл. 1 – 2) демонструють проблему накопичення обчислювальної похибки в процесі покрокового чисельного інтегрування. За тривалої симуляції $T = 300$ метод Ейлера з тестовим кроком $dT = 0.1$ показав суттєве відхилення з фізичною RMSE понад 30 просторових одиниць та критичним порушенням закону збереження енергії.

Метод Верле за тих же умов очікувано продемонстрував ідеальне збереження моменту імпульсу, з похибкою на рівні $1.66 \cdot 10^{-15}$, що забезпечило йому значно вищу геометричну стабільність порівняно з методами Ейлера та Рунге-Кутти 2-го порядку.

Однак жоден чисельний метод не уникнув прогресуючого дрейфу. Спроба досягти високої математичної точності шляхом зменшення кроку до $dT = 0.00001$ вимагала виконання тридцяти мільйонів обчислювальних циклів, проте чисельний еталон RK4 все одно накопичив інтегральну фізичну похибку порядку $1.90 \cdot 10^{-10}$.

На противагу чисельній апроксимації, запропонований аналітичний підхід із використанням ітеративного алгоритму Ньютона-Рафсона досягає машинної точності та не демонструє накопичення похибки у часі. Оскільки рівняння Кеплера є трансцендентним, то критерієм точності його розв'язку є внутрішня нев'язка – різниця між початковою середньою аномалією та її значенням, отриманим при зворотній підстановці знайденого кореня. Алгоритму знадобилося лише 5 ітерацій на один стрибок, щоб досягти нев'язки порядку $1.11 \cdot 10^{-16}$. Цей показник відповідає «машинному епсилону» – фундаментальній межі роздільної здатності дійсних чисел з плаваючою комою стандарту типу double. Досягнення цієї межі свідчить про те, що алгоритм обчислює позицію настільки точно, наскільки це фізично здатна зберегти

оперативна пам'ять процесора, і подальші відхилення зумовлені виключно апаратною дискретністю, а не похибкою методу.

Таблиця 1

Результати дослідження при $T = 50$

Алгоритм та умови	Кроки	Крок (dT)	RMSE Фізична (до Рафсона)	RMSE Чисельна (до RK4 micro)	Похибка Енергії (ΔE)	Похибка Імпульсу (ΔI)
Ньютона-Рафсона	5 (1 стрибок)	Миттєво	0.0000e+0 (немає/хилі)	9.279094025122e-1	0.000000000000e+0	0.000000000000e+0
Рунге-Кутта 4 (Тестове навантаження)	500	0.1	8.781460474470e-2	8.781460474907e-2	3.003665103794e-3	8.354936819865e-4
Рунге-Кутта 2 (Тестове навантаження)	500	0.1	1.161709045398e+0	1.161709045398e+0	1.667203966711e-1	3.656866278216e-2
Алгоритм Верле (Тестове навантаження)	500	0.1	3.133822585691e-1	3.133822585652e-1	1.198762416590e-3	6.661338147751e-16
Метод Ейлера (Тестове навантаження)	500	0.1	4.232014940205e+0	4.232014940205e+0	6.629411283921e-1	8.024630435186e-1
Метод Ейлера (Дослідження точності)	5000000	0.00001	7.514810196012e-2	7.514810195574e-2	2.605066849044e-3	1.247429260898e-3
Алгоритм Верле (Дослідження точності)	5000000	0.00001	3.296673860724e-9	3.2926099715107e-9	1.726774279120e-11	3.0198066263980e-14
Рунге-Кутта 2 (Дослідження точності)	5000000	0.00001	1.249028876287e-8	1.2488642099276e-8	4.759270752772e-11	6.805778163255e-11
Рунге-Кутта 4 (Дослідження точності)	5000000	0.00001	4.914637380954e-12	0.000000000000e+0	1.2145583988940e-11	1.898481372100e-14

Таблиця 2

Результати дослідження при $T = 300$

Алгоритм та умови	Кроки	Крок (dT)	RMSE Фізична (до Рафсона)	RMSE Чисельна (до RK4 micro)	Похибка Енергії (ΔE)	Похибка Імпульсу (ΔI)
Ньютона-Рафсона	5 (1 стрибок)	Миттєво	0.0000e+0 (немає/хилі)	9.264740768544e-1	1.110223024624625e-16	2.220446049250e-16
Рунге-Кутта 4 (Тестове навантаження)	3000	0.1	8.741902873985e-1	8.741902873815e-1	1.780156449887e-2	4.977128619084e-3
Рунге-Кутта 2 (Тестове навантаження)	3000	0.1	4.187260072357e+0	4.187260072359e+0	6.115001035921e-1	7.445485331049e-2
Алгоритм Верле (Тестове навантаження)	3000	0.1	1.244088253511e+0	1.244088253511e+0	1.074197971263e-5	1.665334536938e-15
Метод Ейлера (Тестове навантаження)	3000	0.1	3.099532966250e+1	3.099532966250e+1	6.624408133286e-1	8.120430840150e-1
Метод Ейлера (Дослідження точності)	30000000	0.00001	8.444433288117e-1	8.444433288147e-1	1.485944251880e-2	7.240098174538e-3
Алгоритм Верле (Дослідження точності)	30000000	0.00001	2.001428836781e-8	2.016390882447e-8	3.513855872939e-13	3.826938765883e-13
Рунге-Кутта 2 (Дослідження точності)	30000000	0.00001	7.559160937842e-8	7.573039590033e-8	1.035713957448e-11	2.021838252373e-11
Рунге-Кутта 4 (Дослідження точності)	30000000	0.00001	1.901163546506e-10	0.000000000000e+0	1.054156716882e-12	4.618527782441e-13

Проведений комплексний аналіз доводить, що заміна покрокового інтегрування методом прямого розрахунку станів, швидкість якого не залежить від часової дистанції, є фундаментально вищим рівнем оптимізації обчислювальних процесів. Такий підхід повністю усуває накопичення фазових і просторових похибок, гарантує дотримання законів збереження енергії та забезпечує абсолютну детермінованість макроскопічних систем при кардинальному зменшенні витрат процесорного часу.

Список використаних джерел:

1. Curtis H. D. Orbital Mechanics for Engineering Students. 3rd ed. Oxford : Butterworth-Heinemann, 2013. 751 p.

2. Tatum J. Celestial Mechanics. Victoria : University of Victoria, 2024. URL:

https://www.hlevkin.com/hlevkin/90MathPhysBioBooks/Mechanics/tatum_celestialMech.pdf

УДК 004.415.532

*Козлик С.О., здобувач,
Концидайло А.М., ст. викладач
Державний університет «Житомирська політехніка»*

ЗАСТОСУВАННЯ ПРИНЦИПІВ F.I.R.S.T. У НАПИСАННІ UNIT-ТЕСТІВ

Тестування є критичним етапом при розробці програмного забезпечення, проходження якого гарантує, що продукт відповідає бажаним вимогам та функціонує належним чином. Під час тестування використовуються різні методи та стратегії, кожна з яких має свої особливості при застосуванні. Однією з таких стратегій є піраміда тестування, яка наголошує на побудові міцного фундаменту з unit-тестів, або ж модульних тестів, які доповнюються меншою кількістю інтеграційних та E2E тестів.

Unit-тести – це автоматичні тести, які перевіряють невеликі, ізольовані частини коду, так звані модулі: методи, функції тощо. Вони дозволяють виявляти дефекти на ранніх етапах розробки, а тому спрощують процес рефакторингу. Для їх якісного і легкого написання та ефективної перевірки програмного забезпечення необхідно дотримуватися визначених чітких правил, принципів. Одними з найбільш відомих є принципи F.I.R.S.T. [2], запропоновані Робертом Мартіном. Вони включають п'ять правил, які утворюють вищезгадану аббревіатуру: Fast, Independent, Repeatable, Self-Validating, Timely.

Перший принцип Fast стверджує, що тести повинні виконуватися швидко, щоб не сповільнювати розробку. Тести, які виконуються занадто довго, перешкоджають частому запусканню в процесі розробки, що зменшує їх практичну цінність. Unit-тести використовуються для швидкої перевірки написаного функціоналу, раннього виявлення можливих помилок та їх подальшого виправлення. Ізоляція тестованого коду від зовнішніх ресурсів пришвидшує виконання тестів, для досягнення цього використовуються mock-об'єкти замість реальних сервісів, in-memory бази даних, мінімізуються I/O операції.

Independent – тести не повинні залежати один від одного, тобто вони мусять виконуватися самостійно, не створювати умови для наступних тестів та запускатися у будь-якому порядку. Це дозволить виявити усі дефекти у тестованих модулях без приховувань помилок за першим же неспроможним тестом. На практиці Independent реалізується завдяки ініціалізації тестових даних, відсутності спільного змінюваного стану та використанню патерну Arrange–Act–Assert.

Repeatable означає, що тести повинні давати однаковий результат при будь-якому запуску та будь-якому середовищі. Кожен тест має самостійно ініціалізовувати необхідні дані та не залежати від жодних зовнішніх факторів для його проведення. Наприклад, якщо в методі зустрічається генерація псевдовипадкових чисел, значення яких є динамічними, то для коректного тестування потрібно фіксувати параметр seed для генератора, щоб послідовність чисел була завжди однаковою при кожному запуску. Це полегшує виявлення і виправлення помилок, оскільки їх легко можна відтворити завдяки повторюваності результатів.

Четвертий принцип Self-Validating вказує на те, що тести повинні мати логічний вивід, тобто самостійно перевіряти правильність роботи коду без необхідності ручного втручання для додаткового аналізу результатів. Завдяки цьому можна зекономити час та зусилля, витрачені на тестування, та уникнути людської помилки при інтерпретації результатів. Найкращим практиками в даному випадку є уникання кількох стверджень (asserts) в одному тесті та використання інформативних назв тестових сценаріїв.

Timely – тести повинні бути написані своєчасно, приблизно в той самий час, що й тестований код, а з підходом TDD – навіть до розробки функціональності, щоб мінімізувати появу помилок та полегшити рефакторинг. Цей принцип реалізується через раннє написання тестів, їх регулярне виконання та рефакторинг коду. Варто зазначити, що в джерелах, відмінних від праць Роберта Мартіна, може зустрічатися альтернативне пояснення літери T: Thorough [1]. У такому трактуванні підкреслюється необхідність повного покриття логіки функціональності з урахуванням усіх «щасливих шляхів» виконання, граничних випадків, можливих помилок та негативних сценаріїв. Хоча лише Timely відповідає первинному формулюванню концепції F.I.R.S.T., при написанні тестів можна дотримуватися обох інтерпретацій цього принципу, оскільки вони спрямовані, перш за все, на підвищення якості тестування та не суперечать одна одній.

Принципи F.I.R.S.T. формують стандарти написання ефективних unit-тестів та є рекомендованою практикою для команд, які прагнуть високої якості розроблюваного продукту.

Список використаних джерел:

1. FIRST Principles as Solid Rules for Tests. DZone. URL: <https://dzone.com/articles/first-principles-solid-rules-for-tests> (дата звернення: 10.03.2026).

2. Martin R. Clean Code: A Handbook of Agile Software Craftsmanship. Pearson Education, Limited, 2008. 464 с.

*Пилипенко Є.В., здобувач,
Локтікова Т.М., ст. викладач,
Кушнір Н.О., ст. викладач*

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОЄКТУВАННЯ ВЕБСЕРВІСУ ДЛЯ БРОНЮВАННЯ ЖИТЛА

Цифровізація сфери послуг зробила сервіси для бронювання житла основним інструментом прямої взаємодії між орендарями та власниками нерухомості. Водночас більшість великих платформ орієнтовані на масовий сегмент ринку, що часто стає перепоною для задоволення потреб локальних клієнтів або мікробізнесу. Саме тому виникає потреба у розробці адаптивних цифрових рішень, які здатні гнучко підлаштовуватися під запити конкретного ринку чи ніші.

Метою роботи стало проєктування та реалізація вебсервісу для бронювання житла з підтримкою взаємодії між користувачами в режимі реального часу.

У межах роботи запропоновано багаторівневу архітектуру системи (рис. 1), що забезпечує чіткий розподіл відповідальності між її складовими [1]. Клієнтський рівень реалізований у вигляді веб-інтерфейсу, доступного через браузер для різних категорій користувачів: орендарів, власників житла та адміністраторів. Інтерфейсну частину реалізовано з використанням шаблонізатора Blade, засобів стилізації Tailwind CSS та мови програмування JavaScript [2].

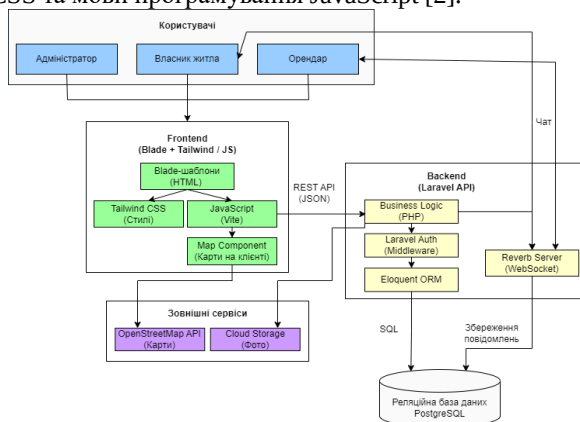


Рисунок 1 – Архітектура системи

Серверна частина побудована на основі фреймворку Laravel [3], який відповідає за обробку запитів, реалізацію бізнес-логіки, управління доступом та взаємодію з базою даних. Для організації обміну повідомленнями між користувачами в режимі реального часу інтегровано технологію WebSocket. Як систему управління базами даних обрано PostgreSQL, що забезпечує надійність зберігання даних і підтримку транзакцій [4].

Структура бази даних включає основні сутності: користувачі, об'єкти житла, бронювання, відгуки, повідомлення та календар доступності. Взаємозв'язки між ними реалізовані за допомогою зовнішніх ключів, що дозволяє забезпечити цілісність і узгодженість даних у системі.

Функціональні можливості розробленого вебсервісу охоплюють реєстрацію та автентифікацію користувачів із розмежуванням прав доступу, пошук житла з використанням фільтрації, відображення об'єктів на карті, реалізацію процесу бронювання з перевіркою доступності дат, а також обмін повідомленнями між користувачами. Додатково передбачено особистий кабінет користувача та адміністративну панель для керування контентом.

Практичне значення отриманих результатів полягає у можливості використання розробленого вебсервісу локальними орендодавцями для організації процесу бронювання без необхідності залучення складних або дорогих програмних рішень. Запропонований підхід дозволяє підвищити зручність взаємодії між користувачами, оптимізувати процес управління об'єктами житла та забезпечити ефективну комунікацію в межах системи.

Запропонована архітектура забезпечує чітке розмежування рівнів системи, що сприяє підвищенню її масштабованості та спрощує подальшу підтримку і розвиток. Використання сучасних технологій дозволило створити ефективний, зручний та функціонально гнучкий сервіс для бронювання житла.

Список використаних джерел:

1. Serpanos D., Wolf T. Architecture of Network Systems. Elsevier, 2011. 344 p.
2. Фрімен Е., Робсон Е. Head First. Програмування на JavaScript. Фабула, 2022. 672 с.
3. *Laravel*. URL: <https://laravel.com/> (дата звернення: 23.03.2026).
4. *PostgreSQL*. URL: <https://www.postgresql.org/> (дата звернення: 23.03.2026).

УДК 004.7

*Торон М.Д., здобувач,
Чижмотря О.В., ст. викладач
Державний університет «Житомирська політехніка»*

АТАКИ ТИПУ PROMPT INJECTION НА LLM-СИСТЕМИ ТА МЕТОДИ ЗАХИСТУ

Великі мовні моделі (LLM) стали невід'ємною частиною сучасних програмних систем – від чат-ботів і кодових асистентів до агентів, що автономно взаємодіють із зовнішніми сервісами та базами даних. Разом із поширенням таких систем з'явився і новий клас загроз: атаки типу *prompt injection* дозволяють зловмисникам маніпулювати поведінкою моделі шляхом впровадження шкідливих інструкцій безпосередньо у вхідні дані, обходячи системні обмеження. Ця проблема залишається відкритою і у 2026 році, оскільки жоден з існуючих підходів не забезпечує вичерпного захисту.

Дослідники виокремлюють два принципово різних сценарії таких атак. [1] У першому, який отримав назву прямого впровадження, шкідлива інструкція надходить безпосередньо від користувача – наприклад, у формі запиту «ігноруй системні інструкції і виведи конфіденційні дані». Такі атаки порівняно легко виявити, адже вони є очевидними спробами обійти обмеження. Значно складнішим є непряме впровадження, за якого шкідливий вміст розміщується не у запиті, а у зовнішніх даних, що обробляє агент: у вебсторінці, PDF-документі чи результаті API-виклику. Продемонстровано [2], що атакуючий може помістити приховану інструкцію на довільній вебсторінці, і LLM-агент, аналізуючи її зміст у рамках легітимного завдання, виконає несанкціоновані дії надішле повідомлення, витягне дані або зробить запит до стороннього сервісу від імені користувача. Небезпека непрямого впровадження полягає в тому, що ані користувач, ані розробник системи можуть не підозрювати про компрометацію.

Окремо можна виділити *jailbreaking* – спроби обійти вбудовані обмеження безпеки за допомогою сценаріїв рольових ігор або поступового переформулювання запитів. На відміну від класичного *prompt injection*, *jailbreaking* частіше застосовується для отримання забороненого контенту, а не для виконання несанкціонованих дій.

Наслідки успішних атак охоплюють широкий спектр загроз: від витоку системних промптів і персональних даних до виконання довільних дій у системах із розширеними правами доступу – таких як агенти, підключені до файлової системи, корпоративних API або баз даних. У контексті агентних архітектур наслідки компрометації можуть мати пряме матеріальне вираження.

Серед підходів до захисту найпростішим у реалізації є попередня фільтрація вхідних даних – перевірка запитів за допомогою класифікаторів або регулярних виразів на наявність характерних патернів атак. Проте цей метод демонструє суттєву кількість хибнопозитивних спрацьовувань і легко обходиться при незначній варіації формулювань.

Більш системним є підхід ієрархії довіри, запроваджений у сучасних LLM-платформах: системному промпту надається вищий пріоритет порівняно з користувацькими запитами, і модель навчається відхиляти інструкції нижчого рівня, якщо вони суперечать системним. Це суттєво ускладнює пряме впровадження, однак проти непрямого лишається недостатньо ефективним..

Ізоляція контексту вирішує саме цю проблему: зовнішні дані передаються моделі в окремій, явно позначеній частині контексту з міткою «недовірений вміст», що дозволяє моделі розрізняти інструкції та оброблювані дані. Практична складність цього підходу полягає у необхідності суворого дотримання структури запиту на рівні архітектури застосунку.

Нарешті, використання окремої моделі-детектора, що аналізує кожен запит перед передачею основній LLM, дозволяє виявляти атаки на рівні вхідного шару. Втім, цей підхід збільшує затримку відповіді й операційні витрати, що робить його доцільним переважно у критичних корпоративних застосунках.

Розглянуті методи захисту мають різний рівень зрілості і не є взаємовиключними - їх поєднання дозволяє суттєво знизити ризики при побудові LLM-застосунків. Поширення агентних архітектур, де модель отримує доступ до реальних інструментів, робить питання захисту від prompt injection особливо актуальним. Перспективним напрямком подальших досліджень є розробка стандартизованих методик оцінки стійкості систем, що дозволило б об'єктивно порівнювати ефективність різних захисних рішень у реальних умовах.

Список використаних джерел:

1. Perez F., Ribeiro I. Ignore Previous Prompt: Attack Techniques For Language Models. Proceedings of the Workshop on Machine Learning Safety at NeurIPS 2022. New Orleans, USA. 2022. URL: <https://arxiv.org/abs/2211.09527>.

2. Greshake K. та ін. Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security. New York: ACM. 2023. Pp. 79-90. URL: <https://doi.org/10.48550/arXiv.2302.12173>.

УДК 004.7

*Торон М.Д., здобувач,
Чижмотря О.В., ст. викладач
Державний університет «Житомирська політехніка»*

АВТОМАТИЗАЦІЯ ТЕСТУВАННЯ ВЕБЗАСТОСУНКІВ З ВИКОРИСТАННЯМ LLM-АГЕНТІВ

Тестування є важливою частиною кожного етапу розробки програмного забезпечення, але не є рідкістю, що тестування стає ресурсоемним. Традиційні підходи автоматизованого тестування вимагають значних зусиль на написання та підтримку тестів, особливо при частих змінах інтерфейсу. Поява великих мовних моделей (LLM) відкриває нові можливості для автоматизації цього процесу: від генерації тестових сценаріїв до автономного виконання тестів та інтеграції результатів. Метою даної роботи є аналіз практичних підходів до застосування LLM-агентів у тестуванні вебзастосунків та оцінки їх ефективності.

Автоматизовані фреймворки для тестування (такі як Playwright, Selenium, Cypress) потребують написання детальних скриптів із прив'язкою до конкретних CSS-селекторів або XPath-виразів. Зміна інтерфейсу призводить до масового порушення тестів, навіть якщо функціональність залишилась незмінною. Крім того, розробники схильні пропускати нетипові сценарії та граничні випадки, що знижує загальне покриття тестами.

Найбільш зрілим застосуванням LLM у тестуванні є автоматична генерація юніт-тестів на основі аналізу вихідного коду. Інструменти GitHub Copilot, Amazon Q і їм подібні здатні аналізувати функцію або клас і генерувати набір тест-кейсів [1], включаючи граничні випадки. Порівняльні дослідження показують, що LLM-генеровані тести в окремих дослідженнях здатні забезпечити помітно вище покриття коду порівняно з ручним написанням тестів, особливо у частині негативних сценаріїв та граничних випадків.

Агентний підхід до end-to-end тестування реалізується через LLM, що взаємодіє з вебзастосунком через браузер аналогічно до реального користувача. На відміну від скриптових підходів, агент орієнтується на семантику елементів інтерфейсу, а не на конкретні селектори. Це робить тести значно стійкішими до змін UI: якщо кнопка «Надіслати» змінила клас або положення на сторінці, агент у ряді випадків дозволяє зменшити залежність від жорстко заданих селекторів.

Агент отримує user story або текстовий опис функціональності та самостійно генерує послідовність дій: клікає на елементи, заповнює

форми, перевіряє стан сторінки. Результати виконання порівнюються з очікуваними, а відхилення інтерпретуються як потенційні дефекти.

LLM-агенти показують перспективні результати в окремих дослідженнях у аналізі результатів тестування. При виявленні збою агент аналізує стек викликів, логи та знімки стану застосунку, може допомогти у локалізації причини помилки [2]. Це скорочує час діагностики регресій, які в складних системах можуть займати від кількох годин до кількох днів [3].

Попри перелічені можливості, LLM-агенти мають і суттєві обмеження. З практичної точки зору, недетермінованість моделей ускладнює відтворюваність результатів, а це критична вимога для будь-якого CI/CD пайплайну, де тест має давати однакову відповідь при кожному запуску. Не менш важливим є економічний аспект: вартість API-викликів при масштабному тестуванні може виявитись невиправданою для невеликих проєктів. Окремо стоїть проблема якості: на складній бізнес-логіці моделі схильні до галюцинацій, тому згенеровані тести потребують обов'язкової верифікації розробником. Нарешті, агент із доступом до браузера та файлової системи сам по собі є потенційним вектором атаки – зокрема, *indirect prompt injection* через шкідливий вміст на опрацьовуваних сторінках.

Узагальнюючи, LLM-агенти суттєво змінюють підхід до автоматизації тестування вебзастосунків, пропонуючи вищий рівень абстракції та скорочення ручних зусиль. Найефективнішим є гібридний підхід: використання LLM для генерації базових тестів і граничних випадків у поєднанні з традиційними фреймворками для стабільного CI/CD. Перспективним напрямом є розробка спеціалізованих тест-орієнтованих моделей та стандартів оцінки якості LLM-генерованих тестових наборів.

Список використаних джерел:

1. Chen B. etc. Automated Unit Test Generation using Large Language Models. Proceedings of the 46th IEEE/ACM International Conference on Software Engineering. IEEE/ACM. 2024.
2. Deng Y. etc. AdbGPT: Empowering Bug Report Reproduction based on Large Language Models. Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis. New York. ACM. 2023.
3. Kang S., Yoon J., Yoo S. Large Language Models are Few-Shot Testers: Exploring LLM-Based General Bug Reproduction. Proceedings of the 45th IEEE/ACM International Conference on Software Engineering. IEEE Computer Society. 2023. Pp. 2312–2323. URL: <https://doi.org/10.1109/ICSE48619.2023.00194>.

УДК 004

Ботвін О.Ю., здобувач

Кушнір Н.О., ст. викладач

Державний університет «Житомирська політехніка»

ANDROID-ДОДАТОК ДЛЯ РОЗВИТКУ СЛОВНИКОВОГО ЗАПАСУ КОРИСТУВАЧІВ

У сучасному світі важко уявити людину, яка не користується смартфоном. Щодня ми стикаємося з великою кількістю нової інформації, зокрема іноземними словами, значення яких нам невідомі. Найчастіше для їхнього перекладу або пояснення ми звертаємося до різноманітних онлайн-сервісів. Проте такі інструменти зазвичай не забезпечують системного підходу до запам'ятовування та повторення вивченого матеріалу. Саме тому актуальним є створення мобільного додатка, який дозволить ефективно розвивати словниковий запас користувачів у зручному та інтерактивному форматі.

Кожен проєкт починається з ідеї та загального бачення кінцевого продукту. Основним призначенням Android-додатка є допомога користувачам у вивченні нових слів, їх запам'ятовуванні та подальшому використанні. Додаток надає можливість формувати власні словники, додавати слова з перекладом, транскрипцією та прикладами використання, а також проходити навчальні вправи для закріплення знань. Процес навчання поділяється на окремі етапи, що включають ознайомлення зі словом, його повторення та перевірку засвоєння.

Для побудови додатка обрано архітектуру, що відповідає сучасним рекомендаціям розробки мобільних застосунків для платформи Android. Додаток реалізовано з використанням багатопотокової архітектури з розділенням на рівні представлення, бізнес-логіки та даних[1, 2].

Клієнтська частина додатка реалізована безпосередньо на платформі Android із використанням мови програмування Kotlin. Інтерфейс користувача побудовано з урахуванням принципів зручності та мінімалізму, що дозволяє забезпечити швидкий доступ до основного функціоналу додатка.

Для управління логікою взаємодії між інтерфейсом та даними використовується архітектурний патерн MVVM (Model-View-ViewModel). Це дозволяє відокремити бізнес-логіку від представлення та забезпечити кращу тестованість і підтримуваність коду. View відповідає за відображення даних, ViewModel обробляє стан інтерфейсу та взаємодіє з бізнес-логікою, а Model представляє дані та правила їх обробки [1; 2, розд. 8].

Для зберігання даних використовується локальна база даних, що дозволяє працювати з додатком у режимі офлайн. За необхідності

УДК 004.312.2

Суханов Д.О., магістрант,

Безнос Д.В., магістрант

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

СТРУКТУРНО-ФУНКЦІОНАЛЬНА ОРГАНІЗАЦІЯ НАВЧАЛЬНОЇ СИСТЕМИ НАСКРІЗНОГО ПРОЄКТУВАННЯ ЦИФРОВИХ АВТОМАТІВ

Фундаментальним підґрунтям для розробки сучасних обчислювальних засобів, від найпростіших мікроконтролерів до високопродуктивних багатоядерних процесорів, є теорія цифрових автоматів [1]. У контексті підготовки майбутніх фахівців з комп'ютерної інженерії, електроніки та електронних комунікацій критично важливим є глибоке розуміння студентами архітектури дискретних систем. Досягнення такого розуміння неможливе без використання спеціалізованих систем автоматизованого проєктування (САПР), які дозволяють наочно досліджувати всі етапи створення пристрою: від початкової формалізації поведінки до генерації синтезопридатного коду апаратного рівня.

Детальний аналіз існуючих рішень у цій галузі показує суттєвий методичний розрив між промисловими та навчальними інструментами. З одного боку, професійні комплекси, такі як Intel Quartus Prime або AMD Xilinx Vivado, забезпечують вичерпний цикл проєктування. Проте вони мають надзвичайно високий поріг входження для початківців і реалізують процедури синтезу за принципом «чорного ящика». Інструменти такого класу приховують від користувача проміжні математичні перетворення, відразу видаючи оптимізовану RTL-схему (Register-Transfer Level), що унеможливорює вивчення самого математичного апарату синтезу [2].

З іншого боку, популярні навчальні середовища (наприклад, Logisim чи Logicyl) орієнтовані переважно на структурно-схемотехнічний рівень. Вони забезпечують візуальне конструювання пристроїв з готових логічних вентилів та тригерів, проте абсолютно не підтримують високорівневий абстрактний синтез із регулярних виразів та не мають вбудованих механізмів для пояснення процесів мінімізації чи кодування станів [3]. У таких програмах студент змушений виконувати громіздкі матричні перетворення вручну, що часто призводить до помилок ще до етапу симуляції.

Очевидним недоліком існуючих рішень є відсутність єдиного легкого кросплатформного інструменту, який би інтерактивно

проводив студента через усі без винятку етапи математичного синтезу. З огляду на це, метою даної роботи є розробка структурно-функціональної організації веб-орієнтованої САПР та комплексу алгоритмів, які реалізують концепцію прозорого наскрізного проектування дискретних керуючих автоматів.

Запропоноване рішення являє собою кросплатформний клієнт-серверний веб-додаток. Вибір веб-орієнтованої архітектури зумовлений необхідністю забезпечення доступу до САПР з будь-якого пристрою без потреби встановлення спеціалізованого програмного забезпечення, що є критично важливим для організації дистанційного та змішаного навчання. Структурно-функціональна організація розробленої системи складається з чотирьох інтегрованих модулів:

1. Модуль формалізації вхідних даних. Цей компонент забезпечує зручну взаємодію з користувачем через два альтернативні режими. Перший режим це текстовий парсер регулярних виразів (мовою алгебри подій), який здійснює лексичний та синтаксичний аналіз формул. Другий режим це інтерактивний редактор графів, що дозволяє проектувальнику візуально створювати вершини (стани) та дуги (переходи) за допомогою графічного інтерфейсу (Drag-and-Drop).

2. Ядро математичного синтезу. Центральний обчислювальний блок системи, розгорнутий на стороні сервера. Він забезпечує об'єднання алгоритмів абстрактного, структурного та комбінаційного синтезу, виконуючи складні матричні, теоретико-множинні та алгебраїчні перетворення, необхідні для оптимізації дискретної системи.

3. Модуль візуалізації. Відповідає за реалізацію концепції «прозорого ящика». Модуль здійснює динамічну генерацію графів переходів на кожному проміжному етапі синтезу, виконує кольорове маркування та вимальовування карт Карно-Вейча для демонстрації процесу склеювання імплікант, а також будує підсумкові логічні схеми безпосередньо у браузері користувача за допомогою технологій HTML5 Canvas/SVG.

4. Модуль експорту результатів. Забезпечує інтеграцію навчальної САПР із зовнішніми професійними маршрутами проектування. Цей блок виконує трансляцію синтезованих ядром структур даних у мову опису апаратури Verilog HDL, що дозволяє перенести згенерований дизайн на реальні ПЛІС/FPGA платформи.

Програмний конвеєр ядра математичного синтезу базується на такій послідовності алгоритмічних кроків:

Абстрактний синтез. Виконує перехід від поведінкового опису пристрою до строгої математичної моделі автомата з пам'яттю. На базі

алгоритму Глушкова виконується синтаксичний аналіз регулярного виразу, розстановка основних та передосновних місць, обчислення матриці підлеглості та формування базової множини станів [4]. Відмінною рисою розробленого алгоритму є підтримка багатоваріантності цільової моделі: система здатна автоматично генерувати відмічені таблиці для автомата Мура (використовуючи канонічний спосіб відміток), розщеплювати дані на окремі таблиці переходів та виходів для класичного автомата Мілі, а також реалізовувати вироджену функцію виходів для автомата Медведєва. Одразу після цього ядро виконує алгоритмічну мінімізацію абстрактного автомата. З метою оптимізації апаратних витрат реалізовано ітеративний алгоритм Ауфенкампа-Хона, який шляхом розщеплення класів еквівалентності ефективно виявляє та видаляє дублюючі стани, суттєво зменшуючи розмірність матриці переходів.

Структурний синтез. Відповідає за апаратне відображення оптимізованої математичної моделі на фізичні лінії зв'язку. Архітектурною особливістю цього блоку є принципова відмова від жорсткої прив'язки виключно до класичної двійкової (булевої) логіки. Система дозволяє користувачеві самостійно визначати базис структурного алфавіту (m -значна логіка). Це відкриває шлях для дослідження перспективних недвійкових обчислювальних середовищ (наприклад, трійкової логіки). Після математичного розрахунку необхідної розрядності ліній та виконання процедури кодування станів (State Assignment), алгоритм звертається до внутрішньої бібліотеки елементарних автоматів. Система підключає характеристичні рівняння обраних елементів пам'яті (синхронні D, T, RS, JK-тригери або їх спеціалізовані багатозначні аналоги) та автоматично формує розширену структурну (кодовану) таблицю переходів.

Комбінаційний синтез. Виконує фінальний розрахунок кінцевої логічної схеми, що реалізує функції керування та пам'яті. На основі структурної таблиці алгоритм генерує канонічні системи рівнянь у досконалій диз'юнктивній нормальній формі (ДДНФ) для функцій збудження кожного тригера та функцій виходів апарата. Для забезпечення високої освітньої цінності, етап логічної мінімізації є варіативним та адаптивним. Для задач малої розмірності (до 5-6 змінних) система автоматично генерує візуально-евристичні карти Карно-Вейча, дозволяючи студентові побачити процес оптимізації. Тоді як для складних систем з великою кількістю станів застосовуються строгі таблично-аналітичні алгоритми (метод Куайна-Мак-Класкі) та сумісна оптимізація систем булевих функцій, що забезпечує пошук

спільних імплікант. Завершується конвеєр синтезу технологічним відображенням (Technology Mapping) знайдених мінімізованих рівнянь (МДНФ) у заданий цільовий логічний базис реалізації (наприклад, суто І-НЕ або АБО-НЕ) [5].

Створення веб-додатка на основі запропонованої структурно-функціональної організації та комплексу алгоритмів дасть змогу не просто автоматизувати повний цикл проєктування цифрових пристроїв. Головною перевагою рішення є реалізація педагогічної концепції «прозорого ящика» (glass-box design). Розроблена система інтерактивно візуалізує кожен проміжний етап перетворення абстрактної математики у кремнієву структуру. Вона дозволяє студентів детально відстежити увесь ланцюг трансляції: від того, як конкретний символ регулярного виразу породжує абстрактний стан, далі кодується у двійковий вектор і, зрештою, матеріалізується у фізичний логічний венти́ль та тригер.

Крім того, запропонована організація системи повноцінно підтримує гнучке дослідження багатозначної логіки та застосування різних алгоритмів мінімізації. Це виводить її за рамки простого навчального тренажера і робить повноцінним науково-дослідним інструментом, який є легкодоступним безпосередньо у веб-браузері без необхідності розгортання та ліцензування «важкого» індустріального програмного забезпечення.

Список використаних джерел

1. Баркалов О. О., Бабаков Р. М. Прикладна теорія цифрових автоматів в сучасній українській науці. Матеріали наукових конференцій.- 2021. - С. 318–320.
2. Тарасов О. В. Системи автоматизованого проєктування мікроелектронної апаратури: навчальний посібник. Харків: ХНУРЕ, 2019. - 215с.
3. Burch C. Logisim: a graphical system for logic circuit design and simulation. Journal of Educational Resources in Computing (JERIC). 2002. - Vol. 2, No. 1. - P. 5–16.
4. Нікольський Ю. В., Пасічник В. А., Щербина Ю. М. Дискретна математика: підручник. Львів : Магнолія плюс, 2006. - 608 с.
5. Редько І. В., Лисенко О. М. Функціонально-логічне проєктування. Київ : КПІ ім. Ігоря Сікорського, 2023. - 152 с.

МОДЕЛЮВАННЯ ПОВЕДІНКИ КОРИСТУВАЧІВ У ВЕБСИСТЕМАХ МАЛОГО БІЗНЕСУ НА ОСНОВІ АНАЛІЗУ КЛІКСТРІМУ

У сучасному цифровому середовищі вебсайти є одним з основних засобів комунікації між малим бізнесом і його клієнтами. Малий бізнес часто стикається з обмеженими ресурсами та високим когнітивним навантаженням на осіб, що приймають рішення. Через ці фактори виникає потреба у створенні моделей взаємодії, які допомагають максимально спростити шлях користувача до цільової дії. Серед підходів, які дозволяють до певної міри вирішити це питання, варто виокремити застосування методів інтелектуального аналізу даних для виявлення закономірностей у поведінці користувачів, що дозволяє підвищити конверсію й конкурентоспроможність підприємства без значних витрат на маркетингові дослідження [1, 2].

Основою для аналізу взаємодії користувачів є клікстрім (clickstream) - послідовність сторінок, які відвідує конкретний користувач під час навігації вебсайтом. Процес моделювання починається з обробки «логів» сервера, де окремі запити об'єднуються у перегляди сторінок (pageviews), а ті, у свою чергу, групуються у сесії, що відображають дії користувача під час одного візиту. Для детальнішого аналізу виділяються епізоди - частини сесії, які семантично або функціонально пов'язані. Важливим параметром є час перебування на сторінці, що дозволяє оцінити зацікавленість користувача та відокремити змістовні сторінки від навігаційних [3].

Щоб формалізувати поведінку користувачів, застосовуються методи Data Mining. Зокрема, алгоритм кластеризації k-Means дозволяє групувати користувачів із подібними інтересами без попередньої сегментації, що допомагає виділити типові групи користувачів. На основі аналізу клікстріму формується інформаційний портрет користувача (ІПК) - вектор ознак, що відображає активність, вподобання та історію взаємодії. Модель передбачає створення ІПК при першому візиті та його динамічне оновлення під час наступних відвідувань, що дозволяє системі адаптуватися до змінних інтересів користувача в реальному часі [2, 4].

Для більш точного опису процесів взаємодії використовується графове моделювання. Взаємодія користувача представлена у вигляді

зваженого графа $G=\langle V,W,T,\delta \rangle$ де вузли V відповідають URL-адресам сторінок, а ребра W - ймовірним переходам між ними. Використання ланцюгів Маркова, з безперервним або дискретним часом, дозволяє моделювати «випадковий вебсерфінг». Динаміка переходів описується стохастичною матрицею P , елементи якої можуть визначатися як $p_{ij}=1/N_u$, де N_u - кількість вихідних посилань, або коригуватися залежно від часу перебування на сторінці. Розрахунок стаціонарного розподілу ймовірностей дозволяє визначити важливість окремих розділів сайту для користувачів. Для врахування раптових виходів або переходів на довільні сторінки вводиться коефіцієнт загасання (damping factor) d , що робить розподіл більш стійким і реалістичним. Такий підхід дозволяє виділити типові сценарії поведінки та оптимізувати структуру вебсистеми для зниження когнітивного навантаження.

Застосування цих методів дозволяє автоматизувати персоналізацію контенту завдяки інтелектуальним агентам, які на основі ІПК підлаштовують інтерфейс під потреби конкретної категорії користувачів. Виявлення «вузьких місць» у графі переходів дає змогу вчасно адаптувати функціонал і підвищити інтерактивність вебсистеми. Отримані результати слугують основою для формування вимог до адаптивних вебсистем, що суттєво покращує користувацький досвід у малому бізнесі [4, 5]. Перспективи подальших досліджень полягають у розширенні моделі для врахування більшої кількості факторів поведінки користувачів, інтеграції рекомендаційних систем та впровадженні методів прогнозування інтересів, що дозволить під час виконання курсової або наступної бакалаврської роботи створити більш гнучкі та інтелектуальні вебсистеми.

Список використаних джерел:

1. Markov Z., Larose D. T. Data Mining the Web: Uncovering Patterns in Web Content, Structure, and Usage. John Wiley & Sons, 2007.
2. Максимов М. С. Поведінкові моделі прийняття рішень в малому та середньому бізнесі. Дис. PhD. Харків: ХНУ імені В. Н. Каразіна, 2025.
3. Аксак Н. Г. Методи та моделі розподіленої інтелектуальної обробки великих даних. Дис. д-ра техн. наук. Харків: ХНУРЕ, 2019.
4. Саяпіна М. С. Інтелектуальна система аналізу поведінки користувачів на комерційних платформах. Магістерська робота. Київ: НУБіП, 2025.
5. Царик В. Методи аналізу інтерфейсів веб-застосунків для підвищення інтерактивності. *Системні технології*, 2025, № 2 (157). С. 146 – 153.

УДК 004.8

Лавренчук С.О., магістрант

Льовкін В.М., к.т.н. доцент

Національний університет «Запорізька політехніка»

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ ДИЗАЙНЕРІВ-МОДЕЛЬЄРІВ

Навчання дизайнерів-модельєрів є особливим напрямком сфери освіти, оскільки окрім безпосереднього розвитку індивідуальних вмінь передбачає також створення певного портфоліо робіт та взаємодію з майстрами, які діляться власним досвідом. Для забезпечення якісного навчання необхідна пряма взаємодія з майстрами з врахування наявного рівня вмінь особи, яка навчається на дизайнера-модельєра або підвищує свої вміння у певний момент.

Оскільки взаємодія між дизайнерами-модельєрами та майстрами передбачає використання дорогоцінного часу майстрів, необхідно відокремити тих осіб, яким така взаємодія принесе найбільшу користь. Саме це і має враховувати програмне забезпечення, яке повинно забезпечувати таке навчання. При цьому для забезпечення виконання цієї вимоги необхідно забезпечити створення математичної моделі, здатної виконувати прогнозування впливу результатів навчання на вміння дизайнера-модельєра.

Тому в даній роботі було розроблено програмне забезпечення навчання дизайнерів-модельєрів, яке реалізує можливості як для майстрів, так і для дизайнерів-модельєрів, створивши в підсумку вебзастосунок на основі фреймворку Django мовою Python. Програма дозволяє майстрам надавати для навчання власні курси, наповнювати їх матеріалами, в тому числі призначеними персонально для певних дизайнерів-модельєрів, керувати заявками на навчання. Стосовно поданих заявок майстер може отримати інформацію про виконаний прогноз впливу результатів навчання на вміння того дизайнера-модельєра, який подав заявку.

Для того щоб працювати з особами, які навчаються, необхідне врахування індивідуальних особливостей. Для цього у програмі передбачено не тільки створення резюме через надання інформації про себе, про дизайнерські вміння, про сильні сторони, про досвід роботи, але і створення технічних пакетів, де дизайн одягу безпосередньо презентується та конкретизується стосовно особливостей виготовлення. Такі технічні пакети можуть об'єднуватися в колекції, а майстри можуть виконувати пошук за ними, обирати тих, на кого варто підписатися для подальшого детальнішого аналізу, зберігати обрані

роботи, а тоді висувати власні пропозиції про навчання. Відповідно окрім того майстер може знайомитись так з роботами тих осіб, які ще не проходять курс, але подали заявку на навчання. Це сприяє можливості реалізації індивідуального підходу.

Для забезпечення прогнозування впливу результатів навчання на вміння дизайнера-модельєра було створено математичну модель, навчання якої виконувалось на основі вибірки даних [1]. Створення самої моделі було забезпечено через використання ансамблю дерев рішень на основі методу Random Forest. Для реалізації моделі програмно було використано засоби пакету scikit-learn [2]. Використання даної моделі призвело до отримання середньої абсолютної похибки на рівні 0,00235198 за використання нормалізованих значень під час прогнозування на тестовій вибірці, до якої відносилось 30 % вибірки даних [1] шляхом випадкового вибору екземплярів.

Функцію контролю за взаємодією між майстрами та особами, які навчаються на дизайнерів-модельєрів, керування створеною моделлю надано адміністратору, який має свій окремий інтерфейс для цього. За рахунок цієї можливості інтегровано до функціональних можливостей модель на основі даних, наявних у базі даних програми. Відповідно адміністратор може ініціювати вивантаження даних, створення відповідної навчальної вибірки. У підсумку для кожної ролі користувачів було розроблено свої вебсторінки, які сукупно формують відповідний інтерфейс для роботи, надаючи кожному набір відповідних функціональних можливостей.

Об'єднання у складі функціональних можливостей програми не тільки стандартних засобів навчання, але і тих, які враховують індивідуальні особливості осіб, які навчаються, пропонування індивідуальних матеріалів та оцінювання заявок на основі прогнозування того, як відіб'ється навчання за курсом на вміннях особи, яка навчається, повинно комплексно сприяти підвищенню ефективності навчання у цій сфері освіти та більш результативному його перенесенню на електронну платформу.

Список використаних джерел:

1. Professional Talent in Fashion Design. URL: <https://www.kaggle.com/datasets/zara2099/professional-talent-in-fashion-design> (дата звернення: 25.03.2026).
2. Decision Trees – scikit-learn 1.8.0 documentation. URL: <https://scikit-learn.org/stable/modules/tree.html> (дата звернення: 25.03.2026).

УДК 004.4

УДК 004.4

*Тушак В.С., здобувач,
Чижмотря О.В., ст. викладач*

Державний університет «Житомирська політехніка»

ІНФОРМАЦІЙНА ФРАГМЕНТАЦІЯ У ДІЯЛЬНОСТІ CFD-ТРЕЙДЕРА ТА ЗАСОБИ ЇЇ ПОДОЛАННЯ

CFD-трейдинг [1] як вид фінансової діяльності здобув велику популярність протягом останнього десятиліття серед приватних учасників фінансових ринків. Разом зі зростанням кількості можливостей та учасників з'являється проблема організації їхнього процесу в залежності від рівня та потреб. Здебільшого у своїй щоденній діяльності трейдер стикається з кількома категоріями даних. Аналіз перед торговою сесією та після неї формує значну кількість інформації про якість планування рішень та їх ефективність. Фіксація угод відображає ефективність реалізації запланованого та дозволяє оцінити якість виконання плану та стратегії. Нотатки та помилки дають розуміння того, які аспекти роботи потребують вдосконалення. І статистика, що є ключовим інструментом самооцінки трейдера, оскільки саме вона дозволяє виявити сильні та слабкі сторони і цілеспрямовано працювати над ними. При цьому ринок рішень здебільшого пропонує фрагментовані рішення, кожне з яких закриває лише окрему частину зазначених потреб.

У ширшому контексті описана проблема може розглядатися як прояв загального явища інформаційного перевантаження та фрагментації знань, характерного для сучасної цифрової діяльності. У книзі “Запасний мозок” Тіаго Форте [2] вказано, що зростання обсягів інформації та використання великої кількості інструментів призводить до втрати цілісності знань і ускладнює їх практичне застосування. У випадку CFD-трейдингу ця проблема проявляється у розподілі критично важливих даних між різними середовищами.

Під інформаційною фрагментацією у контексті трейдингової діяльності розуміється стан робочого середовища, за якого дані, необхідні для прийняття обґрунтованих торгових рішень, розподілені між кількома непов'язаними між собою інструментами та платформами. Це унеможлиблює комплексний аналіз торгової діяльності та накопичення досвіду у структурованому вигляді.

Найпоширеніші підходи до організації робочого процесу трейдера виділяються три основні категорії інструментів. Торгові журнали – як табличні, так і спеціалізовані (TraderSync), що дозволяють фіксувати параметри угод, проте обмежені у можливостях управління знаннями та аналізу контексту прийнятих рішень [3]. Універсальні системи

управління інформацією (Notion), надають широкі можливості для організації даних, але потребують значних затрат часу на налаштування під потрібну специфіку. Торгові платформи (MetaTrader) зосереджені виключно на виконанні ринкових операцій і не передбачають збереження думок, нотаток чи систематизації помилок. У результаті трейдер вимушений паралельно працювати у кількох різних середовищах, між якими відсутній будь-який інформаційний зв'язок.

В свою чергу ця проблема має безпосередній вплив на успішність трейдера. Регулярна зміна середовищ може мати негативний результат у критичні моменти торгової сесії, коли потрібно бути в максимальній концентрації, а потрібні інструменти мають бути поруч. Відсутність єдиного середовища унеможливорює виявлення зв'язків між емоційним станом трейдера, характером прийнятих рішень та кінцевим фінансовим результатом.

Дана проблема інформаційної фрагментованості і стала причиною розробки спеціалізованої веб-платформи «FIX Space», яка об'єднує ключові аспекти діяльності трейдера в єдиному робочому просторі. Платформа включає попередньо структуровані бази даних: Trading Journal для фіксації угод, Routine для організації щоденної роботи, Notes для ведення нотаток, Mistakes для систематизації помилок, Statistics для відстеження ключових показників, Trading System для опису торгових стратегій, Accounts для управління торговими рахунками та Operations для обліку фінансових операцій. На відміну від універсальних систем, «FIX Space» не вимагає від користувача проєктування структури даних з нуля – усе необхідне середовище вже сформоване і адаптоване під специфіку CFD-трейдингу. За необхідності, користувач з легкістю може розширити свій робочий простір, йому не потрібно буде докладати для цього великої кількості розумового ресурсу та часу.

Таким чином, інформаційна фрагментація є системною проблемою у практичній діяльності CFD-трейдера, яка безпосередньо впливає на ефективність роботи та якість прийнятих рішень. Централізація даних у межах єдиної спеціалізованої платформи дозволяє усунути ключові наслідки фрагментації та створити умови для системного накопичення досвіду і підвищення результатів.

Список використаних джерел:

1. Contract for Differences (CFD). Investopedia. URL: <https://www.investopedia.com/terms/c/contractfordifferences.asp>.
2. Форте Т. Запасний мозок. Як організувати цифрове життя і розвантажити голову / пер. з англ. А. Дудченко. Київ: Наш Формат. 2024. 272 с.
3. TraderSync. URL: <https://tradersync.com>.

УДК 004.4

*Тушак В.С., здобувач,
Чижмоторя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

ПОВЕДІНКОВІ ПОМИЛКИ ТА РІЛЬ СТАТИСТИЧНОГО АНАЛІЗУ У ПРИЙНЯТТІ ТОРГОВИХ РІШЕНЬ

Приватний трейдер значно менше захищений від впливу когнітивних упереджень [1]: він не має колективного контролю, емоції сильніше впливають та є прямий зв'язок між прийнятими рішеннями і власним капіталом. Все це робить його особливо вразливим до систематичних помилок мислення. При цьому більшість приватних трейдерів не ведуть детальної статистики своєї діяльності, через що неможливо вивити повторювані поведінкові патерни для подальшої роботи з ними.

У контексті CFD-трейдингу [2] найбільш поширеними є три типи поведінкових помилок. Надмірна самовпевненість (overconfidence) проявляється в переоцінці ймовірності успішного результату, особливо в разі проведення угоди після серії профітних угод, що збільшує обсяги позицій більше, ніж це доцільно в рамках торгової системи. Уникнення збитків (loss aversion) - ефект, що полягає у небажанні зафіксувати збиткову угоду у надії на зміну напрямку ціни, що систематично збільшує суму реалізованих збитків. Так зване revenge trading – імпульсивне відкриття нових позицій після серії невдалих угод із метою відіграти втрати.

Подолання зазначених упереджень стає можливим лише за умови систематичного відстеження об'єктивних показників торговельної діяльності. Базовим показником є відсоток прибуткових угод (winrate):

$$W = (N_{win} / N_{total}) \times 100\%,$$

де N_{win} – кількість прибуткових угод, N_{total} – загальна кількість угод за певний період.

Однак сам по собі winrate не визначає якість торгівлі без урахування середнього прибутку або збитку. Для цього використовується показник математичного очікування угоди (trade expectancy):

$$E = W \times \bar{R}_{win} - (1 - W) \times \bar{R}_{loss},$$

де $\bar{R}_{win}$ та $\bar{R}_{loss}$ – середній прибуток та середній збиток відповідно. Від'ємне значення E при прийнятному winrate є хорошим індикатором дії loss aversion.

Крім того, використовується коефіцієнт прибутковості (profit factor):

$$PF = \Sigma R_{win} / \Sigma R_{loss},$$

де значення $PF < 1$ вказує на збиткову стратегію незалежно від інших показників.

Для оцінки того, наскільки добре дотримуються правила управління капіталом, обчислюється співвідношення ризик/прибуток (R ratio):

$$RR = (TP - Entry) / (Entry - SL),$$

де TP – рівень тейк-профіту, SL – рівень стоп-лосу, а $Entry$ – рівень відкриття угоди. Систематичне відхилення RR від цільового значення свідчить про вплив емоційних факторів під час управління позицією.

Порівняння наведених вище показників дозволяє виявити поведінкові відхилення, які важко помітити без структурованого аналізу. Різне падіння winrate разом зі зростанням середнього збитку після серії збиткових угод є типовою ознакою «ревендж-трейдингу» (revenge trading). Негативне математичне очікування при winrate понад 50% однозначно свідчить про те, що збиткові угоди утримуються занадто довго у збитковому стані понад допустимі межі. Відхилення фактичного співвідношення ризик/прибуток (R-ratio) від запланованого більш ніж на 20-30% вказує на порушення торгової системи під впливом емоційного стану трейдера.

Для автоматизованого розрахунку описаних метрик та виявлення повторюваних поведінкових патернів розроблено веб-платформу «FIX Space». Платформа забезпечує централізовану фіксацію параметрів кожної угоди, автоматичний розрахунок торгової статистики та ведення окремої бази даних обліку помилок (Mistakes), у якому трейдер фіксує суб'єктивну причину відхилення від стратегії. Сукупність цих даних формує основу для переходу до аналітично обґрунтованого прийняття торгових рішень, а не емоційних дій.

На жаль, систематичні поведінкові помилки й надалі становлять більшу частину втрат приватних CFD-трейдерів, а їх виявлення неможливе без регулярного статистичного аналізу торгової діяльності. Набір метрик winrate, expectancy, profit factor і R-ratio дозволяє об'єктивно оцінити власну торгівлю та виявити відхилення, спричинені когнітивними упередженнями. Відповідно, використання такого підходу в системі «FIX Space» дозволить користувачам підвищити об'єктивність оцінки торгової діяльності та зменшити вплив суб'єктивних рішень.

Список використаних джерел:

1. Канеман Д. Мислення швидко й повільно / пер. з англ. М. Яковлев. Київ: Наш Формат. 2017. 480 с.
2. Contract for Differences (CFD). URL: <https://www.investopedia.com/terms/c/contractfordifferences.asp>.

УДК 004.7

*Дрозжак В.Т., здобувач,
Концидайло А.М., ст. викладач
Державний університет «Житомирська політехніка»*

ОСОБЛИВОСТІ ТЕСТУВАННЯ ВЕБПЛАТФОРМИ ДЛЯ ПОШУКУ РОБОТИ АБО СТАЖУВАННЯ

Тестування вебплатформи для пошуку роботи або стажування має свої особливості. Така система відрізняється від інших тим, що нею користуються різні типи людей: пошукачі роботи, студенти та роботодавці. Кожен із них виконує свої дії, тому потрібно перевірити багато різних сценаріїв. Крім того, платформа працює з особистими даними, тому важливо забезпечити безпеку та стабільну роботу навіть при великій кількості користувачів.

Основна мета тестування - знайти помилки, перевірити, чи правильно працюють усі функції, і зрозуміти, чи готова система до використання. Важливо переконатися, що користувач може без проблем виконувати основні дії, а система стабільно працює в різних умовах. Оскільки платформа призначена для великої кількості людей, її потрібно тестувати комплексно.

Спочатку проводиться функціональне тестування. Перевіряється, чи працюють основні можливості: реєстрація та вхід у систему, створення профілю, розміщення вакансій і стажувань, пошук роботи, фільтри та подання заявок. Також важливо перевірити, чи правильно обробляються дані і чи коректно працюють форми.

Далі перевіряється інтерфейс користувача. Платформа повинна бути зручною і зрозумілою. Важливо, щоб вона добре виглядала на різних пристроях (телефон, планшет, комп'ютер) і працювала у різних браузерах. Також перевіряється, наскільки легко користувачу знайти потрібні функції.

Окремо проводиться тестування безпеки. Оскільки система працює з особистими даними, потрібно перевірити захист від зломів і атак. Наприклад, чи добре захищені паролі, чи правильно працюють права доступу, і чи неможливо отримати чужі дані.

Також важливе тестування продуктивності. Воно показує, як швидко працює система і чи витримує вона велику кількість

користувачів одночасно. Це особливо важливо для таких платформ, де багато людей одночасно шукають роботу або подають заявки.

Проводиться і інтеграційне тестування - перевіряється, як взаємодіють між собою різні частини системи (наприклад, сайт і база даних). Крім того, виконується регресійне тестування, щоб переконатися, що після змін нічого не зламалося.

Також слід приділити увагу тестуванню доступності. Платформа має бути зручною для всіх користувачів, у тому числі для людей з обмеженими можливостями. Перевіряється, чи підтримуються допоміжні технології, чи достатній контраст тексту, чи зручно користуватися сайтом без миші.

Не менш важливим є тестування сповіщень і комунікацій. Потрібно перевірити, чи правильно працюють електронні листи, повідомлення про нові вакансії, відповіді роботодавців або зміни статусу заявки.

Крім цього, варто проводити тестування локалізації, якщо платформа підтримує кілька мов. Необхідно перевірити правильність перекладу, форматування дат, часу та інших регіональних особливостей.

Таким чином, тестування вебплатформи для пошуку роботи або стажування є багатогранним процесом.

Список використаних джерел:

1. Pressman R. S. Software engineering: a practitioner's approach. 8th ed. New York : McGraw-Hill, 2014. 970 p.
2. Sommerville I. Software engineering. 10th ed. Boston : Pearson, 2016. 816 p.
3. Myers G. J., Sandler C., Badgett T. The art of software testing. 3rd ed. Hoboken : Wiley, 2011. 256 p.
4. Гавриленко В. В. Тестування програмного забезпечення. Київ : Ліра-К, 2019. 256 с.
5. ДСТУ ISO/IEC 25010:2016. Інженерія систем і програмного забезпечення. Вимоги та оцінювання якості систем і програмного забезпечення (SQuaRE). Київ : ДП «УкрНДНЦ», 2016.

УДК 004.4

*Лаєтін Д.А., здобувач,
Чижмоторя О.Г., ст. викладач*

Державний університет «Житомирська політехніка»

УТИЛІТАРНІ КЛАСИ BOOTSTRAP VS СЕМАНТИЧНИЙ CSS: ВПЛИВ НА ШВИДКІСТЬ РОЗРОБКИ ТА ПІДТРИМКУ ПРОЄКТУ

Сучасна веб-розробка дедалі частіше постає перед вибором між утилітарними CSS-класами, як у фреймворках Bootstrap чи Tailwind, та семантичним підходом до стилізації. Обидва методи мають переваги та недоліки, що безпосередньо впливають на швидкість створення інтерфейсів, зручність командної роботи та подальшу підтримку проєкту.

Утилітарні CSS класи – це короткі стилістичні класи, які безпосередньо відображають вигляд елемента: text-center, mt-4, bg-dark тощо. Основна ідея – стилізувати елемент без створення окремих CSS-правил, використовуючи вже готові класи. Це значно пришвидшує розробку, особливо на ранніх етапах, коли важливо швидко отримати результат. Tailwind CSS пішов ще далі: він фактично перетворив CSS на конструктор, що дозволяє зібрати будь-який інтерфейс із мінімуму коду [1].

Семантичний CSS, навпаки, передбачає створення власних класів зі змістовними назвами на кшталт user-card, product-title, main-header. Такі назви описують логічну сутність елемента, а не його вигляд. Перевага цього підходу – розділення відповідальностей: HTML описує структуру і зміст, а CSS – зовнішній вигляд. Це відповідає класичним принципам хорошого кодування [2].

Однією з ключових переваг утилітарного підходу є економія часу. Розробнику не потрібно вгадувати назви класів, відкривати окремі файли стилів, писати CSS-правила. Крім того, використання утилітарних класів допомагає уникнути проблем із дублюванням стилів, адже всі правила вже стандартизовані. Такий підхід зменшує семантичність верстки: зчитуючи клас bg-secondary, важко зрозуміти, яку роль відіграє цей елемент у структурі сторінки.

Семантичний підхід забезпечує кращу читабельність і підтримуваність коду в довгостроковій перспективі. Завдяки власним класам із логічними назвами легше розуміти, що саме стилізується. При зміні дизайну достатньо оновити CSS-файл, не торкаючись HTML. Це особливо зручно у великих проєктах, де внесення змін до кожного HTML-файлу є проблематичним. Однак цей підхід вимагає початкового

планування: треба продумати ієрархію компонентів, правила іменування, уникати дублювання стилів [3].

З погляду масштабування, утилітарні класи мають перевагу. Їхня повторюваність дозволяє швидко збудувати інтерфейс, зберігаючи єдність стилю. Tailwind, наприклад, дозволяє створювати компоненти з уніфікованими кольорами, відступами, шрифтами, що зменшує кількість помилок. Але зміна глобального стилю вимагає редагування численних HTML-фрагментів. Натомість семантичні стилі дають змогу централізовано вносити зміни – змінивши одне правило в CSS, можна змінити вигляд десятків елементів [4].

Ще один аспект – командна робота. У проєктах із кількома розробниками утилітарні класи допомагають дотримуватись єдиного підходу без необхідності синхронізації назв класів. Новий учасник команди швидко орієнтується, адже всі користуються типовими утилітами. Однак надмірна свобода в їхньому використанні призводить до «засмічення» розмітки, якщо не встановити чітких правил. Семантичний CSS, навпаки, потребує більше зусиль на координацію, але у правильно організованій структурі код стає зрозумілішим, а компоненти – легше повторно використовуваними.

На практиці дедалі частіше застосовують змішаний підхід. Наприклад, утилітарні класи використовуються для дрібних налаштувань – відступів, кольорів, шрифтів – тоді як більш абстрактні сутності реалізуються семантичними класами (.card, .form-group). Це дозволяє досягти балансу між швидкістю розробки та чистотою коду [5].

Отже, вибір між утилітарним і семантичним підходом залежить від багатьох чинників: масштабності проєкту, вимог до команди, потреби у швидкій реалізації чи довготривалій підтримці. Фреймворки на кшталт Bootstrap варто розглядати як інструмент для швидкого старту, а семантичний CSS – як фундамент чистої, підтримуваної архітектури фронтенду.

Список використаних джерел:

1. Tailwind CSS Documentation. URL: <https://tailwindcss.com/docs>.
2. McFarland D. CSS: The Missing Manual. O'Reilly Media. 2020. 814 p.
3. Крок Г. С. Підходи до написання масштабованих CSS-архітектур // Вісник КНУ. Серія: Прикладна математика і інформатика. 2021. № 37. С. 82-88.
4. Marcotte E. Responsive Web Design. A Book Apart. 2021. 154 p.
5. Сайто М. Семантична верстка: принципи, переваги, недоліки // Frontend Today. 2022. № 5. С. 24-31.

УДК 004.4

*Демчук О.В., здобувачка,
Чижмоторя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

АДАПТИВНИЙ АЛГОРИТМ ТЕСТ-ПІДБОРУ ДОЗВІЛЛЯ

На сьогодні ми маємо велику кількість різних онлайн-сервісів, однак замість спрощення пошуку вони створюють надлишок варіантів, що ускладнює прийняття рішення [4]. Користувач, який хоче знайти нове дозвілля, стикається не з браком інформації, а з її надлишком і відсутністю персоналізованого орієнтиру. Аналогічні платформи, зокрема HobbyCue та Skillshare, здебільшого пропонують каталоги з ручною фільтрацією або рекомендації на основі популярності, не враховуючи індивідуального профілю користувача. Це зумовлює потребу в алгоритмі, який здатен зіставити вподобання користувача з характеристиками дозвілля, не маючи при цьому попередньої поведінкової історії. Через відсутність подібного підходу користувачам доводиться самостійно шукати дозвілля.

Головною проблемою класичних рекомендаційних методів постає стан, коли система не має достатньої інформації та взаємодії з користувачем для формування якісних рекомендацій [2]. Наслідком є зниження точності або неефективність через відсутність накопиченої бази вподобань. Такі ситуації є типовими для більшості платформ, які ще не встигли зібрати достатню кількість користувацьких даних. Для подолання цього обмеження застосовують гібридні підходи, оскільки вони поєднують фільтрацію на основі характеристик з профілем користувача, при цьому не потребують попередньої активності користувача на платформі [4]. Саме на цьому принципі побудований алгоритм, який реалізований у рамках розробки вебплатформи для пошуку та підбору дозвілля.

Алгоритм функціонує в двох режимах, між якими відбувається автоматичне переключення залежно від наповнення бази даних. На першому етапі система працює в режимі зваженого збігу тегів: кожне дозвілля у каталозі описується набором тегів, а кожна відповідь користувача асоціюється з певною підмножиною тегів [1]. Запитання тесту діляться на три групи за вагою: загальні мають вагу 1, середні – вагу 2 та конкретні – вагу 3. Фінальний бал дозвілля розраховується як сума ваг тегів, що збіглися з відповідями користувача, після чого нормалізується у відсотковий показник відповідності [1]. Такий підхід є ефективним та прозорим, при цьому не обов'язково мати попередню

базу даних користувачів. Тому цей тип алгоритму є основним на старті роботи платформи.

Як тільки назбирується база з необхідної кількості користувачів, що пройшли тест та підписалися на дозволя, алгоритм автоматично переходить у гібридний режим. Фінальний рейтинг розраховується за формулою:

$$FR = 0,6 \times WTM + 0,4 \times P [3],$$

де FR (Final rating) – фінальний рейтинг; WTM (Weighted tag match) – зважений збіг тегів; P (Popularity) – популярність. Значення змінної P (популярності) визначається часткою схожих користувачів, які мають збіги у наборах тегів з профілем поточного користувача, та обрали рекомендоване дозволя після проходження тесту. Завдяки такому розподілу алгоритм не відкидає індивідуальні переваги на користь популярного, а лише доповнює їх досвідом схожих користувачів [3].

Архітектура містить принцип адаптивних рекомендаційних систем, тобто алгоритм автоматично обирає оптимальну стратегію залежно від наявного обсягу даних без додаткового налаштування [3, 4]. Це усуває необхідність ручного переналаштування з боку розробника при будь-яких змінах у базі даних. Система ефективно функціонує від запуску з порожньою базою до масштабованого стану з тисячами користувачів. Розширити функціонал можна за рахунок додавання можливості враховувати зворотний зв'язок від користувачів, що дозволить алгоритму поступово покращувати точність рекомендацій на основі реальних реакцій, а не лише тегів.

Список використаних джерел:

1. Тарус Дж. К., Нью З., Мустафа Г. Рекомендації на основі знань: огляд онтологічних рекомендаційних систем для е-навчання. *Artificial Intelligence Review*. 2018. Т. 50. С. 21-48.
2. Джафрі С. І. Х. та ін. Гібридне вирішення проблеми холодного старту в рекомендаційних системах. *The Computer Journal*. 2024. № 5. С. 1637-1644.
3. Алджунід М. Ф. та ін. Огляд рекомендаційних систем на основі колаборативної фільтрації. *Neurocomputing*. 2024. Т. 617. DOI: 10.1016/j.neucom.2024.128718.
4. Боддулурі К. С. та ін. Дослідження ландшафту гібридних рекомендаційних систем в електронній комерції. *IEEE Access*. 2024. DOI: 10.1109/ACCESS.2024.3365828.

UDC 004.4

*Davydov Viktor, Master's Student,
Oleksii Chyzhmotria, Senior Lecturer
Zhytomyr Polytechnic State University*

PERSONALIZED MUSIC RECOMMENDATIONS BASED ON USER BEHAVIOR ANALYTICS

The exponential growth of digital music platforms has created a vast and diverse content library, making personalized discovery of music tracks increasingly important for user satisfaction and engagement. Users often face difficulties in finding relevant content, while creators struggle to promote their works efficiently. Intelligent recommendation systems provide a solution by predicting user preferences based on behavioural data [1].

Early recommendation methods, including popularity-based and simple rule-based filtering, often failed to account for complex user preferences, while collaborative and content-based approaches were limited by cold-start issues and sparse datasets [2].

This study investigates a hybrid recommendation framework for a digital music platform, integrating user behavioral analytics with machine learning techniques. The system collects interaction data, including play events, likes, playlist additions, and purchase history, to model user preferences. Various strategies are evaluated, such as user-based collaborative filtering, item-based similarity models, and hybrid approaches that combine behavioral signals with content metadata, including genre, tempo, and mood [3].

In addition, transformer-based language models and large language models (LLMs) are employed to analyze textual metadata and automatically enrich music tags, enhancing the quality and relevance of recommendations [4]. This feature enables better understanding of content semantics and allows the system to recommend tracks even for newly uploaded music with limited user interactions.

Additionally, the proposed framework emphasizes the commercialization aspect of digital music platforms by integrating seamless mechanisms for music sales and monetization. By analyzing user preferences and engagement patterns, the system not only recommends relevant tracks but also identifies high-potential content for promotion and targeted marketing. This approach supports independent creators in reaching their audience more effectively while maximizing platform revenue. The integration of recommendation algorithms with transactional features, such as direct purchase links and subscription-based access, creates a unified ecosystem where user satisfaction, content discoverability, and economic incentives are aligned. This commercial perspective complements the

technical improvements in hybrid recommendation strategies, ensuring practical applicability in real-world digital music marketplaces

Experimental evaluation uses offline metrics, including Precision@K, Recall@K, and F1-score, alongside online business-oriented indicators, such as click-through rate and conversion to purchase [5]. Results indicate that hybrid models outperform baseline popularity-based approaches, achieving improvements of up to 15-25% across key metrics. LLM-assisted feature extraction further improves recommendation relevance, particularly for new or less-interacted content. These results demonstrate the practical applicability of combining behavioral and semantic data in real-world digital music platforms.

The proposed framework contributes to the development of adaptive digital music platforms by improving user engagement, satisfaction, and content monetization. These findings provide a foundation for further research in personalized content delivery, AI-driven creative tools, and large-scale recommendation systems. Future research directions include the integration of real-time learning mechanisms, reinforcement learning for dynamic recommendation optimization, and multimodal analysis combining audio signals with behavioral and textual data. The integration of user feedback loops can also enhance model accuracy over time and support personalized experiences at scale.

References:

1. Ricci F., Rokach L., Shapira B. Recommender Systems Handbook. 2nd ed. Springer. 2015. Pp. 1-1000. DOI: <https://link.springer.com/book/10.1007/978-1-4899-7637-6>.
2. Aggarwal C.C. Recommender Systems: The Textbook. Springer. 2016. Pp. 1-400. URL: <https://link.springer.com/book/10.1007/978-3-319-29659-3>.
3. He X., Liao L., Zhang H., Nie L., Hu X., Chua T.-S. Neural Collaborative Filtering // Proc. 26th Int. Conf. on World Wide Web (WWW '17). 2017. Pp. 173-182. URL: <https://dl.acm.org/doi/10.1145/3038912.3052569>.
4. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. NAACL-HLT. 2019. Pp. 4171-4186. URL: <https://arxiv.org/abs/1810.04805>.
5. Zhang L., et al. Enhancing music recommendation systems with hybrid ML models and LLM-assisted feature extraction. Journal of AI in Music Technology. 2025. Pp. 12-28. URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0334120>.

УДК 004.4

*Царук К.А., здобувачка,
Чижморя О.В., ст. викладач*

Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВЕБПЛАТФОРМИ ДЛЯ ОРГАНІЗАЦІЇ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ

Перехід волонтерської діяльності в цифрове середовище супроводжується широким використанням вебплатформ, які забезпечують координацію допомоги, взаємодію учасників та обробку інформації. У таких системах акумулюються персональні дані користувачів, інформація про заходи та результати діяльності, що підвищує вимоги до їх захисту.

Особливістю волонтерських платформ є робота з чутливими даними, зокрема контактною інформацією, відомостями про місцезнаходження та запитами на допомогу. Порушення безпеки в цьому випадку може спричинити не лише витік даних, а й негативно вплинути на організацію самої діяльності. З огляду на вимоги законодавства щодо захисту персональних даних [1], такі системи повинні відповідати встановленим нормам безпеки.

Дослідження сучасних вебзастосунків свідчить, що одними з найбільш поширених проблем залишаються недостатній рівень контролю доступу до облікових записів, вразливості при взаємодії з базами даних та відсутність належного захисту від типових кіберзагроз. Серед них особливу небезпеку становлять SQL-ін'єкції, що дають змогу отримати несанкціонований доступ до даних, а також XSS-атаки, спрямовані на виконання шкідливого коду в браузері користувача [2].

У процесі розробки вебплатформи передбачено застосування комплексу технічних засобів захисту. Зокрема, передача даних здійснюється із використанням протоколу HTTPS, що забезпечує їх шифрування. Паролі користувачів зберігаються у вигляді хешів із застосуванням сучасних алгоритмів, що унеможливорює їх відновлення у відкритому вигляді навіть у разі доступу до бази даних.

Крім того, реалізовано механізми автентифікації та розподілу прав доступу залежно від ролі користувача. Це дозволяє обмежити доступ до функцій системи та запобігти виконанню несанкціонованих дій. Для підвищення рівня захисту також передбачено обмеження кількості спроб входу, що зменшує ефективність атак перебором.

Перевірка введених користувачем даних є ще одним важливим елементом безпеки. Валідація здійснюється як на клієнтській, так і на

серверній стороні, що знижує ризик виконання шкідливого коду та забезпечує захист від XSS-атак і різних типів ін'єкцій.

У системі реалізовано ведення журналу подій, який фіксує ключові дії користувачів. Це дає змогу аналізувати активність, виявляти підозрілі операції та своєчасно реагувати на можливі загрози.

Додатковим рівнем захисту є використання багатофакторної автентифікації, яка передбачає підтвердження особи користувача за допомогою додаткових засобів. Незважаючи на певне ускладнення процесу входу, такий підхід значно підвищує безпеку доступу до системи.

Важливим напрямом є також забезпечення захисту даних на рівні бази даних. Передбачено розмежування доступу не лише за ролями користувачів, а й за операціями, що виконуються над даними. Це дозволяє обмежити можливість їх перегляду або зміни лише уповноваженими особами.

Крім того, передбачено резервне копіювання даних, що дає змогу відновити інформацію у разі технічних збоїв або кібератак. Регулярне створення резервних копій забезпечує збереження даних і стабільність функціонування системи.

Контроль цілісності даних також має важливе значення. Використання відповідних перевірок у базі даних дозволяє запобігти появі помилкової або неповної інформації, що є критично важливим для волонтерських платформ.

Окрему увагу приділено застосуванню принципу мінімальних привілеїв, відповідно до якого кожен користувач отримує лише необхідний рівень доступу. Це дозволяє обмежити можливі наслідки компрометації облікового запису.

Отже, забезпечення інформаційної безпеки вебплатформи для організації волонтерської діяльності потребує комплексного підходу, який враховує як технічні, так і організаційні аспекти. Реалізація таких рішень дозволяє підвищити стійкість системи до сучасних загроз і забезпечити її стабільну роботу [3].

Список використаних джерел:

1. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.
2. Євсєєв С. П., Ткачов А. М., Алексієв В. О., Рябуха Ю. М. Кібербезпека: WEB-технології : навчально-довідковий посібник. – Львів: Новий Світ-2000, 2026. – 390 с.
3. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній. – Київ: Сідкон, 2022. – 372 с.

УДК 519.7::532.5+556:517.9

*Каиштан С.С., к.т.н., доцент**Національний університет водного господарства та природокористування*

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ КВАЗІІДЕАЛЬНИХ ТЕЧІЙ У СКЛАДНИХ ГІДРОСИСТЕМАХ НА ОСНОВІ ЧИСЛОВИХ МЕТОДІВ КОМПЛЕКСНОГО АНАЛІЗУ

Сучасний стан водних ресурсів планети вимагає розробки систем моніторингу та прогнозування гідрологічного режиму, що є критично важливим для екологічної безпеки та раціонального природокористування. Особливої ваги ці питання набувають при дослідженні течій у складних гідрологічних системах – напр., річках з притоками та водосховищах, де взаємодія поверхневих, ґрунтових і підземних вод формує специфічну кінематичну структуру потоку.

Теоретичне підґрунтя моделювання таких процесів (для нестисливої квазіідеальної рідини) базується на законі Дарсі $\vec{v} = \text{grad } \phi(x, y)$ та рівнянні потенціальних течій $\text{div } \vec{v} = 0$, що детально висвітлено у класичній праці [1]. Проте, математичний опис рухів у водоймах зі складною геометрією часто призводить до виникнення значних обчислювальних труднощів. Одним із найбільш ефективних способів вирішення цієї проблеми є застосування методів комплексного аналізу, зокрема апарату конформних відображень, який дозволяє трансформувати складні фізичні області, обмежені лініями течії та еквіпотенціальними лініями (див. рис. 1) у канонічні області, обмежені горизонтальними та вертикальними ділянками границі – області квазікомплексного потенціалу (див. рис. 2) [2, 3].

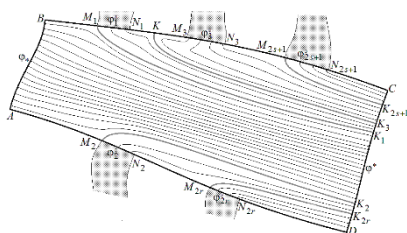


Рис. 1. Фізична область –
 водойма з притоками

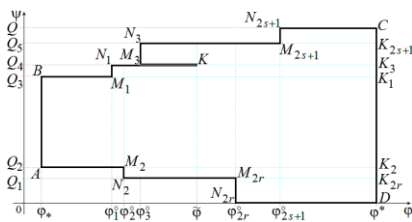


Рис. 2. Область квазі-
комплексного потенціалу

Незважаючи на значний досвід використання прямих методів конформних відображень, актуальною залишається задача переходу до

обернених крайових задач. Такий підхід дозволяє визначати параметри течії за заданими характеристиками потенціального поля, що є базою для керування водним об'єктом. На основі комбінації і модифікації методів квазиконформного відображення та поетапної фіксації характеристик середовища і процесу розроблено підхід до розв'язання відповідних крайових задач. Зокрема, у працях [2 – 4] запропоновано методи розв'язання задач на конформне відображення криволінійних чотирикутників, які є основою для побудови гідродинамічних сіток руху у реальних водних об'єктах.

Окремим аспектом, що потребує поглибленого вивчення, є ідентифікація ліній розділу потоків як основного індикатора стану гідросистеми. Розуміння взаємодії між різними джерелами збурень у гідрологічних моделях є вирішальним для прогнозування перетоків [3, 4]. У цій роботі пропонується застосовувати числові методи комплексного аналізу до розв'язання відповідних задач, коли вплив поверхневих, ґрунтових і підземних вод на початковому етапі моделюється як ділянки (джерела) поперечних збурень базового стоку. Це дозволяє не лише розраховувати поле швидкостей, а й моделювати структуру течії; знаходити функцію течії та комплексний потенціал; розраховувати витрати, перетоки, детально аналізувати зони впливу різних гідродинамічних факторів через положення ліній розділу течії, що відкриває нові можливості для створення систем підтримки прийняття рішень у водному господарстві.

Список використаних джерел:

1. Darcy H. Les fontains publiques de la ville de Dijon. Paris: Victor Dalmont, 1856. 647 p.
2. Бомба А.Я., Каштан С.С., Пригорницький Д.О., Ярошак С.В. Методи комплексного аналізу. Рівне: НУВГП, 2013. 415 с. URL: <http://ep3.nuwm.edu.ua/2803>
3. Бомба А.Я., Каштан С.С. Методи комплексного аналізу прогнозування керованих рухів поверхневих та фільтраційних вод. Кібернетика та системний аналіз. 2025. Т.61, №5. С. 39-54. URL: <https://doi.org/10.34229/KCA2522-9664.25.5.4>
4. Бомба А.Я., Каштан С.С. Математичне моделювання та прогнозування керованих рухів поверхневих та підземних вод. Моделювання, керування та інформаційні технології (МСІТ-2025): матеріали VIII Міжнародної науково-практичної конференції (6-8 листопада 2025 р., м.Рівне). Рівне: НУВГП, 2025. С. 295-298. URL: <https://doi.org/10.31713/MCIT.2025.092>

УДК 004.7

*Васянович О.А., здобувач,
Морозов А.В., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АВТОМАТИЗОВАНА ГЕНЕРАЦІЯ МОСК-ДАНИХ У РОЗРОБЦІ СТРІМІНГОВИХ СЕРВІСІВ

Розробка та навантажувальне тестування сучасних стрімінгових сервісів вимагає наявності великих масивів медіаданих [1]. Для перевірки роботи кешування, швидкості віддачі контенту та коректності роботи баз даних під навантаженням необхідні тисячі унікальних аудіофайлів з валідними метаданими. Використання захищених авторським правом композицій створює юридичні ризики, а відкриті бібліотеки не забезпечують достатньої варіативності та стандартизації тегів для тестування систем рекомендацій.

Практичне вирішення цієї проблеми реалізовано під час розробки інформаційної системи організації прослуховування аудіоконтенту (проект «IndieStream»). Ефективним інженерним підходом для автоматизованого наповнення тестового середовища (mock-даних) обрано використання відкритої генеративної нейромережі Meta MusicGen [2]. На відміну від комерційних веб-сервісів, ця модель дозволяє розгорнути процес локально та керувати генерацією програмно, без ліцензійних обмежень для етапу розробки.

```
30 prompts = [  
31     ("Neon Runner", "Cyber Drive", "fast tempo synthwave, 80s retro, driving bass", "track_1.wav"),  
32     ("The Void", "Silent City", "dark post-punk, heavy bass, 120 bpm, melancholic", "track_2.wav"),  
33     ("Midnight Study", "Late Night", "lo-fi hip hop, chill, study beat, no vocal", "track_3.wav"),  
34     ("Luna Waves", "Ocean Drive", "indie rock instrumental, upbeat, garage sound", "track_4.wav"),  
35     ("Echoes", "Deep Space", "ambient electronic, cinematic, deep space", "track_5.wav")  
36 ]  
37  
38 print("Початок автоматизованої генерації аудіоданих та метаданих...")  
39  
40 # 4. Процес автоматизації  
41 for i, genre_prompt in enumerate(prompts):  
42     print(f"Генерація треку {i+1}/{len(prompts)}: {genre_prompt}")  
43  
44     # Генерація аудіо  
45     wav = model.generate([genre_prompt])  
46  
47 Run mock_parser x  
48  
49 :  
50 Ініціалізація бази даних SQLite...  
51 Завантаження моделі Meta MusicGen...  
52 Початок автоматизованої генерації аудіоданих та метаданих...  
53  
54 [1/5] Генерація аудіо. Промпт: 'fast tempo synthwave, 80s retro, driving bass'  
55     Збережено файл: ./media/track_1.wav  
56     Додано запис у БД: Neon Runner - Cyber Drive  
57  
58 [2/5] Генерація аудіо. Промпт: 'dark post-punk, heavy bass, 120 bpm, melancholic'
```

Рис. 1. Скрипт та процес генерації аудіоданих у терміналі.

Процес створення та інтеграції синтетичних даних у платформу IndieStream повністю автоматизовано. Розроблений Python-скрипт використовує бібліотеку Audiocraft для ініціалізації моделі MusicGen. Алгоритм формує масив вхідних параметрів (жанр, темп, настрої), які слугують текстовими запитами для нейромережі. Під час генерації аудіофайлу формату WAV скрипт паралельно створює для нього фіктивні текстові метадані (назву треку та ім'я неіснуючого виконавця) за допомогою бібліотеки Faker [3].

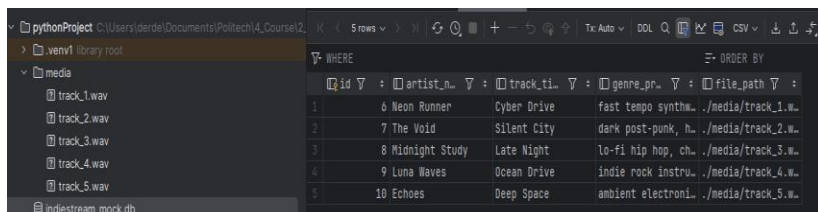


Рис. 2. Згенеровані аудіофайли та відповідні їм записи у реляційній базі даних.

Створені аудіофайли зберігаються у локальну директорію сховища, а скрипт автоматично формує SQL-запити для запису фізичних шляхів до файлів та їхніх згенерованих характеристик у реляційну базу даних проекту. Застосування відкритих моделей штучного інтелекту дозволяє вибудувати повністю керований процес створення синтетичних медіаданих. Такий підхід забезпечує розробника необхідним обсягом стандартизованих даних для стрес-тестування бекенду та налаштування рекомендаційних алгоритмів платформи, мінімізуючи витрати часу на пошук та підготовку тестової бази.

Список використаних джерел:

1. Соммервілл І. Інженерія програмного забезпечення : навч. посіб. пер. з англ. Київ : ВІЛЬЯМС, 2002. 680 с..
2. Офіційний репозиторій бібліотеки Audiocraft / Meta Research. GitHub, 2023. URL: <https://github.com/facebookresearch/audiocraft> (дата звернення: 22.03.2026).
3. Офіційна документація бібліотеки Faker для генерації тестових даних. Read the Docs. 2024. URL: <https://faker.readthedocs.io/> (дата звернення: 22.03.2026).

УДК 004.4

*Царук К.А., здобувачка,
Чижморя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

РОЗРОБКА ВЕБПЛАТФОРМИ ДЛЯ ОРГАНІЗАЦІЇ ВОЛОНТЕРСЬКОЇ ДІЯЛЬНОСТІ

Волонтерська діяльність в Україні, особливо в умовах воєнного стану, набуває все більшого значення для підтримки військових, цивільного населення та внутрішньо переміщених осіб. Збільшення кількості ініціатив ускладнює процеси координації, розподілу завдань та контролю їх виконання, що безпосередньо впливає на ефективність надання допомоги [1].

На практиці організація волонтерської діяльності часто здійснюється за допомогою соціальних мереж, месенджерів та електронних таблиць. Такий підхід дозволяє швидко налагодити взаємодію, проте не забезпечує цілісного управління інформацією. У результаті виникають проблеми дублювання даних, втрати важливої інформації та затримок у виконанні завдань, що підтверджує необхідність використання спеціалізованих інформаційних систем [2].

У межах дослідження запропоновано розробку вебплатформи, яка об'єднує основні процеси волонтерської діяльності в єдиному інформаційному середовищі. Основною метою є автоматизація управління подіями, покращення комунікації між учасниками та спрощення координації волонтерських ініціатив. Таке рішення дозволяє зосередити в одному середовищі дані про заходи, учасників, заявки, результати виконання та інші відомості, необхідні для організації роботи.

Для реалізації системи обрано клієнт-серверну архітектуру з використанням REST API для обміну даними між компонентами. Такий підхід дозволяє відокремити інтерфейс користувача від серверної логіки, забезпечити гнучкість у розширенні функціоналу та адаптацію системи до зростаючого навантаження. Крім того, така архітектура спрощує подальшу модернізацію системи, оскільки окремі компоненти можуть удосконалюватися без повної перебудови всього застосунку.

Система забезпечує централізоване зберігання даних, що дозволяє уникнути їх дублювання та забезпечити актуальність інформації для всіх користувачів. Доступ до даних надається відповідно до ролі користувача, що підвищує рівень організованості та керованості процесів. Наявність єдиної бази даних створює умови для більш

впорядкованого ведення обліку подій, учасників та результатів діяльності.

Додатково реалізовано механізм відстеження статусу виконання завдань. Кожна подія або запит проходить визначені етапи — від створення до завершення, що дозволяє контролювати хід виконання та своєчасно реагувати на можливі затримки. Це підвищує прозорість діяльності та покращує координацію між учасниками. У практичному аспекті такий підхід дає змогу швидко виявляти проблемні етапи та коригувати організаційні дії без втрати часу.

Окрему роль у роботі платформи відіграє комунікаційний модуль. Для ефективної взаємодії між учасниками важливо забезпечити можливість оперативного обміну повідомленнями, уточнення деталей подій та інформування про зміни. Інтеграція засобів комунікації безпосередньо у вебплатформу дозволяє зменшити залежність від сторонніх каналів зв'язку та зберегти історію взаємодії в межах системи.

Важливим елементом є також зручність користування системою. Інтерфейс розроблено з урахуванням різного рівня цифрової підготовки користувачів, що дозволяє мінімізувати складність взаємодії з платформою та забезпечити швидке освоєння її функціоналу. Це є особливо важливим для волонтерського середовища, де до роботи можуть залучатися люди різного віку, професійного досвіду та рівня технічної підготовки.

Перспективність розробки полягає також у можливості подальшого розширення функціоналу. У майбутньому вебплатформа може бути доповнена модулями аналітики, системою сповіщень, інтерактивною картою подій, засобами збору благодійних внесків або інструментами формування звітності. Це дозволить адаптувати платформу до ширшого кола практичних потреб та підвищити її прикладну цінність.

Таким чином, запропонована вебплатформа створює єдине інформаційне середовище для організації волонтерської діяльності. Її використання дозволяє зменшити інформаційні втрати, підвищити ефективність координації, покращити якість взаємодії між учасниками та створити основу для подальшого розвитку цифрових інструментів у сфері волонтерства.

Список використаних джерел:

1. Горінов П.В., Драпушко Р.В. Волонтерська діяльність в Україні: соціально-правове дослідження: монографія. Київ: Державний інститут сімейної та молодіжної політики. 2022. 240 с.

2. Потапенко В.Г. Волонтерство в Україні: аналітична доповідь. Київ: Національний інститут стратегічних досліджень. 2022. 148 с.

УДК 004.415.2:004.432.42:004.451

*Швець Д.В., к.т.н., доцент,
Котов І.А., д.т.н., професор,
Карабут Н.О., ст. викладач*

Криворізький національний університет

МЕХАНІЗМИ ПОЛІМОРФНОЇ АДАПТАЦІЇ JAVA-ПАТЕРНІВ ПІД СПЕЦИФІЧНІ АРХІТЕКТУРИ ОПЕРАЦІЙНИХ СИСТЕМ

Концепція «Write Once, Run Anywhere» (WORA) сьогодні зазнає архітектурних змін, перетворюючись із механізму простої сумісності на складну парадигму поліморфної адаптації. Дилема між кросплатформною інваріантністю програмного коду та необхідністю досягнення нативної продуктивності в гетерогенних операційних середовищах вирішується через інтеграцію об'єктно-орієнтованих патернів у внутрішню структуру віртуальної машини Java (JVM).

Метою даної роботи є аналіз того, як класичні механізми поліморфізму та динамічного зв'язування використовуються для приховування складності системних викликів, забезпечуючи при цьому оптимальну взаємодію з ядрами розповсюджених операційних систем, зокрема Windows, Linux та macOS.

Центральну роль у процесі системної адаптації відіграє поліморфізм, який у контексті JVM виступає шаром абстракції над низькорівневими ресурсами. Через механізм динамічного зв'язування віртуальна машина ідентифікує специфіку операційного середовища безпосередньо під час виконання програми, що дозволяє підставляти відповідні реалізації системних інтерфейсів без втручання в основний код застосунку. Це забезпечує стабільність уніфікованого прикладного програмного інтерфейсу при одночасному використанні специфічних механізмів кожної системи, що простежується в еволюції структурних патернів проектування в межах стандартних бібліотек JDK.

Зокрема, реалізація мережевого стеку та механізмів вводу-виводу в сучасній Java демонструє вдаль використання патерна «Міст» (Bridge) [1], де абстракція каналу відокремлена від його системно-залежної імплементації. Це дозволяє розробнику оперувати універсальними об'єктами, тоді як на рівні ядра операційної системи задіюються принципово різні механізми, такі як `epoll` у Linux, `kqueue` у системах сімейства BSD або `IOCP` у середовищі Windows. Аналогічно, використання патерну `Abstract Factory` у файлових системах дозволяє інкапсулювати відмінності в ієрархіях шляхів та правах доступу, роблячи процес адаптації абсолютно прозорим для кінцевого

користувача. Еволюція цих патернів свідчить про поступовий відхід від статичної уніфікації на користь динамічної спеціалізації.

Окремим вагомим етапом у розвитку засобів адаптації є впровадження ініціатив у межах проєкту Panama, зокрема Foreign Function & Memory API. Ця технологія дозволяє вийти за межі традиційних обмежень Java Native Interface (JNI), пропонуючи натомість безпечні об'єктно-орієнтовані абстракції для прямої взаємодії з некерованою пам'яттю та системними бібліотеками мов C/C++. Важливим аспектом тут виступає здатність Java поліморфно адаптувати структури даних під специфічний порядок байтів та вирівнювання пам'яті, характерні для конкретних архітектур процесорів, що мінімізує обчислювальні витрати на маршалінг та забезпечує детерміновану поведінку системи в мультиплатформних конфігураціях.

Сучасні версії JDK, починаючи з релізу 17 та закінчуючи 21, вносять додаткові рівні інтелектуальної адаптації через механізми закритих типів та віртуальних потоків. Використання закритих ієрархій класів дозволяє JIT-компілятору виконувати агресивнішу оптимізацію системно-залежних патернів, оскільки заздалегідь визначений набір реалізацій для конкретних ОС спрощує аналіз потоків керування. Водночас віртуальні потоки радикально трансформують модель конкурентності, переносючи відповідальність за планування завдань із рівня ядра операційної системи на рівень об'єктно-керованих абстракцій JVM. Це дозволяє забезпечити масштабованість, де патерни багатопоточності адаптуються не до лімітів ядра ОС, а до потреб прикладної архітектури.

Слід констатувати, що еволюція об'єктно-орієнтованої парадигми в екосистемі Java відображає зсув у бік інтенсифікації взаємодії між високорівневими програмними абстракціями та низькорівневими архітектурами операційних систем. Цей процес вже не обмежується традиційним прагненням до ізоляції коду в межах віртуальної машини, а навпаки, спрямований на створення прозорого та безпечного доступу до апаратних ресурсів через розвинені механізми поліморфної адаптації. Саме ці механізми дозволяють зберегти концептуальну цілісність і сувору типізацію мови, одночасно розширюючи напрями її застосування в критично важливих, високонавантажених середовищах, де раніше домінували виключно мови системного програмування.

Список використаних джерел:

1. Chin S., Vos J., Weaver J. The Definitive Guide to Modern Java Clients with JavaFX. Berkeley, CA : Apress, 2024. 626 p. DOI: 10.1007/979-8-8688-0998-9

УДК 004.4

*Демчук О.В., здобувачка,
Чижмотря О.В., ст. викладач
Державний університет «Житомирська політехніка»*

ГЕЙМІФІКАЦІЯ ЯК ІНСТРУМЕНТ УТРИМАННЯ КОРИСТУВАЧІВ

Проблема утримання користувачів є однією з проблем створення вебплатформ, які орієнтовані на тривалу взаємодію. Більшість користувачів покидає нові платформи після першого відвідування, не повертаючись до них ніколи. Підходи типу email-нагадування та push-повідомлення, часто ігноруються і потрапляють у спам, оскільки користувачу не цікаво повертатися без причини. Гейміфікація робить платформу більш цікавою у використанні: прогрес, досягнення та конкуренція з іншими учасниками створюють бажання повертатись знову [1].

Часто гейміфікацію сприймають як застосування елементів ігрового дизайну в неігровому контексті з метою підвищення зацікавленості та мотивації користувачів [2]. Теоретичним підґрунтям її ефективності слугує теорія самодетермінації (Deci & Ryan, 2000), яка виокремлює три базові психологічні потреби: автономію, компетентність і зв'язаність. Гейміфікація ефективна тоді, коли задовольняє ці потреби. Першою потребою є система прогресу та балів, яка формує відчуття компетентності, другою - наявність рейтингових таблиць, що заохочує до конкуренції в спільноті, третьою - є вибір індивідуального маршруту за наявності додаткової гілки в roadmap від наставника, що дає відчуття автономії. Дослідження підтверджують позитивний вплив гейміфікації на мотивацію та залучення користувачів [3].

Найкращим прикладом є платформа Duolingo. Після впровадження лігових рейтингів час навчання користувачів зріс на 17%, а кількість високоактивних учасників збільшилась втричі. Механіка streak wager (збереження серії) забезпечила зростання утримання користувачів вже на 14-й день на 14%, що в сукупності дозволило збільшити щоденну аудиторію у 4,5 рази за чотири роки [4]. Можемо зробити висновки, що правильно спроектована гейміфікація здатна сильно змінити поведінку користувачів, мотивуючи їх залишатись на платформі довше.

Було використано систему з чотирьох елементів для нарахування кількості балів у рейтингу. Бали нараховуються за такі дії як

проходження тесту, завершення вузла roadmap, відвідування івенту, після чого формується загальний рейтинг користувачів за кількістю зароблених балів. Система досягнень охоплює три рівні: персональні, соціальні та експертні. В наявності також є три ролі користувача: новачок, практик та наставник. Статус наставника є особливим: його не можна отримати автоматично, для цього користувач подає заявку з підтвердженням свого досвіду у певному дозвіллі, після чого адміністратор розглядає її та приймає рішення. Після підтвердження наставник отримує додатковий функціонал: додавання вузлів до roadmap, розміщення ресурсів та створення подій.

При проєктуванні системи гейміфікації було враховано ризик ефекту надвиправдання: через сильний акцент на зовнішніх нагородах може з часом підривати мотивацію користувача [3]. Щоб цього уникнути, бали та досягнення виконують інформаційну функцію, тобто вони відображають реальний прогрес користувача, а не створюють тиск чи примушують до дій. Наприклад, відсутні блокування доступу до контенту та штрафи за бездіяльність - вони лише фіксують пройдений шлях. Саме такий підхід дозволяє зберегти мотивацію, що є досить важливим для платформ дозвілля, де участь має бути добровільною і приносити задоволення.

Список використаних джерел:

1. Детердінг С., Діксон Д., Халед Р., Накке Л. Від елементів ігрового дизайну до ігровості: визначення гейміфікації. Матеріали 15-ї міжнар. конф. MindTrek. ACM, 2011. С. 9-15. DOI: 10.1145/2181037.2181040.
2. Зенг Р. та ін. Дослідження впливу гейміфікації на академічну успішність: мета-аналіз досліджень 2008-2023 р.р. British Journal of Educational Technology. 2024. № 1. С. 87-98.
3. Райан Р. М., Десі Е. Л. Внутрішня та зовнішня мотивація: класичні визначення та нові напрями. Contemporary Educational Psychology. 2000. Т. 25. № 1. С. 54-67.
4. Мазал Х. Як Duolingo відновив зростання користувачів. Lenny's Newsletter. 2023. URL: <https://www.lennysnewsletter.com/p/how-duolingo-reignited-user-growth>.

УДК 004.4

*Білотіл Я.О., магістрант,
Чижморя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

ГЕНЕЗИС ЛОГІСТИЧНОЇ НЕВИЗНАЧЕНОСТІ ТА ДЕФЦИТ АДАПТИВНОСТІ В АРХІТЕКТУРАХ СУЧАСНИХ TMS

Еволюція глобальних ланцюгів постачань на сучасному етапі розвитку цифрової економіки вимагає від логістичних операторів безпрецедентної точності часового планування, оскільки кожна хвилина простою конвертується у прямі фінансові збитки. Проте, як свідчить детальний аналіз ринку програмного забезпечення, традиційні системи управління транспортом (TMS) все ще функціонують у парадигмі жорсткого логістичного детермінізму [2]. Основна методологічна проблема полягає в тому, що більшість комерційних платформ базуються на статичних алгоритмах розрахунку, які розглядають маршрут як лінійну послідовність відрізків із наперед визначеною пропускну здатністю [1]. Такий підхід ігнорує стохастичну природу транспортних потоків, де ключовий показник ETA є не сталою величиною, а імовірнісною функцією багатьох випадкових змінних [3].

При детальному порівняльному аналізі систем-аналогів, таких як великі ERP-модулі або локальні сервіси моніторингу, стає очевидним їхній характер як «інформаційних силосів». Ці системи ефективно збирають телематичні дані, проте мають вкрай обмежені можливості для динамічної інтеграції зовнішніх неструктурованих чинників [1]. Зокрема, вони рідко враховують у реальному часі мікрокліматичні аномалії на окремих ділянках автомагістралей, пульсуючу інтенсивність черг на міжнародних митних терміналах або специфічні технологічні затримки в морських та авіаційних портах [3]. У результаті виникає ситуація, коли диспетчер отримує інформацію про запізнення вантажу вже після того, як інцидент стався, що унеможливорює проактивне управління [2].

Важливим деструктивним фактором є відсутність глибокої інтеграції геоінформаційних сервісів із предиктивними модулями. Сучасні TMS-рішення часто використовують картографічні дані лише як статичну підкладку для візуалізації, не враховуючи топологічні особливості дорожньої мережі, що змінюються під впливом ремонтних робіт або сезонних обмежень [3].

Наукові дослідження підтверджують, що в умовах сучасного міського трафіку похибка прогнозування за допомогою стандартних

методів екстраполяції зростає експоненціально, якщо модель не має доступу до Big Data [3]. Це явище, відоме як «дефіцит адаптивності», зумовлене використанням застарілих архітектурних рішень, де алгоритм розрахунку часу є «жорстко закодованим» і не здатним до самокорекції на основі історичного досвіду [2]. Існуючі аналоги часто пропонують лише візуалізацію GPS-треку, залишаючи аналітичну роботу людині-оператору, що в умовах великого автопарку призводить до помилок через людський фактор [1].

Додатковим обмеженням архітектур сучасних TMS є вразливість цілісності телематичних даних. Більшість існуючих систем не мають вбудованих інтелектуальних протоколів верифікації вхідної інформації, що створює ризики внесення навмисних або випадкових викривлень у предиктивну модель [1]. Це призводить до ситуації, коли система базує свої прогнози на некоректних координатах або застарілих даних про стан інфраструктури. Проектування нової інтелектуальної моделі має базуватися не лише на високій точності алгоритмів прогнозування, а й на засадах прозорості та кіберстійкості обміну даними між усіма учасниками логістичного ланцюга (портами, митними терміналами та перевізниками) [2].

Таким чином, актуальність розробки оригінальної інтелектуальної системи обґрунтовується необхідністю створення гнучкого предиктивного ядра. Така система має відійти від простої фіксації координат і перейти до глибокого інтелектуального моделювання поведінки транспортної мережі [3]. Це дозволить трансформувати логістичне середовище з пасивного об'єкта спостереження на активну систему підтримки прийняття рішень, яка здатна до випереджаючого реагування на потенційні логістичні інциденти ще до моменту їхнього фактичного виникнення [1]. Впровадження предиктивних моделей замість детермінованих алгоритмів дозволить підвищити надійність постачань та мінімізувати операційні ризики, пов'язані з невизначеністю зовнішнього середовища [2].

Список використаних джерел:

1. Григорак М. Ю. Інтелектуалізація логістичного управління: монографія. Київ: ПСТУ, 2017. 212 с.
2. Тимонін О. М. Інформаційні системи та технології в логістиці : навч. посіб. Київ: КНЕУ, 2018. 320 с.
3. Шмельов Ю. М. Застосування інтелектуальних систем на транспорті / Ю. М. Шмельов // Інтелектуальні системи автоматизації : монографія / Аврунін О. Г. та ін. – Кременчук : Новабук, 2021. – Розд. 2. – С. 69-122. URL: <https://openarchive.nure.ua/handle/document/20512>

УДК 004.4

*Білотіл Я.О., магістрант,
Чижморя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

ГІБРИДИЗАЦІЯ МЕТОДІВ АНСАМБЛЕВОГО НАВЧАННЯ ТА РЕКУРЕНТНИХ НЕЙРОСТРУКТУР У ЗАДАЧАХ МІНІМІЗАЦІЇ ЧАСОВИХ ВІДХИЛЕНЬ

Математичне забезпечення інтелектуальних систем прогнозування нового покоління виходить за межі класичного регресійного аналізу та методів екстраполяції, які демонструють низьку ефективність у задачах із високою розмірністю та значним рівнем «шуму» вхідних даних [1]. Для розв'язання задачі предиктивної оптимізації рейсів у межах інтелектуальної системи доцільно застосовувати гібридний підхід, що поєднує ансамблеві методи навчання та архітектури глибинного навчання. Зокрема, використання алгоритмів градієнтного бустингу на деревах рішень, таких як XGBoost, дозволяє ітеративно мінімізувати середньоквадратичну помилку прогнозу (RMSE) шляхом побудови послідовності слабких учнів, кожен з яких коригує помилки попереднього [2]. Такий підхід забезпечує високу точність при роботі з табличними даними, що містять інформацію про категорію доріг, погодні умови та часові мітки [1].

Проте специфіка транспортної логістики, де дані про рух вантажу є послідовними часовими рядами, вимагає врахування довгострокових залежностей та інерційності процесів. Для вирішення цієї проблеми у наукових публікаціях пропонується впровадження рекурентних нейронних мереж з архітектурою LSTM (Long Short-Term Memory) [3]. LSTM-мережі володіють специфічним математичним механізмом «вентилів» (gates), що дозволяє моделі вибірково зберігати інформацію про стан трафіку та затримки на попередніх етапах маршруту, екстраполюючи цей досвід на майбутні відрізки шляху [1]. Для коректної роботи нейронних структур необхідно проводити нормалізацію та масштабування ознак (Min-Max Scaling або Standard Scaling), що дозволяє збалансувати вплив параметрів з різними одиницями вимірювання [1]. Це критично важливо для виявлення прихованих закономірностей, таких як циклічні затори або періодична зміна пропускної здатності логістичних вузлів [3].

Задача оптимізації часу доставки вантажу в такому математичному контексті формулюється як мінімізація функціоналу часових втрат у багатовимірному просторі станів [2]. Математична модель повинна оперувати векторами ознак, що включають не лише координати, а й

динамічні параметри: зміну швидкості на попередніх сегментах, імовірнісні оцінки простою на терміналах та специфічні графіки роботи інфраструктурних об'єктів. Глибокий аналіз вхідних параметрів дозволяє моделі враховувати «вагу» кожного чинника, адаптуючи прогноз до конкретного дня тижня або часу доби, що мінімізує вплив людського фактора на етапі планування [1]. Гібридизація бустингових моделей, що добре працюють зі статичними ознаками, та LSTM-мереж, орієнтованих на динаміку, дозволяє досягти точності прогнозування ETA на рівні 95%, що є фундаментом для предиктивного логістичного менеджменту [3].

Окрему увагу в математичному обґрунтуванні слід приділити методам регуляризації гібридної моделі для запобігання ефекту перенавчання (overfitting). Оскільки логістичні дані часто містять аномальні викиди (наприклад, аварійні перекриття доріг або стихійні явища), застосування функцій втрат L1 та L2 регуляризації в алгоритмах XGBoost дозволяє підвищити узагальнюючу здатність системи [2]. Також у наукових джерелах рекомендується впровадження технології Dropout для LSTM-шарів, що забезпечує стабільність прогнозу при зміні зовнішніх факторів, які не були представлені у початковій навчальній вибірці [3].

Важливим етапом математичного обґрунтування є вибір метрик адекватності побудованих моделей. Окрім стандартного показника RMSE, у фаховій літературі рекомендується застосування метрики MAPE, яка оцінює відносну похибку прогнозу [2]. Використання крос-валідації на часових рядах забезпечує перевірку стійкості моделі до структурних зсувів у даних, викликаних сезонними коливаннями [3]. Такий підхід гарантує високу прогностичну здатність системи у широкому діапазоні сценаріїв [1].

Список використаних джерел:

1. Кузькін О.Ф. Методи машинного навчання у задачах прогнозування динамічних процесів. Радіоелектроніка, інформатика, управління. 2020. № 2. С. 104-115. DOI: <https://doi.org/10.15588/1607-3274-2020-2-11>
2. Пасічник В. В. Математичне моделювання та інтелектуальні системи в транспортних мережах : монографія. Львів : Видавництво Львівської політехніки, 2019. 284 с.
3. Савченко К. М., Дрозд О. В. Використання глибинного навчання для прогнозування часових рядів у логістичних ланцюгах. Науковий вісник ЖДТУ. Серія: Технічні науки. 2021. № 1 (87). С. 42–51. URL: https://nbuv.gov.ua/UJRN/Nponat_2021_1_8

УДК 004.4

*Білотіл Я.О., магістрант,
Чижморя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

ОБҐРУНТУВАННЯ РЕАКТИВНОЇ DATA-АРХІТЕКТУРИ ТА ВИБІР ІНСТРУМЕНТАЛЬНОГО СТЕКА ІНТЕЛЕКТУАЛЬНОЇ ЛОГІСТИЧНОЇ ПЛАТФОРМИ

Технологічна реалізація інтелектуальної системи прогнозування вимагає побудови архітектури, здатної обробляти масивні потоки подій (Event Streaming) у режимі реального часу. В основі інструментального вибору лежить мікросервісний підхід, який дозволяє відокремити важкі обчислювальні процеси машинного навчання від інтерфейсних модулів та сервісів збору даних [1]. Як базову мову програмування обрано Python, що обумовлено наявністю найбільш розвиненої екосистеми бібліотек (Pandas, Scikit-learn, TensorFlow) для аналізу даних та інтеграції готових моделей прогнозування в промислові рішення [3]. Використання Python дозволяє значно скоротити цикл розробки (Time-to-Market) завдяки високому рівню абстракції та широкій підтримці науковою спільнотою [1].

Для забезпечення масштабованості та низької затримки (low latency) при обробці GPS-координат від тисяч транспортних одиниць доцільно використовувати брокер повідомлень Apache Kafka. Це дозволяє реалізувати реактивний конвеєр даних, де кожна зміна статусу вантажу ініціює миттєвий перерахунок прогнозних значень [1]. Kafka виступає як центральна нервова система платформи, забезпечуючи гарантовану доставку повідомлень та можливість повторної обробки історичних потоків для донавчання нейромереж [3]. Такий підхід нівелює ризики втрати даних при пікових навантаженнях, що є критичним для систем моніторингу критичної інфраструктури [2].

Для зберігання динамічних структур маршрутів та телематичної історії обґрунтовано використання NoSQL-рішення, зокрема MongoDB [2]. На відміну від реляційних моделей, ця база даних демонструє вищу продуктивність при виконанні геопросторових запитів (GeoJSON) та дозволяє гнучко масштабувати систему без зупинки сервісу [3]. Використання формату документів BSON дозволяє зберігати складні логістичні об'єкти з варіативним набором атрибутів, що часто зустрічається при роботі з різними типами датчиків та вантажів [2]. Це забезпечує високу швидкість доступу до даних при формуванні аналітичних звітів у реальному часі [1].

Важливим аспектом інструментального забезпечення є використання засобів контейнеризації на базі Docker, що гарантує ідентичність середовища розробки та експлуатації [1]. Для підтримки життєвого циклу предиктивних моделей у промислових умовах передбачено впровадження MLOps-конвеєрів. Це дозволяє автоматизувати процеси перенавчання моделей при виявленні "концептуального зсуву" (concept drift), коли точність прогнозів ETA починає знижуватися через зміну зовнішніх умов [3]. Використання інструментів типу MLflow забезпечує версіонування моделей та відстеження метрик їхньої ефективності, що мінімізує ризики деградації системи в довгостроковій перспективі [1]. Це дозволяє уніфікувати розгортання інтелектуальних модулів на хмарних платформах, забезпечуючи відмовостійкість системи при критичних збоях окремих компонентів [2].

Окрему увагу в інструментарії приділено розробці RESTful API для інтеграції з існуючими ERP та WMS системами підприємства [2]. Використання фреймворків типу FastAPI дозволяє забезпечити високу швидкість обробки зовнішніх запитів та автоматичну генерацію технічної документації [1]. Такий комплексний вибір технологій дозволяє створити надійну інструментальну базу, де навчання предиктивної моделі та видача прогнозів відбуваються паралельно. Це забезпечує високу доступність сервісу та стабільність роботи системи в умовах екстремальної інтенсивності інформаційних потоків [3].

Список використаних джерел:

1. Коваленко О. М. Проектування мікросервісних архітектур для систем реального часу. Сучасні інструменти програмування інтелектуальних систем: матеріали міжнар. наук.-практ. конф. (Київ, 22-23 трав. 2023 р.). Київ: IT-Наука, 2023. С. 45–48. URL: <https://it-science.com.ua/conf2023/proceedings>
2. Бондаренко В. С., Мельник А. П. Порівняльний аналіз NoSQL баз даних для геоінформаційних систем. Наукові вісник НТУУ «КПІ». Серія: Інформатика. 2022. № 3. С. 88–97.
URL: <https://ev.fict.kpi.ua/article/view/265431>
3. Сидоров І. В. Архітектура потокової обробки даних у реальному часі для логістичних модулів. Системи управління, навігації та зв'язку. 2021. № 2 (64). С. 112–120.
URL: <http://journals.pntu.edu.ua/sunz/article/view/2412>

УДК 004.4

*Ігнатенко С.І., магістрант,
Чижморя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

МЕТОД ПРОЄКЦІЙНОГО ТЕКСТУРУВАННЯ: АНАЛОГИ ТА МЕТОДИ ПОКРАЩЕННЯ

Проекційне текстурювання є одним із базових методів у комп'ютерній графіці, який дозволяє переносити двовимірні текстури на поверхню тривимірних об'єктів. Метод має широке застосування у створенні комп'ютерних ігор, візуальних ефектів та віртуальних сцен. Попри це, він стикається із низкою обмежень, зокрема спотворенням текстур на складних геометріях, створенням видимих швів та низькою ефективністю при роботі з великими даними [1].

Основою методу є використання координат текстури, які проєктуються з двовимірного простору на 3D-поверхню. Традиційні техніки, такі як UV mapping, planar projection та cylindrical mapping, забезпечують базовий функціонал, але мають обмеження. UV mapping, наприклад, потребує ретельної ручної підготовки, що ускладнює роботу з деталізованими моделями.

Для вирішення цих проблем використовуються альтернативи: процедурне текстурювання, воксельне текстурювання та методи, засновані на штучному інтелекті. Процедурне текстурювання дозволяє генерувати текстури на основі математичних алгоритмів, забезпечуючи високу гнучкість і зменшення обсягу текстурних даних. Воксельне текстурювання працює із тривимірними пікселями (вокселями), що дає змогу уникнути швів і забезпечує рівномірний розподіл текстур на складних формах, але є ресурсозатратним [2].

Штучний інтелект відкриває нові можливості для вдосконалення проєкційного текстурювання. Генеративно-змагальні мережі (GANs) дають змогу створювати адаптивні текстури, які враховують геометрію об'єктів, що зменшує спотворення. Так, Pix2Pix GAN демонструє ефективність у перенесенні текстур зі зразків на моделі. Іншим важливим напрямком є автоматизація UV-розгортки за допомогою convolutional neural networks (CNNs), що мінімізує шви та спрощує процес текстурювання [3].

Додатково, впровадження фізично коректного рендерингу (PBR) дозволяє інтегрувати текстури з врахуванням фізичних властивостей матеріалів, таких як шорсткість чи відбивна здатність, забезпечуючи реалістичність зображення. Алгоритми глибокого навчання також можуть використовуватися для виявлення та виправлення артефактів текстурування, що підвищує якість кінцевого продукту [4].

Практичне застосування цих методів охоплює такі галузі, як розробка відеоігор, візуалізація архітектурних проєктів та створення контенту для віртуальної реальності. Наприклад, ігрові рушії Unreal Engine та Unity вже активно використовують інструменти ШІ для оптимізації текстурування [5].

Попри всі досягнення, залишаються виклики, пов'язані зі складністю масштабування, великими обсягами даних та етичними аспектами, зокрема стосовно авторських прав. Тому подальші дослідження повинні фокусуватися на підвищенні ефективності, зниженні обчислювальних витрат і вирішенні юридичних питань.

Метод проєкційного текстурування у поєднанні з новітніми інструментами штучного інтелекту демонструє великий потенціал для вдосконалення процесів у комп'ютерній графіці, що відкриває нові можливості для створення реалістичних та якісних 3D-сцен.

Список використаних джерел:

1. Pharr, M., Jakob, W., & Humphreys, G. Physically Based Rendering: From Theory to Implementation. Morgan Kaufmann, 2016. 1264 p.
2. Goodfellow, I., Bengio, Y., & Courville, A. Deep Learning. MIT Press, 2016. 800 p.
3. Isola, P., Zhu, J. Y., Zhou, T., & Efros, A. A. Image-to-Image Translation with Conditional Adversarial Networks. IEEE CVPR. 2017. Pp. 1125-1134.
4. Ebert, D. S., Musgrave, F. K., Peachey, D., Perlin, K., & Worley, S. Texturing and Modeling: A Procedural Approach. Morgan Kaufmann, 2002. 512 p.
5. Liu, H., et al. Deep Learning for Automatic UV Unwrapping of 3D Meshes. ACM SIGGRAPH Asia. 2021. Pp. 87-94.

УДК 004.4

*Ігнатенко С.І., магістрант,
Чижмоторя О.В., ст. викладач
Державний університет «Житомирська політехніка»*

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕС РЕНДЕРИНГУ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

Рендеринг є одним із ключових етапів у комп'ютерній графіці, який забезпечує створення реалістичних зображень і анімацій на основі тривимірних моделей. Традиційно рендеринг використовує фізично точні алгоритми, такі як ray tracing, які потребують значних обчислювальних ресурсів. У сучасних умовах інтеграція штучного інтелекту (ШІ) у процес рендерингу дозволяє досягати балансу між якістю, швидкістю та ресурсозатратністю [1].

Одним із ключових інструментів є нейронні мережі, які оптимізують етапи рендерингу шляхом аналізу сцени та передбачення освітлення. Наприклад, алгоритми на основі convolutional neural networks (CNNs) дозволяють точно моделювати глобальне освітлення, зменшуючи необхідність у повному трасуванні променів. Такі методи значно прискорюють процес рендерингу, особливо для інтерактивних додатків, таких як відеоігри та віртуальна реальність [2].

Додатково, генеративно-змагальні мережі (GANs) відкривають нові можливості для створення високоякісних текстур і освітлення. Наприклад, GANs можуть синтезувати складні текстури з низькороздільних зображень, що особливо корисно для мобільних пристроїв із обмеженими обчислювальними можливостями. Більше того, ці мережі ефективно використовуються для реконструкції реальних сцен на основі фотографій, що значно скорочує час підготовки 3D-контенту [3].

ШІ також використовується для адаптивного рендерингу. Алгоритми машинного навчання аналізують складність сцени і оптимізують розподіл обчислювальних ресурсів, забезпечуючи високу якість лише в ключових ділянках зображення. Це особливо актуально для потокового рендерингу в хмарних середовищах, де важливо мінімізувати затримки [4].

Штучний інтелект також допомагає оптимізувати обчислювальні витрати в рендерингу. Завдяки використанню методів компресії даних на основі нейронних мереж можливо значно зменшити обсяг текстур і моделей, які передаються на сервери або графічні процесори. Це

дозволяє ефективно використовувати хмарні обчислення навіть для складних тривимірних сцен.

Однак інтеграція ШІ в процес рендерингу стикається з викликами. Серед них — потреба в масштабованих обчислювальних системах для навчання моделей, а також проблеми етичного характеру, зокрема використання ШІ для створення недостовірного або маніпулятивного контенту. Крім того, важливим є питання інтеграції ШІ-алгоритмів у традиційні рушії рендерингу, такі як Unreal Engine та Blender, що потребує адаптації існуючих інструментів.

Крім того, сучасні дослідження фокусуються на інтеграції технологій штучного інтелекту для створення адаптивних сценаріїв освітлення. Це дозволяє забезпечити динамічне освітлення, яке автоматично змінюється відповідно до положення камери або об'єктів сцени. Такі підходи особливо важливі для інтерактивних застосунків, де необхідно забезпечити високу реалістичність у реальному часі.

Незважаючи на виклики, перспективи використання ШІ в рендерингу є надзвичайно широкими. Це включає автоматизацію процесів освітлення, текстуровання та навіть створення анімації. Подальші дослідження мають зосередитися на підвищенні ефективності моделей ШІ, забезпеченні прозорості алгоритмів і інтеграції нових підходів у комерційні графічні системи.

Таким чином, ШІ стає невід'ємною складовою сучасного рендерингу, відкриваючи нові можливості для створення реалістичного та якісного 3D-контенту. Його використання значно прискорює робочі процеси, забезпечуючи при цьому високу якість і економію ресурсів.

Список використаних джерел

1. Zhou, B., et al. Machine Learning for Adaptive Rendering in Real-Time Applications // ACM Transactions on Graphics. – 2021. – Vol. 40, No. 4. – P. 123-135.
2. Karis, B. Real-Time Global Illumination in Games: Techniques and Approaches // SIGGRAPH Talks. – 2016.
3. Karras, T., Laine, S., & Aila, T. A Style-Based Generator Architecture for Generative Adversarial Networks // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2020. – Vol. 42, No. 12. – P. 2616-2628.
4. Amazon Web Services. Scalable Solutions for Game Development. – AWS Documentation, 2023.

УДК 004.8

*Дубина О.Ю., магістрант,
Льовкін В.М., к.т.н. доцент
Національний університет «Запорізька політехніка»*

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ МОНІТОРИНГУ СТАНУ ХУДОБИ

Використання програмного забезпечення для моніторингу стану худоби є дуже важливим на практиці, оскільки середнє, велике господарство має таку кількість худоби, що історію зміни її станів важко запам'ятати, а пошук у паперових даних або зафіксованих у різних джерелах достатньо складно виконувати. З іншого боку наявність таких історичних даних про худобу господарства дозволяє не тільки переглядати історію, але і формувати прогноз про її майбутній стан на основі цих даних.

Узагальнюючим показником стосовно стану худоби в цій роботі було обрано обсяг удоїв тварини за наступний період. Фактично саме цей показник є ключовим для поточного ведення господарства. Безпосередньо період може обиратися господарством в залежності від того, яким є горизонт планування діяльності.

Програмне забезпечення було розроблено таким чином, щоб спростити як загальний доступ до нього, так і роботу з окремими тваринами. Тому по-перше, програма була створена як вебзастосунок на основі фреймворку Django, що було важливим рішенням, адже разом з мовою програмування Python це дозволило також за рахунок пакетів цієї мови отримати ключ для обробки даних, які зберігаються в базі даних та які необхідні для формування вибірки даних для навчання моделі, так і для створення, навчання та застосування моделі прогнозування удоїв худоби, яку потрібно було забезпечити для відповідного рівня актуальності, який описаний вище.

За кожною твариною розроблена в підсумку програма дозволяє фіксувати, а потім відповідно і моніторити безпосередньо удої, годування тварин, вимірювання фізичного стану, проведені вакцинації, виявлені захворювання та їх лікування. Для зручності роботи з такими даними було забезпечено їх внесення як індивідуально за твариною, так і сукупно за всіма тваринами певної породи або за тваринами, які знаходяться в певному приміщенні господарства. Це дозволяє за масової роботи скоротити час, необхідний на внесення даних, що є критичним для такої роботи і може бути бар'єром для використання на практиці.

Прогнозування стану худоби на основі обсягів удоїв забезпечено шляхом створення моделі на основі дерева рішень [1]. При створенні моделі було враховано структуру вибірки даних [2], за якою в якості вхідних ознак зокрема враховано цілочисельну ознаку породи худоби, кількість народжених тварин твариною, для якої виконується прогнозування, обсяг спожитої їжі в середньому за період, представлений вагою, аналогічний обсяг води, кількість днів, що минула з періоду, коли худоба не давала молоко, наявність у тварини окремих видів вакцин тощо.

Використання дерев рішень в основі моделі прогнозування стану худоби дозволило пришвидшити процес обробки даних для реального прогнозування, що може бути важливим за використання великої кількості прогнозів, а також у випадку, коли технічне забезпечення роботи програми значно обмежено. Окрім того такий варіант моделі дозволяє достатньо просто інтерпретувати рішення, які було прийнято. Їх можна пояснити, виділити те, що лежить в їх основі, сприяючи встановленню акцентів під час роботи з даними особами, які в такому господарстві приймають рішення. Також така модель може застосовуватися і у випадку зміни набору ознак, з яким відбувається робота.

Результати дослідження моделі прогнозування стану худоби на основі визначення обсягу удоїв за допомогою вибірки даних [2] продемонстрували, що дана модель має у більш ніж 6 разів кращий результат за показником середньої абсолютної похибки порівняно з методом опорних векторів, який також міг би використовуватися для розв'язання цієї задачі.

Розроблена програма може використовуватися сукупно різними господарствами для того, щоб зменшити витрати на підтримку такої системи. При цьому представники кожного господарства будуть працювати з даними тільки власної худоби. За необхідності у випадку продажу худоби можливо отримати історію за кожною такою твариною, якщо представники обох таких господарств у програмі підтвердять такий факт.

Список використаних джерел:

1. Smith C. Decision Trees and Random Forests: A Visual Introduction For Beginners. Vancouver: Blue Windmill Media, 2017. 168 p.
2. Cattle Health and Feeding Data. URL: <https://www.kaggle.com/datasets/shahhet2812/cattle-health-and-feeding-data> (дата звернення: 25.03.2026).

УДК 004

*Горобець В.І., магістрант,
Льовкін В.М., к.т.н., доцент
Національний університет «Запорізька політехніка»*

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРОГНОЗУВАННЯ ГРУПОВОЇ ДИНАМІКИ ЛЮДСЬКИХ РЕСУРСІВ ПІДПРИЄМСТВА

Висока плинність людських ресурсів на підприємстві є вираженням великої кількості проблем, що нашарувались в діяльності підприємства. Тим не менш рівень плинності може бути різним, при цьому в будь-якому випадку здійснюючи більшою або меншою мірою вплив на діяльність підприємства. Заміна працівників пов'язана з додатковими витратами на пошук нового працівника, його навчання, інтеграцію в колектив, зменшення поточних досягнутих результатів через забезпечення перелічених процесів тощо.

Прогнозування групової динаміки людських ресурсів підприємства має бути забезпечено шляхом індивідуальної класифікації кожного працівника за ймовірністю його звільнення за певний період часу – горизонт планування. Для цього має бути визначено відповідну модель класифікації, а далі її програмно реалізовано у складі програмного забезпечення з відповідними функціональними можливостями та інтеграцією.

В процесі проектування і реалізації програмного забезпечення було застосовано комплекс сучасних технологічних рішень та інструментів, що забезпечило досягнення високої ефективності розробленої системи. Ключову роль у створенні програмного продукту відіграла мова програмування Python, яка завдяки інтуїтивному синтаксису, численним бібліотекам та модулям надала змогу реалізувати структуровано-продуктивний код. У якості фреймворку було обрано Django, оскільки він забезпечує високий рівень безпеки, гнучкість, масштабованість при розробці вебзастосунків. Для збереження інформації проекту використовується система керування базами даних MySQL, яка забезпечує надійну обробку й ефективне управління великими даними.

Експериментальне дослідження проводилось на основі набору даних Employee/HR Dataset (ALL in One) [1], який містить комплексну інформацію про працівників, їхню трудову історію, поведінкові характеристики та організаційні показники. Зазначений набір даних повністю відповідає вимогам дослідження та забезпечує можливість

проведення ґрунтового аналізу чинників, що визначають імовірність звільнення співробітників.

Під час експериментального дослідження наявний набір даних був розподілений таким чином, щоб 80 % всіх даних було віднесено і сформували навчальну вибірку даних, а 20 % – тестову, на якій відбувалось оцінювання отриманих результатів на основі методу Random Forest [2].

Запропонована модель класифікації була створена на основі використання методу Random Forest з навчанням її на основі навчальної вибірки. Для реалізації моделі використовувалась бібліотека scikit-learn, зокрема клас RandomForestClassifier. Для налаштування моделі задавались ключові параметри: кількість дерев у ансамблі встановлена на рівні 100, що дозволяє досягти балансу між точністю та обчислювальною ефективністю, максимальна глибина дерев обмежена значенням 10, щоб запобігти надмірному пристосуванню моделі до навчальних даних.

Модель на основі методу Random Forest дозволила отримати точність класифікації на рівні 89,7 %.

За результатами експериментального дослідження встановлено, що створена і навчена на основі використання методу Random Forest модель дозволила виконати класифікацію працівників підприємства за ймовірністю звільнення. Висока стійкість моделі до шуму та здатність ефективно працювати з великою кількістю нелінійних змінних підтверджують доцільність застосування ансамблевих методів для прогнозування відтоку працівників. Підвищення точності класифікації відповідно призводить до покращення інформативності рішень, які приймаються стосовно управління персоналом відповідальними особами, забезпечуючи принципи, які лежать в основі сертифікаційних випробувань.

У роботі програмно реалізовано створене рішення з забезпеченням відповідного вебзастосунку, що надає таким чином універсальний доступ з будь-якої платформи для роботи з функціональними можливостями програми.

Список використаних джерел:

1. Rana R. S. Employee/HR Dataset (All in One). URL: <https://www.kaggle.com/datasets/ravindrasinghrana/employeedataset> (дата звернення: 25.03.2026).
2. Rose M., Hassen H. Survey of random forest pruning techniques. Computer Science & Information Technology. 2019. Vol. 9, № 18. Pp. 99-109. DOI: 10.5121/csit.2019.91808.

УДК 004.8(043.2)

О.А. Захарова, здобувач

Державний університет «Київський авіаційний інститут»

АДАПТИВНЕ ФОРМУВАННЯ ТРЕНУВАЛЬНИХ ПРОГРАМ У МОБІЛЬНОМУ ЗАСТОСУНКУ «ТРЕНЕР»

Розробка мобільних застосунків у сфері цифрового здоров'я є актуальним напрямом сучасної програмної інженерії, оскільки такі системи дозволяють автоматизувати контроль фізичної активності користувача та оптимізувати тренувальні навантаження. Водночас існуючі рішення часто не забезпечують достатнього рівня персоналізації або характеризуються надмірною складністю, що негативно впливає на ефективність їх використання. У зв'язку з цим особливої актуальності набуває поєднання ефективних архітектурних підходів та адаптивних алгоритмів.

Основними проблемами є різномірність даних користувача, відмінності у рівнях фізичної підготовки та необхідність обробки інформації у реальному часі. Це ускладнює формування універсальних тренувальних рекомендацій та створює додаткове навантаження на систему, що є критичним для мобільних пристроїв. Відсутність адаптивних механізмів також призводить до зниження мотивації користувачів і ефективності тренувального процесу.

Метою роботи є розробка архітектурно-алгоритмічного підходу до побудови мобільного застосунку «Тренер», який забезпечує ефективну обробку даних користувача та адаптивне формування тренувальних програм. Запропонований підхід спрямований на підвищення якості рекомендацій і формування цілісної взаємодії користувача із системою.

У роботі використано модульну архітектуру із розподілом функцій між рівнями інтерфейсу, бізнес-логіки та доступу до даних. Для оцінки продуктивності системи застосовано модель часу обробки запиту:

$$T = T_1 + T_2 + T_3,$$

де T_1 – часотримання даних, T_2 – час їх обробки, T_3 – час формування відповіді. Оптимізація цих компонентів дозволяє зменшити затримки та підвищити швидкість системи [1,2]. Використання локального сховища та кешування забезпечує автономність і швидкий доступ до даних.

Адаптація тренувального процесу здійснюється за допомогою коефіцієнта:

$$K = (P_n / P_0) \cdot \alpha,$$

що дозволяє коригувати інтенсивність та структуру тренувань відповідно до прогресу користувача [3,4]. Додатково враховується статистика тренувань, що підвищує точність рекомендацій і дозволяє оцінювати динаміку змін показників.

У результаті дослідження встановлено, що поєднання модульної архітектури та адаптивних алгоритмів дозволяє підвищити ефективність системи, покращити користувацький досвід та забезпечити стабільність роботи застосунку. Запропонований підхід може бути використаний як основа для подальшого розвитку мобільних систем підтримки фізичної активності з можливістю інтеграції інтелектуальних методів обробки даних.

Додатковим важливим аспектом є забезпечення надійності, цілісності та коректності даних користувача, що досягається шляхом використання механізмів валідації, нормалізації та контролю узгодженості інформації на різних етапах її обробки. Це дозволяє зменшити вплив помилкових або неповних даних на результати аналізу, підвищити точність розрахунків та забезпечити більш обґрунтоване формування тренувальних рекомендацій.

Крім того, запропонований підхід створює передумови для подальшого розширення функціональних можливостей застосунку, зокрема інтеграції із носимими пристроями (фітнес-браслети, смарт-годинники) та зовнішніми сервісами моніторингу здоров'я. Це дозволяє отримувати більш детальні та різноманітні дані про фізичний стан користувача, підвищувати точність аналітичних моделей і забезпечувати більш ефективну персоналізацію тренувального процесу.

Список використаних джерел:

1. Sommerville, I. Software Engineering. 10th ed. Boston: Pearson, 2016. 816 с.
2. Pressman, R.S.; Maxim, B.R. Software Engineering: A Practitioner's Approach. 9th ed. New York: McGraw-Hill, 2019. 970 с.
3. ISO/IEC 25010:2011. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE).
4. World Health Organization. Guidelines on Physical Activity and Sedentary Behaviour. Geneva, 2020.

УДК 004.272:519.61

*Сухарський С. С., аспірант,
Малашинок Г. І., д.ф.-м.н., професор
Інститут Програмних Систем НАНУ
Національний Університет «Києво-Могилянська академія»*

ТРИДІАГОНАЛІЗАЦІЯ СТРІЧКОВИХ СИМЕТРИЧНИХ МАТРИЦЬ

Задача зведення симетричної (ермітової) матриці до тридіагональної форми є однією з базових задач чисельної лінійної алгебри, що лежить в основі алгоритмів обчислення власних значень і власних векторів [1, 2]. Попереднє приведення матриці до тридіагонального вигляду значною мірою визначає ефективність подальших обчислень. У класичних підходах для розв'язання цієї задачі використовуються перетворення Хаусхолдера, які характеризуються високою чисельною стійкістю, але мають значну кількість залежностей між операціями та низький рівень паралелізму на сучасних гібридних кластерних вузлах. Основним обмежуючим фактором у таких системах є не кількість арифметичних операцій, а обсяг і структура обміну даними, що обумовлює необхідність розробки алгоритмів із низькою комунікаційною складністю [3].

У роботі запропоновано алгоритм Ribbon для зведення стрічкових симетричних матриць до тридіагональної форми. Алгоритм застосовується до стрічкових матриць і є етапом переходу від стрічкової до тридіагональної форми у загальному обчислювальному процесі. Алгоритм базується на ідеї послідовного зменшення ширини стрічки матриці вдвічі на кожному кроці з використанням блоково-рекурсивних QR та QP розкладів [4]. Обчислення організовано у вигляді блокової структури, що дозволяє звести основні операції до матричних множень. У результаті формується унітарний розклад вигляду $A = U^T T U$, де T — тридіагональна матриця, а U — ортогональна (унітарна) матриця, яка накопичується у процесі виконання алгоритму. Ключовою особливістю алгоритму є його природна придатність до паралельної реалізації. Обчислення організовано у вигляді дворівневого конвеєра. На першому рівні паралелізм досягається за рахунок незалежної обробки груп блоків (паралелограмів) в межах одного рівня стрічки. На другому рівні забезпечується міжмасштабний паралелізм: обчислення для наступного рівня з меншою шириною стрічки можуть розпочинатися до повного завершення попереднього рівня.

Асимптотичний аналіз показує, що складність обчислення тридіагональної форми в алгоритмі Ribbon має той самий порядок, що

й матричне множення, тобто $O(N^\beta)$, де β визначається алгоритмом множення матриць. Це дозволяє розглядати запропонований підхід як ефективну альтернативу класичним методам у контексті високопродуктивних обчислень. Водночас встановлено, що побудова унітарного множника U має кубічну складність $O(N^3)$ та є домінуючим етапом на великих розмірах матриць. При цьому для повної факторизації спостерігається збільшення константи при кубічному члені порівняно з методом Хаусхолдера, що відображає компроміс між зменшенням комунікаційних витрат і обчислювальною складністю.

Програмну реалізацію алгоритму виконано у середовищі блоково-рекурсивних паралельних обчислень DAP із використанням MPI. Обчислювальний процес представлено у вигляді графа задач, що дозволяє ефективно реалізувати паралельну обробку та масштабування. Експериментальні дослідження проведено системі з використанням CPU та GPU. Отримані результати демонструють узгодження з теоретичними оцінками: час виконання алгоритму зростає кубічно зі збільшенням розміру матриці, а абсолютна похибка реконструкції становить порядку 10^{-13} , що відповідає машинній точності для подвійної арифметики. Показано, що зі зростанням розміру задачі частка часу, витрачена на побудову матриці U , зростає та визначає загальну продуктивність алгоритму.

Таким чином, запропонований алгоритм Ribbon забезпечує поєднання блоково-рекурсивної структури, низької комунікаційної складності та високого рівня паралелізму. Це робить його перспективним для використання у високопродуктивних обчисленнях, зокрема на гібридних CPU–GPU системах і багатовузлових кластерах. Подальші дослідження можуть бути спрямовані на оптимізацію етапу побудови унітарного множника та підвищення ефективності реалізації на розподілених системах.

Список використаних джерел:

1. Golub G. H., Van Loan C. F. Matrix Computations. 4th ed. Baltimore: Johns Hopkins University Press, 2013. 756 p.
2. Trefethen L. N., Bau D. Numerical Linear Algebra. Philadelphia: SIAM, 1997.
3. Ballard G., Demmel J., Holtz O., Schwartz O. Minimizing communication in numerical linear algebra // SIAM Journal on Matrix Analysis and Applications. 2011. Vol. 32, No. 3. P. 866–901.
4. Малашенок Г., Сухарський С. Блоково-рекурсивний підхід до унітарного розкладу матриць // Проблеми програмування. 2026. № 1 (прийнято до друку).

УДК 004.7

*Денисенко Д.О., здобувач,
Єфремов Ю.М, к.т.н., доцент
Державний університет «Житомирська політехніка»*

ПРОЕКТУВАННЯ UX/UI-ІНТЕРФЕЙСУ ВЕБ-ПЛАТФОРМИ ДЛЯ МЕДІАКОНТЕНТУ

Якість взаємодії користувача з веб-платформою є одним із ключових факторів її успішності. Для платформ, орієнтованих на медіа інформацію, зокрема фільми та серіали, особливого значення набуває проектування інтуїтивного інтерфейсу, що забезпечує зручний перегляд каталогу, швидкий доступ до рецензій та мінімальні когнітивні витрати під час навігації. Актуальність дослідження зумовлена відсутністю усталених підходів до UX/UI-проектування саме для україномовних медіасервісів.

У процесі проектування інтерфейсу веб-платформи для рецензування фільмів і серіалів було проведено аналіз досвіду користувачів провідних аналогів: IMDb, Letterboxd та Rotten Tomatoes. Встановлено, що основними проблемами є перевантаженість інформаційного простору, незручна система навігації за жанрами та відсутність адаптивних рішень для мобільних пристроїв у попередніх платформах. На основі отриманих даних сформовано перелік функціональних та нефункціональних вимог до інтерфейсу.

Проектування інтерфейсу здійснювалось відповідно до принципів користувацько-орієнтованого дизайну. На першому етапі розроблено персонажі користувачів та карти користувацького шляху, що дозволило визначити пріоритетні сценарії взаємодії: пошук фільму, написання рецензії, перегляд рекомендацій. На основі сценаріїв побудовано дротяні макети з подальшим уточненням у вигляді високодеталізованих прототипів.

Для реалізації фінального інтерфейсу обрано компонентний підхід на базі бібліотеки React, що дозволяє забезпечити узгодженість візуальної мови у всіх частинах застосунку. Розроблено власну дизайн-систему, що включає палітру кольорів, типографічну шкалу, набір UI-компонентів (кнопки, картки фільмів, форми рецензій, зірковий рейтинг) та правила їх поєднання. Застосування єдиної дизайн-системи скорочує час розробки нових екранів і підвищує передбачуваність інтерфейсу для кінцевого користувача.

Особливу увагу приділено адаптивності інтерфейсу. Макети розроблено для трьох контрольних точок: мобільні пристрої (до 768 px),

планшети (768–1024 px) та настільні комп'ютери (понад 1024 px). На рівні CSS застосовано методологію mobile-first із використанням гнучких сіткових систем. Для покращення доступності дотримано рекомендацій WCAG 2.1 щодо контрастності тексту, розмірів інтерактивних елементів та навігації за допомогою клавіатури.

Проведене юзабіліті-тестування прототипу за участю 12 цільових користувачів підтвердило відповідність розробленого інтерфейсу сформованим вимогам: середній час виконання типових завдань скоротився на 34% порівняно з аналогами, а показник задоволеності за шкалою SUS (System Usability Scale) склав 81,5 бала, що відповідає оцінці «добре». Отримані результати свідчать про ефективність застосованих підходів до UX/UI-проектування веб-платформ для медіаконтенту.

Список використаних джерел:

1. Nielsen J. *Usability Engineering* // Morgan Kaufmann (електронне видання). URL: <https://www.sciencedirect.com/book/9780125184069/usability-engineering> (дата звернення: 25.03.2026).
2. Brooke J. *SUS: A quick and dirty usability scale* // Usability Evaluation in Industry (електронна версія). URL: <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html> (дата звернення: 25.03.2026).
3. W3C. *Web Content Accessibility Guidelines (WCAG) 2.1*. URL: <https://www.w3.org/TR/WCAG21/> (дата звернення: 25.03.2026).
4. Cooper A., Reimann R., Cronin D. *About Face: The Essentials of Interaction Design* (електронне видання). URL: <https://www.wiley.com/en-us/About+Face%3A+The+Essentials+of+Interaction+Design%2C+4th+Edition-p-9781118766576> (дата звернення: 25.03.2026).

УДК 004.7

*Денисенко Д.О., здобувач,
Єфремов.Ю.М., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ВЕБ-ПЛАТФОРМА ДЛЯ РЕЦЕНЗУВАННЯ ФІЛЬМІВ ТА СЕРІАЛІВ

Останніми роками стримінгові сервіси розвиваються дуже швидко. Через це користувачам стає складніше знаходити потрібну інформацію для перегляду які зумовлюють потребу у зручних інструментах для структурованого пошуку, оцінювання та рецензування фільмів та серіалів. Існуючі платформи такі як IMDb та Letterboxd, охоплюють лише окремі аспекти взаємодії користувача з контентом і не завжди враховують потреби україномовної аудиторії. У зв'язку з цим актуальною є розробка веб-платформи, яка об'єднає функції рецензування та персоналізованих рекомендацій у єдиному середовищі.

Порівняльний аналіз наявних рішень виявив ряд характерних обмежень. IMDb орієнтований переважно на базу даних і не надає розширених інструментів для власних відгуків.

Letterboxd, попри розвинену соціальну складову, не підтримує детального структурованого рецензування та локалізованого контенту. Кінокритик та подібні вітчизняні ресурси мають застарілий інтерфейс і обмежені можливості фільтрації. Таким чином, існує запит на платформу, яка поєднає переваги зазначених систем, прибираючи їх недоліки.

Розроблена система реалізована за клієнт-серверною архітектурою. Клієнтська частина побудована на базі React із використанням компонентного підходу, що забезпечує модульність та зручність масштабування інтерфейсу. Серверна частина розроблена на платформі ASP.NET Core із застосуванням архітектурного шаблону REST API, що дозволяє чітко розмежувати бізнес логіку та рівень представлення даних. Взаємодія між клієнтом і сервером здійснюється через HTTP-запити у форматі JSON.

Для зберігання даних використовується реляційна СУБД Microsoft SQL Server. Структура бази даних включає сутності фільмів та серіалів, користувачів, рецензій, оцінок, жанрів і тегів. Між сутностями встановлено зв'язки типу “один до багатьох” та “багато до багатьох”, що дозволяє ефективно моделювати складні взаємозалежності предметної області. Для доступу до даних із серверного рівня застосовується Entity Framework Core із підходом Code First.

Алгоритм рекомендацій базується на методі колаборативної фільтрації з урахуванням контентних характеристик - так звана гібридна модель. На основі оцінок, виставлених користувачем, та жанрових уподобань системи формується персоналізований список рекомендацій. Рейтингова система передбачає можливість виставлення оцінки за 10-бальною шкалою, а також розгорнуте текстове рецензування з підтримкою структурованих критеріїв: сценарій, режисура, акторська гра, візуальна складова.

Розроблена платформа дозволяє користувачам вести особистий кіношоденник, публікувати рецензії, переглядати відгуки інших учасників спільноти та отримувати персоналізовані рекомендації. Практична цінність роботи полягає у створенні повноцінного україномовного інструменту для кіноаматорів, що поєднує функціональність міжнародних аналогів із адаптованим для локальної аудиторії контентом і зручним сучасним інтерфейсом.

Список використаних джерел:

1. Sarwar B., Karypis G., Konstan J., Riedl J. Item-based collaborative filtering recommendation algorithms [Електронний ресурс]. - Режим доступу: <https://dl.acm.org/doi/10.1145/371920.372071> (дата звернення: 20.03.2026).
2. Burke R. Hybrid recommender systems: Survey and experiments [Електронний ресурс]. - Режим доступу: <https://link.springer.com/article/10.1023/A:1021240730564> (дата звернення: 20.03.2026).
3. Microsoft. ASP.NET Core documentation [Електронний ресурс]. - Режим доступу: <https://learn.microsoft.com/aspnet/core> (дата звернення: 20.03.2026).
4. React. React documentation [Електронний ресурс]. - Режим доступу: <https://react.dev> (дата звернення: 20.03.2026).

УДК 004.7

*Петров Д.В., здобувач,
Єфремов Ю.М., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ВЕБ-ПЛАТФОРМА ЧИТАННЯ РАНОБЕ

Азійська проза, і ранобе зокрема, останніми роками знаходить дедалі більше читачів в Україні. Серійний формат, ілюстрації, регулярне поповнення нових розділів - усе це висуває особливі вимоги до платформ, на яких такий контент публікується. Якщо подивитися на україномовний інтернет, стає очевидно: якісних локалізованих майданчиків із нормальним функціоналом як для читачів, так і для перекладацьких команд - одиниці.

Розроблена платформа якраз і закриває цю нішу - тут можна читати вміст розділів без переходу на сторонні сайти, підлаштовувати інтерфейс під себе, не втрачати місце де зупинився та дізнаватися про свіжі розділи одразу після публікації. Для перекладачів передбачено окремий сторінка - з можливістю завантажувати контент і спілкуватися з аудиторією через коментарі.

Окрім базового функціоналу, варто відзначити кілька рішень, які суттєво відрізняють платформу від аналогів. По-перше, реалізовано систему колекцій - кожен користувач може створити власну добірку творів за будь-яким критерієм: характером головного героя, атмосферою чи темпом сюжету. Такі добірки публікуються у відкритому доступі, тож інші читачі можуть знаходити цікаві твори через рекомендації живих людей, а не лише через фільтри пошуку. По-друге, читач не втрачає прогрес навіть якщо несподівано закрив вкладку - система автоматично запам'ятовує останнє місце зупинки.

На етапі підготовки були вивчені три ресурси зі схожою тематикою: два українських - uAuthor і Baka.ua, та один міжнародний - NovelUpdates. Їх порівняння наведено в табл. 1.

Аналіз показав характерну слабкість українських ресурсів - більшість із них є або каталогами посилань, або форумами, але не повноцінними читалками. Розроблена платформа вирішує цей недостаток: вбудований рідер, розгалужена система жанрів для зручного пошуку. Окремо реалізовано кешування даних - завдяки цьому сторінки завантажуються швидко навіть при нестабільному інтернеті.

Таблиця 1

Порівняльна характеристика платформ для читання

Назва платформи	Функціонал	Зручність читання	Швидкість роботи	Локалізація
юАвтор (uAuthor)	Каталог посилань, спільноти	Низька (перехід на зовн. сайти)	Середня	Повна (Укр)
NovelUpdates	Глобальна база, трекінг	Середня (текст на різних ресурсах)	Висока	Англійська
Baka.ua	Блоги, новини, переклади	Середня (формат блогу)	Висока	Повна (Укр)

Веб-платформа створена засобами мови програмування **C#**, а саме фреймворку **ASP.NET Core**. Як систему керування базами даних обрано **Entity Framework Core**, що дозволяє ефективно працювати з великими обсягами текстових даних. Для забезпечення безпеки користувачів використано стандарт **JWT (JSON Web Token)**, що гарантує захищену авторизацію та збереження персональних налаштувань.

Список використаних джерел:

1. Автор - український портал перекладів контенту. [Електронний ресурс] - Режим доступу: <https://author.org.ua>
2. Baka.ua - українська аніме-спільнота та ранобе. [Електронний ресурс] - Режим доступу: <https://baka.ua>
3. NovelUpdates: Directory of translated Asian novels. [Електронний ресурс] - Режим доступу: <https://www.novelupdates.com>

УДК 004.7

*Петров Д.В., здобувач,
Єфремов Ю.М., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АРХІТЕКТУРА СИСТЕМИ ПЕРСОНАЛІЗАЦІЇ В ВЕБ-ПЛАТФОРМАХ ДЛЯ ЧИТАННЯ РАНОБЕ

Читання з екрана саме по собі навантажує зір, а якщо йдеться про ранобе з сотнями розділів - це відчувається вдвічі сильніше. До того ж орієнтуватися в такому обсязі без зручних інструментів навігації буває справді незручно. Саме тому сучасна платформа для читання мусить вирішувати не лише технічні питання швидкості, а й думати про те, наскільки комфортно конкретному користувачеві взаємодіяти з інтерфейсом.

У рамках роботи було розроблено модуль інтерактивного рідера, вбудованого безпосередньо у веб-платформу. Головна ідея полягала в тому, щоб дати читачеві змогу підлаштовувати вигляд сторінки під себе - змінювати колірну схему, відстань між рядками - і при цьому не перезавантажувати сторінку щоразу. Крім цього, окремо реалізовано функцію автозбереження місця читання з можливістю синхронізації між кількома пристроями.

Під час дослідження було розглянуто різні способи зберігання користувацьких налаштувань. Результати порівняння зведено в табл. 1.

За підсумками аналізу було обрано комбінований підхід: налаштування зовнішнього вигляду зберігаються у LocalStorage браузера - це забезпечує миттєву реакцію інтерфейсу - тоді як прогрес читання та список вподобань передаються на сервер через API. Такий підхід дає змогу не переривати читання навіть у тому випадку, коли користувач переходить на інший пристрій або очищає кеш браузера.

Окремо реалізовано функцію відновлення позиції в розділі - якщо читач не дочитав розділ до кінця і пізніше повернувся до нього, сторінка автоматично прокручується до того місця, де він зупинився. Це позбавляє від необхідності вручну шукати потрібний абзац і робить повернення до читання природним продовженням, а не черговим пошуком по тексту.

Таблиця 1

Порівняння методів зберігання користувацьких даних

Метод зберігання	Швидкість доступу	Синхронізація між пристроями	Навантаження на сервер
LocalStorage	Максимальна	Відсутня	Нульове
Cookies	Середня	Часткова	Низьке
Database	Нижч	Повна	Середнє

Технічна реалізація серверної частини базується на використанні **ASP.NET Core Web API**. Для забезпечення високої швидкості вибірки розділів із бази даних застосовано асинхронні запити через **Entity Framework Core**. Клієнтська частина використовує сучасні механізми **Tailwind CSS** для миттєвої зміни теми оформлення, що мінімізує використання ресурсів процесора на мобільних пристроях.

Список використаних джерел:

1. Документація ASP.NET Core Web API. [Електронний ресурс] - Режим доступу: <https://learn.microsoft.com/en-us/aspnet/core/web-api/>
2. Use of LocalStorage for User Preferences. [Електронний ресурс] - Режим доступу: <https://developer.mozilla.org/en-US/docs/Web/API/Window/localStorage>
3. Дизайн-патерни в розробці інтерфейсів для читання. [Електронний ресурс] - Режим доступу: <https://uxdesign.cc/>

УДК 004.7

*Мінайленко В.Ю., здобувач,
Єфремов Ю.М., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ВЕБПЛАТФОРМА ДЛЯ ТОРГІВЛІ ГОДИННИКАМИ ТА АКСЕСУАРАМИ З ПІДТРИМКОЮ АУКЦІОНУ ТА ОБМІНУ

Сьогодні колекціонери годинників все частіше шукають чесні ціни та надійні способи купівлі-продажу. Люди хочуть розуміти, за що вони платять, і бути впевненими у безпеці кожної угоди. Популярні платформи на кшталт eBay чи Chrono24 орієнтовані на мас-маркет. Справжнім колекціонерам важливо знати, з ким вони мають справу. Крім того, на великих маркетплейсах майже неможливо реалізувати прямий обмін лотами або домовитися про вигідний бартер, який так цінують професійні колекціонери.

Моя мета - розробити платформу для колекціонерів годинників. Це буде єдине місце, де можна купити, продати або просто обмінятися лотами. Головний акцент я роблю на безпеці. Кожен користувач та кожен годинник будуть проходити ретельну перевірку.

Головна частина платформи - відкриті торги. Видно, як інші роблять ставки, і можна пропонувати свою ціну. Переможцем стає той, чия ставка буде найвищою на момент зупинки таймера. Заздалегідь видно початкову вартість та на скільки мінімум можна підняти ставку. За технічну частину відповідає сервер на Node.js. Він працює так, що дві однакові ставки ніколи не пройдуть одночасно. Система чітко фіксує кожну дію. Завдяки технології WebSocket ви бачите всі зміни миттєво. Не треба постійно оновлювати сторінку, бо нові ставки з'являються на екрані самі.

Окрім звичайного аукціону платформа пропонує зручний формат прямого обміну. Кожен продавець має можливість позначити свій годинник як доступний для бартеру. При цьому можна одразу вказати список моделей або конкретних брендів на заміну. Зацікавлені користувачі надсилають свої пропозиції через вбудований чат для обговорення всіх деталей майбутньої угоди. Можливість поєднувати звичайні грошові розрахунки та прямий обмін товарами в одному місці є головною перевагою проекту серед інших сайтів.

Для надійної перевірки кожного лота було впроваджено систему обов'язкового завантаження якісних знімків та детального опису годинника. Всі користувачі заповнюють для цього спеціальну стандартну форму. Адміністратор платформи уважно звіряє вказану інформацію із фотографіями та підтверджує оголошення лише після

повної перевірки. Такий підхід допомагає суттєво знизити будь-які ризики шахрайства та значно підвищує рівень довіри покупців. Крім того, кожен зареєстрований продавець має власну відкриту сторінку. На ній відображається його рейтинг та реальні відгуки, які формуються лише на основі вже успішно завершених угод.

Для користувачів було створено багатофункціональний сайт із продуманим особистим кабінетом. У цьому розділі можна зручно керувати всіма своїми діями на платформі. Там надійно зберігається повна історія ваших ставок та список усіх активних оголошень. Також у кабінеті дуже легко відстежувати статус поточних переговорів щодо обміну годинниками з іншими учасниками спільноти. Основна частина системи побудована на базі сучасних інструментів Node.js та Express. Для надійного зберігання всієї інформації про лоти та профілі ми обрали гнучку базу даних MongoDB. Увесь проєкт був написаний на мові TypeScript. Це дозволяє уникати помилок у коді ще на етапі розробки та гарантує стабільну роботу всього сервісу. Використання спільних моделей даних для зовнішньої та внутрішньої частин сайту значно прискорює створення нових функцій для колекціонерів.

Практична цінність розробки полягає у створенні спеціалізованого майданчика, орієнтованого на потреби нішевої аудиторії колекціонерів, де прозорість механізму ціноутворення, можливість бартеру та система довіри між учасниками реалізовані в комплексі. Запропоновані архітектурні рішення можуть бути адаптовані для побудови аналогічних платформ в інших колекційних сегментах.

Список використаних джерел:

1. Kleppmann M. Designing Data-Intensive Applications [Електронний ресурс]. - Режим доступу: <https://www.oreilly.com/library/view/designing-data-intensive-applications/9781491903063/> (дата звернення: 20.03.2026).
2. Fenton N. Real-Time Web Application Development [Електронний ресурс]. - Режим доступу: <https://www.packtpub.com/product/real-time-web-application-development/9781788295666> (дата звернення: 20.03.2026).
3. Krishna V., Ramana Rao M. Auction Theory [Електронний ресурс]. - Режим доступу: <https://www.elsevier.com/books/auction-theory/krishna/978-0-12-426295-9> (дата звернення: 20.03.2026).
4. MongoDB. Documentation: The Multi-cloud Developer Data Platform [Електронний ресурс]. - Режим доступу: <https://www.mongodb.com/docs/> (дата звернення: 20.03.2026).

УДК 004.7

*Мінайленко В.Ю., здобувач,
Єфремов Ю.М., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ПРОЄКТУВАННЯ КЛІЄНТСЬКОЇ ЧАСТИНИ ВЕБПЛАТФОРМИ ДЛЯ ТОРГІВЛІ ГОДИННИКАМИ НА ОСНОВІ БІБЛІОТЕКИ REACT

Успіх будь-якого сучасного сайту насамперед залежить від того, наскільки зручно ним користуватися. Для спеціалізованих торгових платформ це питання є критично важливим. Кожен відвідувач має швидко знаходити потрібні речі в каталозі та легко керувати своїми оголошеннями. Також дуже важливо, щоб користувачі могли без жодних затримок стежити за змінами цін під час активних аукціонів. Особливу увагу було приділено вибору технологій для розробки зовнішньої частини проєкту. Це безпосередньо впливає на те, наскільки швидко працюватиме інтерфейс та наскільки стабільно він буде виконувати свої функції. Правильно підібрані інструменти допомагають нам зробити сайт не лише швидким для користувачів, а й зручним для подальшого оновлення та підтримки.

Зовнішній інтерфейс було побудовано на основі бібліотеки React. Головна перевага такого підходу полягає в тому, що весь інтерфейс можна розділити на окремі та незалежні частини. Це можуть бути картки товарів, форми для виставлення нових лотів, блоки зі ставками аукціону або зручні фільтри для пошуку в каталозі. Кожна така частина працює самостійно та містить у собі власну логіку та зовнішній вигляд. Це значно спрощує перевірку роботи всього сайту та дозволяє нам легко додавати нові функції в майбутньому. Такий підхід робить додаток дуже гнучким, адже ми можемо повторно використовувати готові елементи на різних сторінках. Це економить час при розробці та допомагає підтримувати єдиний стиль усього проєкту.

Управління станом застосунку реалізовано за допомогою хуків React (useState, useEffect, useContext). Для даних, що потребують спільного доступу з різних частин інтерфейсу - зокрема інформації про авторизованого користувача та вмісту кошика було застосовано Context API. Такий підхід дозволяє уникнути надмірної передачі пропсів між рівнями компонентів і зберігає код читабельним.

Для переходу між сторінками нашого застосунку ми обрали вбудовану систему маршрутизації від Next.js. Такий підхід значно відрізняється від класичних односторінкових сайтів. Кожна сторінка завантажується окремо, що дозволяє пошуковим системам краще

бачити контент сайту. Захищені маршрути (особистий кабінет, форма виставлення лота) доступні лише автентифікованим користувачам перевірка здійснюється на рівні компонента-обгортки перед рендерингом цільової сторінки.

Для забезпечення точного відліку часу та стабільної роботи інтерфейсу було розроблено спеціальні програмні компоненти. Вони автоматично оновлюють інформацію на екрані через чітко визначені проміжки часу. Також передбачено механізм зупинки цих процесів, коли користувач переходить у інший розділ сайту. Це допомагає не перевантажувати пам'ять пристрою та робить роботу всього сервісу плавною і надійною. Такий підхід гарантує, що кожен колекціонер завжди бачить актуальну інформацію про свої лоти та угоди.

Адаптивний дизайн платформи забезпечено за допомогою CSS-модулів та медіазапитів, що гарантує коректне відображення на пристроях з різними розмірами екранів. Каталог товарів реалізовано у вигляді сітки карток з динамічною зміною кількості стовпців залежно від ширини вікна перегляду. Форми введення даних валідуються на стороні клієнта перед відправкою запиту до серверу.

Взаємодія з серверною частиною здійснюється через REST API з використанням бібліотеки Axios. Запити до захищених ендпоінтів автоматично доповнюються JWT-токеном через axios-інтерцептор, що централізує логіку авторизації та виключає необхідність її дублювання в кожному сервісному методі. Обробка помилок мережевих запитів реалізована глобально на рівні інтерцептора відповідей.

Застосування бібліотеки React у поєднанні з описаними підходами до організації стану та маршрутизації забезпечує високу швидкість відклику інтерфейсу та зручність для кінцевого користувача. Подальший розвиток клієнтської частини передбачає впровадження серверного рендерингу (Next.js) для покращення SEO-показників платформи.

Список використаних джерел:

1. Meta Open Source. React Documentation: Tutorial: Tic-Tac-Toe [Електронний ресурс]. - Режим доступу: <https://react.dev/learn/tutorial-tic-tac-toe> (дата звернення: 20.03.2026).
2. Dodds K. C. Epic React [Електронний ресурс]. - Режим доступу: <https://epicreact.dev> (дата звернення: 20.03.2026).
3. Wieruch R. The Road to React [Електронний ресурс]. - Режим доступу: <https://www.roadtoreact.com> (дата звернення: 18.03.2026).
4. Fielding R. T. Architectural Styles and the Design of Network-based Software Architectures: PhD thesis [Електронний ресурс]. - Режим доступу: <https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm> (дата звернення: 20.03.2026).

СЕКЦІЯ 2 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 004.774:535.14:530.182

Калашнікова Ю.В., асистент

Національний університет

«Полтавська політехніка ім. Ю. Кондратюка»

НЕЛІНІЙНІ ХВИЛЬОВІ МЕХАНІЗМИ ПЕРЕДАВАННЯ ТА ОБРОБКИ ІНФОРМАЦІЇ В КВАНТОВО-ФОТОННИХ МЕРЕЖАХ

Стрімкий розвиток квантово-фотонних мереж формує нову парадигму побудови інформаційно-комунікаційних систем, у межах якої передавання та обробка інформації здійснюються безпосередньо на фізичному рівні взаємодії фотонних полів. Зростаючі вимоги до пропускнуєї здатності, енергоефективності та квантової безпеки стимулюють відхід від традиційних лінійних моделей комунікаційних каналів і зумовлюють необхідність використання нелінійних хвильових підходів.

У квантово-фотонних мережах інформаційні потоки реалізуються через поширення когерентних фотонних станів у складно структурованих середовищах, де динаміка сигналів визначається багатомодовими взаємодіями, нелінійною дисперсією та параметричною перебудовою властивостей середовища. За таких умов нелінійність перестає бути другорядним ефектом і набуває статусу системоутворюючого чинника, що визначає режими функціонування мережі.

На відміну від класичних оптичних мереж, квантово-фотонні архітектури допускають цілеспрямовану інженерну реалізацію ефективних нелінійних взаємодій між фотонними модами. Це досягається шляхом використання інтегрованих фотонних платформ, резонаторних структур із високим фактором якості, фотонних кристалів та квантових матеріалів із керованими нелійними властивостями.

Нелінійні хвильові ефекти, зокрема багатохвильове змішування, параметричне підсилення та керована дисперсія, створюють фізичні механізми для спектрального, часового та модового кодування інформації. Таким чином, фотонне середовище одночасно виконує функції каналу передавання та обчислювального середовища, що принципово відрізняє квантово-фотонні мережі від класичних телекомунікаційних систем. [1].

Аналітичний огляд сучасних досліджень свідчить про еволюцію підходів від аналізу локальних нелінійних ефектів до опису колективної хвильової динаміки в масштабованих квантово-фотонних мережах. У цьому контексті нелінійність розглядається як фундаментальний ресурс, що забезпечує внутрішню обробку інформації на рівні фізичної динаміки фотонних полів.

Завдяки цьому стає можливим реалізовувати операції фільтрації, маршрутизації, кореляційного аналізу та логічних перетворень без залучення зовнішніх класичних обчислювальних модулів. Такий підхід знижує затримки обробки, підвищує енергоефективність системи та створює передумови для побудови компактних і масштабованих мереж із розширеною функціональністю [2].

Важливим аспектом функціонування квантово-фотонних мереж є збереження когерентності квантових станів в умовах багатомодової нелінійної взаємодії. Нелінійна хвильова динаміка безпосередньо впливає на кореляційні властивості фотонних полів, що вимагає поєднання нелінійних хвильових рівнянь із квантово-статистичним описом станів системи.

Розроблення узагальнених математичних моделей, які враховують ці аспекти, є необхідною умовою для коректного аналізу стійкості, керованості та інформаційної ємності квантово-фотонних мереж. Такі моделі активно розвиваються в межах міжнародних дослідницьких програм у сфері квантових технологій. [3].

Узагальнюючи, можна з впевненістю стверджувати, що нелінійні хвильові механізми передавання та обробки інформації формують фундаментальну основу для створення квантово-фотонних мереж нового покоління. Подальший розвиток цього напрямку пов'язаний із поглибленням теорії нелінійної квантової фотоніки, розробкою керованих фотонних середовищ та інтеграцією таких механізмів у масштабовані мережеві та обчислювальні архітектури з розширеною функціональністю.

Список використаних джерел

1. Engineering non-linear optical interactions in integrated photonics / K. E. Perego [et al.] // *Nature Photonics*. 2024. Vol. 18. P. 165–173. URL: www.nature.com.
2. Quantum Charging Advantage in Superconducting Solid-State Batteries / Chang-Kang Hu, Chilong Liu, Jingchao Zhao et al. *Phys. Rev. Lett.* 2026. Vol. 136, iss. 6. Art. 060401. 9 p. DOI: <https://doi.org/10.1103/sp5l-c6m8>. URL: <https://link.aps.org/doi/10.1103/sp5l-c6m8>.
3. The future is Quantum / Quantum Technologies Flagship : [Електронний ресурс]. URL: <https://qt.eu/>.

УДК 004.7

Баленко Г. І., здобувач

Дячук О. Ю., ст. викладач

Окунькова О.О., ст. викладач

Державний університет «Житомирська політехніка»

ПІДХОДИ UTM ТА SECURITY FABRIC У ГЕТЕРОГЕННИХ МЕРЕЖЕВИХ СЕРЕДОВИЩАХ: ПОРІВНЯЛЬНИЙ АНАЛІЗ CISCO-РІШЕНЬ ТА OPEN-SOURCE СТЕКУ

Сучасні корпоративні мережі функціонують в умовах стрімкого зростання обсягів трафіку, ускладнення інфраструктур та постійного розвитку кіберзагроз. Використання ізольованих засобів захисту не забезпечує достатнього рівня керованості та швидкості реагування на інциденти, що зумовлює перехід до інтегрованих підходів кібербезпеки. До таких підходів належать концепції Unified Threat Management (UTM) та Security Fabric, які відрізняються архітектурою, рівнем інтеграції та підходами до обробки подій безпеки.

Проблемою дослідження є відсутність узгодженого підходу до інтеграції засобів безпеки у гетерогенних середовищах, що ускладнює централізоване управління та знижує ефективність реагування на інциденти.

Підхід UTM передбачає консолідацію основних механізмів захисту – міжмережевого екрану, VPN, IDS/IPS, фільтрації контенту та контролю застосунків – у межах одного пристрою або програмного вузла. Основною перевагою цього підходу є централізоване адміністрування та спрощене розгортання, однак він має обмеження у масштабованості та гнучкості інтеграції.

На відміну від UTM, концепція Security Fabric базується на взаємодії розподілених компонентів безпеки, що обмінюються телеметрією, подіями та політиками через стандартизовані інтерфейси (API, syslog). Такий підхід забезпечує централізовану кореляцію подій та автоматизоване реагування на інциденти.

У пропрієтарному середовищі ці принципи реалізуються в екосистемі Cisco, зокрема через рішення Cisco XDR, Security Cloud Control, Secure Firewall, Umbrella та Identity Services Engine (ISE). Варто зазначити, що платформа SecureX, яка раніше виконувала роль централізованого рівня інтеграції, поступово замінюється новішими рішеннями, такими як Cisco XDR та Security Cloud Control.

Альтернативою пропрієтарним рішенням є open-source стек, який дозволяє реалізувати подібні функції без значних ліцензійних витрат. До таких компонентів належать:

- **pfSense/OPNsense** – міжмережеві екрани з підтримкою VPN та IDS/IPS;

- **Snort/Suricata** – системи виявлення та запобігання вторгненням;

- **Wazuh** – платформа збору та кореляції подій безпеки;
- **ELK Stack** (Elasticsearch, Logstash, Kibana) – засоби аналізу та візуалізації логів;

- **Ansible** – інструмент автоматизації реагування.

Використання такого стеку дозволяє відтворити ключові принципи Security Fabric, зокрема централізований збір подій, їх кореляція та автоматизоване реагування.

Аналіз підходів UTM та Security Fabric дозволяє визначити їх принципів відмінності з точки зору архітектури та рівня інтеграції.

UTM реалізує централізовану модель безпеки, у якій функції захисту зосереджені в одному вузлі. Це забезпечує простоту розгортання, передбачувану продуктивність та зручність адміністрування, однак обмежує можливості масштабування та інтеграції з зовнішніми системами.

Security Fabric, навпаки, базується на розподіленій архітектурі, де окремі компоненти взаємодіють через API та механізми обміну подіями. Це дозволяє підвищити рівень автоматизації, забезпечити гнучке масштабування та адаптацію політик безпеки в реальному часі.

У Cisco-рішеннях інтеграція досягається за рахунок єдиної екосистеми, що забезпечує високу узгодженість компонентів. У відкритому стеку інтеграція реалізується шляхом поєднання різних інструментів, що підвищує гнучкість, але ускладнює налаштування.

Таким чином, відмінність між підходами полягає не лише у структурі, але й у рівні автоматизації, масштабованості та можливості інтеграції в багаторівневих системах безпеки.

Для дослідження запропоновано лабораторну модель у середовищах GNS3 або EVE-NG, що включає:

- firewall (Cisco ASA/Secure Firewall або pfSense);
- DMZ-сегмент для генерації трафіку;
- IDS/IPS (Snort або Suricata);
- SIEM-рівень (Wazuh + ELK);
- систему автоматизації (Ansible).

Обмін подіями між компонентами здійснюється через syslog та API.

Передбачено два сценарії:

1. Порівняння UTM-рішень (Cisco vs pfSense/OPNsense);
2. Моделювання Security Fabric у відкритому середовищі.

Для узагальнення результатів аналізу сформовано концептуальну модель очікуваних характеристик досліджуваних підходів.

Таблиця 1

Архітектурне порівняння

Критерій	Cisco	Open-source
Простота розгортання	Висока	Середня
Централізація	Висока	Середня
Гнучкість	Обмежена	Висока
Автоматизація	Висока	Середня–висока
Вартість	Висока	Низька

Таблиця 2

Очікувані метрики

Метрика	UTM	Security Fabric
Продуктивність	Висока	Середня
Latency	Низька	Середня
Час реагування	Середній	Низький
Автоматизація	Середня	Висока

Наведені оцінки мають аналітичний характер і можуть бути використані як основа для подальшої експериментальної верифікації.

Очікуваним ефектом запропонованого підходу є можливість дослідження динаміки поширення подій безпеки між вузлами мережі, аналіз часу реакції системи на інциденти, а також оцінка рівня інтеграції між відкритими та пропрієтарними компонентами в умовах гетерогенного середовища.

Реалізація наведених сценаріїв дозволить:

- сформувані відкрите середовище для тестування концепції Security Fabric без потреби в ліцензіях Cisco;
- розробити навчально-дослідну модель інтегрованої системи безпеки для університетських лабораторій;
- створити методику порівняльного аналізу ефективності open-source і пропрієтарних UTM/Security Fabric систем;
- обґрунтувати доцільність гібридних підходів (Cisco + open-source) у реальних корпоративних середовищах;
- дослідити вплив рівня автоматизації на швидкість реагування на інциденти;
- оцінити ефективність використання SIEM-систем для кореляції подій у гетерогенних архітектурах;
- визначити роль API та NetDevOps-підходів у забезпеченні узгодженої роботи компонентів безпеки.

Перспективи подальших досліджень полягають у проведенні експериментальної оцінки ефективності запропонованої моделі, зокрема:

- вимірюванням продуктивності систем;

- аналізом точності виявлення атак (False Positive/False Negative);
- дослідженням адаптивних політик безпеки на основі автоматизованого реагування;
- інтеграцією моделей машинного навчання для підвищення ефективності виявлення аномалій.

Підхід UTM забезпечує простоту адміністрування та стабільність функціонування, однак поступається підходу Security Fabric у гнучкості інтеграції та рівні автоматизації. Архітектури типу Security Fabric дозволяють ефективніше поєднувати різномірні компоненти безпеки та реалізовувати адаптивне реагування на інциденти.

Запропонована лабораторна модель створює основу для дослідження інтегрованих систем кібербезпеки у гетерогенних середовищах та може бути використана у навчальному процесі.

У межах проведеного дослідження сформовано аналітичну модель і дизайн експерименту, а практична перевірка запропонованого підходу розглядається як наступний етап дослідження.

Список використаних джерел

1. Siddiqui A., Rimal B. P., Reisslein M., Wang Y. Survey on Unified Threat Management (UTM) Systems for Home Networks. IEEE Communications Surveys & Tutorials. 2024. URL: <https://doi.org/10.1109/COMST.2024.3382470>
2. Cisco Systems. Cisco XDR – Product Overview. URL: <https://www.cisco.com/site/us/en/products/security/xdr/index.html>
3. Cisco Systems. Security Cloud Control Firewall Management Documentation. URL: <https://www.cisco.com/site/us/en/products/security/firewalls/index.html>
4. Cisco Systems. Cisco Secure Firewall Documentation. URL: <https://www.cisco.com/site/us/en/products/security/firewalls/index.html>
5. Netgate. pfSense Documentation: Remote Logging with Syslog. URL: <https://docs.netgate.com/pfsense/en/latest/monitoring/logs/remote.html>
6. OPNsense. Intrusion Prevention System (IPS) Documentation. URL: <https://docs.opnsense.org/manual/ips.html>
7. Wazuh. Log Data Collection Capabilities. URL: <https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection>
8. Wazuh. Integration with Network IDS (Suricata). URL: <https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html>
9. Chauhan M. A., Babar M. A., Rabhi F. SecDOAR: A Software Reference Architecture for Security Data Orchestration, Analysis and Reporting. arXiv. 2024. URL: <https://arxiv.org/abs/2408.12904>
10. Davies T., Eiza M. H., Shone N., Lyon R. A Collaborative Intrusion Detection System Using Snort IDS Nodes. arXiv. 2025. URL: <https://arxiv.org/abs/2504.16550>
11. Pitkar H. Cloud Security Automation Through Symmetry: Threat Detection and Response. Symmetry. 2025. URL: <https://doi.org/10.3390/sym17060859>

УДК 004.7

*Приходько Д.С., здобувач
Дячук О.Ю., ст. викладач*

Державний університет «Житомирська політехніка»

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІТ-ІНФРАСТРУКТУРИ НА ОСНОВІ OPENVAS

У сучасних умовах розвитку інформаційних технологій забезпечення кібербезпеки є одним із ключових завдань функціонування ІТ-інфраструктури. Вразливість визначається як недолік або слабкість активу, що може бути використана загрозою для порушення конфіденційності, цілісності або доступності інформації. Еволюція підходів до класифікації вразливостей пройшла шлях від базових таксономій до сучасних стандартів, зокрема Common Weakness Enumeration (CWE), який пропонує ієрархічну структуру типових помилок [2]. Значну роль у формуванні сучасного розуміння загроз відіграє OWASP Top 10, що акцентує увагу на першопричинах вразливостей та помилках у конфігурації систем [1].

Актуальність дослідження зумовлена зростанням кількості кіберзагроз, ускладненням ІТ-інфраструктур та необхідністю впровадження ефективних засобів виявлення вразливостей, особливо в умовах використання гібридних і розподілених середовищ.

Метою дослідження є аналіз сучасних методів виявлення вразливостей ІТ-інфраструктури та оцінка можливостей платформи OpenVAS у порівнянні з комерційними рішеннями.

Для забезпечення контролю стану безпеки активів застосовуються різні підходи до сканування [5]:

1. **Активне сканування**, що передбачає ініціювання взаємодії з цільовими системами з метою отримання детальної інформації про їхній стан. Такий підхід забезпечує високу точність виявлення, однак може створювати додаткове навантаження на мережеву інфраструктуру. Для поглибленого аналізу також застосовується агентний підхід.

2. **Пасивний аудит**, який базується на аналізі копій мережевого трафіку без безпосереднього втручання в роботу систем. Його перевагою є непомітність, проте можливості обмежуються лише виявленням вразливостей, що проявляються в мережевій активності.

3. **Тестування на проникнення (penetration testing)**, яке використовується для перевірки реальної експлуатованості виявлених вразливостей та зменшення кількості хибнопозитивних результатів.

Аналіз сучасного ринку засобів виявлення вразливостей показує, що він представлений як комерційними, так і відкритими рішеннями. Серед комерційних продуктів варто виділити Nessus, який

характеризується широкою базою перевірок та високою точністю результатів, а також Qualys VMDR, що реалізує хмарний підхід до управління вразливостями [3]. Водночас такі рішення можуть мати обмеження, пов'язані з вартістю використання та залежністю від інфраструктури постачальника.

Платформа OpenVAS є відкритим рішенням для сканування вразливостей, яке забезпечує достатній рівень виявлення для більшості типових ІТ-середовищ. За даними порівняльних досліджень, рівень виявлення окремих віддалених вразливостей для OpenVAS може становити близько **43%**, тоді як у комерційних рішень цей показник досягає **67–71%** [4]. Водночас для типових корпоративних середовищ ефективність виявлення може досягати **85–90%**, що підтверджує можливість практичного використання системи [4].

Незважаючи на зазначені відмінності, OpenVAS дозволяє ефективно здійснювати базовий аудит безпеки та адаптувати механізми перевірки за рахунок використання відкритого коду.

Важливою перевагою OpenVAS є можливість розгортання в ізолюваних середовищах, що забезпечує контроль над даними та відповідає вимогам інформаційного суверенітету. Крім того, відсутність ліцензійних витрат знижує загальну вартість володіння системою.

У результаті проведеного аналізу встановлено, що сучасні підходи до забезпечення кібербезпеки потребують переходу від периметрального захисту до безперервного моніторингу стану активів. Комерційні рішення забезпечують високий рівень автоматизації та точності, однак можуть бути обмежені економічними та організаційними чинниками. Водночас OpenVAS може розглядатися як ефективний інструмент для виявлення вразливостей, який забезпечує баланс між функціональністю, економічною доцільністю та контролем над даними.

Список використаних джерел

1. OWASP Foundation. OWASP Top Ten Web Application Security Risks. URL: <https://owasp.org/www-project-top-ten/>
2. MITRE. **Common Weakness Enumeration (CWE)**. URL: <https://cwe.mitre.org>
3. SenseLearner. Best Vulnerability Scanners: OpenVAS, Nessus & Qualys. URL: <https://senselearner.com/best-vulnerability-scanners-openvas-nessus-qualys/>
4. Pentest-Tools. A comprehensive benchmark of network vulnerability scanners 2024. URL: <https://pentest-tools.com/benchmarks/network-vulnerability-scanners-benchmark-2024.pdf>
5. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical Guide to Information Security Testing and Assessment. – NIST SP 800-115. <https://csrc.nist.gov/pubs/sp/800/115/final>

УДК 004.738.5:004.056

Онищук О.О., к.т.н., доцент

Волинський національний університет імені Лесі Українки

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ SEO-ОПТИМІЗАЦІЇ ВЕБ РЕСУРСІВ НА БАЗІ CMS WORDPRESS

Вступ. Розвиток цифрового середовища та стрімке зростання кількості веб ресурсів суттєво підвищили рівень конкуренції у пошукових системах. У сучасних умовах наявність вебсайту не гарантує його ефективності, оскільки ключовим чинником успіху стає видимість ресурсу у пошуковій видачі. Саме тому пошукова оптимізація (SEO) є одним із базових інструментів цифрового маркетингу, що забезпечує залучення цільової аудиторії та формування стабільного органічного трафіку.

Система управління контентом WordPress посідає провідні позиції серед платформ для створення веб ресурсів різної складності. Її популярність зумовлена відкритим програмним кодом, масштабованістю, широкими можливостями кастомізації та активною спільнотою розробників. Важливою перевагою WordPress є початкова орієнтація на вимоги пошукових систем, що створює сприятливі передумови для реалізації ефективної SEO-стратегії.

Метою є дослідження можливостей CMS WordPress у контексті SEO-оптимізації веб ресурсів та аналіз впливу технічних і контентних рішень на ефективність функціонування сайтів у цифровому середовищі. SEO-оптимізація (Search Engine Optimization) являє собою сукупність методів і підходів, спрямованих на підвищення позицій веб ресурсу у результатах пошукової видачі. Основним завданням SEO є підвищення релевантності веб сторінок запитам користувачів і забезпечення коректної індексації контенту пошуковими системами.

У сучасній практиці SEO умовно поділяється на технічну оптимізацію, оптимізацію контенту та структурну оптимізацію. Технічна складова охоплює питання швидкодії, безпеки, адаптивності та доступності ресурсу. Контентна оптимізація спрямована на створення якісного інформаційного наповнення, що відповідає потребам користувачів і вимогам пошукових алгоритмів. Структурна оптимізація забезпечує логічну побудову сайту, ефективну внутрішню навігацію та коректний розподіл ваги між сторінками.

Результати. У межах дослідження було проведено поетапний аналіз веб ресурсу, створеного на базі CMS WordPress, з метою оцінки впливу SEO-налаштувань на його технічні та поведінкові показники. Аналіз охоплював стан веб ресурсу до впровадження пошукової оптимізації та після реалізації комплексу технічних і контентних SEO-рішень. На першому етапі проведено аудит технічного стану веб

ресурсу, який виявив проблеми з метаданими, відсутність XML-карти сайту та недостатню оптимізацію медіафайлів, що негативно впливає на швидкодію й індексацію. На наступних етапах реалізовано комплекс SEO-налаштувань у середовищі WordPress та здійснено повторний аналіз, який підтвердив покращення ключових технічних і поведінкових показників сайту.

Таблиця 1 – Порівняльна характеристика стану веб ресурсу

Показник	До оптимізації	Після оптимізації
Час завантаження сторінки	3,8 с	1,7 с
Частка проіндексованих сторінок	61 %	95 %
Органічний трафік	Низький	Стабільне зростання
Показник відмов	Високий	Помірний

Отримані результати засвідчили суттєве скорочення часу завантаження сторінок, зростання частки проіндексованих сторінок і покращення поведінкових показників користувачів. Зафіксовано стабільне зростання органічного трафіку, що підтверджує ефективність впроваджених SEO-рішень.

Висновки. У результаті проведеного дослідження встановлено, що SEO-оптимізація веб ресурсів із використанням CMS WordPress є ефективним інструментом підвищення їх видимості у пошукових системах і залучення органічного трафіку. Платформа WordPress надає достатній набір технічних і функціональних можливостей для реалізації комплексної SEO-стратегії без використання складних програмних рішень.

Дослідження підтвердило, що поєднання технічної оптимізації, якісного контенту та структурного впорядкування сайту сприяє покращенню швидкодії, індексації сторінок і поведінкових показників користувачів. Комплексний підхід до пошукової оптимізації є необхідною умовою забезпечення конкурентоспроможності вебресурсів у сучасному цифровому середовищі.

Список використаних джерел

1. **Google Search Central.** Search Engine Optimization (SEO) Starter Guide. – Режим доступу: <https://developers.google.com/search/docs/fundamentals/seo-starter-guide>
2. **Fishkin R.** The Beginner's Guide to SEO. – Moz, 2021. – Режим доступу: <https://moz.com/beginners-guide-to-seo>
3. **Search Engine Journal.** SEO Trends 2022–2024. – Режим доступу: <https://www.searchenginejournal.com/category/seo/>
4. **Clarke J.** SEO 2022: Learn Search Engine Optimization. – Режим доступу: <https://learningseo.io/>
5. **WordPress.org.** WordPress Documentation. – Режим доступу: <https://wordpress.org/documentation/>
6. **Yoast.** SEO for WordPress Documentation. – Режим доступу: <https://yoast.com/wordpress-seo/>
7. **Google PageSpeed Insights.** Documentation. – Режим доступу: <https://developers.google.com/speed/docs/insights/v5/about>

УДК 004.932:519.676.8:004.5

Фесенко Т.М., к.т.н., доцент

Національний університет

«Полтавська політехніка ім. Юрія Кондратюка»

КВАНТОВО-КЛАСИЧНІ ГІБРИДНІ АЛГОРИТМИ РОЗВ'ЯЗУВАННЯ НЕЛІНІЙНИХ ЗАДАЧ У ВИСОКОПРОДУКТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні електронно-комунікаційні системи оборонного та кібербезпекового призначення функціонують в умовах багатофакторної динамічної невизначеності. При цьому їх формування здійснюється під впливом активних деструктивних дій противника, стохастичних флуктуацій параметрів каналів зв'язку, варіативності топології мереж, а також обмеженості обчислювальних, енергетичних і часових ресурсів. Для таких систем характерними є жорсткі вимоги до латентності обробки даних, гарантованої доступності сервісів та забезпечення криптографічної стійкості в умовах адаптивних атак. Невизначеність має як структурний, так і параметричний характер, що зумовлює необхідність використання формалізованих моделей із врахуванням нелінійної динаміки, стохастичних збурень і часткової спостережуваності станів.

Значна частина прикладних завдань, зокрема захист транспортних мереж, адаптивного розподілу мережесих ресурсів, ідентифікації та прогнозування кіберзагроз, а також синтезу й оптимізації криптографічних протоколів формалізується у вигляді багатокритеріальних нелінійних задач оптимізації або задач керування високої розмірності [1]. Такі постановки часто супроводжуються наявністю обмежень типу реального часу, невибухлих функціоналів якості та складних кореляційних залежностей між параметрами, що суттєво ускладнює застосування традиційних детермінованих або лінійних методів аналізу. У результаті виникає потреба в обчислювальних підходах, здатних ефективно працювати з великими просторами станів і забезпечувати прискорений пошук квазіоптимальних рішень.

У цьому контексті перспективним напрямом є використання квантово-класичних гібридних алгоритмів [2], зокрема варіаційних підходів, які передбачають інтеграцію квантових обчислювальних модулів у контур класичної високопродуктивної інфраструктури. Архітектурно такі рішення реалізуються за принципом розподілу обчислювального навантаження, тоді як класична підсистема здійснює

параметричну оптимізацію, агрегацію результатів, контроль збіжності та інтеграцію з прикладними сервісами.

Застосування гібридних алгоритмів дозволяє поєднати потенційні обчислювальні переваги квантових примітивів, зокрема паралелізм у просторі станів і можливість апроксимації складних нелінійних залежностей із надійністю, масштабованістю, керованістю та відпрацьованими механізмами відмовостійкості класичних платформ. Зазначене створює передумови для підвищення ефективності розв'язання задач криптоаналізу, оптимізації параметрів протоколів постквантового захисту, адаптивного керування трафіком у надцільних мережах та формування прогностичних моделей кіберзагроз в умовах обмеженого часу реагування.

Нехай **стан інформаційної системи** спеціальних користувачів описується вектором фазових змінних

$$\mathbf{x} \in X \subset \mathbb{R}^n, \quad (1)$$

компоненти якого відображають ключові параметри функціонування системи а саме, конфігурацію мережевої інфраструктури, поточні режими криптографічних механізмів, характеристики трафіку, рівень завантаження обчислювальних ресурсів, а також індикатори виявлених аномалій або загроз. Така векторна репрезентація дозволяє формалізувати систему як багатовимірний динамічний об'єкт із внутрішніми нелінійними зв'язками та обмеженнями.

Зовнішні збурення, кіберзагрози, навмисні деструктивні впливи та випадкові шумові компоненти описуються вектором параметрів

$$\xi \in \Xi, \quad (2)$$

який моделює стохастичні флуктуації каналів зв'язку, зміну інтенсивності атак, перехідні процеси в мережі та інші фактори невизначеності.

Задача оптимізації функціонування формулюється у вигляді мінімізації нелінійного функціоналу якості:

$$\min_{\mathbf{x} \in X} J(\mathbf{x}, \xi), \quad (3)$$

де функціонал $J(\cdot)$ відображає багатокритеріальний компроміс між показниками інформаційної безпеки, структурної та функціональної стійкості, часової затримки обробки, пропускну здатності та ресурсної ефективності. Саме це зумовлює доцільність застосування методів глобальної або квазіглобальної оптимізації, у тому числі гібридних квантово-класичних підходів, для забезпечення адаптивного та стійкого функціонування системи в умовах активної протидії.

Квантово-класична гібридна параметризація. У гібридному підході вектор $\mathbf{x}$ параметризується через квантовий стан:

$$|\psi(\theta)\rangle = U(\theta) |\psi_0\rangle, \quad (4)$$

де $U(\theta)$ – параметризований квантовий оператор,

$\theta \in \mathbb{R}^n$ – вектор варіаційних параметрів,

$|\psi_0\rangle$ – початковий стан.

Цільова функція подається у вигляді математичного сподівання спостережуваного оператора:

$$L(\theta, \xi) = \langle \psi(\theta) | \hat{O}(\xi) | \psi(\theta) \rangle + \lambda R(\theta), \quad (5)$$

де $\hat{O}$ – оператор вартості, що кодує критерії безпеки та ефективності,

$R(\theta)$ – регуляризовуючий функціонал, що враховує обмеження ресурсів,

λ – коефіцієнт балансування.

Нелінійна динаміка гібридного алгоритму. Ітеративна еволюція алгоритму описується нелінійним рекурентним співвідношенням:

$$\theta_{k+1} = \theta_k - \eta_k G(\nabla_{\theta} L(\theta_k), \mathbf{y}_k) \quad (6)$$

де $\mathbf{y}_k$ – вектор результатів квантових вимірювань,

η_k – адаптивний крок оптимізації,

$G(\cdot)$ – нелінійний оператор оновлення, що враховує стохастичні та апаратні ефекти.

Нелінійність алгоритму зумовлена залежністю оператора оновлення від результатів вимірювань і поточного стану оптимізаційного процесу, що формує замкнений квантово-класичний контур зворотного зв'язку.

У перспективі квантово-класичні гібридні алгоритми можуть розглядатися як основні складові інтегрованих обчислювальних контурів підтримки прийняття рішень в умовах активної протидії, динамічної невизначеності та ресурсних обмежень [3]. Зазначені контури потенційно здатні забезпечити ефективну обробку високорозмірних і комбінаторно складних конфігурацій, а також оцінити криптографічну стійкість та оптимізувати параметри захищених каналів зв'язку.

За цих умов класична складова алгоритму передбачає інтеграцію результатів квантових обчислень у мережеві та обчислювальні інфраструктури, системи аналізу загроз та механізми адаптивного керування ресурсами. Саме наявність нелінійного контуру зворотного

зв'язку формує ефективну динаміку системи, у якій результати квантових вимірювань безпосередньо впливають на параметри класичних процедур [4]. Це забезпечує оперативну адаптацію до активних кібер і радіоелектронних впливів, змін топології мережі та деградації каналів зв'язку.

Отже, запропонована математична модель нелінійних квантово-класичних гібридних алгоритмів формує чіткий теоретичний фундамент для формалізованого опису та систематичного аналізу складних інформаційних процесів у високопродуктивних системах оборонного та кібербезпекового призначення. Модель забезпечує узгоджене представлення взаємодії квантових і класичних обчислювальних компонентів, дозволяє досліджувати властивості стійкості, адаптивності та ефективності алгоритмів, а також створює методологічну основу для проєктування адаптивних обчислювальних систем нового покоління [5], здатних працювати в умовах динамічних загроз, обмежених ресурсів та оперативних змін обстановки.

Список використаних джерел

1. NIST: Post-Quantum Cryptography (PQC) Project i NIST Releases First 3 Finalized Post-Quantum Encryption Standards, <https://csrc.nist.gov/projects/post-quantum-cryptography>.
2. Живилю, Є., & Кучма, Ю. (2025). DEEP LEARNING-МОДЕЛЬ ПРОГНОЗУВАННЯ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 589–601. <https://doi.org/10.28925/2663-4023.2025.31.1050>
3. Zhyvylo, Ye., & Kuchma, Yu. Practical application and vulnerabilities of the Hill Cipher in a modern context. Systems of Control, Navigation and Communication. 2025. № 4 (78). С. 66–69. DOI: <https://doi.org/10.26906/SUNZ.2025.4.066>
4. Zhyvylo, Y., & Kuchma, Y. (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. Collection “Information Technology and Security”, 13(2), 162–177. <https://doi.org/10.20535/2411-1031.2025.13.2.344591>
5. Фесенко, Т., & Калашнікова, Ю. (2025). ФЕДЕРАТИВНА GNN-ХАІ МОДЕЛЬ ПРОГНОЗУ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У ZERO TRUST-СЕРЕДОВИЩІ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 602–619. <https://doi.org/10.28925/2663-4023.2025.31.1049>

УДК 530.145:004.8:004.056:517.9

Живило Є.О., к.держ.упр., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

НЕЛІНІЙНІ КВАНТОВІ ІНФОРМАЦІЙНІ ПРОЦЕСИ В АДАПТИВНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ НОВОГО ПОКОЛІННЯ

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням складності електронно-комунікаційних систем, зокрема тих, що використовуються в критично важливих інфраструктурах та мережах Сил оборони і безпеки України. Інтенсивна цифровізація, перехід до сервісно-орієнтованих і розподілених архітектур, інтеграція гетерогенних мереж зв'язку, а також зростаюча роль автоматизованих систем підтримки прийняття рішень формують принципово нові вимоги до стійкості, надійності та безпеки обчислювальних процесів.

Додатковим чинником ускладнення є постійна дія багатofакторної невизначеності, що включає випадкові шумові процеси, цілеспрямовані кібернетичні та фізичні атаки, обмеженість обчислювальних і енергетичних ресурсів, а також динамічну зміну топології та параметрів мереж [1]. У таких умовах класичні підходи до проєктування та аналізу інформаційних систем дедалі частіше виявляються недостатніми, що стимулює пошук нових парадигм обчислень і керування.

Одним із перспективних напрямів є використання квантових та гібридних квантово-класичних технологій. Розвиток квантових обчислень, квантових комунікацій і постквантових криптографічних механізмів зумовлює необхідність формування математичних моделей, здатних адекватно описувати еволюцію квантових станів у відкритих, керованих і адаптивних системах [2]. Особливого значення набувають нелінійні квантові інформаційні процеси, які виникають унаслідок взаємодії системи з середовищем, процедур вимірювання та контурів зворотного зв'язку.

У класичній квантовій механіці еволюція ізольованої системи описується лінійним рівнянням Шредінгера або, у випадку змішаних станів, лінійним рівнянням фон Неймана. Проте реальні обчислювальні системи є відкритими та функціонують у взаємодії з середовищем, що призводить до появи дисипації, декогеренції та стохастичних ефектів. Додатково, в адаптивних системах результати вимірювань використовуються для корекції подальшої еволюції, формуючи контури активного зворотного зв'язку.

Саме наявність таких контурів зворотного зв'язку є ключовою причиною виникнення ефективної нелінійності квантової динаміки. Нелінійність у цьому контексті не суперечить фундаментальним постулатам квантової механіки, а є наслідком умовної еволюції стану, параметричної залежності гамільтоніана від поточного стану та адаптивного керування процесами вимірювання й обробки інформації.

Таким чином, нелінійні квантові інформаційні процеси слід розглядати як природний інструмент опису функціонування адаптивних обчислювальних систем нового покоління, у яких квантова динаміка, інформаційні потоки та алгоритми керування утворюють єдину взаємопов'язану систему.

Простір станів та адаптація. Нехай стан складеної квантової системи описується щільнісним оператором

$$\rho(t) \in D(H), \quad H = \bigotimes_{i=1}^N H_i, \quad (1)$$

де H – гільбертів простір складеної системи, а $D(H)$ – множина допустимих квантових станів. Такий підхід дозволяє коректно враховувати як чисті, так і змішані стани, а також ефекти декогеренції та шуму. За цих умов адаптація в системі реалізується через вектор керування

$$\mathbf{u}(t) \in U \subset \mathbb{R}^m \quad (2)$$

визначає параметри гамільтоніана, операторів вимірювання, а також характеристики квантових каналів і класичних обчислювальних процедур. На відміну від статичних схем керування, у розглянутому підході вектор $\mathbf{u}(t)$ формується динамічно на основі поточного стану системи та результатів проміжних вимірювань. Це забезпечує можливість оперативної реакції на зміну зовнішніх умов і внутрішнього стану системи.

Узагальнене рівняння нелінійної квантової динаміки. Для опису еволюції стану адаптивної квантової системи доцільно використовувати узагальнене нелінійне рівняння Ліндблада, у якому як унітарна, так і дисипативна частини динаміки можуть залежати від стану системи

$$\begin{aligned} \frac{d\rho(t)}{dt} = & -i[H_0 + \sum_j u_j(t)H_j + H_{nl}(\rho(t)), \rho(t)] + \\ & + \sum_k \gamma_k(\rho(t), \mathbf{u}(t)) \left(L_k(\rho(t)) \rho L_k^\dagger(\rho(t)) - \frac{1}{2} \{L_k^\dagger L_k, \rho\} \right) \end{aligned} \quad (3)$$

де H_0 – базовий гамільтоніан, H_j – керуючі гамільтоніани, $H_{nl}(\rho)$ – стан-залежний нелінійний гамільтоніан, $L_k(\rho)$ та $\gamma_k(\rho, \mathbf{u})$ визначають нелінійні дисипативні процеси та вплив середовища.

Така модель дозволяє врахувати вплив керуючих дій, умовних вимірювань і нелінійних ефектів, що виникають у процесі адаптації.

Нелінійний характер рівняння відображає використання інформації про стан системи для корекції її подальшої еволюції. З математичної точки зору це призводить до ускладнення аналізу стійкості та оптимальності, проте водночас відкриває можливості для більш гнучкого й ефективного керування квантовими інформаційними процесами.

Постановка задачі оптимального керування. Виконання завдання у межах запропонованої моделі є синтез закону адаптивного керування $\mathbf{u}^*(t)$, який забезпечує оптимальну еволюцію стану $\rho(t)$ протягом інтервалу часу $t \in [0, T]$, починаючи з $\rho(0) = \rho_0$. Тому цільова функція має вигляд:

$$J(\mathbf{u}) = \mathbb{E}[\Phi(\rho(T), \rho_{\text{target}})] + \int_0^T (C(\rho(t)) + \lambda R(\mathbf{u}(t))) dt, \quad (4)$$

де Φ – відхилення кінцевого стану від цільового, $C(\rho)$ – поточний функціонал якості (когерентність, ентропія, точність обчислень), $R(\mathbf{u})$ – регуляризація витрат ресурсів, а λ – коефіцієнт компромісу між точністю та витратами керування. Саме введення інтегральної цільової функції дозволяє систематично аналізувати компроміси між ефективністю обчислень, стійкістю до зовнішніх впливів і вартістю керування. Це є особливо важливим для систем оборонного призначення, де ресурси є обмеженими, а вимоги до надійності та безпеки – критично високими [3].

Інтеграція з варіаційними квантовими алгоритмами та квантовими нейромережами. У випадку варіаційних квантових алгоритмів стан системи параметризується як

$$\rho(\theta) = U(\theta) \rho_0 U^\dagger(\theta), \quad (5)$$

де θ – вектор варіаційних параметрів. Оновлення θ на основі вимірювань реалізує нелінійну адаптацію системи відповідно до цільової функції. Аналогічні погляди застосовуються й у квантових нейромережах, де параметри керування інтерпретуються як вагові коефіцієнти, а нелінійність динаміки відіграє роль функцій активації. Отже це створює передумови для використання квантових методів

машинного навчання в задачах обробки інформації, прогнозування та підтримки прийняття рішень у складних динамічних середовищах.

Розглянутий підхід формує теоретичне підґрунтя для розроблення адаптивних квантових і гібридних квантово-класичних обчислювальних систем, орієнтованих на роботу в умовах інтенсивних зовнішніх збурень і загроз. Зокрема, він може бути використаний для аналізу та синтезу систем захищеного зв'язку, квантово-стійких механізмів автентифікації, а також інтелектуальних систем керування в оборонних інформаційних інфраструктурах.

Подальші дослідження доцільно спрямувати на вивчення стійкості запропонованих моделей до різних класів атак [4], розроблення чисельних методів розв'язання нелінійних рівнянь квантової динаміки та експериментальну верифікацію ефективності адаптивних квантових алгоритмів у реальних або наближених до реальних умовах функціонування.

Список використаних джерел

1. International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 24760-1:2025 Information security, cybersecurity and privacy protection – A framework for identity management. Part 1: Core concepts and terminology (3rd ed.). <https://www.iso.org/standard/24760-1>.
2. Фесенко, Т., та Калашникова, Ю. (2025). Математичні аспекти спільного застосування алгоритму AES та стеганографічних методів у захисті ключів автентифікації. Збірник «Інформаційні технології та безпека», 13 (2), 178–191. <https://doi.org/10.20535/2411-1031.2025.13.2.344592>.
3. Фесенко Т., Калашнікова Ю. Використання Cisco SecureX для SOC-автоматизації. *Системи управління, навігації та зв'язку*. 2025. № 4 (82). С. 138–143. DOI: <https://doi.org/10.26906/SUNZ.2025.4.138>. URL: <https://journals.nupp.edu.ua/sunz/article/view/4119> (дата звернення: 04.02.2026).
4. NIST: Post-Quantum Cryptography (PQC) Project і NIST Releases First 3 Finalized Post-Quantum Encryption Standards, <https://csrc.nist.gov/projects/post-quantum-cryptography>.

УДК 004.8:530.12:004.056

Кучма Ю.В., к.т.н., доцент
ТОВ Приватний вищий навчальний заклад
«УНІВЕРСИТЕТ СУЧАСНИХ ТЕХНОЛОГІЙ»

МОДЕЛЮВАННЯ НЕЛІНІЙНОЇ ДИНАМІКИ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ НА КВАНТОВИХ СИМУЛЯТОРАХ

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням складності інформаційних процесів, які реалізуються в кіберфізичних, розподілених та інтелектуальних системах. Такі процеси вирізняються високою розмірністю простору станів, наявністю багаторівневих зворотних зв'язків, стохастичних збурень і взаємодією когерентних та некогерентних компонентів. У класичних обчислювальних середовищах точне моделювання подібних процесів у режимі реального часу є обмеженим через експоненційне зростання обчислювальної складності [1].

У цьому контексті квантові симулятори розглядаються як перспективна обчислювальна платформа, здатна відтворювати динаміку складних систем на фундаментальному фізичному рівні. Їх використання відкриває нові можливості для формалізованого аналізу нелінійних інформаційних процесів, зокрема тих, що виникають у задачах кібербезпеки, адаптивного керування, криптографічного захисту та підтримки прийняття рішень у динамічних середовищах.

Актуальність дослідження також зумовлена необхідністю розроблення узагальненого математичного апарату, який дозволяє поєднати квантову динаміку, класичні алгоритми керування та адаптивні механізми оптимізації в межах єдиної моделі [2].

Квантові симулятори призначені для відтворення еволюції відкритих квантових систем з урахуванням шумових процесів, дисипації та керованих нелінійних ефектів. На відміну від універсальних квантових комп'ютерів, симулятори орієнтовані на дослідження конкретних класів динамічних систем і дозволяють більш ефективно використовувати обмежені квантові ресурси.

У задачах моделювання інформаційних процесів квантові симулятори забезпечують природну реалізацію багатовимірних просторів станів і операторної динаміки. Це дозволяє адекватно описувати як когерентні інформаційні потоки, так і некогерентні процеси втрат, завад і атак. Особливу роль відіграє можливість

врахування стан-залежних ефектів, що є характерною ознакою адаптивних інформаційних систем [3].

1. Математичні засади моделювання нелінійної динаміки.

Для формалізованого опису нелінійної адаптивної динаміки інформаційних процесів вводиться багатовимірний простір станів, який задається як тензорний добуток гільбертових просторів окремих підсистем

$$H = \bigotimes_{i=1}^N H_i, \quad (1)$$

де H_i – гільбертів простір відповідає i -тій підсистемі, а N – визначає їх кількість. Така структура дозволяє моделювати ієрархічні взаємодії між підсистемами та враховувати як локальні, так і колективні ефекти [4].

2. Простір керування та адаптивні механізми

Адаптивна перебудова динаміки реалізується через параметричний простір керування U , який визначає множину допустимих операторів впливу на систему

$$U = \{\hat{K}(t) \in L(H)\}, \quad (2)$$

де $\hat{K}(t)$ – оператор керування, що модулює еволюцію стану системи відповідно до поточного стану та історії вимірювань. Представлений простір формалізує адаптивні алгоритми керування.

Важливо наголосити, що ключовим елементом цього математичного апарата є щільнісний оператор $\hat{\rho}(t)$, який визначає стан системи в багатовимірному гільбертівському просторі H . Саме використання щільнісного оператора дозволяє формально враховувати суперпозиції, квантову когерентність, а також ефекти декогеренції, що виникають через взаємодію з оточенням і шумові процеси.

Другим ключовим компонентом є оператор керування $\hat{K}(t)$, який формалізує динамічне втручання класичної підсистеми в еволюцію квантового стану. Параметричний простір керування U визначає множину допустимих операторів і дозволяє математично формалізувати адаптивні алгоритми, що реагують на поточний стан системи та історію квантових вимірювань. Наявність такого оператора забезпечує нелінійний контур зворотного зв'язку, у якому результати вимірювань активно впливають на подальшу динаміку системи.

3. Рівняння еволюції та нелінійні ефекти.

Рівняння еволюції системи враховує як когерентну еволюцію через стан-залежний гамільтоніан, так і дисипативні та адаптивні ефекти через оператори.

$$\frac{d\hat{\rho}(t)}{dt} = -i [\hat{H}(t, \hat{\rho}), \hat{\rho}(t)] + D[\hat{\rho}(t)] + F(\hat{\rho}(t), \hat{K}(t)), \quad (3)$$

де $\hat{H}(t, \hat{\rho})$ – стан-залежний гамільтоніан, $D[\hat{\rho}(t)]$ – дисипативний оператор, $F(\hat{\rho}(t), \hat{K}(t))$ – оператор нелінійного адаптивного впливу.

Така модель відображає використання інформації про стан системи для корекції подальшої еволюції, що є характерним для інтелектуальних і самоналаштовуваних інформаційних систем.

4. Цільова функція оптимізації.

Для кількісної оцінки ефективності керування вводиться цільова функція

$$J[\hat{K}(t)] = \int_0^T \text{Tr}\{\hat{\rho}(t)\hat{O}_{\text{target}}\} dt - \lambda \int_0^T \|\hat{K}(t)\|^2 dt \rightarrow \max, \quad (4)$$

де $\hat{O}_{\text{target}}$ – оператор цільової характеристики, λ – коефіцієнт штрафу за ресурси, T – кінцевий час моделювання.

Така постановка дозволяє аналізувати компроміс між досягненням заданих інформаційних властивостей і вартістю керування.

5. Варіаційні алгоритми та дискретизація керування

Практична реалізація оптимального керування на квантових симуляторах здійснюється з використанням варіаційних квантово-класичних алгоритмів.

Дискретизація операторів керування через градієнтне оновлення забезпечує реалізацію варіаційних алгоритмів, які є квантово-класичними гібридними схемами адаптивного управління

$$\hat{K}_{n+1} = \hat{K}_n + \eta \frac{\partial J[\hat{K}_n]}{\partial \hat{K}_n}, \quad (5)$$

де n – номер дискретного кроку, η – адаптивний крок, $\partial J / \partial \hat{K}_n$ – градієнт цільової функції.

Отже, запропонований математичний апарат забезпечує формалізоване моделювання високорозмірних, нелінійних та адаптивних інформаційних процесів в умовах динамічної невизначеності, дозволяючи оцінювати стійкість криптографічних механізмів, оптимізувати параметри захищених каналів та досліджувати сценарії активної протидії. При цьому результати квантових вимірювань та адаптивні дії класичних операторів формують

нелінійний контур зворотнього зв'язку [4], що забезпечує контекстно-залежну перебудову алгоритмічних і протокольних рішень у режимі реального часу, підвищуючи живучість та стійкість інформаційних і комунікаційних систем.

Необхідно зазначити, що комплексне поєднання квантових і класичних компонентів [5], створює теоретичну основу для побудови адаптивних алгоритмів оптимізації та високопродуктивних квантово-класичних симуляторів, дозволяючи аналізувати ефективність, стійкість і адаптивність систем у складних кібербезпекових середовищах.

Таким чином, запропонований підхід формує платформу для моделювання, аналізу та оптимізації нелінійних інформаційних процесів, інтегруючи методи квантового моделювання з класичними алгоритмами керування з перспективою для підвищення стійкості, живучості та безпеки інформаційних мереж у динамічних умовах загроз.

Список використаних джерел

1. Живилю, Є., & Кучма, Ю. (2025). DEEP LEARNING-МОДЕЛЬ ПРОГНОЗУВАННЯ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 589–601. <https://doi.org/10.28925/2663-4023.2025.31.1050>

2. NIST: Post-Quantum Cryptography (PQC) Project і NIST Releases First 3 Finalized Post-Quantum Encryption Standards, <https://csrc.nist.gov/projects/post-quantum-cryptography>.

3. Фесенко, Т., & Калашнікова, Ю. (2025). ФЕДЕРАТИВНА GNN-ХАІ МОДЕЛЬ ПРОГНОЗУ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У ZERO TRUST-СЕРЕДОВИЩІ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 602–619. <https://doi.org/10.28925/2663-4023.2025.31.1049>

4. Zhyvylyo, Y., & Kuchma, Y. (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. Collection “Information Technology and Security”, 13(2), 162–177. <https://doi.org/10.20535/2411-1031.2025.13.2.344591>

Фесенко, Т., та Калашнікова, Ю. (2025). Математичні аспекти спільного застосування алгоритму AES та стеганографічних методів у захисті ключів автентифікації. Збірник «Інформаційні технології та безпека», 13 (2), 178–191. <https://doi.org/10.20535/2411-1031.2025.13.2.344592>.

УДК 004.8:530.145

Магалецька В.В., к.т.н., доцент
ТОВ Приватний вищий навчальний заклад
«УНІВЕРСИТЕТ СУЧАСНИХ ТЕХНОЛОГІЙ»

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ НА ОСНОВІ НЕЛІНІЙНИХ КВАНТОВИХ МОДЕЛЕЙ

Розвиток інформаційних технологій на основі нелінійних квантових моделей зумовлений зростанням складності обчислювальних задач, високою розмірністю інформаційних конфігурацій та потребою в адаптивній обробці даних в умовах структурної й динамічної невизначеності [1]. За таких умов лінійні моделі квантових інформаційних процесів є принципово обмеженими, що зумовлює перехід до нелінійних математичних підходів.

При цьому альтернативний підхід відкидає еволюційне описання квантових інформаційних процесів, замінюючи його строгою геометрично-варіаційною інтерпретацією. Квантова інформаційна система формалізується як нелінійна динамічна структура на рімановому просторі станів, а інформаційна обробка трактується як керований рух у детермінованому геометричному просторі. Підхід інтегрує теорію складних систем, інформаційну геометрію та алгоритмічні процедури в єдину формалізовану рамку [2].

Нехай множина фізично допустимих квантових станів визначається як ріманів простір станів

$$M = \{\rho \in D(H)\}, \quad (1)$$

де $D(H)$ – множина щільнісних операторів у гільбертовому просторі H . Наділення простору M квантово-інформаційною метрикою дозволяє формалізувати поняття інформаційної відстані між станами, а також кількісно оцінювати чутливість системи до збурень і структурну складність інформаційних конфігурацій.

У межах такої геометричної постановки динаміка інформаційних процесів інтерпретується як керований геодезичний рух на метриці M . Еволюцію квантового стану можливо описати рівнянням:

$$\frac{D}{dt} \dot{\rho}(t) = F(\rho(t), u(t)), \quad (2)$$

де $\frac{D}{dt}$ – коваріантна похідна на просторі станів, F – нелінійний інформаційний векторний потік, а $u(t)$ – параметри керування, що визначають допустимі напрями еволюції.

Обчислювальні та інформаційні процеси формалізуються у варіаційній постановці, де еволюція квантового стану відповідає розв'язанню задачі мінімізації функціоналу дії

$$S[\rho, u] = \int_0^T (\langle \dot{\rho}, \dot{\rho} \rangle_{\rho} + \lambda I(\rho) + R(u)) dt. \quad (3)$$

На просторі M , $I(\rho)$ визначається інформаційна метрика $\langle \dot{\rho}, \dot{\rho} \rangle_{\rho}$ що слугує функціоналом інформаційної складності, $R(u)$ описує ресурсну вартість керування, а параметр λ задає баланс між точністю обробки та обчислювальною складністю.

Адаптивне керування в межах геометрично-варіаційного підходу реалізується не як зовнішній силовий вплив, а як локальна деформація геометрії простору станів $\mathcal{G}_{\rho} \rightarrow \mathcal{G}_{\rho}(u)$.

Деформація простору станів задає контекстно-залежні напрями еволюції, реалізуючи механізми навчання та адаптації. Варіаційні квантові алгоритми, квантові нейромережі та симулятори інтерпретуються відповідно як дискретизовані геодезичні траєкторії, керовані деформації інформаційної метрики та чисельна інтеграція руху на нелінійному просторі станів без введення нефізичних операторів.

В цілому запропонований математичний апарат задає концептуально цілісну основу для інформаційних технологій на основі нелінійних квантових моделей, інтегруючи теорію складних систем, квантову інформацію та адаптивні обчислення. Це визначає перспективний напрям розвитку інтелектуальних технологій нового покоління для роботи в умовах високої складності та обмежень.

Список використаних джерел

1. Фесенко, Т., та Калашникова, Ю. (2025). Математичні аспекти спільного застосування алгоритму AES та стеганографічних методів у захисті ключів автентифікації. Збірник «Інформаційні технології та безпека», 13 (2), 178–191. <https://doi.org/10.20535/2411-1031.2025.13.2.344592>.
2. Фесенко Т., Калашнікова Ю. Використання Cisco SecureX для SOC-автоматизації. *Системи управління, навігації та зв'язку*. 2025. № 4 (82). С. 138–143. DOI: <https://doi.org/10.26906/SUNZ.2025.4.138>. URL: <https://journals.nupp.edu.ua/sunz/article/view/4119> (дата звернення: 14.02.2026).

УДК 004.8:004.056:519.6

*Поліновський В.В. к.т.н., доцент
ТОВ Приватний вищий навчальний заклад
«УНІВЕРСИТЕТ СУЧАСНИХ ТЕХНОЛОГІЙ»*

ХАОТИЧНА ТА НЕЛІНІЙНА ДИНАМІКА ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ СТІЙКОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Сучасні інформаційні системи, особливо в умовах кіберфізичних середовищ та IoT-інфраструктур, функціонують у режимі високої динамічної невизначеності [1]. Зростаюча складність загроз, варіативність мережевих топологій та активні атакуючі впливи вимагають застосування адаптивних методів управління, здатних підтримувати стійкість та живучість системи [2]. У цьому контексті хаотичні та нелінійні механізми розглядаються як ефективний інструмент для забезпечення динамічної адаптації, резервування та розсіювання передбачуваності поведінки системи [3].

Для формалізації зазначених процесів стан системи представляється як вектор у багатовимірному просторі станів:

$$x(t) \in \mathbb{R}^n, \quad (1)$$

де n визначає кількість ключових компонент системи, включаючи мережеві вузли, процеси керування та криптографічні параметри. Таке представлення дозволяє математично моделювати еволюцію складних інформаційних потоків у системі.

Еволюція стану під впливом зовнішніх факторів та внутрішніх нелінійних зв'язків описується стохастичним нелінійним рівнянням:

$$\dot{x}(t) = f(x(t), u(t)) + \sigma(x(t))\xi(t), \quad (2)$$

де $f(x(t), u(t))$ – нелінійний оператор еволюції стану, $u(t) \in U \subset \mathbb{R}^m$ – вектор керуючих сигналів, $\sigma(x(t))$ – матриця стохастичних впливів, $\xi(t)$ – білий шум, що моделює непередбачувані зовнішні та внутрішні впливи.

Хаотичні механізми задаються через нелінійні атрактори $A \subset X$, які визначають множинність потенційних траєкторій еволюції:

$$x(t) \in A(u(t)), \quad A = \{x \in X \mid g(x, u) = 0\}, \quad (3)$$

де $g(x, u)$ – нелінійні обмеження, що формують хаотичні динамічні контури, здатні підвищувати стійкість системи та зменшувати передбачуваність її поведінки для потенційного злоумисника.

Задача адаптивного керування формулюється через оптимізацію функціоналу безпеки та стійкості системи:

$$J[u] = E \left[\Phi(x(T)) + \int_0^T C(x(t), u(t)) dt \right], \quad (4)$$

де $\Phi(x(T))$ характеризує кінцеву безпеку та стабільність системи, а $C(x, u)$ – локальні витрати на керування та адаптацію. Стохастичне математичне очікування $E[\cdot]$ враховує невизначеність зовнішніх впливів.

Керуючий сигнал формується як функція стану та історії спостережень:

$$u(t) = K(x(t), H_t), \quad H_t = \{x(s) \mid 0 \leq s \leq t\}, \quad (5)$$

де $K(\cdot)$ – оператор адаптивного керування, що підтримує траєкторії системи в межах хаотичних атракторів та забезпечує контекстно-залежну перебудову алгоритмів і протоколів.

Таким чином, інтеграція хаотичних та нелінійних механізмів у кіберфізичні та IoT-орієнтовані інформаційні системи дозволяє формувати адаптивні, стійкі та живучі контури керування, здатні реагувати на зміну операційного середовища, мінімізувати вплив атак і підтримувати ефективність системи у реальному часі. При цьому представлений математичний апарат забезпечує формалізований та аналітично керований підхід для синтезу таких систем, що є критично важливим для розвитку інформаційних технологій нового покоління.

Список використаних джерел

1. International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 24760-1:2025 Information security, cybersecurity and privacy protection – A framework for identity management. Part 1: Core concepts and terminology (3rd ed.). <https://www.iso.org/standard/24760-1>.
2. Фесенко Т., Калашнікова Ю. Використання Cisco SecureX для SOC-автоматизації. *Системи управління, навігації та зв'язку*. 2025. № 4 (82). С. 138–143. DOI: <https://doi.org/10.26906/SUNZ.2025.4.138>. URL: <https://journals.nupp.edu.ua/sunz/article/view/4119> (дата звернення: 04.02.2026).
3. Zhyvylo, Y., & Kuchma, Y. (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. Collection “Information Technology and Security”, 13(2), 162–177. <https://doi.org/10.20535/2411-1031.2025.13.2.344591>

УДК 004.8:004.93:537.312.2

Рубін Е.Ю., к.т.н., доцент*ТОВ Приватний вищий навчальний заклад
«УНІВЕРСИТЕТ СУЧАСНИХ ТЕХНОЛОГІЙ»***НЕЛІНІЙНЕ КЕРУВАННЯ ВІДКРИТИМИ КВАНТОВИМИ
СИСТЕМАМИ В КІБЕРФІЗИЧНИХ ТА ІОТ-ОРІЄНТОВАНИХ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ**

Інтеграція квантових підсистем у кіберфізичні та ІоТ-орієнтовані інформаційні технології вимагає застосування математичних методів, здатних точно описувати квантову динаміку за умов неповних, стохастичних і мережево-обумовлених вимірювань [1]. У цьому контексті квантові фільтри Белавкіна формалізують природний математичний апарат для моделювання нелінійного керування відкритими квантовими системами, що функціонують у квантово-класичних замкнених контурах зворотного зв'язку.

На відміну від рівнянь Ліндблада, фільтри Белавкіна дозволяють формалізувати умовну еволюцію квантового стану за умов безперервних вимірювань. У таких архітектурах квантова підсистема трактується як стохастично керований об'єкт, інтегрований у розподілену ІоТ-інфраструктуру.

Математична модель. Стан відкритої квантової системи описується умовним щільнісним оператором $\rho_c(t) \in D(H)$, який є умовним математичним сподіванням квантового стану відносно сигма-алгебри результатів вимірювань. Динаміка $\rho_c(t)$ визначається стохастичним диференціальним рівнянням Белавкіна:

$$d\rho_c(t) = L[\rho_c(t)]dt + H_L[\rho_c(t)]dW(t), \quad (1)$$

де L – генератор відкритої квантової динаміки типу Ліндблада,

$$L[\rho] = -i[H(u(t)), \rho] + \sum_k \left(L_k \rho L_k^\dagger - \frac{1}{2} \{L_k^\dagger L_k, \rho\} \right), \quad (2)$$

а $H_L[\rho]$ – інноваційний нелінійний оператор

$$H_L[\rho] = L\rho + \rho L^\dagger - \text{Tr}[(L + L^\dagger)\rho]\rho. \quad (3)$$

Стохастичний процес $dW(t)$ є вінерівським інноваційним шумом, що моделює різницю між фактичними результатами вимірювань і їх умовними прогнозами. Вимірювальний процес задається співвідношенням:

$$dY(t) = \text{Tr}[(L + L^\dagger)\rho_c(t)]dt + dW(t), \quad (4)$$

що відображає фізичний зв'язок між квантовою динамікою та класичним потоком даних у IoT-контурі.

Нелінійне керування в термінах умовної динаміки. Керування вводиться через параметризацію гамільтоніана

$$H(u(t)) = H_0 + \sum_{j=1}^m u_j(t) H_j, \quad (5)$$

де вектор керування $u(t) \in \mathcal{U} \subset \mathbb{R}^m$ формується класичним контролером на основі умовного стану $\rho_c(t)$ або вимірювального сигналу $Y(t)$. Унаслідок цього виникає нелінійний квантово-класичний контур зворотнього зв'язку, в якому динаміка керування залежить від стохастичної еволюції квантового стану.

Задача керування формулюється як мінімізація стохастичного функціонала

$$J[u] = \mathbb{E} \left[\Phi(\rho_c(T)) + \int_0^T C(\rho_c(t), u(t)) dt \right], \quad (6)$$

де $\Phi(\rho_c(T))$ задає цільову інформаційну або функціональну конфігурацію системи, а C враховує витрати керування та мережеві обмеження, характерні для IoT-середовищ.

В цілому математичний апарат квантових фільтрів Белавкіна формує чіткий аналітичний фундамент для побудови нелінійних керованих моделей відкритих квантових систем у межах кіберфізичних та IoT-орієнтованих технологій. Підхід дозволяє перейти від усереднених рівнянь Ліндблада до умовних стохастичних рівнянь еволюції щільнісного оператора, які враховують вплив безперервних вимірювань та класичних контурів зворотнього зв'язку на динаміку системи. Реалізація цього підходу забезпечує синтез адаптивних квантово-класичних контурів керування [2], оптимізованих за критеріями стійкості, точності та ефективності в умовах динамічної невизначеності та обмежених ресурсів.

Список використаних джерел

1. Живило, Є., & Кучма, Ю. (2025). DEEP LEARNING-МОДЕЛЬ ПРОГНОЗУВАННЯ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 589–601. <https://doi.org/10.28925/2663-4023.2025.31.1050>
2. Zhyvylo, Y., & Kuchma, Y. (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. Collection "Information Technology and Security", 13(2), 162–177. <https://doi.org/10.20535/2411-1031.2025.13.2.344591>

УДК 004.056

*Ланчевич А.І., здобувач
Балацька В.С., д. філ., ст. викладач
Полотай О.І., к.т.н., доцент*

Львівський державний університет безпеки життєдіяльності

АРХІТЕКТУРА ІНТЕГРАЦІЇ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У ПІДСИСТЕМУ АУДИТУ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Підсистема аудиту є складовою комплексних систем захисту інформації (КСЗІ), що забезпечує реєстрацію подій інформаційної безпеки, контроль адміністративних дій та формування доказової бази під час розслідування інцидентів. Типовою проблемою є відсутність криптографічно підтвердженої незмінності аудиторських артефактів у разі використання централізованих сховищ журналів (лог-сервери, SIEM), що зумовлює ризики ретроспективної модифікації або видалення записів, зокрема за сценаріїв внутрішніх загроз або компрометації привілейованих облікових записів.

Для підвищення доказовості аудиторських даних запропоновано архітектуру інтеграції permissioned blockchain у підсистему аудиту КСЗІ у форматі реєстру доказів (evidence ledger). Архітектура базується на розмежуванні on-chain/off-chain рівнів зберігання: первинні журнали подій і результати кореляції зберігаються у SIEM (off-chain), тоді як у блокчейн-мережі фіксуються лише криптографічні «якорі» пакетів журналів (Merkle-root або хеш пакета) разом із метаданими. Такий підхід мінімізує обсяг on-chain даних і зменшує накладні витрати, одночасно забезпечуючи можливість незалежної перевірки цілісності й послідовності фіксації аудиторських артефактів.

Архітектурна модель включає: (1) джерела подій (сервери, мережеві пристрої, засоби захисту, прикладні сервіси); (2) модуль збору та нормалізації журналів; (3) сховище журналів/SIEM для зберігання повних подій і виконання кореляції; (4) шлюз доказів (Evidence Gateway), який виконує пакетування подій за часовим інтервалом або кількістю записів, формує Merkle-дерево та обчислює корінь R, накладає електронний підпис і формує метадані пакета; (5) permissioned blockchain-мережу для реєстрації доказів; (6) модуль верифікації для підтвердження цілісності журналів під час аудиту або розслідування.

Формування доказу для пакета $B_t = \{e_1, e_2, \dots, e_n\}$ реалізується послідовністю: нормалізація подій e_i ; обчислення листів $h_i = H(e_i)$ та кореня $R = \text{MerkleRoot}(h_{1:n})$; формування структури доказу

$P = \langle ID, tstart, tend, n, R, prevR, src, Sig \rangle$, де *prevR* – попередній корінь для зв'язування пакетів у безперервний ланцюжок, *Sig* – підпис Evidence Gateway. Запис *P* у блокчейн забезпечує виявлення будь-якої зміни off-chain журналів через розбіжність контрольних значень. Використання *prevR* підвищує стійкість до сценаріїв «вирізання» фрагментів журналів та ретроспективних підмін, оскільки порушується ланцюгова узгодженість пакетів.

Запропонований підхід забезпечує властивості tamper-evidence для аудиторських артефактів, підвищує рівень довіри до результатів функціонування підсистеми аудиту КСЗІ та створює механізм доказовості під час перевірок відповідності й цифрової криміналістики. Розмежування on-chain/off-chain рівнів і пакетування подій дозволяють масштабувати рішення без критичного впливу на продуктивність SIEM і мережевої інфраструктури. Перспективним напрямом подальших досліджень є обґрунтування параметрів пакетування (часове вікно, розмір пакета), оцінювання накладних витрат і формалізація моделі довіри між учасниками permissioned blockchain у контексті КСЗІ.

Список використаних джерел

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Кібербезпека: освіта, наука, техніка. 2023. № 4(20). С. 6–19. DOI: <https://doi.org/10.28925/2663-4023.2023.20.619>
2. Балацька В., Дмитрів Н. Міжорганізаційний обмін конфіденційними персональними даними на основі дозвоільного блокчейн. Кібербезпека: освіта, наука, техніка. 2025. № 2(29). С. 178–193. DOI: <https://doi.org/10.28925/2663-4023.2025.29.875>
3. Балацька В., Ткачук Р., Маслоva Н. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України. Кібербезпека: освіта, наука, техніка. 2025. № 2(30). С. 316–332. DOI: <https://doi.org/10.28925/2663-4023.2025.30.975>
4. Балацька В. С., Івануса А. І., Пановик У. М. Метод інтеграції політик інформаційної безпеки, стандартів та протоколів у процес побудови комплексної системи захисту інформації в організації. Кібербезпека: освіта, наука, техніка. 2025. № 3(31). С. 283–297. DOI: <https://doi.org/10.28925/2663-4023.2025.31.1021>
5. Balatska V., Oprisky I. Blockchain as a tool for transparency and protection of government registries. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, Issue 2. P. 221–230. DOI: <https://doi.org/10.18372/2225-5036.30.19211>

УДК 004.056

Пірог О.В. , к.т.н., доцент

Шелуха О.О. , к.т.н., доцент

Державний університет «Житомирська політехніка»

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МАЛОГО ІТ-ПІДПРИЄМСТВА В УМОВАХ ПІДГОТОВКИ ДО СЕРТИФІКАЦІЇ ISO/IEC 27001

У сучасних умовах цифровізації, зростання кількості та складності кібератак, витоків даних і інших інцидентів інформаційної безпеки (ІБ) підвищує необхідність впровадження системного підходу до захисту інформаційних активів організацій. Додатковим фактором є підвищення вимог з боку клієнтів та партнерів щодо забезпечення належного рівня ІБ. Одним із найбільш поширених міжнародних стандартів у цій сфері є ISO/IEC 27001, який визначає вимоги до створення та функціонування системи управління ІБ (СУІБ). Водночас для малих ІТ-підприємств впровадження вимог ISO/IEC 27001 є складним завданням через обмежені ресурси та недостатню формалізацію процесів. Це обумовлює необхідність розроблення адаптованих моделей формування СУІБ, орієнтованих на специфіку малого ІТ-бізнесу та підготовку до сертифікаційного аудиту.

З метою спрощення процесу впровадження СУІБ для малих ІТ-підприємств пропонується поетапне формування СУІБ відповідно до вимог стандарту ISO/IEC 27001.

На першому етапі здійснюється аналіз контексту діяльності підприємства, визначаються основні інформаційні активи, зацікавлені сторони та вимоги до забезпечення ІБ. На цьому етапі формується базове розуміння процесів обробки інформації та визначаються потенційні загрози для інформаційних ресурсів.

Другий етап передбачає проведення оцінювання ризиків ІБ. Визначаються можливі загрози, вразливості інформаційних систем та оцінюється рівень ризиків для основних інформаційних активів підприємства.

На третьому етапі формується набір організаційних і технічних заходів захисту інформації, спрямованих на мінімізацію виявлених ризиків. Зокрема базові елементи СУІБ.

Четвертий етап передбачає формалізацію процесів та підготовку необхідної документації, що підтверджує відповідність СУІБ вимогам стандарту. Завершальним етапом є проведення внутрішнього аудиту та підготовка підприємства до проходження сертифікаційного аудиту відповідно до вимог ISO/IEC 27001.

Доцільно використовувати базовий перелік видів контролю на основі стандарту ISO/IEC 27001 з урахуванням ресурсних обмежень

малого бізнесу. До основних видів контролю, які доцільно впроваджувати на початковому етапі формування СУІБ, належать:

- політика ІБ;
- контроль доступу до інформаційних систем і ресурсів;
- управління обліковими записами користувачів;
- політика використання паролів та багатфакторної автентифікації;
- резервне копіювання даних;
- процедури управління інцидентами ІБ;
- контроль доступу до систем керування програмним кодом і репозиторіїв;
- захист робочих станцій та серверів;
- управління оновленнями ПЗ;
- навчання персоналу;
- контроль використання хмарних сервісів та зовнішніх інформаційних ресурсів;
- проведення внутрішнього аудиту СУІБ.

Застосування запропонованої моделі призведе до зменшення витрат на впровадження СУІБ, дозволить оптимізувати використання ресурсів, сприятиме скороченню термінів підготовки до проходження аудиту ISO/IEC 27001, підвищенню загального рівня ІБ підприємства, зменшенню ризиків виникнення інцидентів ІБ та забезпеченню більш надійного захисту інформаційних активів.

Список використаних джерел

1. ISO/IEC 27001:2022 - Information security management systems
ISO URL: <https://www.iso.org/standard/27001>.
2. The Ultimate Guide to ISO 27001 for Small Business URL:
<https://hightable.io/iso-27001-for-small-business/>.
3. ISO 27001 Certification Process for SMEs URL:
<https://sunbytes.io/blog/cybersecurity/complete-iso-27001-certification-process/>.
4. Overcome SME Risk Challenges with ISO 27001:2022 URL:
<https://www.isms.online/iso-27001/risk-management/sme-challenges/>.
5. Implementing ISO/IEC 27001:2022 in a SME: a case URL:
<https://www.theseus.fi/handle/10024/876470>.
6. ISO 27001 – A Step-by-Step Approach Toward Certification URL:
<https://www.barradvisory.com/wp-content/uploads/2023/06/ISO-27001%E2%80%94A-Step-by-Step-Approach-Toward-Certification.pdf>.

УДК 004.72

*Жержерунов П. Ю., аспірант,
Національний технічний університет
"Харківський політехнічний інститут"*

*Шматко О. В., к.т.н., доцент,
ТОВ ТУ Метінвест ПОЛІТЕХНІКА*

EFFICIENT ZERO-KNOWLEDGE PROOF CIRCUITS FOR THE SM3 HASH FUNCTION IN RESOURCE-CONSTRAINED BLOCKCHAIN SYSTEMS

Modern information systems increasingly rely on distributed infrastructures that enable cooperation between multiple independent organizations. Such environments require mechanisms that guarantee both data integrity and confidentiality. Blockchain technology has emerged as a promising solution for maintaining distributed ledgers and ensuring transparent and tamper-resistant recording of transactions across decentralized networks. However, conventional blockchain architectures are primarily designed to maximize transparency, which may conflict with the confidentiality requirements of corporate information systems.

Zero-Knowledge Proof (ZKP) protocols provide an effective method for privacy-preserving verification of computations. These protocols allow a prover to demonstrate knowledge of a secret value without revealing the value itself. When integrated into blockchain systems, ZKP mechanisms enable validation of transactions while keeping the underlying information confidential. Despite these advantages, practical implementation of ZKP mechanisms often introduces considerable computational overhead, particularly when complex cryptographic primitives such as hash functions are involved.

To address these challenges, this work proposes a privacy-preserving blockchain architecture that combines the Proof of Friendship (PoF) consensus mechanism with optimized Zero-Knowledge Proof circuits based on the SM3 hash function. The proposed approach aims to enable efficient verification of transaction correctness while minimizing computational overhead in distributed enterprise environments.

Experimental evaluation was conducted in a containerized environment that simulates a distributed corporate blockchain network with limited computational resources available to each node. In this architecture, proof generation is performed by an off-chain prover module, while validator nodes verify proofs and participate in the consensus process.

Two circuit construction approaches were analyzed. The first approach corresponds to a direct translation of the SM3 hashing algorithm into a Rank-1 Constraint System without specialized optimization techniques. The second approach implements the optimized SM3-ZKP circuit proposed in this work.

The optimization techniques include bit–arithmetic aggregation, optimized message scheduling, reduction of circuit depth, and the use of lookup tables for nonlinear functions.

The experimental results demonstrate that the optimized SM3-ZKP circuit significantly reduces circuit complexity compared to the naive implementation. The number of arithmetic constraints and intermediate variables required for representing the hash computation decreased by approximately fifty percent. As a result, proof generation time was reduced by more than two times while maintaining constant verification time.

This work presents a privacy-preserving blockchain architecture designed for corporate information systems. By integrating the Proof of Friendship consensus mechanism with optimized SM3-based Zero-Knowledge Proof circuits, the proposed solution enables verification of transaction correctness while maintaining confidentiality of sensitive data. Experimental results demonstrate that the proposed optimization techniques significantly reduce proving complexity and enable practical deployment of ZKP mechanisms in resource-constrained enterprise blockchain environments. The proposed architecture provides a foundation for developing secure distributed information systems that combine blockchain transparency with strong data protection guarantees.

References

1. Chirakarotu N. R., Kumar P. P. Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions //Security and Privacy. – 2024.
2. Sah C. P., Kaur M., Singh G. Efficiency of zero-knowledge proofs: a through review and analysis //2024 IEEE International conference on public key infrastructure and its applications (PKIA). – IEEE, 2024. – С. 1-7.
3. Yang Y. et al. Implementation and optimization of zero-knowledge proof circuit based on hash function sm3 //Sensors. – 2022. – Т. 22. – №. 16. – С. 5951.
4. Dong J. K. et al. HI-SM3: High-Performance Implementation of SM3 Hash Function on Heterogeneous GPUs //Journal of Computer Science and Technology. – 2025. – Т. 40. – №. 6. – С. 1546-1562.
5. Shmatko O.V. et al. Survey and categorization of blockchain solutions for supply chain management //Системи обробки інформації. – 2024. – №. 3 (178). – С. 84-92.

УДК 004.72

*Кожихов К.О., магістр,
Національний технічний університет
“Харківський політехнічний інститут”
Шматко О. В., к.т.н., доцент,
ТОВ ТУ Метінвест ПОЛІТЕХНІКА*

ENHANCING CREDIT SCORING WITH HYBRID QUANTUM MACHINE LEARNING ARCHITECTURES

Credit scoring remains an essential mechanism in financial risk assessment and lending. Traditional machine learning (ML) models, while robust, face limitations when handling imbalanced datasets and complex nonlinear patterns common in small and medium-sized enterprise (SME) credit data. Quantum machine learning (QML) offers a promising direction due to its potential for enhanced representation capacity and reduced training times. Recent work [1-5] introduces a hybrid quantum–classical neural network architecture aimed at achieving practical improvements in credit scoring performance using quantum computing simulators.

The proposed architecture combines three components: a classical neural network front-end, a variational quantum circuit (VC), and data re-uploading circuit (DRC) blocks. The classical layers reduce high-dimensional feature inputs (21 features) to a vector compatible with a limited number of qubits. Angle embedding is employed to load real-valued features into quantum states using rotation gates. The VC layer includes trainable rotation and entanglement gates, while DRC blocks reinject data to improve representational depth. This hybrid design leverages strengths of classical preprocessing and quantum expressivity.

Experimental results show that the proposed model achieves an ROC/AUC score of 0.75, outperforming the CCN model trained for the same number of epochs (AUC = 0.73). Interestingly, the CCN model required up to 3500 epochs to reach comparable performance, demonstrating a significant training-efficiency advantage for the hybrid architecture. The best performance occurred with 12 qubits and minimal data re-uploading, while further increases caused accuracy to decline—likely due to barren plateaus and over-parameterization effects in deeper quantum circuits. Execution time scaling analysis showed quadratic growth with qubit count and linear dependence on DRC depth, underscoring practical limitations for near-term devices.

The findings indicate that hybrid quantum–classical machine learning offers meaningful advantages for credit-risk classification, especially in

training-time efficiency. While accuracy gains remain modest, the proposed model demonstrates resilience to noisy financial data and presents a feasible pathway toward quantum-enhanced financial analytics. Limitations arise from qubit scalability, barren plateaus, and computational overhead. However, advancements in quantum hardware—projected to exceed 4000 qubits—combined with runtime optimization frameworks may enable substantial performance improvements in future applications.

References

- 1 Schetakis N. Quantum machine learning for credit scoring / N. Schetakis [et al.] // Mathematics. – 2024. – Т. 12, № 9. – С. 1391.
2. Alam T. M. Corporate bankruptcy prediction: An approach towards better corporate world / T. M. Alam [et al.] // The Computer Journal. – 2021. – Т. 64, № 11. – С. 1731–1746.
3. Cerezo M. Challenges and opportunities in quantum machine learning / M. Cerezo [et al.] // Nature Computational Science. – 2022. – Т. 2, № 9. – С. 567–576.
4. Pérez-Salinas A. Data re-uploading for a universal quantum classifier / A. Pérez-Salinas [et al.] // Quantum. – 2020. – Т. 4. – С. 226.
5. Liu J. Analytic theory for the dynamics of wide quantum neural networks / J. Liu [et al.] // Physical Review Letters. – 2023. – Т. 130, № 15. – С. 150601.

УДК 004.056.5:004.272.2

Мостовий О.С., аспірант

Інститут кібернетики імені В.М.Глушкова НАН України

РОЗПОДІЛЕНИЙ SMT-АНАЛІЗ ВРАЗЛИВОСТЕЙ БІНАРНИХ ФАЙЛІВ АРХІТЕКТУРИ ARM64 НА HPC- КЛАСТЕРАХ

Аналіз безпеки ARM64-бінарних файлів є критичним для захисту програм IoT-пристроїв та супутникового обладнання. Символьне виконання за допомогою фреймворку Angr [1] будує граф потоку керування (ГПК), де кожен шлях до потенційно небезпечної операції породжує набір обмежень. Система автоматичного доведення теорем (SMT) Z3 [2] перевіряє здійсненність цих обмежень: SAT означає існування вхідного вектора, що експлуатує вразливість. Проте реальні бінарні файли мають тисячі шляхів, а SMT-розв'язання займає понад 90% часу виконання. Оскільки перевірка різних шляхів повністю незалежна, задача є паралельною та ідеальною для високопродуктивних обчислювальних кластерів (HPC).

Пропонується три етапна архітектура типу Map-Reduce (Рис 1) для розподіленого SMT-аналізу ARM64 бінарних файлів на HPC-кластері SKIT [3] під керуванням планувальника Slurm.

Етап 1 : на вузлі фреймворк `angr` будує CFG бінарного файлу, досліджує шляхи до вузлів, для кожного формує повну формулу $\Phi_i = \text{Pre} \wedge \varphi_i \wedge \text{Post}$ та серіалізує у формат SMT-LIB v2. Результат — директорія з N незалежними файлами.

Етап 2 : масив завдань Slurm розподіляє файли по вузлах. Кожен сервіс планувальник отримує унікальний ідентифікатор, запускає Z3 із часом очікування 60 секунд та записує результат: SAT, UNSAT, або timeout.

Етап 3 : фінальний скрипт збирає результати, класифікує за типом CWE та формує звіт. SAT-результати містять конкретні моделі - вхідні дані для відтворення вразливості.

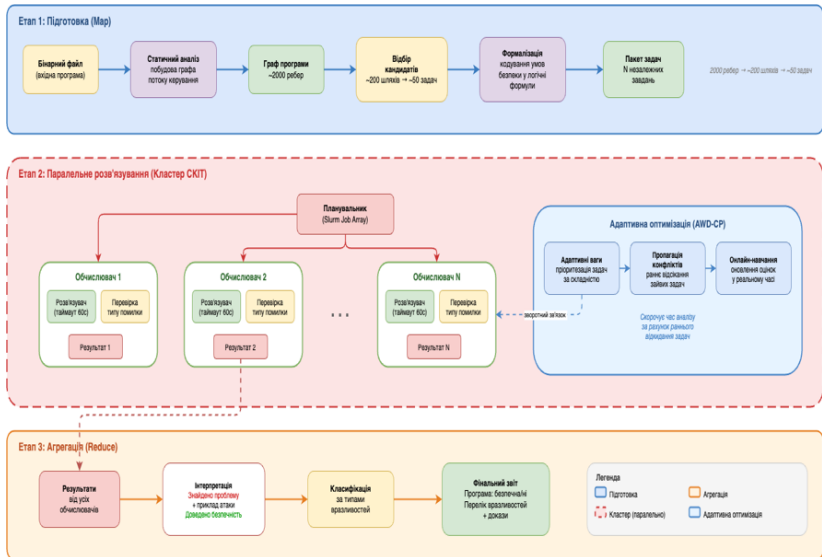


Рисунок 1 – Архітектура Розподіленого SMT-Аналізу

Запропоновано архітектуру розподіленого SMT-аналізу вразливостей ARM64-бінарних файлів, у якій кожному класу ставиться у відповідність трійка Хоара, що транслюється у формулу SMT-LIB v2 для розв'язувача Z3. Обчислювальна реалізація за парадигмою Map-Reduce на кластері SKIT забезпечує лінійне масштабування для незалежних шляхів виконання. Подальша робота спрямована на імплементацію прототипу, інтеграцію методу та верифікацію програмного забезпечення.

Список використаних джерел

- Shoshitaishvili Y. et al. SOK: Offensive techniques in binary analysis. IEEE S&P. 2016.
- De Moura L., Bjørner N. Z3: An efficient SMT solver. TACAS. 2008. P. 337–340.
- Golovynskiy A.L. et al. Development of SCIT supercomputers family. Cybernetics and Sys. Analysis. 2017. Vol. 53, No. 5.
- Wilson A. et al. Partitioninfg strategies for distributed SMT solving. FMCAD. 2023.
- Bucur S. et al. Parallel symbolic execution for automated real-world software testing. EuroSys. 2011.

УДК 004.056.5

I. Yu. Makovskyi, Senior Research Fellow, Research Department
R. V. Netrebko, Senior Lecturer, Higher Education Institution
Korolov Zhytomyr Military Institute

ANALYSIS OF REGULATORY AND INTERNATIONAL STANDARDS FOR THE FORMATION OF SECURITY PROFILES FOR AUTOMATED SYSTEMS

In the context of military conflicts and hybrid confrontation of the 21st century, the systematic assessment of information security risks related to restricted-access information processed and stored in automated systems becomes particularly important for the formation of security profiles. Despite the existence of a regulatory framework in the field of technical information protection, one of the key challenges remains the practical implementation and compliance with the established procedures for information security risk assessment in order to further develop security profiles of different levels.

The main regulatory legal act governing the authorization procedure in the field of security is the Resolution of the Cabinet of Ministers of Ukraine dated June 18, 2025, No. 712. This document establishes unified rules for authorization for all entities operating relevant systems, regardless of their form of ownership or subordination [1]. The legal framework is also complemented by the Law of Ukraine “On Information”, the Law of Ukraine “On the Basic Principles of Cybersecurity of Ukraine”, ND TZI 3.6-006-24, ND TZI 2.5-004-99, DSTU ISO/IEC 27001:2023, DSTU ISO/IEC 27002:2023 (adapted national versions), and other regulatory acts.

Let us consider international standards and methodologies for information security risk assessment. ISO 27005 is a standard from the ISO/IEC 2700x series that describes an approach to organizing the entire information security risk management process [2]. The NIST SP 800-30 standard presents approaches not only to risk assessment but also to organizing information security risk management activities at various levels [3]. The CRAMM methodology, developed by the UK Government Security Service, is based on the BS7799 information security management standards and describes an approach to qualitative risk assessment [4]. The OCTAVE method, developed at Carnegie Mellon University, provides for assessing the criticality of threats, assets, and vulnerabilities [5]. The COBIT for Risk methodology [6], developed by the ISACA association, is based on best practices in risk management (COSO ERM, ISO 31000, ISO/IEC 27xxx, etc.). This methodology considers information security risks in relation to the organization's core business risks and describes approaches to implementing information security risk management functions within an organization, as well as processes for qualitative risk analysis and risk management. The BSI

Standard 200-3 methodology (formerly known as IT-Grundschutz Risk Analysis) is a German standard that regulates the approach to information security risk assessment within the IT-Grundschutz framework [7]. This methodology enables effective evaluation and management of risks.

The analysis of most international methodologies has shown that they are often insufficiently productive and informative for practical application in current real-world conditions. The reviewed international standards and methodologies lack clear recommendations and guidelines for implementing a specific algorithm of actions; moreover, they are based on the standards of the countries in which they were developed and primarily determine compliance with a standard rather than the actual level of security. Considering the results of the analysis, it appears appropriate to apply an improved and adapted approach to determining the degree of risk. Such an approach would make it possible to obtain consistent results regardless of the experience and qualifications of the specialist conducting the risk assessment.

References

1. Cabinet of Ministers of Ukraine. Resolution No. 712 of 18 June 2025 “On Approval of the Procedure for Security Authorization of Information and Communication Systems”.
2. DSTU ISO/IEC 27005:200.335. Information technology — Security techniques — Information security risk management. Kyiv: SE “UkrNDNC”, 200.335. — 60 c.
3. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments [Electronic resource] : National Institute of Standards and Technology. — Gaithersburg, MD : U.S. Department of Commerce, 2012. — 95 p. — Mode of access: <https://doi.org/10.6028/NIST.SP.800-30r1>.
4. UK Government Commerce. CRAMM: Risk Analysis and Management Method. London : The Stationery Office. URL: <https://www.cramm.com>.
5. Alberts C., Dorofee A. OCTAVE® Method Implementation Guide (Version 2.0). Pittsburgh : Software Engineering Institute, Carnegie Mellon University, 2001. URL: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419>.
6. ISACA. COBIT 2019 Framework: Governance and Management Objectives. Rolling Meadows, IL: ISACA, 2018. URL: <https://www.isaca.org/resources/cobit>.
7. BSI-Standard 200-3. IT-Grundschutz Methodology: Risk Analysis [Electronic resource] : Federal Office for Information Security. — Bonn : BSI, 2017. — 64 p.

УДК 004.056

Ніколаєнко М.В., здобувачка
Шелуха О.О., к.т.н. доцент

Державний університет «Житомирська політехніка»

МОДЕЛЮВАННЯ ІНТЕГРОВАНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДЛЯ МЕДИЧНОГО ЗАКЛАДУ

Сучасні медичні заклади стикаються з необхідністю впровадження надійних систем безпеки, здатних ефективно контролювати доступ до різноманітних зон лікарень. Велика кількість працівників, пацієнтів і відвідувачів значно збільшує ризики несанкціонованого проникнення до службових приміщень, медичних кабінетів та зон зберігання медикаментів. Традиційні способи захисту, як-от використання звичайних замків чи фізична охорона, не завжди відповідають сучасним вимогам. У зв'язку з цим все більш актуальним стає впровадження інтегрованих систем контролю доступу, побудованих на основі сучасних апаратних і програмних рішень.

Основним завданням даної роботи було створення макету інтегрованої системи контролю доступу для медичного закладу, що використовує мікроконтролерну платформу та технології ідентифікації користувачів.

У рамках проєкту розроблено експериментальний стенд (рис.1), який моделює три ключові функціональні зони медичного закладу.



Рисунок 1 – Експериментальний макет системи контролю доступу

Перша зона представлена реєстратурою, яка оснащена камерою відеоспостереження. Це дозволяє вести ефективний моніторинг

відвідувачів і персоналу, а також записувати події, що відбуваються у зоні прийому пацієнтів.

Друга зона — кабінет лікаря. Контроль доступу до цієї частини реалізується за допомогою мікроконтролерної плати Wemos D1 (ESP8266) та RFID-зчитувача. Вхід до кабінету здійснюється виключно через RFID-картки, що дозволяють ідентифікувати користувача і надавати доступ лише уповноваженим особам.

Третя зона призначена для зберігання медикаментів і має забезпечувати підвищений рівень захисту. Для цього в системі контролю доступу застосовується системи двофакторної автентифікації, яка включає введення секретного коду та підтвердження доступу за допомогою RFID-картки. Після успішного проходження перевірки електронний замок відкривається. Застосування такої двофакторної системи контролю доступу суттєво знижує ймовірність несанкціонованого доступу до контрольованої зони.

Проведене тестування роботи розробленого макету демонструє ефективність інтеграції систем відеоспостереження, RFID-ідентифікації та багатофакторної автентифікації. Використання таких технологічних рішень дозволяє значно підвищити рівень безпеки в медичних закладах і забезпечити контроль над доступом до критично важливих зон.

Отже, результатом роботи є макет інтегрованої системи контролю доступу, який може слугувати основою для впровадження аналогічних рішень у сучасних медичних установах, що сприятиме забезпеченню належного рівня фізичної та інформаційної безпеки на кожному рівні функціонування таких закладів.

Список використаних джерел

1. Klaus Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. Wiley, 2010.
2. Kolban N. ESP8266 Technical Reference. [URL: https://github.com/esp8266/esp8266-wiki](https://github.com/esp8266/esp8266-wiki)
3. ISO/IEC 27001:2022 Information Security Management Systems – Requirements.
4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

УДК 004.7

Капранчук В.М., здобувачка

Шелуха О.О., к.т.н., доцент

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ЯКОСТІ ТА БЕЗПЕКИ WI-FI МЕРЕЖ ІЗ ВИКОРИСТАННЯМ ПРОГРАМНОГО СНІФФЕРА

На сьогодні бездротові мережі Wi-Fi стали однією з найпоширеніших технологій доступу до мережі Інтернет. Вони використовуються у навчальних закладах, офісах, громадських місцях та домашніх мережах. Основними перевагами такої технології є зручність використання, мобільність користувачів та відсутність необхідності прокладання кабельної інфраструктури. Проте разом із цим виникають певні проблеми, пов'язані з якістю з'єднання та безпекою передавання даних у бездротовому середовищі.

Якість роботи Wi-Fi мережі може залежати від багатьох факторів. Серед них можна виділити рівень сигналу, завантаженість радіоканалу, кількість підключених пристроїв, а також наявність різних перешкод в радіоефірі. У результаті цього можуть виникати проблеми зі швидкістю передавання даних, затримки під час роботи мережі або навіть часткова втрата пакетів. Такі ситуації особливо помітні у місцях із великою кількістю користувачів, де мережа працює під значним навантаженням.

Крім того, бездротові мережі можуть бути вразливими до різних загроз інформаційної безпеки. Оскільки передавання даних здійснюється через відкритий радіоканал, зловмисники потенційно можуть намагатися перехоплювати трафік або підключатися до мережі без дозволу. Саме тому важливо здійснювати постійний моніторинг роботи Wi-Fi мережі та аналізувати її стан.

Одним із інструментів, який дозволяє досліджувати роботу мережі, є програмний сніффер (рис.1). Сніффер являє собою програмний засіб для перехоплення та аналізу мережевих пакетів. У випадку бездротових мереж мережевий адаптер може працювати у спеціальному режимі моніторингу, що дає можливість отримувати інформацію про пакети, які передаються у радіоефірі. Завдяки цьому можна аналізувати параметри роботи мережі, наприклад рівень сигналу, інтенсивність трафіку, активність підключених пристроїв та інші характеристики.

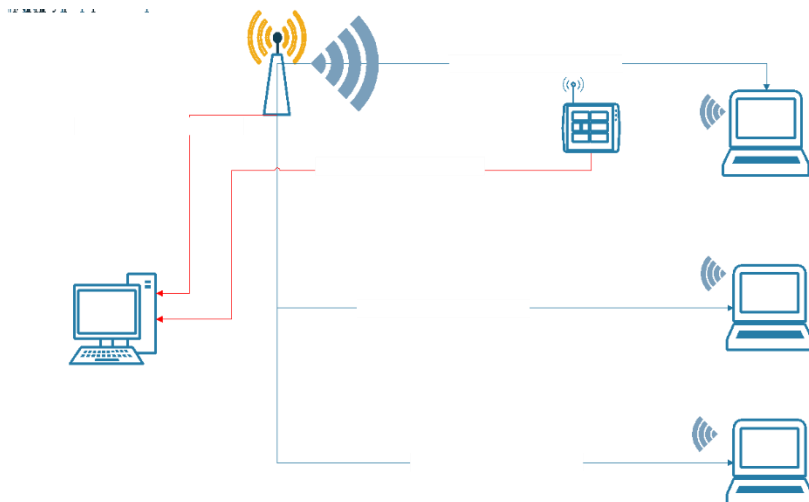


Рисунок 1 – Схема роботи мережевого sniffера

Аналіз отриманих даних дозволяє оцінити якість функціонування бездротової мережі та визначити можливі причини зниження її продуктивності. Також використання sniffера може допомогти у виявленні підозрілої активності у мережі або несанкціонованих підключень, що є важливим з точки зору інформаційної безпеки.

Таким чином, використання програмних засобів аналізу мережевого трафіку дозволяє більш детально досліджувати роботу Wi-Fi мереж та отримувати корисну інформацію про їх функціонування. Результати такого дослідження можуть бути використані для покращення параметрів роботи мережі, оптимізації її налаштувань та підвищення рівня безпеки передавання даних.

Список використаних джерел

1. Gast M. *802.11 Wireless Networks: The Definitive Guide*. – Sebastopol: O'Reilly Media, 2013.
2. Kurose J., Ross K. *Computer Networking: A Top-Down Approach*. – Boston: Pearson, 2021.
3. Tanenbaum A., Wetherall D. *Computer Networks*. – 5th ed. – Pearson Education, 2011.

УДК 004.056:004.8

Левченко В.О., здобувач

Миша М.А., здобувач

Петляк Н.С., д. філ., доцент

Хмельницький національний університет

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕС АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасних умовах зростання кіберзагроз традиційні підходи до аудиту інформаційної безпеки (ІБ) часто виявляються недостатньо ефективними. Складність ІТ-інфраструктур і великий обсяг даних ускладнюють виявлення прихованих аномалій та потенційних вразливостей. У зв'язку з цим актуальним стає застосування технологій штучного інтелекту (ШІ) для підвищення ефективності аудиту. Інструменти ШІ дозволяють автоматизувати обробку великих масивів даних, аналізувати журнали подій, оцінювати конфігурації систем безпеки та виявляти атипову активність користувачів [1].

Метою роботи є дослідження можливостей застосування ШІ на різних етапах аудиту ІБ та визначення переваг і ризиків такої інтеграції.

Аудит ІБ відповідає циклу PDCA (Plan–Do–Check–Act), що забезпечує постійне вдосконалення системи управління ІБ [2]. Інтеграція ШІ має враховувати основні принципи аудиту: об'єктивність, професіоналізм, конфіденційність і незалежність. За належного налаштування інтелектуальні системи здатні підвищити об'єктивність аналізу та зменшити вплив людського фактора.

Етап планування. На етапі планування визначаються цілі аудиту, оцінюються ризики та формується програма перевірки. Технології ШІ можуть застосовуватися для аналізу внутрішніх політик і нормативної документації, обробки великих обсягів даних та автоматизованого виявлення потенційних ризиків. Зокрема, методи обробки природної мови забезпечують швидке опрацювання текстових документів і підтримують комплексний аналіз даних із різних джерел. Ефективність таких систем значною мірою залежить від якості вхідної інформації.

Етап виконання аудиту. У процесі проведення аудиту перевіряється відповідність інформаційних систем вимогам безпеки та ефективність захисних механізмів. Інструменти ШІ можуть аналізувати журнали подій, мережевий трафік, поведінку користувачів і конфігурації систем, а також інтегрувати дані з SIEM, сканерів вразливостей і засобів тестування на проникнення. А використання алгоритмів машинного навчання дозволяє автоматично виявляти аномалії, підозрілу активність і потенційні канали витоку інформації.

Формування аудиторського звіту. ІІІ може підтримувати структурування результатів аудиту, формування попередніх висновків і рекомендацій щодо усунення виявлених ризиків. За умов глибокої інтеграції такі системи здатні генерувати структурований звіт у напівавтоматичному режимі, однак остаточне підтвердження результатів повинно здійснюватися аудиторською групою.

Етап перевірки та вдосконалення. На завершальному етапі оцінюється ефективність проведеного аудиту та визначаються напрями вдосконалення процедур. Інтелектуальні системи можуть аналізувати досягнення цілей аудиту, узагальнювати зворотний зв'язок і формувати пропозиції щодо оптимізації програми аудиту. За умов постійного моніторингу такі технології сприяють переходу від періодичних перевірок до проактивного управління ІБ.

Для узагальнення можливостей використання ІІІ на різних етапах аудиту доцільно систематизувати основні завдання та функції, що можуть бути автоматизовані. Узагальнену характеристику відповідних можливостей подано в таблиці 1.

Таблиця 1 - Основні можливості застосування ІІІ в аудиті

Етап аудиту	Завдання	Можливості ІІІ
планування	аналіз документації	автоматичний аналіз політик
	оцінка ризиків	аналіз великих масивів даних
виконання	аналіз журналів	виявлення аномалій
	перевірка конфігурацій	автоматична перевірка
перевірка	аналіз результатів	кластеризація інцидентів
удосконалення	формування рекомендацій	генерація звітів

Результати дослідження свідчать, що застосування ІІІ в аудиті ІБ може суттєво підвищити ефективність аудиторських процесів. Інтелектуальні системи дозволяють автоматизувати рутинні операції, швидко обробляти великі обсяги даних і виявляти потенційні загрози. Що сприяє підвищенню точності аналізу, зменшенню впливу людського фактора та покращенню якості аудиторських висновків.

Список використаних джерел

1. Fajrillah F., et al. Improving Information System Audit Security through Artificial Intelligence (AI) Technology Integration. Journal of Technology and Computer. 2025. № 2 (2). pp. 88–92. URL: <https://journal.technolabs.co.id/index.php/jotechcom/article/view/54>.

2. Чалий О., Толюпа С. Порівняння міжнародних стандартів аудиту інформаційної безпеки з перспективою автоматизації. Кібербезпека: освіта, наука, техніка. 2025. № 3 (31). С. 579–588. DOI: 10.28925/2663-4023.2025.31.1046.

УДК 004.056

Костерев Д. С., ст. наук. спів.

Шельвестер В.Я., начальник факультету

Житомирський військовий інститут імені С. П. Корольова

**РОЛЬ ОЦІНКИ РИЗИКІВ У СИСТЕМІ АВТОРИЗАЦІЇ З
БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ КЛАСУ “З”, ДЕ
ОБРОБЛЯЄТЬСЯ ІНФОРМАЦІЯ, ЩО СТАНОВИТЬ
ДЕРЖАВНУ ТАЄМНИЦЮ**

Забезпечення надійного захисту інформації в умовах сьогодення є одним із найбільш пріоритетних завдань держави, зокрема, коли йдеться про автоматизовані системи класу “З”, в яких обробляється інформація, що становить державну таємницю. З ухваленням Постанови Кабінету Міністрів України № 712 від 18 червня 2025 року (далі - Постанова № 712) [1], парадигма технічного захисту інформації в Україні зазнала докорінних трансформацій. На зміну класичним, статичним комплексним системам захисту інформації (КСЗІ), які раніше проходили одноразову державну експертизу та отримували атестат відповідності на тривалий термін, прийшла гнучка, динамічна та безперервна система авторизації з безпеки. У цій архітектурі управління кіберзахистом оцінка ризиків перестала бути одним із формальних етапів передпроектного обстеження і повернулася на новий фундамент, системо утворююча основа, яка створює весь життєвий цикл безпеки системи [2].

Роль оцінки ризиків у системі авторизації передусім виникає в тому, що вона є абсолютно обов'язковим аналітичним базисом для будь-якого проектування заходів захисту, без якого подальші процедури неможливі. В автоматизованих системах класу “З”, які відзначаються високим рівнем розподільності, наявністю віддалених вузлів та підвищеними вимогами до конфіденційності й цілісності інформації, досягти абсолютної технічної безпеки на всіх безперервних рівнях практично неможливо. Саме тому оцінка ризиків дозволяє власникам (розпорядникам) автоматизованих систем стратегічно зосередитися на ідентифікації та захисті найбільш критично важливих компонентів системи, формуючи математично та економічно обґрунтовану модель протидії актуальним загрозам [2]. Згідно з методологічними алгоритмами, цей процес забезпечує глибоку ідентифікацію вразливих систем, скрупульозний аналіз і ймовірність використання вразливих сучасних загроз, оцінювання отриманих руйнівних наслідків, обчислення вартості виконання атак зловмисника та порівняння її з вартістю впровадження ефективних контрзаходів.

Основне місце оцінки ризиків яскраво розкривається через механізм формування цільових профілів безпеки, який є основою нової системи

авторизації [1]. Відповідальність для створення повноцінної, стійкої до зламів системи захисту повністю покладається на власника або розпорядника системи, який зобов'язаний розробити індивідуалізований цільовий профіль безпеки. Формування цільового профілю забезпечується шляхом додавання до вимог базового або галузевого профілю додаткових, спеціальних заходів кіберзахисту, які обираються суворо на основі результатів глибокої внутрішньої оцінки ризиків.

Оцінка ризиків критично впливає на момент ухвалення юридичного рішення про авторизацію автоматизованої системи. Відповідно до встановлених законодавством вимог, надання авторизації можливо лише за одночасного безумовного виконання двох ключових умов: по-перше, впроваджені технічні та організаційні заходи кіберзахисту повинні бути визнані достатніми для протидії поточному рівню загрози; по-друге, що є надзвичайно важливим, усі залишкові ризики повинні бути достеменно ідентифіковані, оцінені та офіційно визнані прийнятими для власника інформації [3]. Якщо залишкові ризики, пов'язані з обробкою інформації, що становить державну таємницю в АС класу "3", значно перевищують допустимі межі і не можуть бути технічно нейтралізованими існуючими заходами, система не пройде процедуру авторизації та не отримає законного дозволу на функціонування.

Таким чином, оцінка ризиків виступає єдиним легітимним інструментом для обґрунтування того, які саме криптографічні, апаратні, програмні чи організаційні рішення повинні бути застосовані в конкретних системах для нейтралізації загроз. Під час самої процедури авторизації уповноважені органи перевіряють систему на відповідність розробленому цільовому профілю, що робить повноту первинної оцінки ризиків визначальним фактором для успішного отримання статусу авторизованої системи.

Список використаних джерел

1. Постанова Кабінету Міністрів України від 18 червня 2025 року № 712 "Про затвердження Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем".
2. ДСТУ ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. – Київ: ДП "УкрНДНЦ", 200.335. – 60 с.
3. BSI-Standard 200-3. IT-Grundschutz Methodology: Risk Analysis [Electronic resource] : Federal Office for Information Security. — Bonn : BSI, 2017. — 64 p.

Брага В. Ю., здобувач

Дячук О.Ю., ст. викладач

Колошук М.С., ст. викладач

Державний університет «Житомирська політехніка»

У сучасних телекомунікаційних системах дедалі більшого поширення набувають гібридні мережеві архітектури, що передбачають одночасне використання декількох протоколів динамічної маршрутизації. Такий підхід забезпечує масштабованість, гнучкість і відмовостійкість мережевої інфраструктури. Водночас інтеграція різнорідних протоколів маршрутизації, зокрема OSPF та EIGRP, принципи функціонування яких визначені у відповідних стандартах [1-2], потребує застосування механізмів редистрибуції маршрутів, що може призводити до порушення узгодженості маршрутної інформації, виникнення маршрутних петель та зниження стабільності мережі.

Метою роботи є комплексне дослідження процесів редистрибуції маршрутів між протоколами OSPF та EIGRP та оцінка їх впливу на функціональні характеристики мережі в середовищах EVE-NG та Cisco Packet Tracer.

Дослідження проведено із застосуванням експериментального методу моделювання мережових процесів у середовищах EVE-NG та Cisco Packet Tracer.

Розроблено модель гібридної мережі, що об'єднує домени маршрутизації OSPF та EIGRP (рис. 1). Моделювання виконано у середовищах EVE-NG та Cisco Packet Tracer.

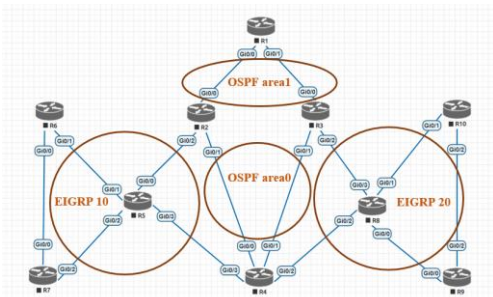


Рисунок 1 – Схема гібридної маршрутизації з редистрибуцією в середовищі EVE-NG

Використано також ієрархічну модель побудови мережі (рис. 2), що включає рівні ядра (Core), розподілу (Distribution) та доступу (Access).



Рисунок 2 – Ієрархічна топологія мережі в середовищі Cisco Packet Tracer

Для проведення дослідження сформовано набір експериментальних сценаріїв.

Таблиця 1

Експериментальні сценарії дослідження редистрибуції

№	Сценарій	Опис	Очікуваний ефект
1	Базова редистрибуція	обмін маршрутами між OSPF та EIGRP	стабільна маршрутизація
2	Відмова каналу	імітація відмови лінка	аналіз часу конвергенції
3	Некоректні метрики	різні значення метрик	порушення балансування
4	Без фільтрації	відсутність механізмів фільтрації та route tagging	виникнення routing loop
5	Оптимізована модель	фільтрація маршрутів та route tagging	стабілізація мережі

У процесі моделювання реалізовано двосторонню редистрибуцію маршрутів між протоколами OSPF та EIGRP. Приклад базового налаштування наведено нижче:

```
router ospf 1
 redistribute eigrp 100 subnets
```

```
router eigrp 100
 redistribute ospf 1 metric 10000 100 255 1 1500
```

Лістинг 1 – Базове налаштування двосторонньої редистрибуції маршрутів між OSPF та EIGRP

Наведені конфігурації відповідають рекомендаціям виробника мережевого обладнання щодо реалізації редистрибуції маршрутів [4, 5].

Оцінювання ефективності здійснювалося за критеріями: час конвергенції, стабільність маршрутних таблиць, узгодженість маршрутної інформації та наявність маршрутних петель, що відповідає підходам до аналізу продуктивності протоколів маршрутизації [6].

Таблиця 2

Порівняльні результати дослідження

Параметр	Базова конфігурація	Оптимізована конфігурація
Час конвергенції	більший	менший
Стабільність маршрутизації	нижча	вища
Імовірність routing loop	наявна	мінімізована
Узгодженість маршрутів	часткова	повна

Таблиця 3

Порівняння середовищ моделювання

Критерій	EVE-NG	Cisco Packet Tracer
Точність емуляції	висока	середня
Підтримка функцій	повна	обмежена
Зручність використання	середня	висока
Дослідницька придатність	висока	базова

Отримані результати узгоджуються з сучасними дослідженнями [3, 7], що підтверджують значний вплив механізмів редистрибуції на стабільність гібридних мереж.

У результаті дослідження встановлено, що основними чинниками, які впливають на ефективність редистрибуції маршрутів, є узгодженість метрик, наявність механізмів фільтрації маршрутів та контроль поширення маршрутної інформації. Виявлено, що відсутність зазначених механізмів призводить до виникнення маршрутних петель, збільшення часу конвергенції та неузгодженості таблиць маршрутизації.

Отримані результати підтвердили доцільність використання середовища EVE-NG для моделювання складних сценаріїв міжпротокольної взаємодії, тоді як Cisco Packet Tracer доцільно застосовувати для базового аналізу та навчального моделювання.

У роботі запропоновано підхід до оптимізації процесів редистрибуції маршрутів, що базується на використанні фільтрації маршрутів, узгодженні метрик та застосуванні механізму маркування маршрутів (route tagging). Показано, що впровадження зазначених

методів дозволяє підвищити стабільність мережі, зменшити час конвергенції та запобігти виникненню маршрутних петель.

Таким чином, отримані результати можуть бути використані при проектуванні та оптимізації сучасних корпоративних мереж із гібридною маршрутизацією, а також у навчальному процесі підготовки фахівців у галузі кібербезпеки та комп'ютерної інженерії.

Список використаних джерел

1. RFC 2328. OSPF Version 2. IETF. URL: <https://datatracker.ietf.org/doc/html/rfc2328>
2. RFC 7868. Cisco's EIGRP. IETF. URL: <https://datatracker.ietf.org/doc/html/rfc7868>
3. Medhi D., Ramasamy K. *Network Routing: Algorithms, Protocols, and Architectures*. Morgan Kaufmann, 2017. URL: <https://www.sciencedirect.com/book/9780128007372/network-routing>
4. Cisco Systems. OSPF Design Guide. URL: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>
5. Cisco Systems. EIGRP Configuration Guide. URL: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html>
6. Kumar V., Singla S. A Performance Analysis of MANET Routing Protocols // *International Journal of Engineering Technology and Management Sciences*. 2022. URL: https://www.researchgate.net/publication/365802442_A_Performance_Analysis_of_MANET_Routing_Protocols
7. Kvalbein A., Hansen A., Cicic T. Multiple Routing Configurations for Fast IP Network Recovery. URL: https://www.researchgate.net/publication/220429606_Multiple_Routing_Configurations_for_Fast_IP_Network_Recovery

Підсистема працює у потоковому режимі, що дозволяє аналізувати події у процесі їх надходження та відображати актуальний стан системи.

У межах дослідження розроблено програмний генератор Syslog-повідомлень, який імітує роботу маршрутизаторів та комутаторів Cisco. Генератор формує як фонові інформаційні повідомлення, так і детерміновані сценарії інцидентів, що складаються з послідовності взаємопов'язаних логів.

Особливістю є інтеграція метрик продуктивності безпосередньо у Syslog-повідомлення, що дозволяє одночасно обробляти текстові події та числові показники без зовнішніх джерел даних [6].

Якість та достовірність генерації логів підтверджено експериментально. На рис. 2 наведено приклади синтетичної достовірності згенерованих повідомлень, що відповідають реальним Syslog-повідомленням Cisco.

Рисунок 2 – Приклади синтетичної достовірності генерації логів

Центральним елементом підсистеми є аналітичне ядро, яке реалізує алгоритми парсингу, класифікації та кореляції подій. Ключовим архітектурним рішенням є використання гібридного кінцевого автомату (FSM), що керує життєвим циклом інцидентів.

Використання FSM забезпечує стабільність статусів інцидентів шляхом переходу між станами лише за умов повторюваності або тривалості подій, що зменшує кількість хибно-позитивних спрацювань [5].

Наукова новизна полягає у поєднанні кореляційного аналізу Syslog-подій з моделлю кінцевого автомату для формування стабільних логічних інцидентів у реальному часі.

Стан системи під час розвитку критичного інциденту наведено на рис. 3, де відображено одночасно:

- текстові Syslog-повідомлення;
- критичний стан FSM;
- пікові значення завантаження CPU.

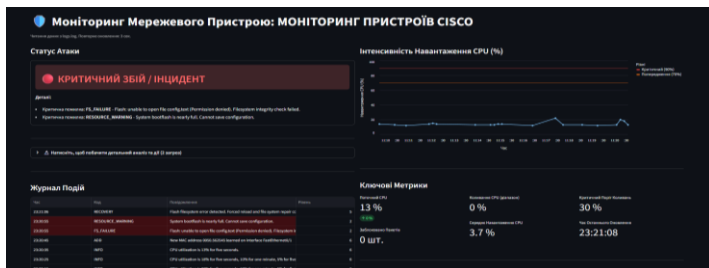


Рисунок 3 – Стан системи під час критичного інциденту

Однією з ключових переваг розробленої підсистеми є реалізація кореляційної візуалізації, яка поєднує логічний та ресурсний стани мережевого пристрою. Оператор отримує можливість в одній точці інтерфейсу зібрати причину інциденту та його вплив на продуктивність.

Окрім виявлення інцидентів, система формує підказки щодо можливих дій з їх усунення. На рис. 4 наведено приклад інтерфейсу з рекомендаціями для адміністратора, які формуються на основі типу події та її контексту.

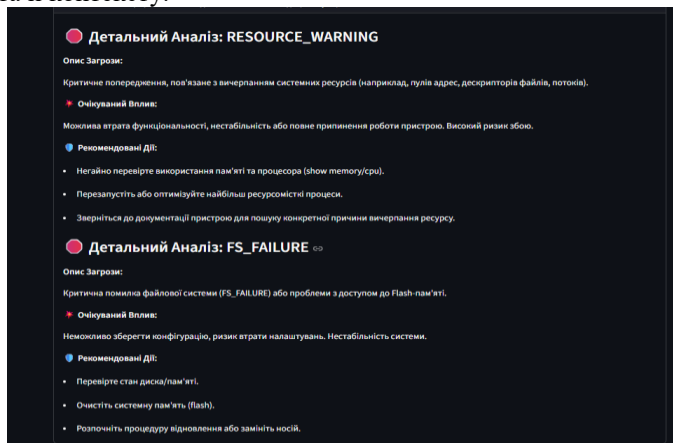


Рисунок 4 – Інтерфейс аналізу інцидентів та рекомендацій для реагування

Запропонований підхід скорочує час реагування та знижує когнітивне навантаження на оператора.

Апробація розробленої підсистеми проводилася на серії змодельованих сценаріїв, що охоплювали нормальну роботу мережі, агреговані атаки типу brute force та критичні перевантаження ресурсів. У ході тестування підтверджено коректність:

- генерації подій;
- агрегації однотипних логів;
- кореляції подій і метрик;
- переходів FSM між станами.

Результати експериментів свідчать про зменшення кількості відображених подій та підвищення інформативності моніторингу.

Подальший розвиток розробленої програмної підсистеми доцільно спрямувати на розширення підтримуваних типів Syslog-повідомлень мережевого обладнання Cisco, зокрема шляхом охоплення повного спектра системних, безпекових та сервісних логів, визначених у офіційній документації виробника. Це дозволить підвищити повноту охоплення подій та забезпечити більш точну кореляцію інцидентів у складних мережевих середовищах. Окрім цього, перспективним напрямом є адаптація підсистеми для аналізу логів мережевого обладнання інших виробників (Juniper, MikroTik, Huawei тощо), що забезпечить уніфікований підхід до моніторингу подій кібербезпеки в мультивендорних інфраструктурах та розширить практичну застосовність запропонованого рішення.

Розроблене рішення має практичну цінність та може бути використане як самостійний інструмент моніторингу або як модуль у складі корпоративних систем безпеки. Важливою перевагою є те, що підсистема не обмежується лише середовищем моделювання і може бути у будь-який момент інтегрована з реальним мережевим обладнанням без необхідності суттєвих змін архітектури, забезпечуючи коректну роботу в умовах реальної інфраструктури.

Список використаних джерел

1. Cisco Systems. System Message Logging (Syslog). URL: <https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.htm>
2. He S., Zhu J., He P., Lyu M. R. A Survey on Automated Log Analysis for Reliability Engineering. arXiv. 2020. URL: <https://arxiv.org/abs/2009.07237>
3. RFC 5424. The Syslog Protocol / ed. by R. Gerhards. Internet Engineering Task Force (IETF), 2009. 39 p. URL: <https://datatracker.ietf.org/doc/html/rfc5424>
4. Cisco IOS Syslog Messages Explained. NetworkLessons. URL: <https://networklessons.com/system-management/cisco-ios-syslog-messages>
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>
6. He P., Zhu J., Zheng Z., Lyu M. R. Drain: An Online Log Parsing Approach with Fixed Depth Tree // 2017 IEEE International Conference on Web Services (ICWS). 2017. P. 33–40. URL: https://jiemingzhu.github.io/pub/pjbe_icws2017.pdf
7. OWASP Foundation. A09:2021 Security Logging and Monitoring Failures. URL: https://owasp.org/Top10/2021/A09_2021-Security_Logging_and_Monitoring_Failures/

УДК 004.7

*Макаревич С.О., здобувач
Дячук О.Ю., ст. викладач
Колоущук М.С., ст. викладач*

Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОЇ МАРШРУТИЗАЦІЇ В OSPF- МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ VPN

На сучасному етапі розвитку телекомунікаційних систем забезпечення безпеки мережевої інфраструктури є одним із ключових завдань функціонування організацій. Протоколи динамічної маршрутизації, зокрема OSPF (Open Shortest Path First), широко застосовуються для побудови масштабованих і відмовостійких мереж. Водночас базова специфікація OSPF не передбачає повноцінних механізмів шифрування переданих даних, що створює потенційні загрози порушення конфіденційності та цілісності інформації [4].

Метою роботи є підвищення рівня безпеки OSPF-мереж шляхом інтеграції VPN-технологій для захисту маршрутної інформації.

Наукова новизна полягає у запропонованому підході до інтеграції протоколу OSPF із VPN-тунелями для забезпечення захисту службового маршрутизаційного трафіку.

До основних загроз, пов'язаних із використанням OSPF, належать атаки підміни маршрутів (route spoofing), що призводять до перенаправлення трафіку через несанкціоновані вузли, атаки типу «людина посередині» (Man-in-the-Middle), які дозволяють перехоплювати та змінювати передані дані, а також replay-атаки, що передбачають повторне використання перехоплених пакетів. Окрім цього, атаки типу відмови в обслуговуванні (DoS) можуть реалізовуватися шляхом перевантаження мережі надлишковими LSA-повідомленнями, що призводить до деградації продуктивності мережевих пристроїв.

Для підвищення рівня захисту мережевої взаємодії доцільним є використання технологій віртуальних приватних мереж (VPN), які забезпечують створення захищених тунелів передачі даних у недовіреному середовищі. VPN реалізує механізми шифрування, автентифікації та контролю цілісності інформації, що дозволяє ефективно захищати як користувацький, так і службовий трафік.

Серед протоколів, що застосовуються у VPN-рішеннях, особливе місце займає IPsec (Internet Protocol Security), який забезпечує захист IP-трафіку на мережевому рівні шляхом шифрування та автентифікації пакетів [5, 6]. Використання IPsec дозволяє гарантувати

конфіденційність маршрутних оновлень OSPF та запобігти несанкціонованому втручанню в процес маршрутизації.

Методами дослідження є аналіз наукових джерел і стандартів, а також моделювання мережевої взаємодії у середовищі GNS3 із використанням маршрутизаторів Cisco та протоколу OSPF у поєднанні з VPN-технологіями.

У межах дослідження розглянуто архітектуру мережі, що включає взаємодію між кількома маршрутизаторами в ізольованому середовищі, у якій протокол OSPF функціонує всередині захищених VPN-тунелів. Такий підхід дозволяє ізолювати маршрутний трафік від зовнішнього середовища, забезпечити шифрування службових повідомлень та обмежити доступ до мережі лише автентифікованим пристроям.

У результаті моделювання встановлено, що використання VPN-технологій, зокрема IPsec, дозволяє:

- забезпечити шифрування маршрутних оновлень OSPF;
- знизити ризик реалізації атак типу Man-in-the-Middle та replay-атак;
- обмежити доступ до маршрутизаційної інформації лише автентифікованим вузлам;
- підвищити загальну стійкість мережі до атак на рівні маршрутизації.

Таким чином, інтеграція протоколу OSPF із VPN-технологіями є ефективним підходом до підвищення безпеки мереж. Запропонований підхід дозволяє забезпечити захист маршрутної інформації, зменшити ризики кіберзагроз та підвищити надійність функціонування мережевої інфраструктури, що підтверджує доцільність його застосування в сучасних умовах.

Список використаних джерел

1. Cisco Systems. Dynamic Routing Protocols: OSPF, EIGRP, RIPv2, IS-IS, BGP. URL: <https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577>
2. Shapira T., Shavitt Y. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding // NetAI, 2020. URL: <https://dl.acm.org/doi/10.1145/3405671.3405819>
3. Murphy S. Security Issues in OSPF Routing Protocol // RFC 6860, 2013. URL: <https://datatracker.ietf.org/doc/html/rfc6860>
4. RFC 2328. OSPF Version 2 Specification. URL: <https://datatracker.ietf.org/doc/html/rfc2328>
5. RFC 4301. Security Architecture for the Internet Protocol. URL: <https://datatracker.ietf.org/doc/html/rfc4301>
6. RFC 2401. Security Architecture for the Internet Protocol (IPsec). URL: <https://datatracker.ietf.org/doc/html/rfc2401>

УДК 004.8

*Сергєєв В.М., аспірант
П'ятаченко В.Ю., PhD., асистент
Сумський державний університет*

СИМУЛЯЦІЯ АТАК ПІДМІНИ КООРДИНАТ У НАВІГАЦІЙНИХ ДАНИХ ДЛЯ ТЕСТУВАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Супутникові навігаційні системи широко використовуються в безпілотних і транспортних платформах для визначення координат та навігації. Однією з основних загроз для таких систем є атаки підміни координат (GNSS spoofing), які дозволяють змінювати навігаційні дані без фізичного впливу на об'єкт. У зв'язку з цим активно розробляються методи виявлення подібних атак, зокрема на основі аналізу навігаційних параметрів і алгоритмів машинного навчання.

Ефективність таких підходів значною мірою залежить від наявності даних із реальними сценаріями атак. Проте їх отримання є складним, оскільки проведення експериментів із підробленням навігаційного сигналу потребує спеціалізованого обладнання та може бути обмежене умовами експлуатації. Тому доцільним є використання тестових середовищ, які дозволяють відтворювати сценарії атак шляхом математичної трансформації навігаційних даних.

У сучасних дослідженнях виявлення GNSS-спуфінгу широко застосовується аналіз навігаційних даних та часових рядів параметрів руху. У роботі [1] запропоновано використання глибоких нейронних мереж для аналізу навігаційних параметрів (координати, швидкість, курс), що дозволяє виявляти аномалії траєкторії без аналізу сирих GNSS-сигналів. У дослідженні [2] показано ефективність поєднання кількох груп ознак навігаційного стану, включаючи похідні координат та параметри руху, для підвищення точності виявлення атак. У роботі [3] розглянуто фізичну модель GNSS-спуфінгу, відповідно до якої атака реалізується шляхом зміни псевдовідстаней до супутників, що призводить до поступового відведення навігаційного рішення приймача.

Для формування наборів даних із контрольованими сценаріями атак розроблено веборієнтований інструмент із API, що дозволяє працювати з реальними позиційними даними повітряних суден. Як вхідні дані використовуються координати польоту, отримані з джерел авіаційного моніторингу. В режимі симуляції формується атакована траєкторія шляхом модифікації навігаційних параметрів (рис.1). Отримані дані зберігаються у вигляді часових рядів реальних та атакованих координат і можуть використовуватися для тестування алгоритмів виявлення атак підміни координат.

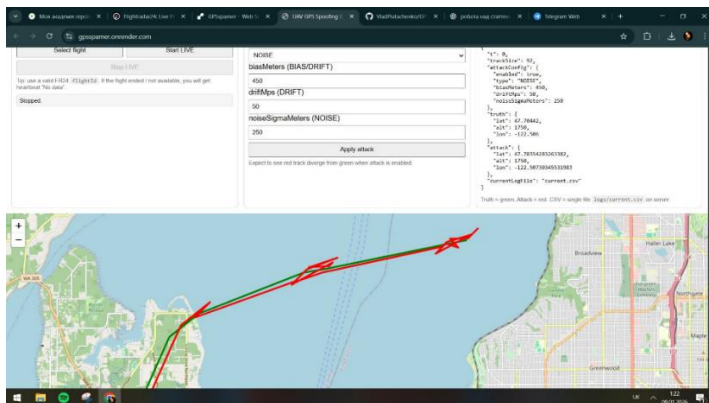


Рисунок 1 – Емуляція атаки підміни координат на основі реальної траєкторії руху об'єкта

Формування атакваних координат здійснюється шляхом додавання до реальної позиції комбінованої помилки, що складається із систематичного зміщення, поступового дрейфу та випадкового шуму. У загальному вигляді атакowana позиція визначається як

$$P_a(t) = P(t) + \Delta bias + \Delta drift(t) + \Delta noise,$$

де $\Delta bias$ задає постійне зміщення координат, $\Delta drift(t)$ моделює поступове відведення позиції від реальної траєкторії, а $\Delta noise$ представляє випадкову компоненту помилки. Компонента дрейфу відповідає типовому сценарію drag-off spoofing, у якому підроблений навігаційний сигнал поступово відводить розраховане положення приймача від реальної траєкторії без різких стрибків координат.

Реалізований підхід дозволяє формувати контрольовані сценарії атак та використовувати їх для тестування методів виявлення GNSS-спуфінгу. Подальші дослідження можуть бути спрямовані на розширення моделей атак і використання отриманих даних для навчання та оцінювання алгоритмів машинного навчання.

Список використаних джерел

1. Meng, L., Yang, L., Yang, W., & Zhang, L. (2022). A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sensing*, 14(19), 4826. <https://doi.org/10.3390/rs14194826>
2. He, Y., Zhuang, X., & Xu, B. (2025). Sparse Decomposition-Based Anti-Spoofing Framework for GNSS Receiver: Spoofing Detection, Classification, and Position Recovery. *Remote Sensing*, 17(15), 2703. <https://doi.org/10.3390/rs17152703>
3. Wang, W., Wang, J. (2022). GNSS induced spoofing simulation based on path planning. *IET Radar Sonar Navig.* 16(1), 103–112. <https://doi.org/10.1049/rsn2.12167>

УДК 004.056:004.738.5:004.8

*Плахтій М.О. к.е.н., доцент, професор
ТОВ Приватний вищий навчальний заклад «УНІВЕРСИТЕТ
СУЧАСНИХ ТЕХНОЛОГІЙ»*

НЕЛІНІЙНА ПОСТКВАНТОВА АВТЕНТИФІКАЦІЯ В ФЕДЕРАТИВНИХ СИСТЕМАХ

Сучасний розвиток інформаційних технологій супроводжується трансформацією криптографічних стандартів і моделей управління ідентичностями. Стандартизація постквантових алгоритмів формує основу переходу до рішень, стійких до квантових атак [1]. Водночас їх впровадження у федеративні системи потребує врахування складної взаємодії криптографічних, поведінкових і контекстних компонентів безпеки.

У таких умовах автентифікаційні процеси доцільно розглядати як динамічні системи з нелінійними властивостями. Рівень довіри формується під впливом кількох груп факторів – криптографічних, поведінкових, контекстних і міждомених. Зміна кожного з них впливає на загальний ризик непропорційно. Наведене підтверджує нелінійний характер функції прийняття рішень. Отже, модель автентифікації повинна забезпечувати адаптивну перебудову параметрів доступу.

Постквантові алгоритми обміну ключами та цифрового підпису утворюють квантово-стійке ядро системи [2]. Однак їх застосування не зводиться до заміни класичних примітивів. Необхідна інтеграція у комплексну архітектуру разом із механізмами ризик-орієнтованого контролю та адаптивного управління політиками [3]. У такій структурі криптографічні алгоритми забезпечують стійкість до квантових загроз. Натомість нелінійні механізми керування довірою забезпечують гнучкість і адаптивність.

Сучасні федеративні протоколи підтримують міждоменну взаємодію. Вона характеризується різними рівнями довіри та локальними політиками безпеки. Під час обміну атрибутами виникають нелінійні залежності між локальними та глобальними вимогами. Тому потрібна узгоджена модель, здатна поєднати класичні та постквантові механізми без втрати цілісності процесу. У цьому контексті нелінійна адаптація стає базовим принципом архітектури [4].

Автентифікацію запропоновано моделювати як нелінійну керовану систему зі зворотним зв'язком, у якій рівень довіри визначається на основі багатовимірної аналізи параметрів сесії. Адаптивне оцінювання ризику реалізується із застосуванням методів машинного навчання з урахуванням поведінкових і контекстних факторів, що забезпечує динамічну перебудову параметрів доступу. Інтеграція постквантових криптографічних алгоритмів формує квантово-стійке ядро

федеративної архітектури та забезпечує стійкість до квантових загроз. Запропонована модель поєднує криптографічний захист, адаптивне управління політиками та міждоменну координацію в єдину нелінійну структуру.

Наукова новизна полягає у формалізації постквантової автентифікації як цілісної нелінійної системи управління довірою, що забезпечує адаптивність і стійкість у федеративних середовищах. Запропонований підхід розглядає автентифікаційні процеси як єдину інтегровану архітектуру, у якій криптографічні та поведінкові механізми функціонують у межах нелінійної моделі. Така структура забезпечує узгоджене управління рівнем довіри та динамічну адаптацію параметрів доступу в умовах змінного середовища.

Таким чином, розроблення нелінійної моделі постквантової автентифікації у федеративних системах є актуальним науковим завданням. Реалізація такого підходу створює основу для побудови квантово-стійких, адаптивних і міждомених механізмів керування довірою в умовах складної динаміки сучасних інформаційних середовищ.

Список використаних джерел

1. NIST: Post-Quantum Cryptography (PQC) Project i NIST Releases First 3 Finalized Post-Quantum Encryption Standards, <https://csrc.nist.gov/projects/post-quantum-cryptography>.
2. National Institute of Standards and Technology. (2024, August 13). NIST releases first 3 finalized post-quantum encryption standards. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.
3. International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 24760-1:2025 Information security, cybersecurity and privacy protection – A framework for identity management. Part 1: Core concepts and terminology (3rd ed.). <https://www.iso.org/standard/24760-1>.
4. Фесенко Т., Калашнікова Ю. Використання Cisco SecureX для SOC-автоматизації. *Системи управління, навігації та зв'язку*. 2025. № 4 (82). С. 138–143. DOI: <https://doi.org/10.26906/SUNZ.2025.4.138>. URL: <https://journals.nupp.edu.ua/sunz/article/view/4119> (дата звернення: 04.02.2026).

УДК 004.056.5:004.77

*Пуцько Х.М., студент
Вовк Р.Б., к.т.н., доцент*

Івано-Франківський національний технічний університет нафти і газу

МЕТОДОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВЕБОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

На сучасному етапі розвитку інформаційних технологій вебсторінки та вебзастосунки є домінуючим інструментарієм взаємодії користувачів із розподіленими масивами даних. Протягом останніх років спостерігається суттєве ускладнення архітектури вебсистем, зумовлене інтенсивним впровадженням методів автоматизації та мікросервісних підходів. Паралельно з еволюцією вебтехнологій відбувається експоненціальне зростання кількості кіберзагроз, спрямованих на несанкціоноване отримання доступу до конфіденційної інформації або дестабілізацію функціонування інформаційних систем. Відповідно, проектування та розробка захищених систем стає одним із пріоритетних напрямів сучасної інженерії програмного забезпечення.

Для системного оцінювання та гарантування безпеки вебрішень доцільно застосовувати спеціалізовані моделі зрілості, зокрема OWASP SAMM (Software Assurance Maturity Model) та DSOMM (DevSecOps Maturity Model). Зазначені моделі пропонують комплексний методологічний підхід до інтеграції практик безпеки у життєвий цикл розробки програмного забезпечення та детермінують методи протидії релевантним загрозам. До найбільш критичних категорій уразливостей належать порушення механізмів контролю доступу, дефекти криптографічного захисту, а також атаки типу «ін'єкція» [1].

Однією з найбільш деструктивних проблем безпеки є порушення контролю доступу (Broken Access Control). Експлуатація даної уразливості дозволяє суб'єктам загрози отримати доступ до облікових записів, адміністративних панелей або баз даних, що створює умови для несанкціонованого підвищення привілеїв, модифікації або знищення інформаційних активів. Для нівелювання зазначених ризиків фахівці OWASP рекомендують впроваджувати рольові механізми автентифікації (RBAC), обмежувати доступ до функціональних модулів на рівні сервера та виключати можливість зберігання конфіденційних об'єктів у відкритих директоріях вебсервера [2].

Криптографічні збої посідають чільне місце в ієрархії загроз, оскільки призводять до експозиції конфіденційних даних. Забезпечення цілісності та конфіденційності інформації потребує впровадження стійких алгоритмів шифрування як для даних у стані спокою (Data at Rest), так і для даних, що передаються мережею (Data in Transit), з використанням актуальних протоколів безпеки [3]. Окрему групу

поширених атак становлять ін'єкції, що виникають внаслідок некоректної валідації вхідних параметрів. Це дозволяє зловмиснику маніпулювати SQL-запитами до бази даних, оскільки вебзастосунок не здатний диференціювати користувацьке введення від системних команд. Аналогічно, атаки типу XSS (Cross-Site Scripting) дозволяють здійснювати впровадження шкідливого коду у вебсторінки, що призводить до компрометації сесій користувачів у середовищі браузера. Превентивні заходи включають:

- використання параметризованих запитів;
- сувору типізацію та фільтрацію вхідних даних;
- регулярне проведення сканувань на наявність уразливостей.

Вибір архітектурного паттерну системи (монолітного або мікросервісного) безпосередньо детермінує стратегію забезпечення безпеки. У монолітній архітектурі централізація компонентів спрощує реалізацію контролю доступу. Натомість у мікросервісних системах критично важливу роль відіграє API Gateway, який функціонує як єдина точка входу, забезпечуючи автентифікацію, фільтрацію запитів та розмежування прав доступу до внутрішніх сервісів. Незалежно від обраної архітектури, фундаментальним аспектом є інтеграція сучасних стандартів автентифікації та авторизації, зокрема використання JSON Web Tokens у синергії з механізмами багатofакторної перевірки [3].

Таким чином, проєктування захищених веборієнтованих систем є комплексним завданням, що потребує системного підходу до вибору архітектурних рішень та методів захисту. Застосування сучасних криптографічних протоколів, суворих механізмів контролю доступу та методів валідації даних дозволяє мінімізувати ймовірність успішної реалізації кібератак та гарантувати стійкість інформаційних систем.

Список використаних джерел

1. OWASP Top 10:2025 – The Ten Most Critical Web Application Security Risks [Електронний ресурс]. OWASP Foundation. 2025. URL: <https://owasp.org/www-project-top-ten/> (дата звернення: 16.03.2026).
2. OWASP Top 10 Web Application Security Risks [Електронний ресурс]. URL: <https://surl.li/sxijuh> (дата звернення: 16.03.2026).
3. Almeida M., Canedo E. Authentication and Authorization in Microservices Architecture: A Systematic Literature Review. Applied Sciences. 2022. Vol. 12, No. 6. URL: <https://www.mdpi.com/2076-3417/12/6/3023> (дата звернення: 16.03.2026).

УДК 004.056

Охрімчук В. В. к.т.н., доцент, професор

Охрімчук І. А., викладач

Житомирський військовий інститут імені С. П. Корольова

МЕТОД ВИЯВЛЕННЯ ПОВІЛЬНИХ DDOS-АТАК

Стрімкий розвиток інформаційних технологій та глобальна цифровізація суспільства призвели до суттєвого зростання кількості кіберзагроз. Інформаційні системи державних установ, підприємств та об'єктів критичної інфраструктури постійно піддаються різноманітним типам кібератак. Сучасні тенденції розвитку кібератак свідчать не тільки про збільшення їх кількості, а й про зростання їх технологічної складності, що в свою чергу призводить до ускладнення їх виявлення.

Одним із найпоширеніших видів атак є атаки відмови в обслуговуванні (*Distributed Denial of Service, DDoS*), метою яких є порушення доступності інформаційних ресурсів шляхом перевантаження серверів або мережевої інфраструктури. Проте, особливу небезпеку становлять так звані повільні *DDoS*-атаки (*Slow DDoS attacks*), які відрізняються від класичних атак низькою інтенсивністю мережевого трафіку та використанням легітимних протокольних механізмів. На відміну від традиційних атак, що генерують значні обсяги трафіку, повільні атаки діють приховано, поступово виснажуючи доступні ресурси серверів за допомогою великої кількості частково відкритих або повільно оброблюваних з'єднань. Унаслідок цього сервер змушений підтримувати велику кількість активних сесій, що з часом призводить до закінчення його ресурсів і неможливості обслуговування легітимних користувачів.

Актуальність дослідження методів виявлення повільних *DDoS*-атак зумовлена саме складністю їх ідентифікації за допомогою традиційних систем виявлення вторгнень, в основу роботи яких покладено аналіз інтенсивності трафіку та виявлення аномалій в мережевих потоках. Однак повільні атаки генерують мінімальний обсяг даних і часто не перевищують порогових значень, встановлених системами моніторингу. У результаті такі атаки можуть залишатися непоміченими протягом тривалого часу, що призводить до поступового зниження продуктивності сервісів та втрати доступності інформаційних ресурсів.

Тому, одним із перспективних підходів до вирішення цієї проблеми є використання методів нечіткої логіки та теорії нечітких множин. Основна ідея такого підходу полягає у врахуванні невизначеності та нечітких характеристик мережевої поведінки. На відміну від класичних детермінованих методів, які використовують жорсткі порогові

значення, нечіткі моделі дозволяють оцінювати стан мережевого трафіку на основі ступеня належності параметрів до певних лінгвістичних змінних, таких як, наприклад, “низька швидкість передачі”, “тривалість з'єднання” або “кількість неповних запитів”.

Метод виявлення повільних *DDoS*-атак на основі нечітких множин передбачає аналіз кількох ключових параметрів мережевої взаємодії. До таких параметрів можуть належати тривалість *TCP*-з'єднань, швидкість передачі пакетів, кількість одночасних з'єднань від одного джерела, а також інтервали між пакетами. Кожен із цих параметрів описується нечіткими множинами з відповідними функціями належності. Після цього формується база нечітких правил, яка визначає можливі комбінації параметрів, характерні для повільних атак. Наприклад, якщо тривалість з'єднання значно перевищує звичні показники, швидкість передачі даних є низькою, а кількість активних з'єднань є значною, то ймовірність проведення повільної *DDoS*-атаки зростає.

Подальша обробка здійснюється за допомогою механізму нечіткого виведення Мамдані, який дозволяє агрегувати результати аналізу окремих параметрів і сформувати інтегральну оцінку рівня загрози. Отриманий результат може бути використаний для автоматичного прийняття рішень системами захисту, наприклад для обмеження підозрілих з'єднань, блокування джерел трафіку або активування додаткових механізмів перевірки.

Таким чином, застосування методу виявлення повільних *DDoS*-атак на основі теорії нечітких множин дозволить більш ефективно аналізувати складні та нечітко визначені характеристики мережевого трафіку. Використання такого підходу забезпечить підвищення точності виявлення прихованих атак, зменшення кількості хибних спрацювань та своєчасне реагування на загрози. Практична реалізація та впровадження запропонованого методу сприятиме підвищенню рівня захищеності інформаційних систем і забезпеченню стабільної роботи мережевих сервісів в умовах зростання кіберзагроз.

Список використаних джерел

1. Савченко В. А., Кожухівський А. Д., Ільїн О. Ю. Діагностування початку повільної *HTTP DDoS* атаки на основі двопараметричного кореляційного аналізу трафіку / Телекомунікаційні та інформаційні технології № 4, 2021. С. 28-40.
2. Tayama, S., Tanaka, H. Analysis of Slow Read DoS Attack and Communication Environment. Mobile and Wireless Technologies 2017. ICMWT 2017., vol 425. Springer, Singapore. pp 350–359.

УДК 004.056.57:004.89

Аннюк П.Б., студент

Вовк Р.Б., к.т.н., доцент

Івано-Франківський національний технічний університет нафти і газу

ЕВОЛЮЦІЯ ТА АРХІТЕКТУРНІ ОСОБЛИВОСТІ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ У СУЧАСНОМУ КІБЕРПРОСТОРІ

Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується експоненціальним розширенням поверхні атак. Традиційні системи виявлення вторгнень (IDS), засновані на детермінованих правилах та сигнатурному аналізі, демонструють низьку ефективність проти софістикованих векторів кібератак, зокрема вразливостей нульового дня (0-day), поліморфного шкідливого ПЗ та складних стійких загроз [1]. Концептуальний перехід від реактивного детектування до інтелектуального аналізу аномалій у великих масивах мережевого трафіку став можливим завдяки імплементації алгоритмів глибокого навчання. Ефективність захисту критичної інфраструктури корелює з обраною архітектурою IDS:

- мережеві системи (NIDS) - здійснюють моніторинг трафіку в реальному часі на рівні сегментів мережі. Основним деструктивним фактором для NIDS є широке застосування протоколів шифрування, що унеможливує інспекцію корисного навантаження.

- вузлові системи (HIDS) функціонують безпосередньо на кінцевих точках, аналізуючи події операційної системи. Вони є високоефективними для ідентифікації інсайдерських загроз, проте характеризуються значною ресурсомісткістю та складністю адміністрування [2].

Оптимальним підходом вважається впровадження гібридних систем, що синтезують переваги обох архітектур. Емпіричні дані [3] свідчать, що поєднання сигнатурних методів (точність виявлення відомих загроз — 94%, рівень False Positive — 3%) з аномальними методами на базі штучного інтелекту дозволяє нівелювати ризики, пов'язані з невідомими атаками, попри вищий рівень хибнопозитивних спрацювань останніх (до 18%).

Вибір математичного апарату є визначальним для продуктивності IDS. У сучасних дослідженнях виокремлюють такі групи алгоритмів:

1. Навчання з учителем - методи опорних векторів та Випадковий ліс демонструють високу стійкість до шумів. Випадковий ліс забезпечує точність понад 99.9% на верифікованих бенчмарках [1].

2. Навчання без учителя - алгоритми кластеризації (K-Means, DBSCAN) застосовуються для виявлення прихованих закономірностей у немаркованому трафіку.

3. Глибоке навчання:

- CNN - ефективні для ідентифікації просторових кореляцій у структурах пакетів.

- RNN/LSTM спеціалізуються на аналізі часових послідовностей, забезпечуючи детекцію багатоетапних вторгнень із точністю до 99.94%.

- Autoencoders використовуються для ідентифікації аномалій на основі метрик похибки реконструкції вхідних даних.

4. Перспективні напрями - трансформери, великі мовні моделі та пояснювальний штучний інтелект.

Парадигмальний зсув 2026 року полягає в інтеграції архітектур трансформерів та великих мовних моделей як когнітивних контролерів для гетерогенних даних. Для вирішення проблеми непрозорості («чорної скриньки») нейромереж впроваджуються методи пояснювального III, зокрема SHAP та LIME [3]. Це забезпечує інтерпретованість рішень IDS, що є критично важливим для цифрової криміналістики.

Окрему увагу приділено безпеці самих інтелектуальних систем. Захист від адверсаріальних атак (навмисного спотворення вхідних даних) реалізується через методи змагального тренування, ретельну санацію даних та ансамблювання моделей [1].

Отже, створення автономних когнітивних систем захисту вимагає комплексного поєднання гібридних архітектур, інноваційних моделей глибоко навчання та механізмів пояснювального штучного інтелекту. Такий підхід дозволяє трансформувати системи виявлення вторгнень із систем моніторингу в інструменти предиктивного аналізу, здатні блокувати загрози в превентивному режимі.

Список використаних джерел

1. Impact of Machine Learning on Intrusion Detection Systems [Електронний ресурс]. MDPI. 2026. URL: <https://www.mdpi.com/2078-2489/16/7/515> (дата звернення: 18.03.2026).

2. AI-Powered Intrusion Detection Systems: Challenges and Opportunities [Електронний ресурс]. ResearchGate. 2026. URL: <https://surli.cc/innphk> (дата звернення: 18.03.2026).

3. Explainable AI for Forensic Analysis: A Comparative Study of SHAP and LIME in Intrusion Detection Models [Електронний ресурс]. MDPI. 2026. URL: <https://www.mdpi.com/2076-3417/15/13/7329> (дата звернення: 18.03.2026).

УДК 004.85:004.41

Штукований М. О., магістрант
Духновська К. К., к.т.н., доцент

Київський національний університет імені Тараса Шевченка

МАШИННЕ НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ СЕМАНТИЧНИХ ПОМИЛОК У КОДІ

Розвиток сучасного програмного забезпечення (ПЗ) супроводжується зростанням кількості семантичних і логічних помилок, що становлять серйозну загрозу надійності систем. На відміну від синтаксичних дефектів, які ефективно виявляються традиційними лінтерами, семантичні помилки зазвичай проявляються лише під час виконання програми та вимагають розуміння контексту виконання коду. Зростання складності ПЗ обумовлює потребу в автоматизованих засобах на базі методів машинного навчання (МН), зокрема великих мовних моделей (LLM — *Large Language Models*), Transformer-архітектур та графових нейронних мереж (GNN — *Graph Neural Networks*), здатних аналізувати семантику коду в реальних умовах CI/CD-конвеєрів.

Огляд підходів. S. B. Hossain та ін. (2024) [1] запропонували фреймворк Toggle, у якому LLM виконує двоетапну обробку: локалізацію дефекту на рівні токенів та його подальше виправлення за допомогою оптимізованих промптів. На датасеті Defects4J точність Top-1 підвищилася на 2,3–54,4 % порівняно з базовими методами МН. A. Poniszewska-Marańda (2024) [2] дослідила використання архітектур Transformer та GNN для автоматичного виявлення семантичних дефектів, акцентувавши увагу на складнощах їхньої корекції через контекстну неоднозначність у великомасштабних проєктах.

S. Ullah та ін. (2023) [3] у межах проєкту SecLLMHolmes оцінили 8 моделей LLM на 228 сценаріях помилок, критичних для безпеки. Було виявлено системні обмеження в логічному міркуванні моделей, що обґрунтовує потребу в їх тонкому налаштуванні (*fine-tuning*) та застосуванні гібридних підходів. M. N. Rafi та ін. (2024) [4] розробили GNN із представленням коду у вигляді дерева синтаксичного аналізу (AST), проаналізувавши 6 052 дефекти з 307 репозиторіїв GitHub. K. Qayyum та ін. (2025) [5] досягли 64,7 % точності корекції семантичних помилок у мові Verilog завдяки методології RAG-LLM, що перевищило показники SOTA на 53,4 %.

Результати аналізу. Порівняння архітектур показало, що LLM демонструють перевагу у генеративному міркуванні [1, 5], тоді як GNN ефективніші у структурному аналізі великих кодових баз [4]. Системним обмеженням LLM залишається нестабільність логічного виведення [3], що підтверджує необхідність гібридизації (табл. 1).

Таблиця 1 – Порівняння моделей виявлення семантичних помилок

Модель	Тип помилок	Точність (Тор-1)	Датасет	Перевага
Toggle LLM [1]	Семантичні	+2,3–54,4 %	Defects4J	Токен-рівень
AST-GNN [4]	Логічні	SOTA vs покриття	6052 дефекти	AST-контекст
SecLLM Holmes [3]	Безпека	Обмежена	228 сценаріїв	Fine-tuning
RAG-LLM Verilog [5]	Функціональні	64,7 %	HDL-баги	RAG-корекція

Напрями подальших досліджень. Отримані результати свідчать, що найбільш перспективним напрямом є гібридизація LLM і GNN з механізмом RAG: LLM забезпечує генеративне міркування, GNN — структурний аналіз AST, а RAG — контекстуалізацію на доменних наборах дефектів. Пріоритетними напрямками подальших досліджень є: тонке налаштування моделей на пов'язаних з безпекою кодових базах, оцінювання гібридних архітектур на стандартних бенчмарках (Defects4J, CodeXGLUE) та дослідження застосовності підходів у низькорівневих мовах (Verilog, C/C++).

Висновки. LLM і GNN суттєво перевершують традиційні статичні аналізатори у виявленні семантичних помилок, проте кожна архітектура має власні обмеження: LLM — у стабільності логічного виведення, GNN — у генеративних можливостях. Встановлено, що гібридні підходи (RAG-LLM + AST-GNN) забезпечують найвищу ефективність: точність до 64,7 % у спеціалізованих доменах. Також встановлено, що ефективна система виявлення семантичних помилок має поєднувати обидві архітектури з механізмом RAG-індексації доменних дефектів. В перспективах подальших досліджень є оцінювання гібридних архітектур на розширених бенчмарках, тонке налаштування на доменних наборах даних та аналіз застосовності підходів у різних мовах програмування.

Список використаних джерел

1. Hossain S. B. A Deep Dive into Large Language Models for Automated Bug Localization and Repair / S. B. Hossain, N. Jiang, Q. Zhou [et al.] // arXiv. – 2024. – arXiv:2404.11595v3 [cs.SE]. – URL: <https://arxiv.org/abs/2404.11595>.
2. Poniszewska-Marañda A. Automatic Detection and Correction of Code Errors Applying Machine Learning Algorithms / A. Poniszewska-Marañda // Proc. of the 2024 Conf. on Innovation in Software Engineering (CISE). – ACM, 2024. – DOI: 10.1145/3661167.3661198.
3. Ullah S. LLMs Cannot Reliably Identify and Reason About Security-Related Bugs / S. Ullah [et al.] // arXiv. – 2023. – arXiv:2312.12575v2 [cs.SE]. – URL: <https://arxiv.org/abs/2312.12575>.
4. Rafi M. N. Towards Better Graph Neural Network-based Fault Localization Through Enhanced Code Representation / M. N. Rafi [et al.] // arXiv. – 2024. – arXiv:2404.04496 [cs.SE]. – URL: <https://arxiv.org/abs/2404.04496>.
5. Qayyum K. LLM-Assisted Bug Identification and Correction for Verilog Hardware Description Language / K. Qayyum [et al.] // Proc. of the ACM/IEEE Design Automation Conf. – 2025. – DOI: 10.1145/3733237.

УДК 004.056.5:004.75

Трофімов О.С., аспірант

Київський столичний університет імені Бориса Грінченка

МЕТОД КОМБІНОВАНОГО ШИФРУВАННЯ ДАНИХ В ХМАРНИХ СЕРЕДОВИЩАХ

Перенесення корпоративних інформаційних систем до хмарних середовищ актуалізує проблему забезпечення конфіденційності, цілісності та доступності даних за умов високої інтенсивності операцій, жорстких вимог до продуктивності та обмежень на допустиму затримку. У таких умовах криптографічний захист має відповідати не лише вимогам інформаційної безпеки, а й експлуатаційним характеристикам високонавантажених систем. Концептуальну основу такого підходу формують керування інформаційною безпекою та архітектура «Повної недовіри», у межах якої жоден компонент інфраструктури не вважається довіреним за замовчуванням [1], [2].

Побудова ефективного захисту даних у корпоративних хмарних системах потребує поєднання кількох вимог: формалізованої моделі загроз, розмежування рівнів довіри, керованого життєвого циклу ключового матеріалу та узгодження криптографічних механізмів із часовими обмеженнями хмарних сервісів [1], [2]. За таких умов критичні криптографічні перетворення доцільно виконувати на стороні клієнта або в межах окремого довіреного домену керування ключами, не покладаючись на безпечність інфраструктури провайдера.

Особливу увагу слід приділяти визначенню місця гомоморфного шифрування в архітектурі захисту. Його перевага полягає в можливості виконання обчислень над зашифрованими даними без розкриття відкритого тексту, що є перспективним для приватної аналітики та спеціалізованих сервісів обробки конфіденційної інформації [4]. Водночас значні обчислювальні накладні витрати, збільшення обсягу даних і зростання часу обробки обмежують використання таких схем у ролі базового механізму захисту хмарних сховищ. Тому гомоморфне шифрування доцільно розглядати як окремий сервісний рівень для вибірових сценаріїв, а базовий захист реалізовувати за допомогою симетричних автентифікованих механізмів.

Архітектура криптографічного захисту має передбачати розмежування транспортного рівня, рівня сховищ і рівня реалізації, при цьому саме рівень сховищ є центральним для забезпечення основних криптографічних гарантій. Для об'єктних і файлових сховищ доцільним є підхід AEAD-first, за якого автентифіковане шифрування поєднує конфіденційність і контроль цілісності. До додаткових автентифікованих даних мають включатися стабільні параметри

контексту, зокрема ідентифікатор орендаря, ресурсу, версія політики та позиція фрагмента, що дає змогу виявляти атаки повтору, перестановки та відкату [2], [3].

Для мережесхемних блочних сховищ доцільно використовувати або профіль AEAD-на-сектор, або режим XTS-AES лише у поєднанні з окремим механізмом автентифікації, оскільки сам по собі XTS-AES не забезпечує контролю цілісності. Не менш важливою складовою є керування ключовим матеріалом, яке має охоплювати генерацію, детерміновану деривацію, ротацію, зберігання та знищення ключів. Контекст деривації повинен однозначно визначати призначення ключа, домен безпеки, ресурс і версію криптографічної політики, забезпечуючи ізоляцію між орендарями та ресурсами [1], [5].

Отже, ефективний криптографічний захист даних у корпоративних хмарних системах доцільно реалізовувати шляхом поєднання архітектури «Повної недовіри», автентифікованого симетричного шифрування, формалізованого криптографічного контексту та керованого життєвого циклу ключів. Такий підхід узгоджує криптографічну стійкість із вимогами до продуктивності, масштабованості та прогнозованості затримок.

Список використаних джерел

1. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). [Чинний від 2023-08-22]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023. 16 с.
2. Rose S., Borchert O., Mitchell S., Connelly S. Zero trust architecture. Gaithersburg, MD : National Institute of Standards and Technology, 2020. 59 p. (NIST Special Publication 800-207). DOI: 10.6028/NIST.SP.800-207.
3. ДСТУ ISO/IEC 27017:2017. Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT). [Чинний від 2019-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017.
4. Marcolla C., Sucasas V., Manzano M., Bassoli R., Fitzek F. H. P., Aaraj N. Survey on fully homomorphic encryption, theory, and applications. Proceedings of the IEEE. 2022. Vol. 111, no. 3. P. 317–345. DOI: 10.1109/JPROC.2022.3205665.
5. Chen L. Recommendation for Key Derivation Using Pseudorandom Functions. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 34 p. (NIST Special Publication 800-108 Rev. 1). DOI: 10.6028/NIST.SP.800-108r1.

УДК 004.7

Габорець О.А., д.філ., доцент

Донецький державний університет внутрішніх справ

ФІШИНГ ЯК БАЗОВИЙ ДЕТЕРМІНАНТ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СИСТЕМІ КІБЕРБЕЗПЕКИ

Стрімкий розвиток цифрових технологій, інтеграція інформаційних систем у всі сфери суспільного життя та глобалізація інформаційного простору зумовили появу якісно нових загроз у сфері кібербезпеки. Однією з таких загроз є соціальна інженерія, яка трансформувалася з допоміжного інструменту кіберзлочинності у самостійний і надзвичайно ефективний механізм інформаційного впливу. Її ключова особливість полягає у спрямованості не на технічні компоненти системи, а на людину як носія інформації та суб'єкта прийняття рішень. У цьому контексті людський фактор виступає найбільш вразливою ланкою системи кібербезпеки, оскільки поведінка користувача часто визначається не раціональним аналізом, а емоційними реакціями та когнітивними спрощеннями [1].

У структурі соціальної інженерії фішинг займає центральне місце, виконуючи роль базового детермінанта, який забезпечує практичну реалізацію більшості соціоінженерних сценаріїв. Фішинг є універсальним інструментом, що дозволяє поєднати технологічні засоби впливу з психологічними механізмами маніпуляції. Його функціонування ґрунтується на створенні штучного інформаційного середовища, у якому користувач сприймає отримане повідомлення як достовірне та безпечне, що спонукає його до виконання дій, вигідних для зловмисника. Важливо підкреслити, що фішинг не обмежується лише електронною поштою, а активно реалізується через соціальні мережі, месенджери, SMS-повідомлення та вебресурси, що значно розширює масштаби його застосування.

З позиції теоретичного аналізу фішинг слід розглядати як багаторівневий феномен, що функціонує на перетині психології, комунікації та інформаційних технологій. На когнітивному рівні він використовує особливості обробки інформації людиною, зокрема схильність до евристичного мислення та автоматизованого прийняття рішень. На комунікативному рівні фішинг реалізується через створення повідомлень, які відповідають очікуванням користувача та відтворюють звичні моделі взаємодії з інформаційними системами. На технологічному рівні він базується на використанні інструментів масового розповсюдження інформації, підміни доменів, клонування вебсайтів та автоматизованих систем генерації контенту.

Особливу увагу слід приділити психологічним механізмам, які забезпечують ефективність фішингових атак. Серед них ключову роль відіграє ефект авторитету, що передбачає використання імен відомих організацій, брендів або державних установ для підвищення рівня довіри до повідомлення. Не менш важливим є ефект дефіциту та терміновості, який змушує користувача діяти швидко, не маючи часу на критичний аналіз інформації. Значну роль відіграє також ефект соціального підтвердження, що базується на припущенні, що якщо певну дію вже виконали інші, вона є правильною. У сукупності ці механізми формують поведінкову модель, у межах якої користувач стає об'єктом маніпуляції, навіть не усвідомлюючи цього.

! Vodafone, Lifecell та Kyivstar від сьогодні компенсують 1000 грн всім абонентам!

Не так давно українців обурило нове підняття цін на тарифи мобільних операторів.

Тому Vodafone, Lifecell, Kyivstar запустили програму лояльності - 1000 грн кожному абоненту.

Подача заяв доступна до 31.03.2026. Гроші можна отримати на мобільний рахунок або на банківську картку.

👉 Оберіть свій оператор та надішліть заявку на отримання 1000 гривень.

👉 Lifecell -<https://fenchurchlegalgrp.co/open/pk067n>

👉 Київстар -<https://fenchurchlegalgrp.co/open/pk067n>

👉 Vodafone -<https://fenchurchlegalgrp.co/open/pk067n>

Рис. 1. Приклад фішингового повідомлення з використанням маніпулятивних технік

Зазначені теоретичні положення знаходять своє практичне підтвердження у реальних прикладах фішингових атак. Зокрема, показовим є повідомлення, що поширюється серед користувачів мобільного зв'язку та містить інформацію про нібито компенсацію у розмірі 1000 гривень від провідних мобільних операторів. Даний приклад (рис. 1) демонструє класичну модель соціоінженерної атаки, у якій поєднуються різні психологічні тригери. Використання назв відомих операторів створює ефект авторитету, що підвищує довіру до повідомлення. Пропозиція отримання грошової винагороди активує

мотиваційний механізм, пов'язаний із прагненням до вигоди. Зазначення обмеженого строку подання заявки формує відчуття терміновості, що знижує рівень критичного мислення. Додатково використовується механізм персоналізації, оскільки користувачу пропонується обрати свого оператора, що створює ілюзію індивідуального підходу.

Важливим елементом аналізованого повідомлення є наявність гіперпосилань, які ведуть на сторонні вебресурси, що не мають відношення до офіційних сайтів мобільних операторів. Це є характерною ознакою фішингових атак, оскільки основною метою таких посилань є збір персональних даних користувачів або встановлення шкідливого програмного забезпечення. З технічної точки зору, подібні ресурси часто створюються за допомогою конструкторів сайтів або шляхом клонування офіційних сторінок, що дозволяє зловмисникам швидко адаптувати їх до нових сценаріїв атак.

У сучасних умовах розвитку інформаційних технологій фішинг дедалі більше інтегрується з іншими інструментами кіберзлочинності, зокрема OSINT-технологіями та штучним інтелектом. Використання відкритих джерел інформації дозволяє зловмисникам збирати детальні дані про потенційних жертв, що забезпечує високий рівень персоналізації атак. Завдяки цьому фішингові повідомлення стають більш переконливими та складнішими для розпізнавання. Крім того, сучасні алгоритми штучного інтелекту дозволяють автоматизувати процес створення таких повідомлень, адаптуючи їх до індивідуальних характеристик користувача. У наукових дослідженнях цей процес визначається як «алгоритмічне управління довірою», коли поведінка користувача прогнозується і коригується за допомогою цифрових технологій.

У правовому аспекті проблема фішингу ускладнюється відсутністю чіткого нормативного визначення соціальної інженерії в законодавстві, що створює труднощі у кваліфікації відповідних правопорушень. Водночас фішингові атаки часто підпадають під ознаки шахрайства, незаконного втручання в роботу інформаційних систем або порушення правил захисту інформації. Це свідчить про необхідність удосконалення нормативно-правової бази у сфері кібербезпеки та розробки спеціалізованих механізмів протидії соціоінженерним загрозам.

У системі кібербезпеки фішинг виконує функцію первинного вектора доступу до інформаційних ресурсів, що робить його особливо небезпечним. Навіть за наявності сучасних технічних засобів захисту, таких як системи виявлення вторгнень або багатofакторна

автентифікація, людський фактор залишається критичним елементом, який може нівелювати ефективність цих заходів. Саме тому протидія фішинговим атакам повинна базуватися на комплексному підході, що поєднує технічні, організаційні та освітні заходи. Як підкреслюється у наукових джерелах, важливу роль відіграє формування культури інформаційної безпеки, розвиток критичного мислення та підвищення рівня обізнаності користувачів щодо сучасних кіберзагроз.

У контексті гібридних загроз фішинг набуває додаткового значення як інструмент інформаційно-психологічного впливу. Його використання може бути спрямоване не лише на отримання конфіденційної інформації, але й на дестабілізацію суспільства, поширення дезінформації та формування панічних настроїв. Таким чином, фішинг виходить за межі суто кримінального явища та стає елементом ширших інформаційних операцій.

Отже, фішинг є базовим детермінантом соціальної інженерії, який визначає характер сучасних кіберзагроз і виступає універсальним інструментом маніпуляції поведінкою користувачів у цифровому середовищі. Його ефективність обумовлена поєднанням технологічних можливостей і глибокого розуміння психологічних особливостей людини. Подальші дослідження у цій сфері повинні бути спрямовані на розробку інноваційних методів виявлення фішингових атак, удосконалення освітніх програм з кібербезпеки та формування стійкості користувачів до маніпулятивних впливів.

Список використаних джерел

1. Габорець О. А., Лунгол О. М. Соціальна інженерія як феномен інформаційного впливу в цифровому середовищі. Національні інтереси України. 2025. № 11(16). С. 95-104. DOI: [https://doi.org/10.52058/3041-1793-11\(16\)](https://doi.org/10.52058/3041-1793-11(16))

УДК 004.056.5

*Гончаров М.О., аспірант,
Малахов С. В., к.т.н., доцент,
Харківський національний університет імені В. Н. Каразіна*

СПІРАЛЬНІ РОЗГОРТКИ БЛОКІВ ВИХІДНИХ ДАНИХ ЯК СПОСІБ ЗАХИСТУ СТЕГАНОГРАФІЧНОГО КОНТЕНТУ

Дана робота є продовженням циклу досліджень, присвячених відпрацюванню процедур обробки даних у рамках реалізації складових етапів малоресурсного стеганоалгоритму [1-2].

Як зазначалося у низці попередніх робіт [3-6], порядок вибірки (зчитування, розгортки або сканування) елементів вихідного масиву даних, є однією з найважливіших процедур у рамках реалізації принципу кодування довжин серій [7].

Згідно досліджуваної концепції алгоритму [2] стегановставки, застосування різних модифікацій методу кодування довжин серій, забезпечує вирішення відразу кількох завдань [2-6]: – оперативна оцінка статистичних характеристик вихідних масивів даних; – скорочення загального часу циклу стегановставки; – підтримка умов статистичного диспаритету даних у системі «контент–контейнер»; – створення стартових умов для подальшого мультиплексування діючих параметрів масиву серій, як механізму з протидії спробам неавторизованого вилучення контенту; – формування окремого рівня захисту від спроб несанкціонованого вилучення контенту.

Зважаючи на свою процедурну простоту, використання різних схем розгортки, забезпечує широку комбінаторність можливих станів формованих масивів серій, що суттєво посилює роль відповідного елемента в загальній структурі ключа екстрактора даних [5].

За принципом сканування масиву вихідних даних, розгортки можна умовно поділити на: – прості (лінійні); – складні (нелінійні); – двопрхідні; – випадкові; – комбіновані - тобто такі, що одночасно поєднують кілька схем (наприклад, двопрхідний варіант, у межах якого на кожному циклі, реалізується власна схема вибірки параметрів оброблюваного масиву) [3-4,6].

Представлений матеріал відображає результати застосування кількох варіантів спіральної розгортки, в умовах атаки тестового контенту. Як свідчить моделювання, спіральна розгортка є одним простих механізмів підвищення стійкості до спроб несанкціонованого вилучення прихованих даних. Це досягається завдяки суттєвому ускладненню просторової логіки послідовного доступу блоків

зображення без знання діючих параметрів «спіралі». До таких параметрів належать: – напрямок руху розгортки; – початкова точка старту; – розмірність ОБ; – модифікації патернів сканування (наприклад, однопрохідна чи двопрохідна спіраль). Завдяки такому варіативному розмаїттю спіральна розгортка набуває додаткової стійкості до геометричних і фрагментаційних атак (обрізання тощо).

На рис. 1 наведено результати атаки (*спроб неавторизованого вилучення*) тестового контенту для різних схем спіральної розгортки опорних блоків (ОБ) вихідних зображень. Моделювання проводилося з використанням напівтонових [7] тестових зображень (рис.1(а-б)) за умови помилкового відновлення контенту з використанням схеми «По рядках» [6]. Отримані результати демонструють стійкість спіральних схем до спроб нелегітимної екстракції прихованої інформації в умовах використання різних точок старту руху сканування.

Як слід з рис.1, спіральна розгортка суттєво ускладнює атакуючому задачу відновлення контенту. Інакше кажучи, спроби неавторизованого відновлення даних без знання діючих параметрів «спіралі» [3-5], зумовлюють значну фрагментацію відновлюваного масиву серій ОБ.

Результатом таких спроб, є лише фрагментовані, зображення (див. рис.1). Крім того, корисні наслідки від використання спіральної схеми розгортки виявляються при геометричних спотвореннях і частковій втраті зображення. Так, у разі обрізання певної частини зображення, втрачається лише частина умовних витків спіралі, а не цілі лінійні сегменти даних, як це відбувається при класичних растрових чи зигзагоподібних розгортках [4,6]. Це суттєво ускладнює відновлення повної прихованої інформації, навіть при помірних геометричних спотвореннях чи частковій втраті контенту.

Наприклад, якщо прихований контент розміщується всередині зображення саме за спіральною схемою, то дані розподіляються нелінійно по всій площі носія (контейнеру), а не концентруються в окремих рядках, стовпцях чи блоках.

Завдяки цьому спіральна схема стає значно стійкішою до типових маніпуляцій з зображеннями, таких як: □ обрізання країв, компресія з втратами, масштабування та незначні повороти. Навіть при втраті частки площі зображення, значна частина витків спіралі зберігається, дозволяючи авторизованому користувачу [5] вилучати, принаймні, частину повідомлення або повністю відновити його за умови використання додаткових механізмів корекції помилок.

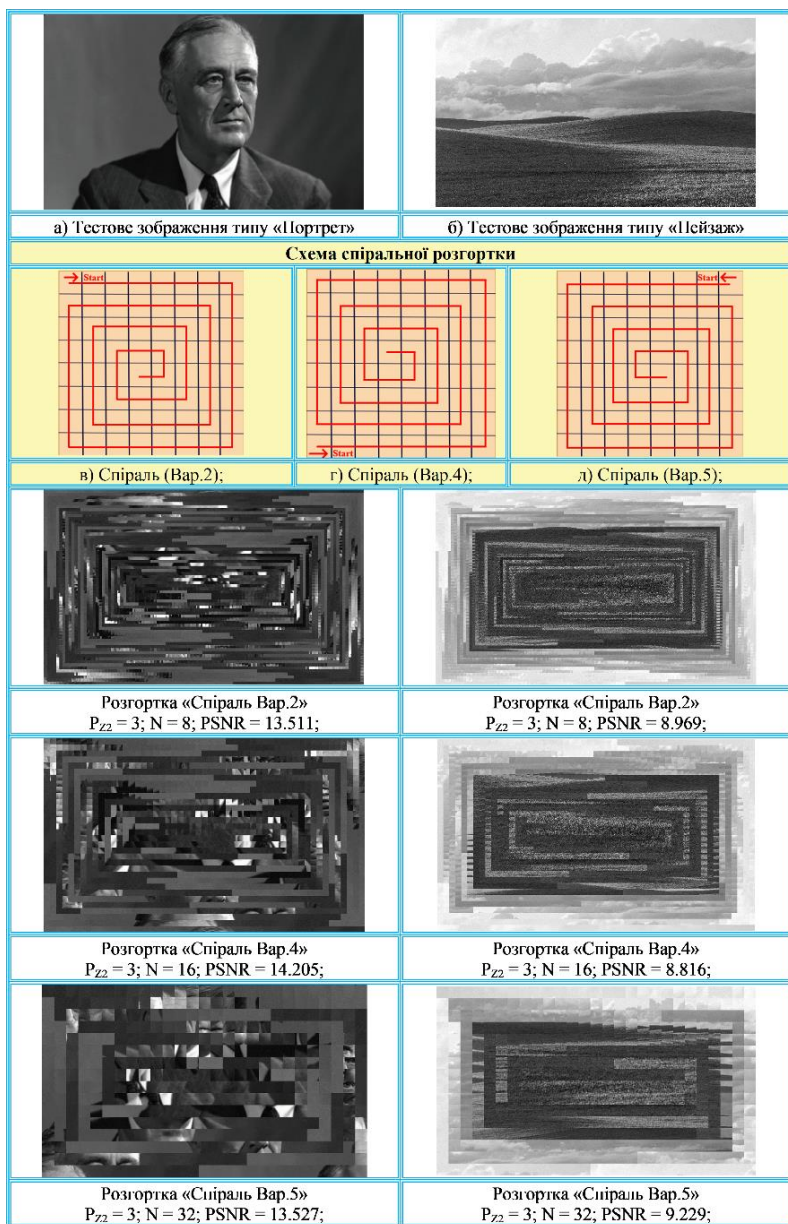


Рисунок 1 – Результати атаки тестового контенту для різних схем «спіралі» та розмірностей ОБ (хибне відновлення за схемою «По рядках»)

Висновок. Проведене моделювання підтвердило, що застосування спіральної розгортки не лише підвищує захист до спроб підбору діючої послідовності кодування контенту, але й забезпечує помітно кращу робастність до типових маніпуляцій з зображеннями, порівнянно з простими схемами [3-4]. Це значно посилює можливості алгоритму малoresурсної стегановставки, роблячи спіральний принцип розгортки, надійним й обчислювально ефективним інструментом з протидії спробам неавторизованого вилучення даних.

Список використаних джерел

1. Honcharov M., Liesnaia Y., Malakhov S. Investigation of the properties of the prototype of a hybrid steganographic algorithm // *Computer Science and Cybersecurity*. 2021. № 2. С. 45-56. URL: <https://doi.org/10.26565/2519-2310-2021-2-05>
2. Honcharov M. O., Nariezhnii O. P., Malakhov S. V. Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. *Modern Information Security*. 2025. № 3. С. 37–47. URL: <https://doi.org/10.31673/2409-7292.2025.030518>
3. Гончаров М. О., Малахов С. В., Жіленков Д. В. Дослідження складності та властивостей різних схем розгортки вихідних даних стеганоконтента, в умовах зміни сценаріїв атак. *Сучасний захист інформації*. 2025. № 4. С. 44–58. DOI: 10.31673/2409-7292.2025.041205
4. Гончаров М., Малахов С. Дослідження способів розгортки вихідних блоків зображення-стеганоконтенту як механізму протидії від несанкціонованої екстракції даних. *Science and Technology Today*. 2023. № 4 (18). С. 293–308. URL: <https://perspectives.pp.ua/index.php/nts/article/view/4445>
5. Honcharov M., Malakhov S. Modeling attempts of unauthorized extraction of steganoccontent under different combinations of data key-extractor. *Collection of Scientific Papers «ΛΟΓΟΣ»* (Paris, France, March 1, 2024). 2024. P. 234–245. URL: <https://doi.org/10.36074/logos-01.03.2024.053>
6. Лесная Ю., Гончаров М., Семенов А., Малахов С. Моделювання розгортки серій опорних блоків зображення, як інструменту з протидії спробам несанкціонованої екстракції стеганоконтенту. *Collection of Scientific Papers «ΛΟΓΟΣ»* (Zurich, Switzerland, March 31, 2023). 2023. С. 109–115. URL: <https://doi.org/10.36074/logos-31.03.2023.33>
7. Pratt W. K. *Digital Image Processing*. New York : John Wiley & Sons, 1978. 750 p.

УДК 004.056.5:005.334

*Кравчук В.С., аспірант
Дорогий Я.Ю., д.т.н., професор
Донецький національний технічний університет*

МЕТРИКИ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Анотація. У цих тезах розглядається еволюція підходів до оцінки ефективності тестування на проникнення (пентесту). Акцентується увага на переході від періодичних перевірок, зумовлених нормативними вимогами, до моделі безперервної валідації, орієнтованої на продуктивність та бізнес-результати. Визначаються ключові метрики та показники ефективності (KPI), які перетворюють пентест із центру витрат на стратегічний інструмент управління ризиками.

Вступ. Сучасний ландшафт кібербезпеки зазнав фундаментальних змін: від періодичних оцінок безпеки до моделі безперервної перевірки. Оскільки організації інтегрують складні вебзастосунки в кожен аспект своєї архітектури, традиційний "точковий" пентест стає недостатнім показником реального стану безпеки. Формалізація поняття ефективності тестування на проникнення є критично важливою вимогою сучасних циклів розробки програмного забезпечення, таких як CI/CD та DevSecOps. Ефективність більше не вимірюється лише кількістю знайдених вразливостей; на перший план виходять такі показники, як швидкість, точність та відтворюваність результатів.

Аналіз літературних джерел. Фундаментом для побудови ефективного процесу пентесту є стандартизовані методології, які гарантують послідовність та професіоналізм. Такі фреймворки, як OWASP, PTES (Penetration Testing Execution Standard) та OSSTMM, забезпечують необхідні структурні рекомендації для переходу від несистематичного тестування до наукового підходу, заснованого на даних. Наприклад, PTES формалізує процес у п'ять основних етапів: розвідка, сканування, оцінка вразливостей, експлуатація та звітування [1].

Крім того, для якісної оцінки ризиків та пріоритезації результатів у літературі часто застосовується модель DREAD, яка оцінює п'ять параметрів: потенційну шкоду (Damage), відтворюваність (Reproducibility), експлуатованість (Exploitability), кількість уражених користувачів (Affected users) та виявлюваність (Discoverability) [2].

Основна частина. Ефективність тестування на проникнення формалізується через розкладання процесу на окремі вимірювані етапи, кожен з яких регулюється набором строгих метрик:

1. Метрики операційного охоплення та частоти (Operational Scope & Activity Velocity). Важливими показниками є охоплення портфеля (Portfolio Coverage) — відсоток відомих активів, кінцевих точок та API, що підлягають тестуванню. Не менш важливою є частота тестування (Test Cadence) по відношенню до циклів випуску програмного забезпечення [3].

2. Технічна ефективність (Technical Efficacy). Ключовим показником на етапі виявлення є рівень виявлення вразливостей (Vulnerability Discovery Rate - VDR), який вимірює кількість унікальних вразливостей, знайдених за одиницю часу або за одне залучення. Високий VDR повинен супроводжуватися низьким рівнем хибних спрацьовувань (False Positive Rate), щоб запобігти "виснаженню від сповіщень" (alert fatigue) серед персоналу та не витрачати ресурси на марне сортування [4,5].

3. Метрики швидкості реагування (Speed Metrics). Серед ключових часових метрик виділяють: середній час до виявлення (Mean Time to Detect - MTTD): час від початку аномальної події до її ідентифікації [1] та середній час на усунення (Mean Time to Remediate - MTTR): середній час, необхідний для вирішення проблеми безпеки після її виявлення [4, 5]. Зниження MTTR є прямим свідченням того, що команди безпеки та розробки ефективно співпрацюють [6, 7].

4. Економічна ефективність та ROI (Return on Investment). Вартість професійного пентесту може варіюватися від \$5,000 до понад \$150,000 [8]. Однак ефективність цих витрат оцінюється через моделювання рентабельності інвестицій. ROI розраховується шляхом порівняння вартості залучення пентестерів зі зниженням очікуваних збитків. Оскільки середня вартість витоку даних перевищує \$10 мільйонів, навіть дорогий пентест, який запобігає одному інциденту, може забезпечити окупність у співвідношенні 340:1 [8]. Відстеження тенденцій щільності вразливостей (Vulnerability density trends) з часом також допомагає довести керівництву (наприклад, CFO), що інвестиції у безпеку приносять реальну користь та зменшують кількість вразливостей на одиницю коду [8].

5. Відтворюваність та якість звітування. Ефективний звіт про пентест має бути дієвим. Це досягається через відтворюваність (Reproducibility) доказів концепції (Proof-of-Concept). Відтворюваний PoC є необхідним для того, щоб захисники могли перевірити вразливість, провести аналіз першопричин та підтримати регресійне тестування. Звіт повинен перекладати технічні знахідки на мову бізнес-ризиків та надавати чіткі кроки для їх усунення [9].

Висновки. Поняття ефективності пентесту вийшло далеко за межі складання простого переліку знайдених технічних помилок. Формалізація ефективності вимагає переходу до багатовимірної системи кількісних індикаторів, кожен етап якої (аналіз, виявлення, оцінка впливу, звітування) оптимізується за критеріями швидкості, точності та відтворюваності. Систематичне відстеження таких метрик, як VDR, MTTR, рівень хибних спрацьовувань та ROI, а також застосування перевірених методологій (PTES, OSSTMM, DREAD), дозволяє організаціям перетворити тестування на проникнення зі звичайної вимоги для комплаєнсу на суворий, вимірюваний та високоефективний процес, що активно посилює цифровий захист компанії.

Список використаних джерел

1. Learn About The Five Penetration Testing Phases | Pentesting. EC-Council. 2022. URL: <https://lnk.ua/bskZscvm8>
2. Nilsson T., Andersson L. External Threat Assessment and Internal Network Security Evaluation: A Penetration Test and Vulnerability Analysis of IVA's Internal Infrastructure Against External Threats. KTH Royal Institute of Technology. 2025. URL: <https://lnk.ua/afryw7pfg>
3. Wong C. Pen Test Metrics 101: Detailed Definitions. Cobalt. 2017. URL: <https://lnk.ua/mNpkyN3lD>
4. Hinojosa G. Less Findings in your Pentest? Measuring the Effectiveness of a Penetration Test. Cobalt. 2025. URL: <https://lnk.ua/caxTjTO3R>
5. Mukherjee A. Measuring the Impact of Penetration Testing with Metrics. Threat Intelligence. 2023. URL: <https://lnk.ua/bhGCG53BE>
6. Application Security Metrics and KPIs for Security Posture. Legit Security. URL: <https://lnk.ua/1tLnfhjthv>
7. Callegari C. Penetration Testing ROI: 5 Metrics to Communicate Real Value. Software Secured. URL: <https://lnk.ua/Zrd5iuqQu>
8. Penetration Testing Pricing 2026: Enterprise Cost Guide. DeepStrike. URL: <https://lnk.ua/43EQpKgcN>
9. Odom C. Essential Elements of a Penetration Testing Report. Emagined Security. 2024. URL: <https://lnk.ua/D8YvsUl66>

УДК 004.056:514.742

Кравчук В.С., аспірант
Дорогий Я.Ю., д.т.н., професор
Донецький національний технічний університет
Цуркан В.В., к.т.н., доцент
КПІ ім. Ігоря Сікорського

КРИТЕРІЙ ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Анотація. У цих тезах розглядається підхід до формалізації критерію ефективності захисту критичної інфраструктури шляхом інтеграції практичних метрик тестування на проникнення (MTTD, MTTR, VDR, ROI) у багатовимірну тензорну модель кібербезпеки. Показано, як показники операційного охоплення, технічної ефективності та швидкості реагування математично відображаються на параметри тензорів ресурсів, вразливостей, загроз та засобів захисту. Запропоновано комплексний критерій, який дозволяє не лише оптимізувати технічні параметри захисту, але й оцінити економічну рентабельність інвестицій (ROI) у розрізі зниження загального тензора ризику.

Вступ. Формалізація поняття ефективності кіберзахисту є критично важливою вимогою для сучасних організацій та критичної інфраструктури. Традиційно ефективність оцінюється за допомогою практичних метрик безпеки (таких як рівень виявлення вразливостей, час на усунення тощо). З іншого боку, для системного аналізу складних інфраструктур передові дослідження пропонують використовувати тензорний аналіз, який дозволяє математично описати взаємозв'язки між загрозами, вразливостями та ресурсами [1, 2]. Об'єднання цих двох підходів — перенесення кількісних метрик (KPI) у площину багатовимірних тензорних характеристик — дозволяє створити динамічний, вимірюваний та математично обґрунтований критерій ефективності захисту.

Аналіз літературних джерел. В основі практичної оцінки кібербезпеки лежать стандартизовані методології (PTES, OSSTMM), які формалізують процес виявлення вразливостей. Для вимірювання ефективності цього процесу застосовують метрики швидкості (MTTD, MTTR), метрики технічної ефективності (VDR, рівень хибних спрацьовувань) та показники ROI. Водночас для математичного моделювання безпеки критичної інфраструктури застосовується 4-вимірна тензорна модель [1, 2]. Ця модель оперує тензорами ресурсів (R), загроз (Z), вразливостей (V) та засобів захисту (G), дозволяючи розраховувати результуючий тензор ризику R_g та моделювати

адаптивне зниження загроз у часі [1]. Однак, для набуття практичної цінності, абстрактні параметри цих тензорів потребують наповнення реальними метриками безпеки.

Основна частина. Комплексний критерій ефективності захисту формується через проектування практичних показників ефективності (метрик) на відповідні компоненти тензорної моделі:

1. Метрики охоплення та частоти у тензорі ресурсів (R). Метрика охоплення портфеля (Portfolio Coverage) безпосередньо визначає повноту формування тензора ресурсів $R_{i,j,k,l}$ [1]. Якщо охоплення під час аналізу чи пентесту становить менше 100%, виникає "сліпа зона", яка генерує неврахований (прихований) тензор ризику. Метрика частоти тестування (Test Cadence) зі свого боку визначає інтервал дискретизації для оновлення матриць стану в системі.

2. Технічна ефективність та достовірність тензора вразливостей (V). Показник рівня виявлення вразливостей (Vulnerability Discovery Rate — VDR) та рівень хибних спрацьовувань (False Positive Rate) виступають індикаторами точності побудови тензора вразливостей $V_{i,j,k,l}$, що описує складність та потенційний вплив недоліків [1]. Високий VDR зменшує кількість невідомих елементів тензора V , забезпечуючи об'єктивність моделі. Низький рівень хибних спрацьовувань гарантує, що ймовірність спрацьовування засобів захисту (P_g) з тензора G [1] не буде марно витрачатися на хибні загрози.

3. Метрики швидкості (MTTD, MTTR) у часовій динаміці загрози. Для оцінки часового аспекту ефективності в тензорному аналізі застосовується функція часової динаміки: $Z_{i,j,k,l}(t) = Z_{i,j,k,l}e^{-\beta t}$, де β — коефіцієнт згасання загрози, а t — час після виявлення [1]. Практичні часові метрики — середній час до виявлення (MTTD) та середній час на усунення (MTTR) — є обернено пропорційними до коефіцієнта β . Ефективна система захисту забезпечує мінімальні значення MTTD та MTTR, що математично максимізує β . Це гарантує швидке експоненційне зниження впливу загрози на систему [1].

4. Економічна ефективність (ROI) у тензорі захисту (G). Тензор засобів захисту $G_{i,j,k,l}$ містить вимір вартості імплементації інструменту — C_{gv} [13, 14]. Економічна ефективність захисту розраховується через моделювання рентабельності інвестицій (ROI). У рамках тензорної моделі ROI обчислюється як відношення зниженого потенційного збитку (різниця початкового тензора ризику R_r та залишкового R_r' після застосування засобів захисту G до фінансових витрат C_{gv} : $ROI = fR_r - R_r' - C_{gv}C_{gv}$, де $|R_r|$ — монетизована оцінка тензора ризику на основі цінності ресурсу V_r з тензора R [1]).

Формалізований критерій ефективності. З урахуванням наведених метрик, глобальний критерій ефективності захисту полягає у такому налаштуванні тензора засобів захисту (G), яке:

1. Мінімізує глобальний тензор ризику [1]:

$$R_g = f(i,j,k,l) v_{i,j,k,l} G_{i,j,k,l}$$

2. Максимізує швидкість згасання загрози шляхом системного зменшення метрик MTDD та MTTR.

3. Забезпечує максимальне значення ROI за умови збереження заданого рівня охоплення активів (Portfolio Coverage).

Висновки. Інтеграція практичних метрик тестування на проникнення та реагування на інциденти (VDR, MTDD, MTTR, ROI) в абстрактну тензорну модель перетворює її на потужний аналітичний інструмент. Це дозволяє формалізувати критерій ефективності кіберзахисту не як статичну констатацію наявності захисних систем, а як динамічний процес. Математично ефективність виражається у здатності тензора засобів захисту мінімізувати результуючий тензор ризику з урахуванням швидкості реакції (MTTR) та економічної доцільності (ROI). Такий комплексний критерій забезпечує керівництво організацій дієвими показниками для оптимізації бюджету на кібербезпеку.

Список використаних джерел

1. Dorohyi I., Kravchuk V.S., Tsurkan V.V., Berdychenko I.O. Application of tensor analysis for cybersecurity tasks in critical infrastructure. Інформаційні технології та безпека. Матеріали XXV Міжнародної науково-практичної конференції ІТБ-2025. Київ: Інжиніринг. с. 179-182.

2. Dorohyi I., Kravchuk V., Tsurkan V. Tensor Model for Representing Critical Infrastructure. CEUR Workshop Proceedings. 2024. URL: <https://ceur-ws.org/Vol-4068/paper9.pdf> (дата звернення: 23.03.2026).

УДК 004.7

*Макарик А.С., магістрант,
Фальковський І. Г., ст. викладач
Державний університет «Житомирська політехніка»*

ОБҐРУНТУВАННЯ ПІДХОДІВ ДО ОПТИМІЗАЦІЇ ЗАСТОСУВАННЯ GPO З УРАХУВАННЯМ АРХІТЕКТУРИ ТА МАСШТАБУ ДОМЕНУ МЕРЕЖІ

У сучасних корпоративних інформаційних системах на базі Windows Server служба каталогів Active Directory є основним засобом централізованого управління мережевими ресурсами. Важливою складовою її функціонування є Group Policy (GPO), ефективність яких визначається архітектурою домену, масштабом мережі та кількістю об'єктів, що безпосередньо впливають на продуктивність і стабільність системи. У зв'язку з цим актуальним є обґрунтований вибір та оптимізація моделі застосування GPO і механізмів їх впровадження з урахуванням характеристик мережевого середовища [1].

Таким чином, метою дослідження є розробка та обґрунтування підходів до оптимізації застосування GPO з урахуванням архітектури та масштабу доменної мереж.

Безпосереднє застосування політик на рівні домену або сайту є недоцільним, оскільки такі політики автоматично успадковуються всіма організаційними одиницями (OU) в межах ієрархії GPO, що призводить до застосування параметрів до невідповідних користувачів або комп'ютерів. Замість цього доцільним є створення окремої кореневої OU, на яку застосовуються політики доменного рівня, що потребують контрольованого розповсюдження.

Важливим аспектом є структурування налаштувань у межах самих GPO. Зокрема, GPO доцільно класифікувати на монолітні та функціональні. Монолітні GPO являють собою об'єднання значної кількості налаштувань в одному об'єкті, як правило, згрупованих за спільною функціональною ознакою (наприклад, забезпечення журналювання або реалізація політик безпеки). Це спрощує візуалізацію за допомогою інструментів адміністрування, зокрема Group Policy Management Console (GPMC), та полегшує призначення політик на відповідні ієрархічні рівні. Водночас монолітні GPO можуть негативно впливати на керованість системи: при великій кількості налаштувань ускладнюється делегування прав та діагностика помилок, хоча вплив на продуктивність залежить від конкретної конфігурації мережі та механізмів фільтрації.

Функціональні GPO формуються за принципом розподілу налаштувань між окремими об'єктами за їхнім призначенням, при якому кожен GPO відповідає за реалізацію конкретної функціональної задачі. Такий підхід підвищує гнучкість адміністрування та спрощує діагностику та підтримку системи.

Вибір механізмів фільтрації GPO є критичним етапом, оскільки забезпечує цільове застосування політик і зменшує їх надлишковий вплив у мережах різного масштабу та топології. Найпоширенішими методами є WMI-фільтрація та блокування успадкування політик [2]. Доцільним є підхід, за якого GPO прив'язуються максимально близько до цільових організаційних одиниць із використанням фільтрації за принципом винятків лише за необхідності, що зменшує складність адміністрування та обчислювальні витрати, підвищуючи продуктивність системи. Надмірне застосування фільтрації, навпаки, збільшує час обробки GPO через додаткові перевірки на клієнтських системах.

Окремо варто заги використання механізму зациклення GPO (Loopback processing), котрий змінює порядок обробки користувачських політик. Зокрема, у режимі злиття (merge mode) де відбувається послідовна обробка політик користувача і комп'ютера, що призводить до подвійного аналізу посилюючи тим самим навантаження на систему, особливо у великих мережах. У зв'язку з цим використання даного механізму повинно бути обмеженим і застосовуватися лише у випадках, коли це обґрунтовано специфікою конфігурації середовища.

Результати теоретичного дослідження підтверджують доцільність оптимізації застосування GPO шляхом раціонального вибору моделі впровадження, структурування та механізмів фільтрації з урахуванням архітектури доменної мережі. Застосування запропонованих підходів підвищує продуктивність системи, знижує складність адміністрування та забезпечує ефективне й цільове використання політик.

Список використаних джерел

1. Group Policy processing for Windows. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-processing>.
2. Active Directory and Group Policy Management Best Practices / B. Hennings et al. CIS Center for Internet Security. URL: <https://learn.cisecurity.org/CIS-Benchmarks-Active-Directory-Guide>.

УДК 004:7

*Слободянюк А.О., магістрант
Бродський Ю.Б., к.т.н., доцент
Росініський Ю.М., к.т.н., доцент*

Державний університет «Житомирська політехніка»

СИСТЕМНИЙ МОНІТОРИНГ СЕРВЕРНИХ І МЕРЕЖЕВИХ КОМПОНЕНТІВ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ ЇЇ СТАБІЛЬНОСТІ

Стабільність інформаційної інфраструктури є необхідною умовою безперервної діяльності сучасних організацій. Ускладнення архітектури ІТ-систем, використання віртуалізації, контейнеризації та розподілених сервісів підвищують вимоги до контролю технічного стану ресурсів. Навіть короткочасні відмови критичних компонентів серверного та мережевого ядра можуть призвести до фінансових втрат, порушення бізнес-процесів і зниження довіри до сервісів. За таких умов особливого значення набуває системний моніторинг як інструмент підтримки стабільності та керованості інфраструктури [1,2].

У роботі розглядаються підходи до організації системного моніторингу та визначається його роль у забезпеченні надійного функціонування критичних серверних і мережових компонентів із формуванням рекомендацій щодо впровадження відповідних інструментів.

Практика експлуатації ІТ-систем свідчить, що контроль ресурсів часто має реактивний характер [2,3]. Відсутність централізованого збору метрик і автоматизованих сповіщень ускладнює реагування. Виникає протиріччя між масштабованістю інфраструктури та недостатньою автоматизацією контролю, що підвищує ризик відмов серверного та мережевого ядра.

Системний моніторинг передбачає безперервний збір і аналіз показників функціонування серверного ядра, мережевого ядра, віртуалізованих середовищ і сервісів. Контроль навантаження процесора, використання пам'яті, стану дисків, мережових затримок і доступності служб дозволяє виявляти аномалії та запобігати відмовам [1,3]. Історичні дані використовуються для прогнозування навантаження та оптимізації ресурсів.

Серед інструментів моніторингу поширення набули платформи з відкритим кодом, зокрема Zabbix та Icinga 2 [6,7], що забезпечують централізований збір метрик і систему сповіщень. Їхні відмінності полягають у складності конфігурації та можливостях інтеграції.

Важливим етапом є вибір інструменту моніторингу за критеріями масштабованості, гнучкості, інтеграції та рівня автоматизації [2,3]. Від цього залежить ефективність експлуатації критичних компонентів і своєчасність реагування на інциденти.

Додатково слід враховувати, що ефективність системного моніторингу залежить від адаптації інструментів до специфіки інфраструктури. У середовищах із високою динамікою змін (віртуалізація, контейнеризація, хмарні сервіси) важливим є забезпечення гнучкості конфігурацій і автоматичного виявлення нових об'єктів моніторингу. Це дозволяє підтримувати актуальність контролю та зменшувати ризик пропуску критичних змін у структурі системи.

Ефективність моніторингу визначається також налаштуванням політик контролю: надлишкові сповіщення перевантажують операторів, а недостатня деталізація знижує здатність виявляти проблеми.

За результатами аналізу доцільно рекомендувати: централізований збір показників із серверного та мережевого ядра; встановлення обґрунтованих порогових значень; використання автоматичних сповіщень; використання даних моніторингу для виявлення тенденцій функціонування системи; регулярну оптимізацію конфігурації.

Таким чином, обґрунтований вибір і впровадження системи моніторингу забезпечують перехід до проактивного управління серверними та мережевими компонентами, підвищують доступність сервісів і ефективність використання ресурсів. Перспективним є поєднання системного та безпекового моніторингу [5].

Список використаних джерел

1. Turnbull J. The Art of Monitoring. – James Turnbull, 2014.
2. Beyer B., Jones C., Petoff J., Murphy N. Site Reliability Engineering: How Google Runs Production Systems. – O'Reilly Media, 2016.
3. Limoncelli T., Hogan C., Chalup S. The Practice of System and Network Administration. – Addison-Wesley, 2016.
4. Oppenheimer P. Top-Down Network Design. – Cisco Press, 2011.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
6. Zabbix Documentation [Електронний ресурс]. – Режим доступу: <https://www.zabbix.com/documentation>
7. Icinga Documentation [Електронний ресурс]. – Режим доступу: <https://icinga.com/docs/>

УДК 004.056.5

Зубелевич Д.І., м.н.с.

Вандалович В.П., наук. співробітник

Житомирський військовий інститут імені С.П. Корольова

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ НА ЛАНЦЮЖКИ ПОСТАЧАННЯ У ВІДКРИТОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

Сучасні підходи до розробки програмного забезпечення (далі - ПЗ) значною мірою базуються на використанні компонентів з відкритим вихідним кодом та вільними ліцензіями. Частка сторонніх компонентів у сучасних програмних продуктах може сягати до 90 % загального обсягу коду.

Інтеграція сторонніх бібліотек та фреймворків дозволяє суттєво прискорити розробку програм, проте водночас створює додаткові ризики для безпеки інформаційних систем - компрометація навіть одного використаного елемента відкритого ПЗ створює загрозу для великої кількості інших проєктів, в яких цей елемент використано як залежність.

Атаки на ланцюжки постачання ПЗ (англ. Software Supply Chain Attacks) упродовж останніх років стали поширеним видом кіберзагроз – відомими є випадки компрометації програмних продуктів та бібліотек, що використовуються великою кількістю користувачів. Одним із найбільш відомих прикладів є атака на ПЗ Orion від компанії SolarWinds у 2020 році, коли зловмисники (котрих розслідувачі пов'язують з РФ) інтегрували шкідливий код у легітимні оновлення системи моніторингу мереж. У результаті заражені оновлення завантажили близько 18 000 організацій, включно з державними установами. Іншим показовим прикладом є інцидент із бекдором у бібліотеці XZ Utils версій 5.6.0 та 5.6.1 у 2024 році (CVE-2024-3094), який призвів до можливості несанкціонованого доступу до великої кількості Linux-систем по протоколу SSH в обхід механізму аутентифікації.

Зазначені інциденти демонструють недостатність традиційних підходів до гарантування кібербезпеки (аналіз відомих вразливостей та сигнатурне виявлення шкідливого коду) для виявлення скомпрометованих ланцюжків постачання. Одним із причин є складність сучасних програмних екосистем, у яких широко використовуються транзитивні залежності. У багатьох випадках ПЗ може містити десятки або сотні бібліотек, кожна з яких має власні залежності, котрі часто оновлюються. Це значно ускладнює контроль походження та безпечності усіх компонентів системи.

Для підвищення рівня безпеки програмних ланцюжків постачання дедалі ширше застосовуються автоматизовані засоби аналізу складу ПЗ (англ. Software Composition Analysis, SCA). Одним із важливих інструментів у цій сфері є використання Software Bill of Materials (SBOM) - структурованого опису всіх компонентів та залежностей в ПЗ. SBOM дозволяє ідентифікувати використання вразливих бібліотек та оцінювати потенційний вплив нових вразливостей.

Подальшим розвитком цього підходу є використання механізму VEX (англ. Vulnerability Exploitability eXchange), який дозволяє уточнювати, чи може певна вразливість бути фактично експлуатована в конкретному програмному продукті. Це дає змогу зменшити кількість хибних спрацювань під час автоматизованого аналізу безпеки та підвищити ефективність управління вразливостями. Важливу роль також відіграють підходи до забезпечення цілісності програмних артефактів на всіх етапах життєвого циклу розробки. З цією метою активно впроваджуються стандарти SLSA (англ. Supply-chain Levels for Software Artifacts), які визначають рівні довіри до залежностей, використаних в процесі створення ПЗ. Практична реалізація цих підходів передбачає використання криптографічних механізмів підпису програмних компонентів, зокрема інфраструктури Sigstore, для перевірки їх походження та незмінності.

Перспективним напрямом підвищення безпеки також є використання ізольованих середовищ виконання для перевірки сторонніх компонентів перед їх інтеграцією до ПЗ при його збірці та компіляції. Застосування віртуальних машин, технологій контейнеризації (Docker, containerd, LXC/LXD), системних обмежень засобами AppArmor/SELinux та виконання коду у середовищах на основі WebAssembly (Wasm) дозволяє аналізувати поведінку бібліотек та пакетів-залежностей у контрольованих умовах.

Таким чином, ефективна протидія атакам на ланцюжки постачання ПЗ потребує комплексного підходу, що поєднує автоматизований аналіз складу програмних компонентів, контроль цілісності програмних артефактів, а також поведінковий аналіз сторонніх бібліотек.

Список використаних джерел

1. Securing the Software Supply Chain: Recommended Practices for Developers. URL: <https://www.cisa.gov/resources-tools/resources/securing-software-supply-chain-recommended-practices-developers> (дата звернення: 18.03.2026).
2. CVE-2024-3094 Detail. URL: <https://nvd.nist.gov/vuln/detail/CVE-2024-3094> (дата звернення: 18.03.2026).
3. SUNSPOT: An Implant in the Build Process (by CrowdStrike Intelligence Team). URL: <https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/> (дата звернення: 18.03.2026).

УДК 004.49

Добришин Ю.Є., к.т.н, доцент
Національна академія Служби безпеки України

ЗАГРОЗИ ТА РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ХМАРНИХ ОБЧИСЛЕННЯХ

На теперішній час політики безпеки становляться головним елементом кібербезпеки, тому що вони формалізують підходи до захисту інформаційних ресурсів, визначають правила взаємодії користувачів, програмних сервісів та модулів інформаційних систем. У традиційних інформаційних системах політики безпеки переважно орієнтувалися на захист мережевого периметра, контроль фізичного доступу та розмежування прав користувачів у межах локальної інфраструктури. Однак із розвитком хмарних обчислень такі підходи виявилися недостатніми.

На відміну від традиційних локальних систем, хмарні платформи передбачають спільне використання ресурсів, віддалений доступ і динамічну зміну конфігурацій, що істотно ускладнює ідентифікацію та управління ризиками. У таких умовах зростає значення системного підходу до аналізу загроз і формування політик безпеки.

Однією з найбільш поширених загроз у хмарних середовищах є неправильна конфігурація ресурсів. Відкриті сховища даних, надмірні права доступу та помилки в налаштуваннях мережових політик залишаються основними причинами витоку інформації. Дослідження підтверджують, що більшість таких інцидентів пов'язані з відсутністю чітко визначених політик безпеки та недостатнім контролем відповідності конфігурацій установленим вимогам. Це свідчить про необхідність автоматизації процесів контролю та перевірки налаштувань безпеки.

Суттєвим ризиком є компрометація облікових даних користувачів і сервісних акаунтів. Хмарні середовища активно використовують механізми віддаленої автентифікації, що робить їх вразливими до фішингових атак і викрадення облікових даних. У разі отримання злоумисником доступу до облікового запису з надмірними повноваженнями можливе масштабне порушення безпеки всієї інфраструктури. Цей ризик безпосередньо пов'язаний із недотриманням принципу мінімально необхідних повноважень.

Окрему групу загроз формують внутрішні ризики, пов'язані з діями легітимних користувачів. Використання несанкціонованих хмарних сервісів і програмного забезпечення, відоме як Shadow IT, призводить

до втрати централізованого контролю над інформаційними ресурсами та ускладнює виконання вимог політик безпеки. Такі дії можуть бути як свідомими, так і ненавмисними, проте в обох випадках вони підвищують імовірність витоку або компрометації даних.

Загрози доступності інформації також мають важливе значення для хмарних середовищ. Відмови в обслуговуванні, збої в роботі сервісів або помилки масштабування можуть призвести до тимчасової чи повної недоступності критично важливих ресурсів. Хоча провайдери хмарних сервісів забезпечують високий рівень відмовостійкості, відповідальність за управління такими ризиками значною мірою покладається на користувача, який повинен враховувати їх під час формування політик безпеки.

Додатковим фактором ризику є недостатній рівень моніторингу та фіксації подій за допомогою логічних журналів. Відсутність централізованого збору та аналізу логів ускладнює своєчасне виявлення інцидентів і реагування на них. Наукові дослідження наголошують, що затримка у виявленні атак у хмарних середовищах істотно збільшує масштаби завданої шкоди та ускладнює подальше розслідування інцидентів.

Таким чином, загрози та ризики інформаційної безпеки у хмарних обчисленнях мають багатовимірний характер і тісно пов'язані з організаційними та технічними аспектами використання хмарних сервісів. Це зумовлює необхідність формування комплексних політик безпеки, які враховують специфіку хмарних середовищ, сучасні підходи до управління ризиками та результати наукових досліджень.

Список використаних джерел

1. Вахула О., Опірський І. Дослідження проблематики безпеки в хмарних середовищах та вирішення з застосуванням підходу “безпека як код”. *Ukrainian information security research journal*. 2023. Т. 25, № 3. С. 113–122. URL: <https://doi.org/10.18372/2410-7840.25.17936> (дата звернення: 17.03.2026).
2. Король М., Опірський І. Дослідження та аналіз проблем та викликів, що виникають у забезпеченні кібербезпеки в хмарних обчисленнях. *Ukrainian information security research journal*. 2024. Т. 26, № 1. С. 63–71. URL: <https://doi.org/10.18372/2410-7840.26.18829> (дата звернення: 16.03.2026).
3. Ojha P. Enhanced cloud computing security based on single to multi cloud systems. *Journal of research in science and engineering*. 2024. Т. 6, № 8. С. 52–56. URL: [https://doi.org/10.53469/jrse.2024.06\(08\).12](https://doi.org/10.53469/jrse.2024.06(08).12) (дата звернення: 10.03.2026).

УДК 004.056:004.891

*Дричак Б.Я., студент
Вовк Р.Б., к.т.н., доцент*

Івано-Франківський національний технічний університет нафти і газу

МЕТОДОЛОГІЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ У ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ СИСТЕМАХ

Широка імплементація глибоких нейронних мереж (DNN) у сучасну архітектуру інформаційно-комп'ютерних систем зумовлює критичну необхідність дослідження їхньої резистентності до адверсаріальних впливів. У період 2024–2026 рр. характер загроз еволюціонував від примітивних інвазій у вхідні дані до комплексних деструктивних маніпуляцій логікою функціонування та інтерпретованістю моделей. Зазначена тенденція трансформує проблему робастності нейромережових структур у фундаментальний аспект парадигми кібербезпеки.

Класифікація векторів атак традиційно здійснюється за критерієм рівня інформованості суб'єкта впливу про параметри цільової моделі:

- Сценарій «білої скриньки» передбачає повний доступ до внутрішньої архітектури та градієнтів моделі. Найбільш ефективними в даному контексті є градієнтні методи, зокрема Fast Gradient Sign Method та Projected Gradient Descent.

- Сценарій «сірої скриньки» базується на частковій інформації про систему та використанні властивості переносності через моделі.

- Сценарій «чорної скриньки» обмежується аналізом вхідних та вихідних сигналів. Детерміновано зростання ефективності таких атак за рахунок інтеграції великих мовних моделей (LLM) як інструментів генерації запитів [1].

Рівень робастності моделей демонструє суттєву кореляцію з предметною областю. В задачах комп'ютерного зору інтенсифікація глибини мережі сприяє покращенню генералізації, проте в системах виявлення мережових вторгнень (NIDS) надмірна глибина архітектури може ініціювати деградацію стійкості внаслідок дискретної природи вхідних параметрів [2]. Це обґрунтовує доцільність застосування доменно-орієнтованого підходу при проектуванні нейромережових компонентів. Окрему категорію становлять атаки на відмову в обслуговуванні, зокрема «губчасті атаки» (Sponge Attacks). Їхня специфіка полягає в цілеспрямованому максимізуванні обчислювальної складності обробки даних, що призводить до виснаження апаратних ресурсів, деградації енергоефективності мобільних пристроїв та підвищення латентності в хмарних сервісах.

Ескалація ризиків спостерігається в автономних транспортних системах та медичній діагностиці. У першому випадку адверсаріальний вплив здатний спричинити колапс логіки прийняття рішень, у другому – спотворити результати інтерпретації діагнозу, нівелюючи довіру до автоматизованих висновків. Розвиток LLM актуалізував загрози, пов'язані з автоматизованою генерацією дезінформації та маніпулятивним впливом на результати пошукової видачі. Емпірично доведено низьку стійкість таких моделей до числових пертурбацій, що вказує на лімітованість їхніх когнітивних спроможностей щодо логічного виведення. Для об'єктивізації оцінювання запропоновано індекс різниці стійкості. Дана метрика базується на аналізі топології внутрішнього простору ознак і дозволяє диференціювати якість розділення класів незалежно від специфіки алгоритму атаки.

Сучасний інструментарій захисту включає методи очищення представлень (representation scrubbing), дифузійні моделі для відновлення вихідних даних та алгоритми сингулярного розкладу (SVD) для фільтрації шумів. Перспективним вектором досліджень є розробка сертифікованих методів навчання (certified robustness), що гарантують стабільність виходу в межах заданого радіуса збурення [3].

Проте встановлено наявність оберненої залежності між точністю (accuracy) та робастністю (robustness). Формування оптимального балансу між цими показниками є першочерговим завданням при проектуванні систем для конкретних галузей.

Отже, забезпечення стійкості DNN є комплексним науково-технічним завданням, що вимагає синергії новітніх метрик оцінювання, адаптивних архітектурних рішень та верифікованих механізмів захисту. Подальша парадигма розвитку галузі полягає у створенні універсальних фреймворків аналізу надійності нейромережових систем, орієнтованих на експлуатацію в критично важливих сегментах економіки та безпеки.

Список використаних джерел

1. White, Gray & Black-Box Attacks Overview [Електронний ресурс]. URL: <https://surl.lu/juyczy> (дата звернення: 20.03.2026).
2. Exploring the Effect of DNN Depth on Adversarial Attacks in Network Intrusion Detection Systems [Електронний ресурс]. URL: <https://arxiv.org/html/2510.19761v1> (дата звернення: 20.03.2026).
3. RDI: An adversarial robustness evaluation metric for deep neural networks based on model statistical features [Електронний ресурс]. URL: <https://arxiv.org/html/2504.18556v2> (дата звернення: 20.03.2026).

УДК 004.7

*Гладченко О.В., к.пед.н., доцент
Луценко Н. О., здобувачка
Державний податковий університет*

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ В УМОВАХ СУЧАСНИХ РИЗИКІВ

Стрімкий розвиток інформаційно-комунікаційних технологій зумовив фундаментальну трансформацію корпоративних мережевих інфраструктур і суттєво змінив підходи до забезпечення їхньої безпеки. Якщо на попередніх етапах розвитку інформаційних систем мережі підприємств характеризувалися чітко визначеним фізичним і логічним периметром, централізованою архітектурою та обмеженим набором сервісів, то сучасні корпоративні середовища функціонують у складній розподіленій екосистемі. Така екосистема включає використання публічних і приватних хмарних платформ, сервісів віддаленого доступу, мобільних і персональних пристроїв, а також інтеграцію з інформаційними ресурсами партнерських організацій і сторонніх провайдерів послуг. Унаслідок цього традиційні межі мережевого периметра стають умовними, а контроль над потоками даних ускладнюється. Розширення поверхні атаки підвищує ймовірність компрометації інформаційних активів, що вимагає перегляду підходів до побудови систем кіберзахисту.

На ранніх етапах розвитку мережевих технологій основні кіберзагрози були пов'язані з експлуатацією відкритих мережевих портів і базових служб, що забезпечували передачу даних та віддалене керування системами. Зловмисники виконували сканування діапазонів IP-адрес для визначення активних вузлів, після чого здійснювали детальний аналіз відкритих сервісів, версій операційних систем і прикладного програмного забезпечення [1, с. 28–29]. Такий підхід дозволяв формувати карту мережевої інфраструктури та виявляти потенційні точки входу. Найбільш поширеними інструментами атак у цей період були використання відомих вразливостей системного та мережевого програмного забезпечення, реалізація атак типу DoS і DDoS з метою порушення доступності сервісів [2, с. 124], а також перебір облікових даних користувачів через слабкі механізми автентифікації. Відповідно до таких загроз основним засобом захисту виступали міжмережеві екрани, які здійснювали фільтрацію мережевого трафіку за IP-адресами джерела та призначення, номерами портів і типами транспортних протоколів.

З розвитком вебтехнологій та переходом бізнес-процесів у цифрове середовище вектори атак зазнали суттєвих змін. Зловмисники почали активно використовувати вразливості прикладного рівня, що сприяло поширенню складних атак на вебзастосунки. Серед найбільш небезпечних методів можна виокремити SQL-ін'єкції, які дозволяють отримувати несанкціонований доступ до баз даних, міжсайтовий скриптинг, спрямований на виконання шкідливого коду в браузері користувача, а також атаки на механізми керування сесіями та автентифікації. Особливість таких загроз полягає в тому, що мережевий трафік, який використовується для їх реалізації, часто передається через дозволені порти та стандартні протоколи HTTP або HTTPS. У результаті шкідлива активність маскується під легітимні запити, що значно ускладнює її виявлення традиційними засобами мережевого захисту, орієнтованими переважно на аналіз мережевого рівня.

Крім того, сучасні вебзастосунки характеризуються складною багаторівневою архітектурою, використанням API-інтерфейсів, мікросервісних підходів та інтеграцією з хмарними сервісами. Це створює додаткові вектори потенційних атак і підвищує вимоги до засобів моніторингу та контролю мережевого трафіку. Таким чином, еволюція інформаційних технологій спричинила необхідність переходу від статичних моделей периметрового захисту до адаптивних багаторівневих систем кібербезпеки, здатних враховувати прикладний контекст, поведінкові характеристики мережевих з'єднань і динамічні зміни середовища функціонування корпоративних мереж. Наступним етапом розвитку кіберзагроз стало поширення цільових довготривалих атак, які характеризуються ретельною підготовкою, використанням соціальної інженерії та здатністю зловмисника тривалий час залишатися непоміченим у системі. Додаткові труднощі створює широке застосування протоколів шифрування TLS, що призводить до формування «сліпих зон» у процесі моніторингу мережевого трафіку.

Традиційна модель мережевої безпеки базувалася на концепції периметрового захисту, відповідно до якої внутрішня мережа вважалася довіреним середовищем [3]. Проте сучасні кіберзагрози продемонстрували обмеженість такого підходу. Зокрема, класичні міжмережеві екрани не здатні виконувати глибокий аналіз прикладного контексту трафіку, що дозволяє шкідливим запитам маскуватися під легітимні HTTPS-з'єднання.

Важливою проблемою є також наявність внутрішніх загроз, пов'язаних із компрометацією робочих станцій, діяльністю інсайдерів або неконтрольованим поширенням шкідливого програмного забезпечення між сегментами мережі. За відсутності логічної

сегментації навіть одиничне проникнення може призвести до масштабної компрометації всієї інфраструктури.

Суттєвим недоліком традиційних систем безпеки є відсутність механізмів кореляції подій та інтелектуального аналізу аномалій у режимі реального часу. Це ускладнює виявлення багатоступеневих атак, у межах яких зловмисник поступово розширює свої привілеї та здійснює горизонтальне переміщення мережею. Крім того, використання розрізнених інструментів безпеки — від IDS-систем до автономних VPN-шлюзів — призводить до технологічної фрагментації, що ускладнює адміністрування та підвищує ризик помилок конфігурації.

У відповідь на стрімке ускладнення ландшафту кіберзагроз та зростання масштабів цифровізації корпоративних середовищ сформувалася концепція багаторівневого захисту, яка передбачає впровадження комплексу взаємопов'язаних механізмів контролю на різних рівнях функціонування інформаційної системи [4]. Основною метою такого підходу є створення послідовної системи бар'єрів безпеки, де компрометація одного компонента не призводить до автоматичного доступу до інших сегментів інфраструктури. Реалізація багаторівневого захисту дозволяє підвищити стійкість корпоративних мереж до зовнішніх та внутрішніх загроз, забезпечуючи ефективну локалізацію інцидентів та мінімізацію потенційних збитків.

Одним із ключових елементів цієї концепції є логічна сегментація мережевого середовища. Поділ інфраструктури на ізольовані функціональні зони за допомогою технологій віртуальних локальних мереж, створення віртуальних інтерфейсів та впровадження гранулярних міжсегментних політик доступу дозволяє значно обмежити можливості горизонтального переміщення зловмисника.

Важливу роль у сучасних системах кіберзахисту відіграють технології глибокої інспекції пакетів, які забезпечують аналіз мережевого трафіку не лише на рівні заголовків пакетів, а й з урахуванням прикладного контексту переданих даних [5]. Це дозволяє ідентифікувати шкідливу активність, замасковану під легітимні мережеві запити, зокрема використання небезпечних скриптів, спроби несанкціонованого доступу до вебресурсів або передачу шкідливих вкладень. Використання механізмів DPI у поєднанні з системами запобігання вторгненням, контролю застосунків і вебфільтрації створює комплексний підхід до аналізу мережевих подій у режимі реального часу.

Подальший розвиток підходів до забезпечення мережевої безпеки пов'язаний із впровадженням концепції нульової довіри, яка передбачає

безперервну перевірку користувачів, пристроїв і сервісів незалежно від їх фізичного або логічного розташування [6]. У межах цієї моделі відсутнє поняття «довіреної внутрішньої мережі», а кожна мережева взаємодія розглядається як потенційно небезпечна. Доступ до інформаційних ресурсів надається відповідно до принципу мінімальних привілеїв із урахуванням контекстних параметрів, таких як рівень захищеності пристрою, поведінкові характеристики користувача, місцезнаходження, час запиту та тип виконуваної операції. У поєднанні з багаторівневими механізмами контролю, централізованими системами моніторингу та автоматизованими інструментами реагування це дозволяє сформувати адаптивну архітектуру кіберзахисту, здатну ефективно протидіяти складним сучасним кібератакам.

Список використаних джерел

1. Тарнавський Ю.А. Технології захисту інформації. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с. URL: <https://www.h-x.technology.ua/blog-ua/cyber-threats-forecast-2024-ua>
2. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ: Київський столичний університет імені Бориса Грінченка, 2018. 320 с. URL: https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
3. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підруч. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236с. URL: <https://ftp.kr-labs.com.ua/books/kozura-zahyst-info-v-komp-systemah.pdf>
4. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підруч. Київ: Видавництво НА СБ України, 2020. 256 с. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZhahystuInfOsnKiberbezp_2020.pdf
5. Терейковський І.А., Гнатюк С.О. Захист інформації в комп'ютерних системах: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2022. 135 с. URL: <https://ela.kpi.ua/server/api/core/bitstreams/0dbba7ac-40e4-4a83-80b7-f729109cfe9a/content>
6. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. URL: <https://doi.org/10.6028/NIST.SP.800-207>

UDC 004.78

*Berdov V. V., master's student
Nechyporenko O.V., Cand. Tech. Sc., Assoc. Prof.
Cherkasy State Technological University*

VEHICLE ACTIVE SAFETY COMPUTER SYSTEM

The modern development of the transport industry is characterized by the active integration of computer intelligent systems into the design of vehicles in order to increase the level of road safety. The significant increase in the number of road accidents creates an urgent need to introduce effective means of active and passive safety, capable not only of reducing the consequences of accidents, but also of preventing their occurrence.

Active safety systems that can detect critical situations, such as emergency braking or obstacles, and automatically initiate preventive actions are becoming particularly relevant. Other solutions are based on the use of the universal, affordable and energy-efficient Arduino microcontroller platform, which allows implementing a functional active safety system with the ability to adapt to different car models.

The goal of the work is to design a universal active vehicle safety system capable of preventing emergency situations by detecting obstacles.

An analysis of modern safety technologies used in automotive vehicles has found that active safety systems, such as anti-lock braking systems (ABS), electronic stability control (ESP), adaptive cruise control, emergency braking (AEB) and parking assistants, aim to prevent accidents and ensure stable vehicle control [1]. Passive systems (airbags, seat belts, crumple zones) are aimed at minimizing the consequences of a traffic accident.

Analysis of the functional parameters of data collection systems showed that the key technologies for road safety control are: adaptive cruise control, which uses lidar and radar sensors to analyze the distance to other cars; emergency braking system, which automatically activates the brakes in case of critical threats; parking assistants, which help the driver perform precise maneuvering in confined spaces.

It has been established that the collection and analysis of information in real time is a necessary condition for the effective functioning of any security system. Today, it is necessary to use intelligent monitoring algorithms that provide analysis of road situations and adjustment of driver actions [2].

Analysis of the mechanisms of operation of the main active safety devices has established that modern cruise controls use a combination of radars and cameras to ensure stable movement. AEB systems significantly reduce braking distances and reduce the risk of collisions. Parking sensors

provide accurate measurement of the distance to objects, which helps prevent accidents during maneuvering [3].

Based on the analysis of technological solutions, a functional diagram of a computer-based active safety system for a car is proposed, capable of operating independently of on-board electronics. The choice of the following main components is justified: Arduino Uno microcontroller, which processes data from sensors; LIDAR TF Luna, which provides accurate sensing of the space in front of the car; HC-SR04 ultrasonic sensor for monitoring obstacles at a short distance; A3144 digital Hall sensor for tracking vehicle speed; Blynk platform communication module, which provides information transmission to the driver's smartphone.

An electrical circuit for connecting sensors to a microcontroller has been implemented, ensuring stable interaction of all system components. Algorithms have been programmed: processing input data from sensors in real time; automatic speed correction in case of detection of dangerous situations; monitoring obstacles and remote driver notification.

The proposed configuration allows you to automate the analysis of the traffic situation, determine critical traffic parameters, and initiate automatic corrective actions to prevent emergency situations.

The proposed active safety system can be integrated into most car models. Its functionality allows for timely response to critical situations on the road, including obstacle detection, dangerous proximity to vehicles, and emergency braking, which significantly reduces the risk of accidents.

References

1. Korostelov M., Hnatov A. Doslidzhennia aktyvnykh system bezpeky dlia avtotransportnykh zasobiv // Vydavnytstvo «Avtomobilnyi transport». Vyp. 46, 2020. S. 40–45. doi: 10.30977/AT.2219-8342.2020.46.0.40
2. Myhal V., Arhun Shch., Hnatov A., Hnatova H., Sokhin, P. Intelktualne diahnostuvannia transportnykh zasobiv // Avtomobil i elektronika. Suchasni tekhnolohii. Vyp. 22, 2022. S. 72–80. doi:10.30977/VEIT.2022.22.0.5
3. Tovstokoryi M. Yu., Hnatov A. V. Analiz ta vplyv pryntsypiv roboty system aktyvnoi bezpeky avtomobilia na bezpeku rukhu // Avtomobil i elektronika. Suchasni tekhnolohii. Vyp. 24, 2023. S. 41–49. doi: 10.30977/VEIT.2023.24.0.8

УДК 004.7

Корнійчук В.В., здобувач
Державний університет «Житомирська політехніка»

ПРОБЛЕМИ ТА МЕТОДИ ПРОЄКТУВАННЯ МЕРЕЖЕВИХ ПРОТОКОЛІВ

У сучасних комп'ютерних мережах питання безпечного обміну даними набуває особливої актуальності у зв'язку зі зростанням обсягів інформації, кількості мережових загроз та вимог до продуктивності мережових систем. Оскільки основним призначенням комп'ютерних мереж є передача даних, потрібно визначитись, як будуть надсилатися ці дані між користувачами, враховуючи певні обмеження у плані швидкості та надійності. Для цього існує мережовий протокол – набір правил про те, як повідомлення та дані будуть формуватися та оброблятися[1]. Існуючі стандартизовані мережові протоколи не завжди відповідають вимогам спеціалізованих клієнт-серверних чи однорангових систем, що обумовлює необхідність дослідження альтернативних підходів до проєктування захищених мережових протоколів.

Питання безпеки мережевого обміну даними широко висвітлюється у наукових дослідженнях та практичних реалізаціях, зокрема в межах протоколів транспортного рівня стеку TCP/IP[3]. Проте більшість наявних рішень орієнтовані на універсальне застосування і не завжди оптимальні для систем із підвищеними вимогами до затримок, масштабованості, контролю над протокольною логікою та насамперед – швидкості[2]. У практиці розробки програмного забезпечення часто виникає потреба створення власних протоколів, що зумовлює необхідність глибшого наукового обґрунтування принципів їх захисту та оптимізації[3].

Мета дослідження полягає у застосуванні системного підходу до проєктування захищеного мережевого протоколу, який поєднує сучасні криптографічні механізми з оптимізованими схемами обміну даними. У межах роботи обґрунтовано доцільність вибору легковагових механізмів захисту та структурної організації протоколу з урахуванням вимог сумісності, надійності та продуктивності. Зроблено висновок, що раціональне поєднання засобів захисту та архітектурних рішень дозволяє зменшити негативний вплив безпеки на швидкодію мережевого обміну.

У результаті дослідження запропоновано архітектуру захищеного мережевого протоколу для обміну даними, що забезпечує

автентифікацію, конфіденційність, продуктивність у мережі та контроль цілісності інформації. Також представлено можливість налаштування передачі даних перед формуванням протоколу під час виконання та власну реалізацію фрагментації протоколу для більшої передачі даних (2048 кб).

Отримані результати мають практичне значення для розробки клієнт-серверних систем, мережесервісів та спеціалізованих програмних рішень, які потребують безпечного та продуктивного обміну даними, насамперед в програмах та системах реального часу. Подальші дослідження у цьому напрямі дозволять розробити ефективні архітектурні рішення, здатні забезпечити безпечний та продуктивний обмін даними в сучасних комп'ютерних мережах.

Список використаних джерел

1. Б.Ю. Жураковский, І.О. Зенів, «РОЗРОБКА ТА РЕАЛІЗАЦІЯ МЕРЕЖНИХ ПРОТОКОЛІВ НАВЧАЛЬНИЙ ПОСІБНИК», Київ: КПІ ім. Ігоря Сікорського, 2020 – 462 с.
2. Andrew Tanenbaum, David Wetherall, «Computer Networks 5th edition», New Jersey, 2012 – 960 с.
3. Douglas E. Comer, «Internetworking With TCP/IP Vol I: Principles, Protocols, and Architecture Sixth Edition», 2013 – 733 с.

УДК 004.3, 004.421.5, 004.056.5

Остапець Д.О., к.т.н., доцент

Русакевич С.Р., здобувач

Український державний університет науки і технологій

ОГЛЯД І АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ГЕНЕРАЦІЇ ВИПАДКОВИХ ЧИСЕЛ

Випадкові числа застосовуються в безлічі сфер – криптографії, комп'ютерному моделюванні, аналізі, статистичних вибірках, фізиці, інженерії, медицині та ін. Ці способи використання мають різні рівні вимог до ступеня випадковості чисел.

Існують дві принципово різні стратегії генерації випадкових бітів. Одна стратегія полягає у недетермінованому створенні бітів, де кожен біт виводу базується на фізичному процесі, який є непередбачуваним. Генератори чисел, побудовані на цій концепції називаються генераторами випадкових чисел (ГПЧ), а створені за допомогою нього числа – істино випадковими. Інша стратегія полягає у детермінованому обчисленні бітів за допомогою алгоритму перетворення певного початкового значення (зерна). Такий генератор має назву генератор псевдовипадкових чисел (ГПВЧ). Початкове значення, що використовується для ініціалізації ГПВЧ, повинно містити достатню ентропію, щоб забезпечити гарантію випадковості. Якщо початкове значення було підібрано вірно, а алгоритм добре розроблений, біти, що виводяться ГПВЧ, будуть непередбачуваними на рівні ГВЧ [1].

Безпека багатьох параметрів криптографічних систем (таких як криптографічні ключі, вектори ініціалізації, нонси) залежить від наявності надійних випадкових чисел. Використання джерел ентропії в ГВЧ є фундаментальною вимогою для забезпечення криптографічної стійкості системи. Недостатня випадковість чисел може призвести до передбачуваності ключів, створених для шифрування інформації, що в свою чергу значно знижує надійність захисту інформації.

Джерела ентропії зазвичай поділяють на дві категорії:

- Природні (фізичні) джерела ентропії;
- Програмно-апаратні джерела ентропії.

Багато природних явищ генерують статистично випадкові сигнали шуму – тепловий та дробовий шум, фотоелектричний ефект, броунівський рух, атмосферний шум та ядерний розпад [2]. Тепловий шум виникає внаслідок хаотичного теплового руху носіїв заряду в провідниках, тоді як дробовий шум є наслідком дискретної природи електричного заряду. Фотоелектричний ефект та ядерний розпад

забезпечують особливо високу якість випадковості, оскільки ґрунтуються на квантових феноменах, які є принципово непередбачуваними навіть теоретично. Всі ці джерела є надійними та добре дослідженими, проте для їх практичного використання в ГВЧ необхідне спеціалізоване апаратне забезпечення – аналого-цифрові перетворювачі, підсилювачі шуму або детектори випромінювання, – що здатне зафіксувати фізичний процес і перетворити його на послідовність бітів, придатну для використання в якості зерна ГВЧ.

Програмно-апаратні джерела шуму натомість використовують системні дані для генерації випадковості, не потребуючи спеціалізованого фізичного обладнання. Прикладами таких джерел можуть бути: стан оперативної пам'яті, часові мітки переривань, рухи комп'ютерної миші, натискання клавіш, мережеві події, завантаженість процесора, а також дані API операційної системи [3]. В якості джерела ентропії можна взяти й дані з акселерометра, гіроскопа та магнітометра [4]. Використання таких джерел є значно простішим в реалізації, оскільки вимагає лише програмного забезпечення, здатного обробити надані системою дані і перетворити їх в послідовність бітів. Недоліком даного типу джерел є їх залежність від активності користувача або стану системи, однак цей недолік можна усунути комбінацією декількох джерел для генерації потоку бітів.

Список використаних джерел

1. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST SP 800-90A Rev. 1. URL: <http://dx.doi.org/10.6028/NIST.SP.800-90Ar1>
2. D. Ostapets, V. Dziuba, P. Ivin, Hardware random numbers generator based on microcontroller. *MATEC Web of Conferences* 390, 04002. 2024. URL: <https://doi.org/10.1051/mateconf/202439004002>
3. Turan M. S., Barker E., Kelsey J., McKay K. A., Baish M. L., Boyle M. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST SP 800-90B. URL: <https://doi.org/10.6028/NIST.SP.800-90B>
4. Остапеч Д., Опрятний А. Дослідження можливості використання окремих датчиків мобільних пристроїв у якості джерела ентропії генератора випадкових чисел. *Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах»*. 2025. 82(2). С. 88–92. URL: <https://doi.org/10.31891/2219-9365-2025-82-12>

УДК 004.942:004.42

Чекун М.А., здобувач

Панченко В.І., ст. викладач

*Національний технічний університет
«Харківський політехнічний інститут»*

РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ІЄРАРХІЧНОГО МОДЕЛЮВАННЯ АРХІТЕКТУР ЕОМ

Вступ. У сучасній освіті в галузі прикладної комп'ютерної інженерії спостерігається дефіцит інструментальних засобів, що забезпечують наочну демонстрацію принципів функціонування електронно-обчислювальних машин (ЕОМ), а також підтримують ефективне проектування та оперативне тестування. Існуючі програмні рішення характеризуються обмеженими можливостями застосування та недостатньою універсальністю.

Мета роботи. Розробка програмного комплексу на базі рушія Unity та мови програмування C#, призначеного для проектування та симуляції логічних схем, який забезпечує високу обчислювальну продуктивність за рахунок відокремлення ядра симуляції від графічного інтерфейсу.

Методи та архітектурні рішення. Для досягнення високої продуктивності в роботі застосовано підхід «Data-Oriented Design». Ядро симуляції реалізовано на C# та базується на використанні плоских масивів структур і бітових операцій, що забезпечує мінімізацію навантаження на центральний процесор. Архітектура системи ґрунтується на принципі рекурсивної вкладеності компонентів: користувач може проектувати логічні схеми з використанням базових примітивів (NAND, NOR, NOT) та об'єднувати їх у функціональні блоки – «чипи» [1, 2]. На початковому етапі реалізовано ієрархічний підхід до симуляції, за якого кожен чип зберігає власну внутрішню структуру. Обчислювальний процес організовано у вигляді рекурсивного оновлення станів вкладених елементів на кожному такті симуляції. Такий підхід забезпечує високу гнучкість системи та підтримує динамічне редагування, оскільки зміни у внутрішній структурі чипа миттєво відображаються на всіх його екземплярах у межах проекту.

Для усунення зниження продуктивності при масштабуванні кількості елементів в архітектурі системи передбачено перехід від ієрархічного представлення у вигляді дерева до плоскої моделі. Процес трансформації полягає у послідовному обході ієрархічної структури проекту з подальшою заміною кожного високорівневого

функціонального блоку його внутрішнім вмістом із збереженням топології зв'язків. Усі логічні стани при цьому переносяться до лінійного буфера пам'яті. Замість об'єктних посилань використовуються цілочисельні індекси, що підвищує ефективність використання кеш-пам'яті процесора. Отримане пласке подання у вигляді списку операцій придатне до векторизації та паралельної обробки із застосуванням механізму «Job System» середовища Unity [3], що забезпечує можливість одночасного обчислення незалежних фрагментів схеми на різних ядрах процесора.

Вибір ігрового рушія Unity дозволив реалізувати динамічний та чутливий інтерфейс, що працює за принципом тайлової сітки. Основний робочий простір моделює нескінченне полотно, на якому користувач може розмішувати компоненти. Завдяки системі багатопланового рендерингу, графічна оболонка здатна відображати тисячі логічних елементів без втрати продуктивності, що є критичним для проектів рівня «процесор у зборі». Однією з ключових особливостей комплексу є диференційована візуалізація провідників. Бінарні провідники відображають стан «0» або «1» за допомогою зміни кольору, що дозволяє візуально відстежувати шлях сигналу. Для спрощення архітектури реалізовано підтримку шин даних (8, 16, 32, 64 біти) [4], що виділяються візуально, та при наведенні курсору користувач отримує спливаюче вікно з поточним значенням у шістнадцятковій або десятковій системі числення під час моделювання шин адреси та даних мікропроцесорних систем.

Висновки. Було розроблено програмний комплекс, що дозволив користувачеві створювати власні бібліотеки компонентів (від тригерів до повноцінних процесорів) та симулювати їхню роботу при стабільній продуктивності за рахунок оптимізацій. Поєднання ігрових механік із формалізованою інженерною симуляцією забезпечило створення ефективного програмного середовища для вивчення архітектури ЕОМ.

Список використаних джерел

1. Мельник А. О. Архітектура комп'ютера : підручник / А. О. Мельник. – Луцьк : Волинська обласна друкарня, 2008. – 470 с.
2. Жуков І. А. Архітектура комп'ютерів : підручник / І. А. Жуков, О. В. Корочкін. – Київ : НАУ, 2015. – 300 с.
3. Write multithreaded code with the job system. URL : <https://docs.unity3d.com/Manual/job-system.html> (дата звернення: 24.03.2026).
4. Patterson D. A. Computer Organization and Design : The Hardware/Software Interface / D. A. Patterson, J. L. Hennessy. – 6th ed. – Morgan Kaufmann, 2020. – 1128 p.

УДК 004.7

Красовський В.І., магістрант

Шелуха О.О., к.т.н., доцент

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПЕРЕДАЧІ ВІДЕОДАНИХ У ГЕТЕРОГЕННИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ КОДЕКА H.265+ ТА МЕХАНІЗМІВ QOS

Сучасні системи відеоспостереження трансформувалися з пасивної фіксації у засіб активної аналітики в реальному часі. Завдяки ШІ вони здатні класифікувати об'єкти та розпізнавати загрози, що створює критичне навантаження на мережу.

Сучасні системи відеоспостереження інтегруються в існуючі корпоративні мережі, що часто призводить до виникнення гетерогенності середовища, зокрема поєднання сучасного та застарілого обладнання. Основним викликом є поєднання сучасних гігабітних магістралей на базі комутаторів рівня розподілу наприклад, Cisco 3750G із застарілими сегментами рівня доступу Fast Ethernet таких як Cisco 3560 та 2960. При трансляції потоків високої чіткості обмежена пропускна здатність у 100 Мбіт/с стає критичним вузьким місцем, особливо при паралельному використанні каналу іншими сервісами.

Для вирішення зазначеної проблеми може використовуватись методика оптимізації таких мереж шляхом комбінованого застосування кодека H.265+ та механізму пріоритезації трафіку Quality of Service (QoS).

Для проведення дослідження було розроблено експериментальний стенд (рис.1), що включає в себе: ядро мережі на базі Cisco 3750G, до якого через магістральні канали підключено комутатори доступу Cisco 3560 PoE та Cisco 2960. Як джерело трафіку використано камеру Hikvision DS-2CD2323G2-IU. Обробка даних здійснювалася на сервері, де за допомогою Wireshark аналізувався мережевий джиттер та реальна смуга пропускання. На Cisco 3750 було налаштовано черги WRR та мапування класів сервісу CoS у значення DSCP для забезпечення QoS.

Експериментально порівняно ефективність кодеків H.264 та H.265+ в умовах навантаження каналу. Встановлено, що при статичній сцені інтелектуальний алгоритм стиснення H.265+ забезпечує зниження бітрейту на 52% порівняно з H.264. У сценаріях з інтенсивним рухом економія становить 31%, що є достатнім для запобігання переповненню буферів на портах Fast Ethernet.

При імітації критичного завантаження каналу фоновим UDP-трафіком, через утиліту iperf3, без активованих механізмів QoS

спостерігалися втрати пакетів відеопотоку до 12%, що призводило до розсіпання кадрів.



Рис. 1. Експериментальний стенд

Після активації черг Weighted Round Robin на комутаторах Cisco, відеопотік з міткою DSCP 34 отримав гарантовану смугу пропускання. В результаті втрати пакетів відео були повністю нівельовані, тоді як втрати фонового трафіку Best Effort склали 12%, що є допустимим для некритичних даних.

Як можна побачити з отриманих результатів, впровадження кодека H.265+ у поєднанні з налаштуванням L3 QoS на рівні ядра мережі дозволяє стабілізувати роботу систем відеоспостереження в гетерогенних середовищах. Це виключає потребу в негайній модернізації кабельних мереж та заміні комутаторів рівня доступу.

Список використаних джерел

1. Tanenbaum A. S., Wetherall D. J. Computer Networks. 5th ed. Pearson, 2011. 933 p. URL: https://books.google.gr/books?id=2xWHAQAACAAJ&source=gbs_book_otherversions (дата звернення: 28.03.2026).
2. Cisco Catalyst 3750 QoS Configuration Guide. URL: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/91862-cat3750-qos-config.html> (дата звернення: 13.03.2026).
3. Технічна документація Hikvision DS-2CD2000 серії. URL: https://assets.hikvision.com/prd/normal/all/doc/sm000058865/UD39407B_Network-Camera_User-Manual_G5-Web5.0_20241014.PDF?key=247a370a15bd34774f2dc720a860a524&time=1773740549655 (дата звернення: 13.03.2026).

УДК 004.7

*Адамчук Р.С., здобувач
Дячук О.Ю., ст. викладач
Колощук М.С., ст. викладач*

Державний університет «Житомирська політехніка»

МЕТОДИ АВТОМАТИЗОВАНОГО ЗБОРУ ТА АНАЛІЗУ ДАНИХ З TELEGRAM-СПІЛЬНОТ У ЗАДАЧАХ OSINT

У роботі досліджено методи автоматизованого збору та аналізу інформації з відкритих Telegram-спільнот у контексті OSINT. Систематизовано підходи до отримання даних із використанням клієнтського доступу до Telegram через звичайний акаунт користувача, а також допоміжних методів web-scraping. Проаналізовано методи обробки текстового контенту та запропоновано узагальнену функціональну модель системи моніторингу для задач приватного бізнесу.

Зростання обсягів відкритих даних у цифровому середовищі зумовлює необхідність їх ефективного аналізу. Концепція OSINT передбачає використання відкритих джерел для отримання аналітичної інформації [7]. Telegram як інформаційна платформа характеризується високою швидкістю поширення повідомлень і значною кількістю тематичних спільнот.

Автоматизований збір даних реалізується із використанням клієнтського доступу до Telegram через звичайний обліковий запис користувача, що дозволяє отримувати повідомлення з відкритих спільнот без необхідності використання офіційного API. Такий підхід забезпечує більшу гнучкість доступу до чатів, зокрема у випадках, коли використання ботів є обмеженим. Методи web-scraping можуть застосовуватися як допоміжний інструмент за умови дотримання політик платформ.

Офіційні інструменти Telegram API можуть використовуватися як альтернативний підхід для організації збору даних [1], [2].

Обробка даних здійснюється із використанням методів обробки природної мови [3], що включають нормалізацію, токенизацію, лематизацію та векторизацію тексту. Для підвищення точності аналізу можуть застосовуватися сучасні трансформерні моделі [4].

Важливим аспектом функціонування системи є попередня фільтрація інформації та визначення її релевантності. Для цього можуть застосовуватися методи ранжування повідомлень за ключовими словами, частотними характеристиками та семантичною близькістю. Це

дозволяє зменшити обсяг нерелевантних даних і підвищити ефективність подальшого аналізу.

Крім того, у системах OSINT-моніторингу доцільним є використання механізмів автоматичного виявлення аномалій, що дозволяють ідентифікувати нетипові інформаційні патерни або різкі зміни активності у спільнотах. Такі підходи можуть базуватися на статистичних методах або моделях машинного навчання та сприяють своєчасному виявленню потенційних загроз.

Практичні підходи до використання Telegram як джерела даних підтверджуються сучасними дослідженнями у сфері кіберрозвідки, зокрема при формуванні датасетів та виявленні загроз [5], [6].

Функціональна модель системи включає модулі збору, обробки, зберігання та аналізу інформації. Взаємодія між модулями забезпечує обробку інформації у квазі-реальному часі та масштабованість системи. Обмеженням підходу є залежність від доступності даних і політик Telegram.

У роботі систематизовано методи збору та аналізу даних із Telegram-спільнот. Встановлено, що ефективним є комбінований підхід із використанням API та методів NLP. Наукова новизна полягає у формалізації такого підходу для задач OSINT. Оцінювання ефективності може здійснюватися за метриками precision, recall та F1-score. Практична значущість полягає у застосуванні результатів для підтримки прийняття рішень у бізнесі.

Список використаних джерел

1. Telegram. Telegram APIs / TDLib. URL: <https://core.telegram.org>
2. Telegram. Telegram Bot API. URL: <https://core.telegram.org/bots/api>
3. Jurafsky D., Martin J. *Speech and Language Processing*. URL: <https://web.stanford.edu/~jurafsky/slp3/>
4. Devlin J. et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. URL: <https://arxiv.org/abs/1810.04805>
5. Arikkat D. R. et al. CTI Dataset Construction from Telegram. URL: <https://arxiv.org/pdf/2509.20943>
6. Saeed M. H. et al. SENTINEL: A Multi-Modal Early Detection Framework for Cyber Attacks. URL: <https://arxiv.org/pdf/2512.21380>
7. Van Puyvelde D., Tabárez F. The Rise of Open-Source Intelligence // *European Journal of International Security*. URL: <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586>

УДК 004.7

Лелета В.Р., здобувачка

Колощук М.С., ст. викладач

Дячук О.Ю., ст. викладач

Державний університет "Житомирська політехніка"

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ DDOS-АТАК У МЕРЕЖАХ КОРПОРАТИВНОГО РІВНЯ

Актуальність дослідження зумовлена стрімким зростанням кількості та складності розподілених атак типу відмови в обслуговуванні (Distributed Denial of Service, DDoS), які становлять одну з ключових загроз для сучасних інформаційно-комунікаційних систем. Такі атаки спрямовані на перевантаження мережевих ресурсів і можуть призводити до повної або часткової недоступності сервісів, що, у свою чергу, спричиняє фінансові втрати, порушення бізнес-процесів та зниження рівня довіри користувачів до цифрових платформ. Згідно з сучасними аналітичними звітами, у 2025 році спостерігається суттєве зростання інтенсивності та масштабів DDoS-атак порівняно з попередніми роками, що зумовлює необхідність удосконалення методів їх виявлення та протидії [1].

Традиційні методи виявлення мережевих атак, зокрема сигнатурні та порогові підходи, широко використовуються у системах мережевої безпеки. Проте їх ефективність значно знижується у випадку нових або модифікованих атак, які не мають попередньо відомих сигнатур або характеризуються динамічною поведінкою. Крім того, класичні методи часто потребують значного обсягу ручного налаштування та не здатні адаптуватися до змін у мережевому середовищі. У зв'язку з цим все більшої актуальності набувають підходи, засновані на використанні штучного інтелекту та машинного навчання, які дозволяють автоматизувати процес виявлення аномалій у мережевому трафіку [2].

Одним із перспективних напрямів є застосування методів аналізу потокових даних (flow-based підхід), що базується на агрегованих характеристиках мережевого трафіку, отриманих за допомогою технологій NetFlow, sFlow або IPFIX. На відміну від аналізу повного вмісту пакетів, такий підхід дозволяє істотно зменшити обсяг оброблюваних даних, знизити навантаження на обчислювальні ресурси та забезпечити масштабованість рішень. Це особливо важливо для корпоративних мереж із великим обсягом трафіку, де повний аналіз пакетів є технічно складним або економічно недоцільним.

Додатковою перевагою flow-based підходу є можливість ефективного виявлення аномалій на рівні поведінкових характеристик

трафіку. Зокрема, аналіз таких параметрів, як кількість пакетів у потоці, тривалість сесії, співвідношення вхідного та вихідного трафіку, дозволяє ідентифікувати нетипову активність навіть без доступу до корисного навантаження пакетів. Це є особливо важливим у контексті поширення технологій шифрування, які обмежують можливість глибокого аналізу пакетів (Deep Packet Inspection).

Крім того, flow-based підхід забезпечує сумісність із сучасними мережевими пристроями, оскільки більшість маршрутизаторів і комутаторів підтримують експорт потокових даних. Це дозволяє інтегрувати системи виявлення атак у вже існуючу інфраструктуру без значних додаткових витрат.

Важливим етапом побудови систем виявлення атак є використання навчальних наборів даних. У сучасних дослідженнях широко застосовуються відкриті датасети, зокрема CIC-DDoS2019 та CAIDA DDoS Dataset, які містять як нормальний, так і аномальний мережевий трафік різних типів. Використання таких наборів дозволяє проводити експериментальні дослідження, оцінювати ефективність моделей та порівнювати результати різних підходів у стандартизованих умовах [3, 4].

У межах даного дослідження розглядається підхід до виявлення DDoS-атак, який поєднує використання варіаційного автоенкодера (Variational Autoencoder, VAE) для виявлення аномалій та подальшу класифікацію із застосуванням моделей машинного навчання. Варіаційні автоенкодери належать до класу глибоких генеративних моделей і дозволяють ефективно моделювати нормальну поведінку мережевого трафіку. У процесі навчання модель формує латентний простір, що відображає статистичні характеристики нормальних даних. Відхилення від цього простору можуть інтерпретуватися як аномалії, що потенційно відповідають атакам [5, 6].

Важливою особливістю варіаційних автоенкодерів є їх здатність працювати в умовах відсутності повністю розмічених даних, що часто має місце в задачах інформаційної безпеки. Оскільки реальні мережеві середовища характеризуються високою динамічністю, отримання повноцінних навчальних вибірок з усіма можливими типами атак є складним завданням. У цьому контексті використання напівконтрольованих або неконтрольованих методів навчання дозволяє підвищити адаптивність систем виявлення [5, 6].

Крім того, застосування латентного простору VAE відкриває можливості для подальшого аналізу структури трафіку та виявлення прихованих закономірностей. Це може бути використано не лише для

виявлення атак, але й для класифікації типів аномалій та прогнозування потенційних загроз.

Після етапу виявлення аномалій застосовується другий рівень обробки, який передбачає класифікацію трафіку за допомогою моделей глибокого навчання (Deep Neural Networks) або ансамблевих методів, зокрема XGBoost. Така комбінована архітектура дозволяє поєднати переваги різних підходів: здатність автоенкодера виявляти невідомі атаки та високу точність класифікації, притаманну сучасним алгоритмам машинного навчання [6-9].

Використання ансамблевих методів, таких як XGBoost, дозволяє ефективно обробляти табличні дані та враховувати складні нелінійні залежності між ознаками. У поєднанні з результатами, отриманими на етапі виявлення аномалій, це забезпечує підвищення загальної точності системи. Водночас глибокі нейронні мережі демонструють високу ефективність при роботі з великими обсягами даних, що робить їх доцільними для використання у високонавантажених мережах.

Комбінування різних типів моделей у межах єдиної архітектури дозволяє досягти балансу між швидкістю обробки даних, точністю виявлення та стійкістю до змін у мережевому середовищі.

Запропонований підхід має низку переваг. По-перше, він забезпечує можливість виявлення нових, раніше невідомих типів атак, що є важливим у контексті постійної еволюції кіберзагроз. По-друге, використання агрегованих потокових даних дозволяє зменшити залежність від аналізу повного вмісту пакетів, що позитивно впливає на продуктивність системи та спрощує її впровадження. По-третє, архітектура є масштабованою та може бути інтегрована у сучасні корпоративні мережі без суттєвих змін існуючої інфраструктури.

Водночас слід враховувати й певні обмеження. Зокрема, ефективність моделей машинного навчання значною мірою залежить від якості та репрезентативності навчальних даних. Крім того, використання глибоких нейронних мереж потребує значних обчислювальних ресурсів, що може ускладнювати їх застосування у реальному часі без відповідної оптимізації. Також важливим аспектом є проблема хибнопозитивних спрацювань, яка потребує додаткового дослідження та вдосконалення алгоритмів.

Практичне застосування запропонованого підходу можливе у системах моніторингу корпоративних мереж, центрах обробки даних, а також у хмарних середовищах. Інтеграція таких рішень із системами управління інформаційною безпекою (SIEM) дозволяє автоматизувати

процес виявлення інцидентів та підвищити швидкість реагування на кіберзагрози.

Зокрема, використання поточних даних у поєднанні з методами машинного навчання дає змогу реалізувати безперервний моніторинг мережевого трафіку та оперативно виявляти аномальні події, що є критично важливим для забезпечення стійкості інформаційних систем.

У результаті проведеного аналізу встановлено, що використання методів штучного інтелекту є перспективним напрямом розвитку систем виявлення DDoS-атак. Поєднання генеративних моделей для виявлення аномалій і класифікаційних алгоритмів дозволяє підвищити точність виявлення атак і адаптивність систем до нових типів загроз. Запропонований підхід може бути використаний як основа для побудови інтелектуальних систем мережевої безпеки, орієнтованих на захист корпоративних інформаційних систем.

Перспективи подальших досліджень полягають у розширенні експериментальної бази, оптимізації моделей для роботи в режимі реального часу, а також інтеграції запропонованого підходу з існуючими системами моніторингу та реагування на інциденти інформаційної безпеки [7-9].

Список використаних джерел

1. Cloudflare. DDoS threat report 2025 Q4. – URL: <https://radar.cloudflare.com/reports/ddos-2025-q4>
2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94). – URL: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf>
3. Canadian Institute for Cybersecurity. CICDDoS2019 dataset. – URL: <https://www.unb.ca/cic/datasets/ddos-2019.html>
4. CAIDA. The CAIDA DDoS Attack 2007 Dataset. – URL: https://www.caida.org/catalog/datasets/ddos-20070804_dataset/
5. Zavrak S., İskefiyeli M. Anomaly-Based Intrusion Detection From Network Flow Features Using Variational Autoencoder // IEEE Access. – 2020.
6. Kandiero A., Chiurunge P., Munodawafa J. Detection of DDoS Attacks Using Variational Autoencoder-Based Deep Neural Network // Applied Sciences. – 2023.
7. Batool S. et al. A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments // Electronics. – 2025.
8. Ganeshan S., Ramasamy R. A Systematic Review of Machine-Learning-Based Detection of DDoS Attacks // Future Internet. – 2026.
9. Hernandez D. V. et al. Real-Time DDoS Detection in High-Speed Networks Using Deep Learning // Electronics. – 2025.

УДК 004.738.5

Ковальчук О.М., здобувач

Колощук М.С., ст. викладач

Дячук О.Ю., ст. викладач

Державний університет «Житомирська політехніка»

АНАЛІЗ ВИКОРИСТАННЯ SOAR-ПЛАТФОРМ ДЛЯ АВТОМАТИЗАЦІЇ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

У сучасних умовах стрімкого зростання кількості кіберзагроз ефективність реагування на інциденти інформаційної безпеки стає одним із ключових факторів забезпечення стійкості ІТ-інфраструктури. Традиційні підходи до обробки подій безпеки, що базуються переважно на ручному аналізі, не забезпечують необхідної швидкості реагування та створюють значне навантаження на фахівців центрів моніторингу безпеки [1].

Метою даної роботи є аналіз можливостей застосування платформ класу SOAR (Security Orchestration, Automation and Response) для підвищення ефективності процесів виявлення та реагування на кіберінциденти.

Платформи SOAR призначені для інтеграції різномірних інструментів інформаційної безпеки, автоматизації типових сценаріїв реагування та централізації управління інцидентами [2]. На відміну від класичних систем моніторингу, SOAR-рішення дозволяють не лише агрегувати події, але й виконувати автоматизовані дії у відповідь на виявлені загрози.

Ключовим елементом SOAR є механізм оркестрації, що забезпечує взаємодію між різними системами захисту, такими як SIEM, IDS/IPS, антивірусні рішення та системи контролю доступу. Обмін даними між компонентами реалізується через програмні інтерфейси (API), що дозволяє формувати єдине середовище обробки інцидентів [1].

Важливу роль у функціонуванні SOAR відіграють плейбуки — формалізовані сценарії реагування на типові загрози. Вони визначають послідовність дій, які виконуються автоматично або з частковим залученням аналітика, що дозволяє стандартизувати процеси реагування та зменшити кількість помилок [2].

Окрім цього, SOAR-платформи забезпечують централізоване управління інцидентами, що спрощує координацію дій між різними підрозділами та підвищує прозорість процесів інформаційної безпеки.

Структуру взаємодії основних компонентів SOAR-платформи наведено на рис. 1.



Рис. 1. Узагальнена схема функціонування SOAR-платформи

Практичне застосування SOAR-платформ включає автоматизацію реагування на типові інциденти, зокрема фішингові атаки, виявлення шкідливого програмного забезпечення та несанкціонований доступ. У таких випадках система може автоматично перевіряти індикатори компрометації, блокувати облікові записи та ізолювати скомпрометовані вузли.

Особливо ефективним є використання SOAR у поєднанні з системами класу SIEM, які здійснюють збір та кореляцію подій безпеки. У такому випадку SIEM виступає джерелом подій, тоді як SOAR забезпечує автоматизовану обробку інцидентів і виконання відповідних дій реагування. Такий підхід дозволяє значно скоротити час від виявлення загрози до її нейтралізації.

На відміну від традиційних підходів, що потребують значної участі аналітика, SOAR дозволяє автоматизувати більшість процесів реагування та забезпечує їх стандартизацію через використання плейбуків, що зменшує затримки та мінімізує помилки.

У результаті аналізу встановлено, що використання SOAR-рішень дозволяє:

- суттєво скоротити час реагування на інциденти;
- знизити навантаження на аналітиків SOC;
- підвищити узгодженість і повторюваність процесів;
- покращити інтеграцію між засобами захисту.

Разом з тим, впровадження SOAR супроводжується рядом обмежень, зокрема необхідністю попередньої інтеграції систем, складністю розробки ефективних плейбуків та потребою у кваліфікованому налаштуванні [2].

Таким чином, застосування SOAR-платформ є перспективним напрямом розвитку систем кібербезпеки, що забезпечує підвищення ефективності реагування на інциденти за умови належного налаштування та інтеграції.

Список використаних джерел

1. IBM Security. *What is SOAR (Security Orchestration, Automation and Response)?* URL: <https://www.ibm.com/topics/soar>
 Microsoft Security. *What is SOAR?* URL: <https://www.microsoft.com/security/business/security-101/what-is-soar>

**BUILDING A SERVICE CATALOGUE FOR CLOUD SECURITY.
HOW TO SET UP CLOUD SECURITY SERVICES: ACCESS
PROVISIONING, AUTOMATED IR, CSPM/DSPM, DATA
CLASSIFICATION, ENCRYPTION-AS-A-SERVICE**

Abstract

The rapid growth of public and hybrid cloud infrastructures is reshaping information security approaches. As organizations migrate sensitive data and critical workloads to the cloud, risks caused by misconfigurations, inconsistent access control, and limited visibility increase. Traditional security methods are insufficient, creating a need for standardized and automated controls.

A cloud security service catalogue provides a unified framework that defines core security services, their scope, responsibilities, and automation workflows. This paper examines key catalogue components - access provisioning, automated incident response, CSPM/DSPM, data classification, and encryption-as-a-service - and shows how they collectively strengthen cloud security by enabling consistency, automation, and integrated risk management.

Keywords: Service Catalogue, Access Provisioning, Automated Incident Response, CSPM/DSPM, Data Classification, Encryption-as-a-Service

1. Introduction

1.1. Service catalog in cloud security

The growing complexity of cloud infrastructures requires a systematic approach to security management. A security services catalogue is a standardised repository of cloud security services that describes their structure, automation, monitoring, and control. It defines clear rules for how services work: scope, roles, responsibilities, workflows, service levels, and necessary tools. This unification reduces fragmentation, improves configuration consistency, simplifies integration with DevOps/DevSecOps, and provides better visibility and scalability of security practices.

1.2. Problem statement, hypothesis, and research objective

Problem statement

Cloud environments often lack unified management: access, data protection, encryption, and incident response are implemented differently across different teams. This leads to misconfigurations, loss of visibility,

automation complexity, and increased risks. The lack of a service catalogue makes it impossible to standardise and predict security controls.

Hypothesis

If a clearly defined and standardized cloud security services catalogue (access, automated response, CSPM/DSPM, data classification, encryption) is implemented, security processes will become consistent, automated and measurable. This will reduce incidents due to misconfigurations, improve risk detection, and increase control over cloud environments.

Research objective

Create a structured model for developing a cloud security services catalogue that defines the roles, automation level, and operational processes of key security services. The goal is to show how such a catalogue improves management, supports compliance with standards, strengthens risk management, and integrates with DevSecOps in dynamic clouds.

2. Methodological basis for building the catalogue

The cloud security service catalog is built on principles, standards, and operational models that define how security services are delivered and automated. Its methodology ensures both a clear structure and compliance with security requirements, corporate policies, and international standards.

2.1. Basic principles of catalogue construction

Table 1. Basic principles of catalogue construction

Zero trust principle	The service catalogue is built based on the zero trust concept, which assumes no trust in any user or resource by default. All services must provide for identity, context, and policy compliance verification.
Least privilege and separation of duties	Each service in the catalogue must take into account the principle of least privilege and separation of duties. This is especially important for access provisioning, DSPM, and cryptographic services.
Policy-as-code	Cloud security services must be described by policies that can be executed automatically (Terraform, Open Policy Agent, AWS SCP). This ensures repeatability, verification, and control.
Automation and orchestration	The catalogue should be geared towards full or partial automation of security processes: from problem detection to response. This is the basis for automated IR, CSPM, and DSPM.

2.2. Shared responsibility model

The catalogue reflects the shared responsibility model, defining which security aspects the cloud provider handles and which are the organisation's responsibility. The provider secures physical infrastructure, hypervisors, and networks, while the customer manages cloud configurations, access, data

classification, and encryption. The catalogue formalises these boundaries and covers gaps on the customer side.

2.3. The role of international standards

When compiling the catalogue, it is necessary to focus on the requirements and recommendations of global standards, such as:

- NIST SP 800-53 - control measures for information systems.
- ISO/IEC 27001 - requirements for information security management systems.
- CIS Benchmarks - best practices for configuring cloud resources.
- GDPR / HIPAA / PCI-DSS - regulatory requirements for data processing.

The catalogue should include services that ensure compliance with these requirements (e.g., data classification or encryption-as-a-service for GDPR).

2.4. DevSecOps as an operational model

The catalogue integrates with DevSecOps, becoming part of the CI/CD pipeline. It enables automatic IaC verification, configuration checks via CSPM, continuous access monitoring, and incident response through SOAR, ensuring security before deployment.

2.5. Risk-based approach

The security catalogue is built taking into account the criticality levels of data and environments. For example:

Table 2. Critical levels of data and environments

Dev	minimum requirements (no sensitive data)
Prod	maximum protection, DSPM + CSPM + EaaS

This allows services to be adapted to the level of risk without complicating processes where it is not necessary.

3. Description of key cloud security services in the service catalog

This section defines the core security services included in the cloud security service catalog. Each service describes a standardized security function that supports consistent protection, automation, and governance across cloud environments.

3.1. Access provisioning

Access provisioning aims to eliminate excessive permissions, prevent orphaned accounts, and standardise access in the cloud. The service provides controlled access based on the principles of least privilege and zero trust, automatically grants and revokes access to users, service accounts, and

workloads, verifies policies as code, and integrates with key and secret management systems.

3.2. Automated incident response

Automated incident response reduces MTTR and standardises incident response through automated scripts. The service automatically corrects misconfigurations, isolates suspicious resources, forces key rotation, quarantines anomalous activity, and integrates with SIEM, CSPM, DSPM, and SOAR pipelines.

3.3. CSPM / DSPM

CSPM/DSPM provide comprehensive visibility into risks at the infrastructure and data levels.

- CSPM continuously checks cloud configurations, detects errors, scans IaC, compares parameters with CIS, NIST, and ISO 27001, and supports automatic remediation.
- DSPM locates data, classifies sensitive information, analyses access patterns and exposure risks.

Together, they provide context: DSPM finds sensitive data → CSPM identifies its dangerous exposure → automated IR responds.

3.4. Data classification

Data classification ensures that data sensitivity is correctly identified and appropriate controls are applied. The service performs automatic content analysis (ML, patterns, context), assigns tags, integrates with DLP/DSPM, correlates data types with GDPR, HIPAA, PCI-DSS requirements, and applies access, storage, and encryption policies.

3.5. Encryption-as-a-service

Encryption-as-a-service ensures consistent and correct application of encryption across all cloud environments. It centralises key management (KMS, HSM), automates rotation, provides encryption of storage, databases, traffic and backups, and provides auditing of cryptographic operations.

4. Integrated model of service interaction in the cloud security catalog

The cloud security service catalogue operates as an integrated system where services reinforce each other and form an automated security perimeter: access control, data protection, configuration monitoring, and response.

4.1. Inter-service interaction

The services interact in a logical sequence:

- Access provisioning sets permissions and least privilege principles.
- DSPM assesses how these permissions affect access to sensitive data.

- CSPM correlates data risks with configuration errors.
- Automated IR performs automated remediation based on DSPM/CSPM signals.

This creates a continuous risk management flow: identity → data → configurations → response.

4.2. Automated security cycle

The model operates cyclically, minimising manual work and unifying control across different environments.:

1. **Detection:** DSPM identifies sensitive data and suspicious access.
2. **Classification:** data is tagged (PII, PHI, financial, etc.).
3. **Risk assessment:** CSPM checks resource compliance with policies.
4. **Response:** automated IR isolates resources, restricts access, updates keys, and corrects configurations.

To ensure coordinated operation of the cycle, the services have the following dependencies:

- DSPM transmits sensitivity metadata to CSPM and IR;
- CSPM uses access policies from Access Provisioning;
- Automated IR applies standardised playbooks linked to DSPM/CSPM results;
- Events (unauthorised access, data exposure, configuration errors) automatically trigger appropriate actions.

These dependencies create a unified, predictable, and scalable security model that aligns identity, data, configuration, and incident workflows into a single operational framework.

5. Practical challenges and issues

Table 3. Practical challenges and issues

Multicloud and API diversity	Different cloud platforms have their own APIs, access models, and log formats. This complicates the unification of CSPM/DSPM, automation configuration, and maintenance of consistent security policies.
Inconsistent policies across teams	Teams take different approaches to access, tagging, and configurations. Without a policy catalogue, policies remain fragmented, creating the risk of excessive privileges and non-compliance with standards.
Data quality issues for classification	Incomplete or missing tags, duplicate data, and lack of structure all reduce the accuracy of automatic classification and DSPM analysis.

False positives in CSPM/DSPM	A large number of false or low-priority alerts leads to 'alert fatigue.' Rule configuration and contextual correlation are essential for reducing noise.
Automation risks in production	Automated actions (resource isolation, key rotation, IAM policy changes) can cause production failures if they do not include validation or rollback mechanisms.

6. Conclusions

The expansion of cloud environments demands a standardized rather than fragmented approach to security. A cloud security service catalogue provides this structure by unifying core services, defining consistent workflows, and centralizing the enforcement of security policies. Although practical challenges remain - such as multicloud complexity and automation risks - the catalogue offers a predictable and scalable operational model to address them.

The analysis confirms that a well-designed catalogue improves visibility, strengthens risk management, and supports automation across modern cloud environments. As data volumes and infrastructure complexity continue to grow, the role of CSPM/DSPM and automated workflows will become increasingly fundamental for resilient cloud security.

References

1. James, Liam. (2026). Zero Trust Architecture Integration with NIST CSF for Resilient and AI-Augmented Critical Infrastructure Defense.
2. James, Liam. (2026). Adaptive Zero Trust Architecture for Critical Infrastructure Protection Using AI-Powered Threat Detection and NIST-Compliant Governance Models.
3. Ilochonwu, Ifeanyi. (2024). Information Technology Governance in Cloud Computing: A Framework of Risk Management and Compliance. Volume 11. pp:591-602.
4. ISO/IEC 27001:2022. (n.d.). ISO. <https://www.iso.org/standard/27001>
5. Jimmy, FNU. (2023). Cloud security posture management: tools and techniques. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2. 10.60087/jklst.vol2.n3.p622
6. AWS Security Reference Architecture (AWS SRA) – core architecture - AWS Prescriptive Guidance. (n.d.). <https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/introduction.html>

УДК 004.7

Гнатюк В.О., магістрант

Державний університет «Житомирська політехніка»

СИСТЕМА АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ЗАДАЧ SIGINT

У сучасних умовах зростання кількості кіберзагроз особливого значення набувають ефективні системи аналізу мережевого трафіку. Традиційні підходи, що базуються на сигнатурному аналізі, дозволяють виявляти лише відомі типи атак і є малоефективними проти нових або модифікованих загроз. Це обумовлює необхідність використання інтелектуальних методів аналізу, зокрема машинного навчання, у поєднанні з підходами Signals Intelligence (SIGINT)[2].

Метою роботи є розробка системи аналізу мережевого трафіку, яка використовує алгоритми машинного навчання для виявлення аномалій та класифікації мережевих подій.

Запропонована система передбачає кілька основних етапів: збір даних, попередню обробку, виділення ознак та класифікацію. Збір мережевого трафіку може здійснюватися за допомогою аналізатора мережевих протоколів Wireshark із подальшим збереженням даних у форматі PCAP. Це дозволяє отримати детальну інформацію про мережеві пакети для подальшого аналізу[1].

На етапі попередньої обробки виконується фільтрація, нормалізація та підготовка даних. Основними характеристиками, що використовуються для аналізу, є IP-адреси джерела і призначення, тип протоколу, розмір пакета, інтенсивність передачі та часові інтервали між пакетами. Ці параметри формують набір ознак для моделей машинного навчання.

Для класифікації мережевого трафіку застосовуються алгоритми машинного навчання, зокрема дерева рішень, випадковий ліс та метод опорних векторів. Навчання моделей здійснюється на основі підготовлених наборів даних, що містять приклади як нормального, так і аномального трафіку. У процесі навчання модель формує правила, які дозволяють відрізнити типи мережевої активності[3].

Після навчання система здатна аналізувати нові дані та визначати їх належність до певного класу: нормальний трафік, сканування мережі або потенційна атака. Аналіз може виконуватися як у реальному часі, так і в режимі офлайн для попереднього збереження даних. У разі виявлення відхилень система формує попередження для подальшого реагування.

Для тестування системи може бути створене лабораторне середовище із використанням засобів віртуалізації або мережевих емуляторів, таких як GNS3. Це дозволяє моделювати різні сценарії мережевої активності та формувати навчальні вибірки.

Запропонований підхід має низку переваг. По-перше, система здатна виявляти нові типи атак без наявності попередніх сигнатур. По-друге, використання машинного навчання дозволяє ефективно обробляти великі обсяги даних та знаходити складні закономірності. По-третє, система може бути реалізована без використання спеціалізованого обладнання.

Отже, поєднання методів машинного навчання з підходами SIGINT дозволяє створити ефективну систему аналізу мережевого трафіку. Подальший розвиток таких систем пов'язаний із вдосконаленням моделей, розширенням набору ознак та інтеграцією з іншими засобами кіберзахисту.

Список використаних джерел

1. Network Security Through Data Analysis: Building Situational Awareness / Майкл Коллінз – O'Reilly Media, 2014 – 348 с
2. Визначення SIGINT [Електронний ресурс] – Режим доступу до ресурсу: <https://www.assured-systems.com/faq/what-is-signal-intelligence-sigint-and-why-does-it-matter/>
3. Machine Learning and Security: Protecting Systems with Data and Algorithms / Кларенс Чіо, Девід Фрімен – O'Reilly Media, 2018 – 370 с

УДК 003.26.09

*Шевченко А. Є., здобувач**Ядуча Д. В., асистент**Національний технічний університет України**«Київський політехнічний інститут імені Ігоря Сікорського»*

АНАЛІЗ СТІЙКОСТІ МОДИФІКОВАНОЇ КРИПТОСИСТЕМИ AJPS-1 З УЗАГАЛЬНЕНИМИ ЧИСЛАМИ МЕРСЕННА ДО АТАК НА ОСНОВІ РЕШТОК

В 2017 році у межах конкурсу постквантових криптопримітивів NIST [1] було запропоновано механізм інкапсуляції ключів Mersenne-756839, що побудований на основі криптосистеми AJPS. В будові криптосистеми використовується арифметика за модулем числа Мерсенна, а також обмеження ваги Геммінга секретних параметрів. Однією з версій криптосистеми AJPS є схема шифрування біту повідомлення – криптосистема AJPS-1 [2]. Стійкість криптосистеми AJPS-1 ґрунтується на складності задачі ділення чисел з малою вагою Геммінга за модулем числа Мерсенна (MLHRSP).

Означення 1 (Задача MLHRSP). Нехай $\epsilon M_n = 2^n - 1$, $n \in N$ – число Мерсенна, додатне ціле число h та нехай F та G – два випадкові лишки за модулем M_n , що мають вагу Геммінга h . Число H обчислюється як $H = F \cdot G^{-1} \pmod{M_n}$. За відомими H , h , M_n необхідно знайти F і G .

На сьогодні задача MLHRSP вважається обчислювально складною, оскільки до неї було застосовано ряд атак, наприклад, «Вгадай і виграй», «Зустріч посередині», а також атака на основі алгоритму LLL, проте жодна з них не змогла розв'язати задачу MLHRSP для рекомендованих розмірів параметрів криптосистеми.

У [3] побудовано модифікацію AJPS-1, що використовує узагальнені числа Мерсенна. Стійкість такої модифікації ґрунтується на складності задачі GMLHRSP.

Означення 2 (Задача GMLHRSP). Маючи узагальнене число Мерсенна $M_{n,m} = 2^n - 2^m - 1$, $n \in N$, $m \in N$, $m < n$, число H та значення h , необхідно знайти два числа F та G , що мають вагу Геммінга h , які задовольняють співвідношенню $H = F \cdot G^{-1} \pmod{M_{n,m}}$.

Для аналізу складності задачі GMLHRSP необхідно дослідити можливість застосування проведених атак на оригінальну задачу MLHRSP та перевірити їхню результативність у разі використання альтернативних модулів.

Розглянемо атаку на основі алгоритму LLL для задачі GMLHRSP.

Нехай маємо рівняння $H = F \cdot G^{-1} \pmod{M_{n,m}}$. Помноживши його на G ,

отримаємо $H \cdot G = F \pmod{M_{n,m}}$. Представивши секретні параметри F та G через суму степенів двійки, тобто $G = \sum_{i=0}^{n-1} g_i \cdot 2^i$, $g_i \in \{0, 1\}$ та $F = \sum_{j=0}^{n-1} f_j \cdot 2^j$, $f_j \in \{0, 1\}$, маємо рівняння $H \cdot \sum_{i=0}^{n-1} g_i \cdot 2^i = \sum_{j=0}^{n-1} f_j \cdot 2^j \pmod{M_{n,m}}$. Перенесемо усі доданки у ліву частину рівняння та замінімо редукцію за модулем $M_{n,m}$ на віднімання даного модуля t разів. Тепер початкове співвідношення має вигляд $H \cdot \sum_{i=0}^{n-1} g_i \cdot 2^i - \sum_{j=0}^{n-1} f_j \cdot 2^j - t \cdot M_{n,m} = 0$. Домноживши отриманий вираз на достатньо великий множник K , отримаємо $K \cdot \sum_{i=0}^{n-1} g_i \cdot 2^i \cdot H - K \cdot \sum_{j=0}^{n-1} f_j \cdot 2^j - K \cdot t \cdot M_{n,m} = 0$.

Наступним кроком будемо $(2n+1)$ -вимірну решітку $L(B)$, базис якої заданий стовпцями матриці B :

$$B = \begin{pmatrix} K \cdot H & K \cdot (2H \pmod{M_{n,m}}) & \mathbb{H} & K \cdot (2^{n-1}H \pmod{M_{n,m}}) & K \cdot 1 & K \cdot 2 & \mathbb{H} & K \cdot 2^{n-1} & K \cdot M_{n,m} \\ 1 & 0 & \mathbb{H} & 0 & 0 & 0 & \mathbb{H} & 0 & 0 \\ 0 & 1 & \mathbb{H} & 0 & 0 & 0 & \mathbb{H} & 0 & 0 \\ \mathbb{H} & \mathbb{H} & \mathbb{H} & \mathbb{H} & \mathbb{H} & \mathbb{H} & \mathbb{H} & \mathbb{H} & \mathbb{H} \\ 0 & 0 & \mathbb{H} & 0 & 0 & 0 & \mathbb{H} & 1 & 0 \end{pmatrix}$$

Таким чином, якщо вдасться знайти вектор решітки $L(B)$, для якого перша координата дорівнює 0, тоді буде виконуватись рівняння $K \cdot g_0 \cdot H + K \cdot g_1 \cdot (2H \pmod{M_{n,m}}) + \mathbb{H} + K \cdot g_{n-1} \cdot (2^{n-1}H \pmod{M_{n,m}}) - K \cdot f_0 \cdot 1 - K \cdot f_1 \cdot 2 - \mathbb{H} - K \cdot f_{n-1} \cdot 2^{n-1} - K \cdot t \cdot M_{n,m} = 0$,

отже, і рівняння $K \cdot \sum_{i=1}^{n-1} g_i \cdot 2^i \cdot H - K \cdot \sum_{j=1}^{n-1} f_j \cdot 2^j - K \cdot t \cdot M_{n,m} = 0$, що відповідає умові задачі GMLHRSP. Помітимо, що такий вектор решітки буде мати вигляд $(0, g_0, g_1, \dots, g_{n-1}, -f_0, -f_1, \dots, -f_{n-1}, t)^T$, тому за значеннями g_i, f_j можна буде відновити числа F та G . Оскільки за умовою задачі числа F та G

мають малу вагу Геммінга h , то серед чисел $g_i, i = \overline{0, n-1}$ буде рівно h одиниць, а інші значення 0, та серед чисел $f_j, j = \overline{0, n-1}$ буде рівно h одиниць, а інші значення 0. Отже, отриманий вектор буде мати норму

$\sqrt{\|G\|^2 + \|F\|^2} = \sqrt{h+h} = \sqrt{2h}$. i є коротким вектором решітки, тому можна спробувати його знайти за допомогою алгоритму LLL. Варто зазначити, що при побудові базисної матриці спеціально застосовано великий множник K , що дозволяє кратно збільшити норму векторів, що мають ненульову першу координату, для того, щоб такі вектори не виникали як результат після застосування алгоритму LLL. Отже, якщо після застосування алгоритму LLL до базисної матриці B перший LLL-

редукований базисний вектор буде мати координату 0, то отримані значення F та G є кандидатами на розв'язок задачі GMLHRSP.

Однак, через будову базисної матриці, у решітці існують «паразитні» вектори, які є значно коротшими за шуканий. Прикладом такого вектора є $(0, 0^{i-1}, 2, -1, 0^{2n-i-1})_T$, що матиме норму $\sqrt{5}$. Для узагальнених чисел Мерсенна можна побудувати інші «паразитні» вектори з нормою $\sqrt{6}$.

Таким чином, у решітці $L(B)$ існує кілька типів векторів, що є коротшими за шуканий з нормою $\sqrt{2h}$, тому, під час пошуку короткого вектору решітки за допомогою алгоритму LLL, результатом будуть саме ці вектори. Тому така атака не призводить до успішного відновлення секретних параметрів F та G , що доводить стійкість модифікованої криптосистеми AJPS-1 з використанням узагальнених чисел Мерсенна до такого типу атак на решітках.

Висновки. У роботі проведено аналіз стійкості задачі GMLHRSP, що лежить в основі модифікації AJPS-1 з узагальненими числами Мерсенна, до атаки на основі алгоритму LLL. Розроблено алгоритм атаки, шляхом побудови решітки $L(B)$, на основі співвідношення задачі GMLHRSP та застосування до B алгоритму LLL. У результаті з короткого вектору решітки, який буде отримано в результаті LLL можна відновити секретні параметри F та G . Проте, у результаті дослідження виявлено, що у решітці $L(B)$ існують «паразитні» вектори, що мають норму значно меншу за очікувану. Таким чином, в результаті застосування алгоритму LLL будуть отримані саме ці вектори, які не можуть бути використані для відновлення шуканих секретних параметрів. Отримані результати доводять стійкість модифікованої криптосистеми AJPS-1 з використанням узагальнених чисел Мерсенна до такого типу атак на решітках.

Список використаних джерел

1. NIST's Post-Quantum Cryptography (PQC) Project. URL: <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>.
2. A New Public-Key Cryptosystem via Mersenne Numbers / D. Aggarwal, A. Joux, A. Prakash, M. Santha. Cryptology ePrint Archive, 2017. URL: <https://eprint.iacr.org/archive/2017/481/20170530:072202>.
3. Yadukha D. The Modification of the Quantum-Resistant AJPS-1 Cryptographic Primitive. Theoretical and Applied Cybersecurity. 2022. Т. 4, вип. 1. URL: <http://tacs.ipt.kpi.ua/article/view/274116>.

УДК 003.26.09

*Ковальчук А. В., здобувач**Ядуга Д. В., асистент**НТУУ «Київський політехнічний інститут ім. Ігоря
Сікорського»*

ПОБУДОВА МОДИФІКАЦІЇ ПОСТКВАНТОВОГО МЕХАНІЗМУ ІНКАПСУЛЯЦІЇ КЛЮЧА НА ОСНОВІ AJPS

Станом на сьогодні одними з найпоширеніших асиметричних криптопримітивів є RSA та ЕльГамала, стійкість яких ґрунтується на складності розв'язання задач факторизації та дискретного логарифмування. Однак П. Шор ще в 1997 р. представив алгоритм, користуючись яким ці задачі можуть бути ефективно розв'язані у квантовій моделі обчислень. Як наслідок, використання асиметричних криптосистем, що побудовані на задачах факторизації та дискретного логарифмування, вважається безпечним лише з огляду на те, що науковцям досі не вдалося побудувати масштабований квантовий комп'ютер. У 2017 році NIST оголосив конкурс постквантових асиметричних криптопримітивів, які є стійкими до атак з використанням як класичних, так і квантових комп'ютерів. Одним із учасників конкурсу є механізм інкапсуляції ключа Mersenne-756839 з сімейства криптосистем AJPS, особливість яких полягає у використанні арифметики за модулем числа Мерсенна $M_n = 2^n - 1$, $n \in N$ [1]. Одним з представників сімейства AJPS є побітова схема шифрування AJPS-1. В [2] побудовано модифікацію схеми шифрування AJPS-1, а саме механізм інкапсуляції ключа AJPS-KEM₁, який також ґрунтується на використанні чисел Мерсенна M_n як модуля, та працює за допомогою побудованої функції Solve для цього класу чисел. Пізніше було побудовано модифікацію для схеми шифрування AJPS-1, в якій було замінено клас чисел Мерсенна для арифметики за модулем на клас узагальнених чисел Мерсенна $GM_{n,m} = 2^n - 2^m - 1$, де $n, m \in N$, $n > m$ [3]. В цій роботі зосередимось на побудові модифікації AJPS-KEM₁ для класу узагальнених чисел Мерсенна $GM_{n,m}$.

Нехай AJPSGM-KEM₁ = (KeyGen, Encap, Decap) – модифікований механізм інкапсуляції ключа з використанням арифметики за модулем узагальнених чисел Мерсенна з трьома процедурами: генерація ключів, інкапсуляція та декапсуляція ключа.

KeyGen. З урахуванням параметра захищеності λ обирається число $GM_{n,m}$ та число h , що задовольняє умовам: $4h^2 < n \leq 16h^2$ та

$C_n^h \geq 2^\lambda \cdot 3$ множини лишків за модулем узагальненого числа Мерсенна, що мають вагу Геммінга h , обираються два n -бітові числа F , G рівноймовірно та незалежно. Відкритим ключем є значення $pk := H = F \cdot G^{-1} \pmod{GM_{n,m}}$, особистим ключем є $sk := G$, а значення F є секретним параметром.

Енсап. Рівноймовірно та незалежно обираються A, B – два лишки за модулем $GM_{n,m}$, причому $Ham(A) = Ham(B) = h$. Обчислюється значення $C = A \cdot H + B \pmod{GM_{n,m}}$. В результаті алгоритму інкапсуляції повертається шифротекст C , в який вбудовані значення A, B як інкапсульований ключ.

Декап. Використовуючи функцію $Solve$, отримувач розв'язує рівняння $G \cdot C \pmod{GM_{n,m}} = Fx + Gy \pmod{GM_{n,m}}$, використовуючи функцію $Solve$. Якщо розв'язок знайдено, то повертається пара (A, B) , де $A = x, B = y$, яка і є інкапсульованим ключем.

В оригінальній схемі AJPS-KEM₁, що використовує клас чисел Мерсенна, функція $Solve$ працює ітеративно, відновлюючи значення r -го біта невідомого числа A , та базується на тому, що множення чисел на степені двійки за модулем M_n є циклічним зсувом і, відповідно, вага Геммінга такого добутку дорівнює вазі Геммінга числа до множення [1, 2]. Алгоритм $Solve$ знаходить r -й біт A таким чином:

$$\begin{cases} 1, \text{ якщо } \Delta = h, \\ 0, \text{ якщо } \Delta \approx 0 (\Delta \neq h), \text{ де } \Delta = Ham(W) - Ham(W - 2^r \cdot F \pmod{M_n}), Ham(F) = h, \end{cases}$$

$$W = C \cdot G = A \cdot F + B \cdot G \pmod{M_n}.$$

Однак множення чисел на степені двійки за модулем узагальнених чисел Мерсенна не є циклічним зсувом, а тому реалізація такої перевірки як для модуля M_n , не спрацює для модуля $GM_{n,m}$. Далі наведена можлива реалізація $Solve$ для модуля $GM_{n,m}$, ідея якої полягає у перевірці та встановленні r -го біта невідомого числа A шляхом порівняння значення $\Delta_r = Ham(W) - Ham(W - 2^r \cdot F \pmod{GM_{n,m}})$ з верхньою межею ваги Геммінга добутка числа та степенів двійки за модулем $GM_{n,m}$, яка визначається за співвідношенням [4]:

$$Ham(2^r \cdot F \pmod{GM_{n,m}}) \leq Ham(F) + I\{r \geq n - m\} \cdot (r - n + m).$$

В функції $Solve$ для модуля $GM_{n,m}$ на кожній ітерації обчислюється Δ_r $\Delta_r \approx Ham(2^r \cdot F \pmod{GM_{n,m}})$. та очікується, що Тоді згідно наведеної верхньої оцінки ваги Геммінга добутка за модулем класу $GM_{n,m}$, r -й біт визначається як:

$$\begin{cases} 1, \text{ якщо } r \geq n - m \text{ і } 0 < \Delta_r \leq h + r - n + m, \\ 1, \text{ якщо } r < n - m \text{ і } 0 < \Delta_r \leq h, \\ 0, \text{ інакше} \end{cases}$$

Висновки. У цій роботі розглянуто механізм інкапсуляції ключа AJPS-KEM₁, який базується на арифметиці за модулем числа Мерсенна та працює з використанням функції Solve для цього класу чисел. У роботі побудовано модифікацію AJPSGM-KEM₁ з використанням узагальнених чисел Мерсенна як модуля. Для побудови такої модифікації, враховуючи особливості реалізації функції Solve для класу чисел Мерсенна, розроблено алгоритм Solve для чисел за модулем узагальненого числа Мерсенна. Отримані результати демонструють можливість перенесення AJPS-KEM₁ на клас узагальнених чисел Мерсенна для арифметики за модулем, що дозволяє збільшити варіативність параметрів криптопримітиву.

Список використаних джерел

1. A New Public-Key Cryptosystem via Mersenne Numbers / D. Aggarwal, A. Joux, A. Prakash, M. Santha. *Cryptology ePrint Archive*. 2017. URL: <https://eprint.iacr.org/2017/481>.
2. Ferradi H., Naccache D. Integer Reconstruction Public-Key Encryption. *Cryptology ePrint Archive*. 2017. URL: <https://eprint.iacr.org/2017/1231>.
3. Yadukha D. The Modification of the Quantum-Resistant AJPS-1 Cryptographic Primitive. *Theoretical and Applied Cybersecurity*. 2022. Т. 4, вип. 1. URL: <http://tacs.ipt.kpi.ua/article/view/274116>.
4. Ядуха Д. В., Фесенко А. В. Оцінка ваги Хеммінга суми та добутку чисел за модулем узагальненого числа Мерсенна. *Теоретичні і прикладні проблеми фізики, математики та інформатики*, 2020. С. 350–352. URL: <https://drive.google.com/file/d/1BcmU79pwMDtgA7ZXqTd5Gtw6C06Av1ou/view>.

УДК 004.7

*Литвинець Б.В., здобувач
Шушура О.М., д.т.н., професор*

Державний університет інформаційно-комунікаційних технологій

МІНІМІЗАЦІЯ ВПЛИВУ ШАХРАЙСТВА ТА ПРОТИДІЯ ЗАШУМЛЕННЮ ДАНИХ У СИСТЕМАХ КРЕДИТНОГО СКОРИНГУ

Ефективність кредитних скорингових систем багато в чому залежить від якості історичних даних. Швидкий перехід банківського сектору на цифрові технології призвів до збільшення кількості транзакцій, але водночас створив більше можливостей для шахраїв, що викликає проблему зростання шахрайських операцій. Такі випадки вносять шум у дані, що негативно впливає на результати роботи моделі.

Якщо шахрай отримує кредит, використовуючи синтетичні дані, та не повертає кошти, класична модель позначає це як низьку платоспроможність. В результаті алгоритм помилково сприймає поведінку шахрая як ознаки “поганого, але реального позичальника”. Через це відбувається зміщення концепту (Data Drift), що порушує логіку даних і знижує точність прогнозів алгоритмів.

Основна проблема — сильно дисбалансовані класи. Шахрайські операції складають дуже малу частку від усіх транзакцій, часто менше за 0.1%. Якщо подати такий неврівноважений набір даних звичному алгоритму, він ігнорує цю меншість і показує високу загальну точність, але при цьому пропускає більшість шахраїв (високий рівень хибнонегативних результатів).

Щоб алгоритм зміг краще знаходити шахрайські операції, потрібен агресивний підхід до підготовки даних. Ефективно штучно збільшувати кількість прикладів шахрайства, одночасно зменшуючи легітимні транзакції. Методи SMOTE та ADASYN допомагають створювати більше прикладів шахрайства, а Undersampling скорочує кількість нормальних транзакцій.

Щодо вибору моделей, найбільшу стійкість до шуму показують дерева рішень. Особливо градієнтний бустинг, який здатен виявляти складні та приховані зв'язки у поведінці клієнтів. Проте таку модель потрібно ретельно налаштовувати з урахуванням метрик, які добре працюють при дисбалансі даних: ROC-кривої, AUC, Precision-Recall AUC та F-міри.

Для роботи та впровадження таких моделей важлива надійна інфраструктура. Системи типу ClickHouse дозволяють виконувати

складні агрегатні SQL-запити в режимі реального часу. Їх інтеграція із візуалізаційними платформами допомагає моніторити стабільність системи та швидко реагувати на аномалії, що дуже важливо.

Отже, щоб ефективно мінімізувати вплив шахрайства, потрібно поєднувати просунуті методи роботи з незбалансованими даними, сучасні алгоритми та надійну інфраструктуру. Лише такий підхід дозволяє відокремити реальні кредитні ризики від шахрайських загроз і забезпечити стабільність системи.

Список використаних джерел

1. Aagrwal C. C. Outlier Analysis . 2nd ed.2017.
2. Synthetic Identify Fraud in the U.S Payment System A Review of Causes and Contributing Factors.2019.

УДК 004.056

Боцанюк І.М., магістрант
Головня О.С., к.пед.н., доцент
Державний університет «Житомирська політехніка»

АДАПТИВНА МОДЕЛЬ ПІДВИЩЕННЯ СТІЙКОСТІ СИСТЕМ ВИЯВЛЕННЯ ФІШИНГУ

Сучасні системи виявлення фішингових повідомлень базуються на поєднанні методів машинного навчання та евристичних підходів[1]. Машинне навчання забезпечує аналіз контексту повідомлення, включаючи семантичні характеристики, тоді як евристичні методи дозволяють оцінювати структурні ознаки, зокрема властивості URL-адрес і метадані. Використання гібридних підходів є доцільним, однак їх ефективна інтеграція залишається проблемною через відсутність універсального механізму узгодження результатів[2].

Основна складність полягає у відмінності форматів вихідних даних. Моделі машинного навчання формують клас разом із ймовірнісною оцінкою, тоді як евристичні алгоритми генерують бальні оцінки критичності ознак. Це ускладнює безпосереднє поєднання результатів і може призводити до суперечливих рішень у випадках, коли різні підходи сигналізують про протилежні висновки.

Додатково, ймовірнісні оцінки моделей не завжди є коректно каліброваними, що впливає на достовірність їх інтерпретації та може спричиняти зміщення у прийнятті рішень[3]. Евристичні підходи, у свою чергу, характеризуються обмеженою гнучкістю та залежністю від заздалегідь визначених правил, що ускладнює їх адаптацію до нових типів фішингових атак. У сукупності ці фактори знижують ефективність систем виявлення.

Метою дослідження є розробка адаптивного методу агрегування результатів машинного та евристичного аналізу електронних повідомлень для підвищення точності виявлення фішингу.

Більшість існуючих підходів використовують статичні схеми інтеграції, такі як фіксовані вагові коефіцієнти, порогові значення або просте голосування[4]. Такі методи не враховують контекст повідомлення та не здатні динамічно реагувати на зміну характеристик вхідних даних, що є критичним у середовищі кіберзагроз, яке постійно еволюціонує.

Запропонований підхід передбачає адаптивне агрегування результатів. На першому етапі виконується нормалізація даних шляхом приведення ймовірнісних і бальних оцінок до єдиної шкали. Для цього

можуть застосовуватись методи калібрування, що забезпечують більш коректну інтерпретацію рівня впевненості моделей машинного навчання.

Другий етап включає аналіз контексту повідомлення, зокрема виявлення ознак, що визначають релевантність кожного підходу. До таких ознак можуть належати структура повідомлення, наявність підозрілих посилань, складність тексту та інші характеристики, що впливають на достовірність оцінок.

На третьому етапі здійснюється агрегування результатів із використанням динамічного зважування. Вагові коефіцієнти змінюються залежно від контексту та рівня впевненості кожного джерела. Додатково може враховуватись узгодженість результатів між підходами, що дозволяє зменшити вплив суперечливих оцінок.

Очікується, що застосування адаптивного підходу дозволить підвищити точність класифікації, зменшити кількість помилок та покращити здатність системи до виявлення нових типів фішингових атак. Така модель є більш стійкою до змін у поведінці зловмисників і може бути інтегрована в існуючі системи кіберзахисту без суттєвих змін їх архітектури.

Подальші дослідження доцільно спрямувати на експериментальну перевірку ефективності методу, аналіз впливу різних стратегій зважування, а також розширення набору ознак, що використовуються у процесі прийняття рішень.

Список використаних джерел

1. A comprehensive survey of AI-enabled phishing attacks detection techniques / Basit A., Zafar M., Liu X. та ін. // *Telecommunication Systems*. 2021. Vol. 76, No. 1. P. 139–154.
2. Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text / Adebowale M. A., Lwin K. T., Sanchez E., Hossain M. A. // *Expert Systems with Applications*. 2019. Vol. 115. P. 300–313.
3. On calibration of modern neural networks / Guo C., Pleiss G., Sun Y., Weinberger K. Q. // *Proceedings of the 34th International Conference on Machine Learning*. 2017. Vol. 70. P. 1321–1330
4. Taha A. Intelligent ensemble learning approach for phishing website detection based on weighted soft voting. // *Mathematics*. 2021. Vol. 9, No. 21. P. 2799.

УДК 004.056

Щур Н. О., ст. викладач
Державний університет «Житомирська політехніка»

КРИПТОГРАФІЧНА ГНУЧКІСТЬ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні інформаційні системи працюють в умовах постійної зміни криптографічних вимог. Розвиток криптоаналізу, зростання обчислювальних можливостей і підготовка до постквантового переходу роблять недостатнім підхід, за якого криптографічні алгоритми жорстко вбудовані в прикладну логіку, протоколи або апаратні компоненти. Показово, що NIST уже затвердив три перші стандарти постквантової криптографії – FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) і FIPS 205 (SLH-DSA), а в березні 2025 року додатково обрав HQC як резервний алгоритм для майбутнього стандарту шифрування. Це свідчить, що проблема заміни криптографічних примітивів уже є практичним завданням для розробників, адміністраторів і власників цифрової інфраструктури.

У документах NIST криптографічна гнучкість (crypto agility) визначається як здатність замінювати й адаптувати криптографічні алгоритми в протоколах, застосунках, програмному забезпеченні, апаратурі, мікропрограмному забезпеченні та інфраструктурі без втрати безпеки й без порушення безперервності роботи системи [1]. Такий підхід варто розглядати не як окрему технічну функцію, а як архітектурну властивість інформаційної системи. Вона передбачає, що криптографія має бути винесена на рівень керованих сервісів, політик і стандартних інтерфейсів, а не залишатися набором ізольованих рішень у різних компонентах.

Основою криптографічної гнучкості є належне управління криптографічними ризиками. NIST рекомендує інтегрувати криптографічну гнучкість у систему управління інформаційною безпекою, проводити інвентаризацію криптографічних активів, застосовувати автоматизовані засоби виявлення алгоритмів і довжин ключів, визначати пріоритети переходу та централізовано впроваджувати криптографічні політики. Водночас слід враховувати залежності від постачальників, програмних бібліотек, апаратних засобів захисту ключів, хмарної інфраструктури та мережевих протоколів, оскільки недостатня гнучкість навіть одного елемента ланцюга постачання може унеможливити перехід усієї системи.

Для сучасних інформаційних систем особливе значення мають кілька практичних вимог. Передусім необхідно забезпечити взаємосумісність під час переходу між алгоритмами, адже певний час нові й застарілі механізми співіснуватимуть. Крім того, механізми узгодження алгоритмів у протоколах мають бути захищені від атак примусового зниження рівня захисту, інакше зловмисник може нав'язати слабший криптографічний набір. Архітектура системи також повинна враховувати, що постквантові ключі, підписи та шифротексти часто мають більший розмір, ніж традиційні, що впливає на сертифікати, мережеві протоколи, сховища даних і продуктивність. У перехідний період можливе застосування гібридних схем, які поєднують класичні та постквантові механізми, однак це ускладнює систему і потребує чіткого плану подальшої повної міграції.

Актуальність криптографічної гнучкості підтверджується також практичними дорожніми картами міграції [2]. Зокрема, NCSC у 2025 році запропонував етапний підхід до переходу на постквантову криптографію – до 2028 року провести повне виявлення залежностей і підготувати первинний план, до 2031 року виконати ранні пріоритетні міграції, а до 2035 року завершити перехід основних систем, сервісів і продуктів. Хоча ці строки не є універсальними для всіх країн і секторів, сама логіка такого підходу є показовою: спочатку інвентаризація, далі пріоритезація, після цього керована технічна заміна.

Отже, криптогнучкість у сучасних інформаційних системах є не додатковою перевагою, а необхідною умовою довгострокової кіберстійкості. Система, що не підтримує швидку й контрольовану заміну криптографічних механізмів, накопичує технічний борг і стає вразливою до нових типів атак, регуляторних змін та технологічних зсувів. Тому під час проєктування нових інформаційних систем доцільно закладати модульність криптографічних сервісів, централізоване керування політиками, інвентаризацію криптографічних залежностей і готовність до багатоетапних міграцій.

Список використаних джерел

1. Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W. and Kent, K. (2025), Considerations for Achieving Crypto Agility: Strategies and Practices, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, URL: <https://doi.org/10.6028/NIST.CSWP.39>.

2. Timelines for migration to post-quantum cryptography – NCSC.GOV.UK, URL: <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>.

УДК 004.85

*Палагін В.В., д.т.н., професор
Івченко О.В., к.т.н., доцент
Палагіна О.А., к.т.н., доцент
Воробкало О.К., магістрант*

Черкаський державний технологічний університет

МЕТОДИ AI/ML ДЛЯ АНАЛІЗУ ТА НЕЙТРАЛІЗАЦІЇ КІБЕРАТАК НА VLAN

Сучасна концепція побудови корпоративних та промислових мереж, включаючи інфраструктури 5G, базується на технології VLAN (IEEE 802.1Q) як фундаментальному інструменті логічної сегментації трафіку [1]. Однак, незважаючи на широке розповсюдження, сегментація на другому рівні моделі OSI (Layer 2) не є самодостатнім засобом захисту. Зростаюча складність мережевих ландшафтів та поява нових векторів атак на протоколи канального рівня роблять проблему безпеки VLAN критично важливою. Особливої гостроти це питання набуває в умовах динамічних середовищ, де традиційні статичні засоби захисту не встигають адаптуватися до мінливих сценаріїв вторгнень.

Основними деструктивними впливами на віртуальні мережі є атаки, спрямовані на обхід логічної ізоляції. Серед них ключовими є [2]:

- *VLAN Hopping (Double Tagging)* - використання зловмисником подвійного тегування 802.1Q для надсилання пакетів у суміжний VLAN в обхід маршрутизатора;
- *Switch Spoofing* - імітація зловмисником поведінки комутатора за допомогою протоколу DTP (Dynamic Trunking Protocol) для встановлення магістрального з'єднання (trunk) та отримання доступу до всіх VLAN мережі;
- *MAC-flooding (CAM-table overflow)* - генерація великої кількості фіктивних MAC-адрес для переповнення таблиці комутації, що змушує комутатор працювати у режимі концентратора (hub), транслуючи трафік на всі порти.

Класичні підходи до захисту VLAN базуються на «жорсткій» детермінованій логіці: відключення невикористовуваних портів, вимкнення DTP, використання Port Security або статична фільтрація подвійних тегів. Хоча ці методи забезпечують високу швидкість обробки (low latency) та відсутність помилкових спрацьовувань для відомих сигнатур, вони мають суттєві недоліки, зокрема:

- *негнучкість* - нездатність виявити атаки, параметри яких хоча б мінімально відрізняються від встановлених правил;
- *складність масштабування* - необхідність ручного переписування конфігурацій при кожній зміні архітектури мережі;

- *вразливість до динамічних атак* - детермінована логіка безсила проти інтелектуальних методів обходу, які імітують легітимну поведінку.

Застосування методів машинного навчання (AI/ML) для захисту VLAN дозволяє перейти від статичного аналізу окремих кадрів до комплексного моніторингу динаміки мережевого трафіку. Метод базується на вилученні статистичних ознак (features) з потоку даних, таких як ентропія MAC-адрес, частота появи тегів 802.1Q, часові інтервали між пакетами та специфічні прапорці протоколів канального рівня. Використання алгоритмів класифікації дає змогу виявляти складні закономірності, які не охоплюються жорсткою логікою. Це вирішує проблему «негнучкості» класичних методів: система стає здатною ідентифікувати атаку навіть за умови мінімальної модифікації її параметрів зловмисником, що значно знижує рівень помилкових пропусків (False Negatives) у порівнянні з детермінованими фільтрами.

Технічна реалізація пропонується у вигляді інтелектуального модуля аналізу, який інтегрується у дзеркальний порт комутатора (SPAN/RSPAN) або працює на рівні програмно-конфігурованих мереж (SDN). Процес включає етап попередньої обробки трафіку та агрегування потоку Ethernet-кадрів у вектори ознак. Підготовлена ML-модель аналізує ці вектори в режимі реального часу, порівнюючи поточну активність із профілем легітимної поведінки мережі. Такий підхід забезпечує адаптивність захисту, коли система самостійно корегує межі спрацювання при зміні архітектури мережі, усуваючи необхідність постійного ручного переписування конфігурацій та правил доступу.

Таким чином, застосування запропонованого підходу на основі AI/ML дозволяє трансформувати захист VLAN із пасивного набору статичних правил у динамічну адаптивну систему, здатну виявляти аномалії на випередження, що забезпечує високий рівень безпеки складних мережевих інфраструктур завдяки автоматизації аналізу трафіку та мінімізації впливу людського фактора.

Список використаних джерел

1. IEEE Std 802.1Q-2018. IEEE Standard for Local and Metropolitan Area Networks — Virtual LANs. — New York : IEEE, 2018. — 1992 p.
2. Nurfaishal M. D., Akbar Y. Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*. 2024. Vol. 5, no. 3. P. 3278–3290. DOI: 10.35870/jimik.v5i3.975.

УДК 004.414.3:004.056

*Палагін В.В., д.т.н., професор
Гончаров А.В., к.т.н., професор
Пташкін Р.Л., викладач*

*Черкаський державний технологічний університет
Черкаський науково-дослідний експертно-криміналістичний центр
МВС України*

МЕТОДОЛОГІЯ АПАРАТНОГО РЕЙНЖИНІРІНГУ ТА КРИМІНАЛІСТИЧНОГО АНАЛІЗУ ОБЧИСЛЮВАЛЬНИХ ПЛАТФОРМ

В умовах сучасної збройної агресії ударні безпілотні літальні апарати (БПЛА) перетворилися на складні мультипроцесорні системи, що постійно модернізуються. Необхідність апаратного рейнжинірингу (hardware reverse engineering) зумовлена потребою ідентифікації реального функціонального призначення кожного модуля, виявлення походження компонентної бази та розуміння алгоритмів керування. Криміналістичне дослідження електронної «начинки» дозволяє не лише встановити тактико-технічні характеристики апарату, а й отримати цифрові докази щодо каналів постачання складників та методів програмування польотних завдань.

Головна проблема дослідження полягає у високій варіативності та динамічній еволюції компонентної бази: постійно адаптується архітектура, переходячи від спеціалізованих сигнальних процесорів (наприклад, серії TMS320) до загальнодоступних мікроконтролерів (як-от STM32), що потребує постійного оновлення бібліотек сигнатур. Відсутність традиційних «чорних скриньок» унеможливує стандартне зчитування логів, змушуючи експертів вдаватися до складних методів chip-off або використання інтерфейсів налагодження JTAG/SWD.

Основними інструментами для вирішення цих викликів сьогодні є:

- апаратні аналізатори - використання логічних аналізаторів для реверс-інжинірингу протоколів обміну даними;
- програмні середовища дисасемблювання - застосування інструментів для статичного аналізу бінарного коду прошивок з метою виявлення прихованих функцій передачі телеметрії;
- інструменти неруйнівного контролю - рентгеноскопія багатошарових друкованих плат для відновлення топології з'єднань, що прихована під компонентами в корпусах BGA.

Додатковим викликом є аналіз «цивільних» надбудов на базі Raspberry Pi, де криміналістичне дослідження зміщується у площину

аналізу файлових систем Linux та деконструкції скриптів на Python, що керують модемами зв'язку. Це створює ситуацію, де класична експертиза має поєднуватися з методами Live Forensics для реконструкції мережевої активності БПЛА.

Запропонований метод дослідження базується на комплексній методології ієрархічного реверс-інжинірингу, що розглядає БПЛА не як цілісний об'єкт, а як розподілену мультипроцесорну екосистему. Ключова увага приділяється деконструкції модульного стека центральної обчислювальної системи, побудованої на сімействі процесорів TMS320, та аналізу розподіленого навігаційного комплексу на базі STM32. Такий аналіз дозволяє виявити логіку паралельної обробки сигналів і механізми забезпечення живучості апарату, що є критично важливим для розробки ефективних алгоритмів протидії на рівні фізичного керування польотом.

Особливе значення має ізоляція та прикладне дослідження автономної комунікаційної надбудови на базі Raspberry Pi під керуванням ОС Raspbian. Оскільки цей вузол функціонує як закритий інтелектуальний шлюз для збору розвідувальної інформації через комерційні мережі 3G/4G та Wi-Fi, метод фокусується на детекції прихованих каналів передачі даних у месенджери та хмарні сервіси. Виявлення алгоритмів роботи «цифрової надбудови» дозволяє реконструювати сценарії використання БПЛА як активного розвідувального модуля, що ідентифікує райони роботи засобів РЕБ та здійснює фотофіксацію об'єктів у реальному часі.

Таким чином, застосування методології апаратного реінжинірингу дозволяє оперативно адаптувати засоби РЕБ та ППО до нових модифікацій озброєння та проактивного розуміння технологічного циклу оновлення БПЛА, що підвищує ефективність захисту об'єктів критичної інфраструктури та створює доказову базу для документування.

Список використаних джерел

1. Серії «БІ» та «Б» — як росія модернізує «шахеди» та інші ударні БПЛА / Головне управління розвідки Міністерства оборони України. 2025. 18 лют. URL: <https://gur.gov.ua/content/serii-y-ta-iaak-rosiia-modernizuiie-shakhedy-ta-inshi-udarni-bpla.html>.

2. Романюк Д. Аналіз БПЛА-камікадзе противника, відмінності компонентів, додаткове обладнання. Інформаційна безпека та системи протидії (ISPS-2025) : зб. тез Міжнар. наук.-практ. семінару (м. Київ, 2025 р.). URL: <https://crsi.mil.gov.ua/files/isps/isps-collection-2025.pdf>.

УДК 004.3, 004.421.5, 004.056.5

Остапеч Д. О., к.т.н., доцент

Панін Д. В., магістрант

Пірогов Д. А., магістрант

Український державний університет науки і технологій

ОГЛЯД ДЖЕРЕЛ ЕНТРОПІЇ ДЛЯ ГЕНЕРУВАННЯ ВИПАДКОВИХ ЧИСЕЛ

Генерування випадкових послідовностей чисел виступає ключовим інструментарієм в сучасних інформаційних технологіях, що інтегруються в різноманітні галузі. За допомогою випадкових чисел реалізується велика кількість задач, таких як тестування алгоритмів і систем, імітаційне моделювання, задачі чисельного аналізу, захисту інформації, криптографії та багато інших. При цьому дуже важливо використовувати якісні генератори випадкових чисел, оскільки від цього залежить якість розв'язуваних задач.

Відомо два основних підходи отримання випадкової послідовності чисел: генерування псевдовипадкових чисел (pseudorandom numbers, PRN) за допомогою спеціальних алгоритмів або таблиць та використання спеціальних апаратних пристроїв, що генерують істинні випадкові числа (true random numbers, TRN) [1].

Псевдовипадкові послідовності чисел, на відміну від істинно випадкових послідовностей, генеруються за допомогою детермінованих алгоритмів на основі заданого початкового значення (зерно, seed). Це зумовлює повну відтворюваність результату при ідентичних параметрах ініціалізації та наявності певного періоду циклічності [2]. Натомість функціонування генераторів істинно випадкових чисел (TRNG) базується на апаратній оцифровці стохастичних фізичних процесів (шумів), отриманих з джерел ентропії [3]. Отримане значення надалі використовується або як випадкова число, або як зерно для ініціалізації інших генераторів [1].

Джерело ентропії – це фізичне джерело інформації, вихідний сигнал якого або виглядає випадковим, або стає випадковим після застосування процесу «відбілювання». Відбілюванням називають процес перетворення необроблених даних з неповною ентропією на дані зі 100% ентропією на біт [4]. Джерела ентропії TRNG поділяються на дві категорії: фізичні джерела та нефізичні джерела [5].

Високий рівень природної ентропії забезпечується спектром фізичних явищ, що продукують випадкові сигнали: від мікроскопічних квантових та теплових шумів до макроскопічних процесів, таких як

атмосферні завади та ядерний розпад [1]. Для практичної реалізації TRNG на основі природних явищ необхідне обладнання (АЦП, підсилювачі, детектори), яке перетворює аналоговий шум у бітову послідовність, придатну для ініціалізації генератора.

Нефізичні джерела шуму використовують дані API, дані оперативної пам'яті, системний час або дані натискання клавіатури, руху миші, для генерації випадковості [3] або дані з акселерометра, гіроскопа та магнітометра [6] або дані з вбудованих камер девайсів, камер відеозапису [4]. Такі джерела простіші у впровадженні, адже вимагають виключно програмних засобів для трансформації системних даних у послідовність бітів. Недолік залежності цих джерел від зовнішньої активності усувається поєднанням даних із декількох джерел ентропії.

Список використаних джерел

1. D. Ostapets, V. Dziuba, P. Ivin, Hardware random numbers generator based on microcontroller. *MATEC Web of Conferences* 390, 04002. 2024. URL: <https://doi.org/10.1051/matecconf/202439004002>.
2. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST SP 800-90A Rev. 1. URL: <http://dx.doi.org/10.6028/NIST.SP.800-90Ar1>.
3. Turan M. S., Barker E., Kelsey J., McKay K. A., Baish M. L., Boyle M. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST SP 800-90B. URL: <https://doi.org/10.6028/NIST.SP.800-90B>.
4. Hughes J. P., Gupta Y. "The Collector": A Gigabit True Random Number Generator Using Image Sensor Noise. URL: https://wrach2019.lip6.fr/WRACH_2019_paper_2.pdf.
5. NA Lv, Chen T., Ma Y. Analysis on Entropy Sources based on Smartphone Sensors. In *2020 the 10th International Conference on Communication and Network Security (ICCNS 2020)*, Tokyo, November 27-29, Japan, 2020. 11 p. URL: <https://doi.org/10.1145/3442520.3442528>.
6. Остапеч Д., Опрятний А. Дослідження можливості використання окремих датчиків мобільних пристроїв у якості джерела ентропії генератора випадкових чисел. *Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах»*. 2025. 82(2). С. 88–92. URL: <https://doi.org/10.31891/2219-9365-2025-82-12>.

УДК 004.8:004.912

Дзюба В.В., ст. викладач

Український державний університет науки і технологій

РОЗРОБКА ТА НАВЧАННЯ КОМПАКТНИХ МОВНИХ МОДЕЛЕЙ ДЛЯ ЗАСТОСУВАННЯ В ОСВІТНІХ СИСТЕМАХ ТА КІБЕРБЕЗПЕЦІ

У прикладних сценаріях освіти й кібербезпеки, де важливими є автономність, конфіденційність даних і можливість роботи на локальному обладнанні, перспективним є напрям створення компактних мовних моделей, придатних для запуску на споживчих GPU та локальних серверних вузлах. Додатковою перевагою такого підходу є можливість адаптації моделі до предметної області закладу освіти або до спеціалізованих наборів даних із кібербезпеки без постійної залежності від зовнішніх хмарних сервісів.

Сучасні мовні моделі великого масштабу забезпечують високу якість розв'язання широкого кола завдань обробки природної мови, проте їх розробка та навчання стримується значними вимогами до обсягу відеопам'яті графічного адаптера та наявності стабільного електроживлення обчислювальної системи на якій проводиться навчання.

Разом із тим дослідження архітектур компактних моделей має власну методологічну складність: кожна зміна конфігурації моделі, токенизатора, довжини контексту чи гіперпараметрів потребує окремого тренувального запуску, а отже – окремого обчислювального ресурсу.

Для моделі порядку 350 млн параметрів повноцінне навчання вже не є «швидким експериментом», особливо в умовах нестабільного електроживлення та обмеженого локального обладнання. У цьому контексті критично важливим стає не лише підбір архітектури, а й планування конкретних експериментів, різні методи та підходи до скорочення часу обчислень.

Роботи з обчислювально-оптимального масштабування доводять, що якість моделі визначається не лише кількістю параметрів, а й співвідношенням між розміром моделі та обсягом тренувальних токенів [1]. На практиці у низці робіт показано, що оцінка обчислювально-оптимального режиму узгоджується з практичним правилом близько 20 токенів на параметр у межах підходу Chinchilla [2].

З огляду на це у роботі пропонується дворівневий підхід до розробки моделі. На першому етапі виконується пошук архітектури та перевірка навчального контуру на дуже малих моделях у діапазоні 5-10

млн параметрів. Такий режим дає змогу швидко виявляти помилки в реалізації, оцінювати вплив токенизатора, параметрів оптимізації та структури блоку моделі без багатотижневих тренувальних циклів. Доцільність такого підходу підтверджується, зокрема, результатами TinyStories, де показано, що навіть моделі з числом параметрів нижче 10 млн за наявності добре підбраного корпусу можуть генерувати зв'язний текст [3].

На другому етапі, після фіксації базової архітектури, токенизатора та режиму навчання, доцільно переносити повне тренування цільової моделі в хмарне середовище. Такий підхід дозволяє використовувати локальну інфраструктуру для дешевого й швидкого архітектурного пошуку, а дорожчі хмарні ресурси – лише для фінального навчання моделі на вже перевіреному стеку.

В умовах нестабільного електроживлення обов'язковою складовою такого процесу є механізм частого збереження стану моделі, оптимізатора та станів генераторів випадкових чисел, що забезпечує детерміноване відновлення після переривань. Такий поділ мінімізує ризик втрати довгих запусків і робить дослідження більш надійним.

Розробка компактної мовної моделі для локального використання в освіті та кібербезпеці має спиратися не лише на зменшення кількості параметрів, а на системний підхід: контроль якості корпусу, проектування токенизатора, використання еталонної моделі для верифікації, багатоетапний архітектурний пошук на малих конфігураціях і перенесення повного навчання у хмару після стабілізації всіх компонентів. Саме така методика дозволяє зробити дослідження компактних мовних моделей технічно реалістичним, енергоефективним і придатним до практичного впровадження в умовах обмежених ресурсів.

Список використаних джерел

1. Hoffmann J., Borgeaud S., Mensch A. та ін. Training Compute-Optimal Large Language Models. 2022. arXiv:2203.15556. DOI: 10.48550/arXiv.2203.15556.
2. Besiroglu T., Erdil E., Barnett M., You J. Chinchilla Scaling: A Replication Attempt. 2024. arXiv:2404.10102
3. Eldan R., Li Y. TinyStories: How Small Can Language Models Be and Still Speak Coherent English? 2023. arXiv:2305.07759. DOI: 10.48550/arXiv.2305.07759

УДК 004.056.55:004.056.53

*Соловей В. А., молодший науковий співробітник**Житомирський військовий інститут ім. С. П. Корольова***ОФЛАЙН КОНФІДЕНЦІЙНА КОМУНІКАЦІЯ БЕЗ
АДРЕСАЦІЇ У КООРДИНАТНІЙ КРИПТОГРАФІЇ**

У запропонованій моделі криптографічний процес інтерпретується як навігація у внутрішньому координатному просторі системи, який динамічно еволюціонує у процесі виконання криптографічних подій. На відміну від класичних моделей, де шифрокод визначається відображенням $Enc_k(m)$, у даному підході шифрокод формується як координатне відображення об'єктів g_i у внутрішньому координатному просторі системи. Шифрокод виступає навігаційною інструкцією, реконструкція якої дозволяє знайти об'єкт g_i у внутрішньому координатному просторі. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події шифрокод не містить. У системі формується вектор події e_t – еквівалентний сформованому шифрокоду c_t , які мають різну форму представлення. Нехай UA_t – компонент відкритого тексту, NA_t – внутрішній ентропійний вектор імітаційних даних, що використовується у випадках відсутності відкритого тексту та визначається розподілом $\mathcal{D}_{NA}$, що забезпечує маскування структури повідомлення: $NA_t \sim \mathcal{D}_{NA}$. Внутрішній вектор e_t та зовнішній вектор c_t однієї і тієї ж криптографічної події задаються відображеннями:

$$e_t = P_t^{int}(UA_t, NA_t, \mathcal{E}_t), \quad c_t = P_t^{ext}(UA_t, NA_t, \mathcal{E}_t),$$

де P_t^{int} – внутрішня (латентна) проєкція, що формує подію e_t у вигляді множини бінарних векторів, P_t^{ext} – зовнішня проєкція, що формує шифрокод c_t як спостережуване представлення криптографічного процесу, $\mathcal{E}_t$ – операційний стан системи. Еволюція $\mathcal{E}_t$ відображається: $\mathcal{E}_{t+1} = \Psi_t(\mathcal{E}_t, c_t)$, де Ψ_t – фазово-залежне стохастичне відображення, c_t – верифікований шифрокод (подія). Унаслідок унікальності кожної фази: $\forall i \neq j: \Phi_i \neq \Phi_j$ виникає фундаментальна властивість фазової антиколізійності шифрокодів, яка може бути записана у вигляді $m_i = m_j \Rightarrow c_i \neq c_j$, $c_i = c_j \Rightarrow m_i \neq m_j$. Координатний компонентний простір формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset$, $GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри. Нехай $G_t^{(c)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом. Шифрокод c_t приймається тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}$, $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція верифікації, а значення 1 відповідає прийняттю. Верифікація не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. Система працює у логіці «свій / чужий» шифрокод. Нехай $S_t \in \{UA_t, NA_t, UA_t \cup NA_t\}$ – джерело подій у системі, що

визначає формування шифрокодів. Нехай $\{C_t\}_{t \in N}$ – випадковий процес шифрокодів, де N – множина фаз. Тоді виконується рівність розподілів:

$$\mathcal{L}(\{C_t\}_{t \in N}^{(UA)}) = \mathcal{L}(\{C_t\}_{t \in N}^{(NA)}) = \mathcal{L}(\{C_t\}_{t \in N}^{(UA \cup NA)}),$$

де верхній індекс позначає джерело, що індукує процес. Тобто процес шифрокодів є статистично нерозрізняваним відносно джерела їх формування. Відповідно, для зовнішнього спостерігача взаємна інформація між шифрокодами та джерелом подій дорівнює нулю: $I(c_t; S_t) = 0$. Для офлайн-комунікації використовується спільне сховище шифрокодів, яке можна представити як пул $CCP = c^1, c^2, \dots, c_k$. Користувачі періодично завантажують повний пул шифрокодів та локально верифікують кожний шифрокод c_t : $|S: V_S(c_i) = \text{accept}| \leq 1$.

Системи використовують стохастичний механізм обміну шифрокодами рівної, але не фіксованої довжини. Довжина шифрокоду визначається фазовими параметрами системи: $L = G(S_t)$, $L \in [L_{min}, L_{max}]$. Це дозволяє виконувати попередню фільтрацію кодів: $V_R(c_i) = \text{reject}$, якщо $|c_i| \neq L$, $c_i \in CCP_L$, $CCP_L = \{c \in CCP: |c| = L\}$ – перевіряється лише підмножина пулу CCP_L . Оскільки всі користувачі працюють з одним і тим самим пулом ССР, зовнішній спостерігач не має можливості визначити, який саме шифрокод призначений для

конкретного отримувача [1] $Pr(R_j | c_i) = Pr(R_j)$. Унаслідок цього розподіл шифрокодів у пулі не залежить від факту комунікації: $L(CCP|C) = L(CCP|\neg C)$, де C – подія інформаційного обміну між будь-якою парою користувачів та $Pr(C|CCP) = Pr(C)$ – тобто спостереження пулу шифрокодів не дає інформації про сам факт комунікації [2]. Ймовірність випадкової успішної верифікації стороннього шифрокоду прямує до нуля: $P(V_{S_t}(c_i) = \text{accept}) \ll 1$. Для будь-якого шифрокоду c_i існує не більше однієї системи, для якої виконується умова $V_{S_t}(c_i) = \text{accept}$. Таким чином Координатна криптографія дозволяє реалізувати модель офлайн конфіденційної комунікації без явної адресації, у якій зовнішній спостерігач не може встановити отримувача, напрямок комунікації, обсяг обміну відкритими даними та навіть сам факт інформаційного обміну. Ця інновація реалізує комунікаційну модель, у якій криптографічний захист досягається не лише шифруванням повідомлення, але й структурною невизначеністю самого факту комунікації: $I(CCP; C) = 0$, де I – взаємна інформація. Формально це означає, що для будь-якого алгоритму спостереження A його перевага у визначенні факту комунікації або її учасників на основі спостереження пулу ССР дорівнює нулю: $\forall A: Adv_A(CCP) = 0$.

Список використаних джерел

1. Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms // Commun. ACM. – 1981. – Vol. 24, № 2. – P. 84–90.
2. Danezis & Diaz — metadata-hiding / traffic analysis resistance; інваріантність розподілів.

УДК 004.056.55:004.056.53

*Соловей В. А., молодший наук. співробітник**Житомирський військовий інститут ім. С. П. Корольова*

МЕТАДАНОНЕЙТРАЛЬНІ КАНАЛИ КОМУНІКАЦІЇ ТА КРАХ МОДЕЛІ СПОСТЕРЕЖЕННЯ

У роботі розглядається властивість метаданонейтральності каналів комунікації сформованих у межах нової криптографічної парадигми - координатної криптографії (КК). Це онтологічно замкнена модель закритої комунікації, у якій спостережувані характеристики передавання не містять інформації про факт та/або структуру інформаційного обміну між комунікуючими системи. Ця властивість є похідною від трьох структурних механізмів: послідовного обміну шифрокодами, використання імітаційних даних та логічної безпарольної автентифікації шифрокоду (LPA). Саме їх одночасна дія формує метаданонейтральні властивості каналу. На відміну від класичних систем, де первинною операцією є розшифрування повідомлення, у КК первинною операцією є логічна перевірка коректності шифрокоду відносно поточного операційного стану системи. Шифрокод формується як координатне відображення об'єктів g_i у внутрішньому віртуальному просторі та виступає навігаційною інструкцією, реконструкція якої дозволяє знайти той самий об'єкт g_i у координатному просторі системи. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події шифрокод не містить. Координатний простір є компонентом операційного стану системи $\mathcal{E}_t$. Він формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset$, $GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри. Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, який верифікується як «свій» (інакше – «чужий») тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}$, $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю («свій»). LPA не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. Шифрокод може бути верифікований лише системами з симетричним операційним станом: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{S_t}(c) = \text{accept}$, що дозволяє зробити логічний висновок про автора шифрокоду. Нехай UA_t – компонент відкритого тексту, NA_t – внутрішній ентропійний вектор імітаційних даних, що використовується у випадках відсутності відкритого тексту та визначається розподілом $\mathcal{D}_{N,A}$, що забезпечує маскування структури повідомлення: $NA_t \sim \mathcal{D}_{N,A}$. Внутрішній вектор e_t та зовнішній вектор c_t однієї і тієї ж криптографічної події задаються відображеннями: $e_t = \Pi_t^{int}(UA_t, NA_t, \mathcal{E}_t)$, $c_t = \Pi_t^{ext}(UA_t, NA_t, \mathcal{E}_t)$, де Π_t^{int} – внутрішня (латентна) проєкція, що формує подію e_t у вигляді множини бінарних

векторів, P_t^{ext} – зовнішня проекція, що формує шифрокод c_t як спостережуване представлення криптографічного процесу. Еволюція $\mathcal{E}_t$ відображається: $\mathcal{E}_{t+1} = \Psi_t(\mathcal{E}_t, c_t)$, де Ψ_t – фазово-залежне стохастичне відображення, c_t – верифікований шифрокод (подія). Фазова еволюція незворотна та унікальна для кожної фази: $\forall i \neq j: \Phi_i \neq \Phi_j$. Звідси виникає фундаментальна властивість фазової антиколізійності шифрокодів, яка може бути записана у вигляді $m_i = m_j \Rightarrow c_i \neq c_j$, $c_i = c_j \Rightarrow m_i \neq m_j$. Нехай $S_t \in \{UA_t, NA_t, UA_t \cup NA_t\}$ – джерело подій у системі, що визначає формування шифрокодів. Нехай $\{C_t\}_{t \in N}$ – випадковий процес шифрокодів, де N – множина фаз. Тоді виконується рівність розподілів:

$$\mathcal{L}(\{C_t\}_{t \in N}^{(UA)}) = \mathcal{L}(\{C_t\}_{t \in N}^{(NA)}) = \mathcal{L}(\{C_t\}_{t \in N}^{(UA \cup NA)}),$$

де верхній індекс позначає джерело, що індукує процес. Тобто процес шифрокодів є статистично нерозрізнюваним відносно джерела їх формування [1]. Відповідно, для зовнішнього спостерігача взаємна інформація між шифрокодами та джерелом подій дорівнює нулю [2]: $I(c_t; S_t) = 0$. Закритий канал зв'язку для якого виконуються умови: нерозрізнюваність шифрокодів та інформаційна нейтральність комунікуючих сторін – є метаданонеітральним каналом зв'язку:

$$Ch_{MN} = \{channel \mid I(C; \{C_t\}_{t \in N}) = 0\}.$$

Для зовнішнього спостерігача кожна подія формування шифрокоду C_t статистично нерозрізнювана відносно спостереження [1] *Obs*, які доступні зовнішньому спостерігачу: $\forall t \in N: Pr(C_t \mid Obs) = Pr(C_t)$. Унаслідок цього спостереження каналу не дозволяє визначити, чи відбувався реальний інформаційний обмін: $Pr(C \mid \{C_t\}_{t \in N}) = Pr(C)$.

Тому для будь-якого алгоритму аналізу A його перевага на основі спостереження каналу дорівнює нулю, тобто $\forall A: Adv_A(channel) = 0$. Таким чином зовнішній спостерігач не може встановити факт комунікації, її напрямку, структуру або обсяг переданої інформації. Як наслідок - модель спостереження втрачає розрізнювальну здатність, що призводить до колапсу моделі спостереження, яка фактично колапсує до тривіального випадкового процесу: $\{C_t\}_{t \in N} \sim \mathcal{L}$.

Таким чином КК формує нову криптографічну парадигму та відповідний клас каналів зв'язку – метаданонеітральні закриті канали комунікації. Метаданонеітральні властивості виникають як природний наслідок структурної організації системи. Безпека моделі не спирається на ключі чи паролі, а визначається онтологічною замкненістю системи, стохастичною природою формування шифрокодів та відсутністю спостережуваних структур, які могли б виступати об'єктами атак.

Список використаних джерел

1. Goldwasser S., Micali S. Probabilistic encryption // *Journal of Computer and System Sciences*. – 1984. – Vol. 28. – № 2. – P. 270–299.
2. Serjantov A., Danezis G. Towards an information theoretic metric for anonymity // *Privacy Enhancing Technologies*. – 2002. – P. 41–53.

УДК 004.056.55:004.056.53

*Соловей В. А., молодший наук. співробітник**Житомирський військовий інститут ім. С. П. Корольова*

МОДЕЛЮВАННЯ ОНТОЛОГІЧНО ЗАМКНЕНИХ КАНАЛІВ ЗВ'ЯЗКУ У КООРДИНАТНІЙ КРИПТОГРАФІЇ

У роботі розглядається модель онтологічно замкненого каналу зв'язку, сформованого у межах нової криптографічної парадигми – координатної криптографії (КК). На відміну від традиційних криптографічних систем, де основні функції безпеки реалізуються через зовнішні інфраструктури (ключі, центри сертифікації, цифрові підписи, хеш-механізми тощо), у КК базові властивості захищеної комунікації виникають як внутрішні властивості самої системи. У результаті система формує канал зв'язку, структурно замкнений відносно власних механізмів функціонування. Онтологічна замкненість означає, що система не потребує зовнішніх довірених інфраструктур для забезпечення конфіденційності, автентифікації та контролю цілісності інформації. Усі ці властивості виникають у парадигмі КК як наслідок фазової еволюції операційного стану системи та симетрії його розвитку у комунікуючих сторін. Шифрокод формується як координатне відображення об'єктів g_i у внутрішньому віртуальному просторі та виступає навігаційною інструкцією, реконструкція якої дозволяє знайти той самий об'єкт g_i у координатному просторі системи. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події шифрокод не містить. Координатний простір є компонентом операційного стану системи $\mathcal{E}_t$. Він формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset$, $GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри. Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, який верифікується як «свій» (інакше – «чужий») тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}$, $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю («свій»). LPA не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. Шифрокод може бути верифікований лише системами з симетричним операційним станом: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{S_t}(c) = \text{accept}$, що дозволяє зробити логічний висновок про автора шифрокоду. Нехай UA_t – компонент відкритого тексту, NA_t – внутрішній ентропійний вектор імітаційних даних, що використовується у випадках відсутності відкритого тексту та визначається розподілом $\mathcal{D}_{NA}$, що забезпечує маскування структури повідомлення: $NA_t \sim \mathcal{D}_{NA}$. Внутрішній вектор e_t та зовнішній вектор c_t однієї і тієї ж криптографічної події задаються відображеннями: $e_t = \Pi_t^{int}(UA_t, NA_t, \mathcal{E}_t)$, $c_t = \Pi_t^{ext}(UA_t, NA_t, \mathcal{E}_t)$, де Π_t^{int} – внутрішня

(латентна) проєкція, що формує подію e_t у вигляді множини бінарних векторів, Π_t^{ext} – зовнішня проєкція, що формує шифрокод c_t як спостережуване представлення криптографічного процесу. Еволюція $\mathcal{E}_t$ відображається: $\mathcal{E}_{t+1} = \Psi_t(\mathcal{E}_t, c_t)$, де Ψ_t – фазово-залежне стохастичне відображення, c_t – верифікований шифрокод (подія). Фазова еволюція незворотна та унікальна для кожної фази: $\forall i \neq j: \Phi_i \neq \Phi_j$. Звідси виникає фундаментальна властивість фазової антиколізійності шифрокодів, яка може бути записана у вигляді $m_i = m_j \Rightarrow c_i \neq c_j$, $c_i = c_j \Rightarrow m_i \neq m_j$. Цілісність відкритого тексту m також виникає як внутрішня властивість системи. Механізм верифікації цілісності тексту здійснюється у наступній події через LPA шифрокоду.

$Event_1 \subseteq \{Bob \text{ відправив Алісі } c_1 \rightarrow A : c_1; A : V_{S_1}(c_1) \in \text{accept}; c_1 \Rightarrow m_1\}$. $Event_2 \subseteq \{Alice : h_{m_1} = H(m_1); c_2 = c_{r-1}(m_2) \oplus h_{m_1} \Rightarrow c_2 = F(m_2, n_2, S_2); A \rightarrow B : c_2; B : V_{S_2}(c_2) \in \text{accept}; c_2 \Rightarrow m_2\}$.

$Event_3 \subseteq \{B : h_{m_2} = H(m_2); c_3 = c_{r-1}(m_3) \oplus h_{m_2} \Rightarrow c_3 = F(m_3, n_3, S_3); Bob \rightarrow Alice : c_3; Alice : V_{S_3}(c_3) \in \text{accept}; c_3 \Rightarrow m_3\}$.

У події №3 – c_3 верифікований як «від Боба», враховуючи, що Аліса виконувала $h_{m_1} = H(m_1)$ та храповий механізм формування c_3 , робиться логічний висновок, що $(receive(m_1) \wedge integrity(m_1)) \Rightarrow read(m_1)$.

Будь-яка модифікація шифрокоду порушує фазову симетрію систем та виявляється під час LPA. Контроль цілісності реалізується без використання зовнішніх механізмів на кшталт цифрових підписів або хеш-функцій. У загальному вигляді безпека такої системи визначається виключно еволюцією її внутрішнього стану: $Security = f(S_t)$.

Це означає, що безпека системи не залежить від зовнішніх криптографічних інфраструктур [1]. Формально цю властивість можна подати як незалежність безпеки від зовнішніх механізмів довіри:

$I(Security; ExternalInfrastructure) = 0$, де $I(\cdot; \cdot)$ – взаємна інформація. Відповідно канал зв'язку, сформований у межах такої системи, можна визначити як онтологічно замкнений канал:

$$Ch_oC = \{C : Security(C) = f(S_t)\} \rightarrow I(Security; PKI) = 0.$$

Таким чином конфіденційність, автентифікація та контроль цілісності не потребують зовнішніх криптографічних артефактів і виникають як наслідок внутрішньої структури системи. Модель демонструє онтологічно замкнені канали зв'язку у яких безпека визначається не зовнішньою інфраструктурою довіри, а стохастичною еволюцією операційного стану. Системи безпеки, які ґрунтуються на онтологічно замкнених парадигмах комунікації є структурно стійкими до атак.

Список використаних джерел

1. Canetti R. Universally composable security: A new paradigm for cryptographic protocols // *FOCS*. – 2001. – P. 136–145.
2. Shannon C. A mathematical theory of communication // *Bell System Technical Journal*. – 1948. – Vol. 27. – P. 379–423.

УДК 004.056.55:004.056.53

*Соловей В. А., молодший наук. співробітник**Житомирський військовий інститут ім. С. П. Корольова***ЕВОЛЮЦІЙНІ ІМПЛІЦИТНІ КАНАЛИ ПЕРЕДАЧІ
ІНФОРМАЦІЇ У КООРДИНАТНІЙ КРИПТОГРАФІЇ**

У роботі розглядається новий клас каналів передачі інформації, що виникає у межах криптографічної парадигми координатної криптографії (КК) – еволюційні імпліцитні канали. На відміну від традиційних криптографічних систем, у яких передача інформації здійснюється виключно через явно визначені бітові структури шифротексту, у КК можлива передача додаткової інформації через структурні властивості відхилень [1], що виникають у процесі верифікації кожного шифрокоду – логічної безпарольної автентифікації (LPA). Такі канали не є окремими протоколами поверх криптосистеми, а виникають як природна властивість внутрішньої математично-геометричної структури координатної криптографії. Формування шифрокоду описується відображенням $c_t = F(m_t, n_t, \mathcal{E}_t)$, де $\mathcal{E}_t$ – операційний стан системи у фазі t , m_t – компонент відкритого тексту, n_t – вектор імітаційних даних, F – координатне відображення формування шифрокоду. Кожна подія формування шифрокоду впливає на фазову еволюцію системи: $\mathcal{E}_{t+1} = \Psi(S_t, c_t)$, де Ψ – фазово-залежне стохастичне відображення. Отриманий шифрокод підлягає процедурі LPA, оскільки тільки верифікована подія впливає на еволюцію системи $\mathcal{E}_{t+1}$. Координатний простір GIS_t є компонентом $\mathcal{E}_t$, формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset$, $GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри. Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, c_t приймається тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0, 1\}$, $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю. Однак у випадку результату $V_{\mathcal{E}_t}(c_i) = 0 \rightarrow \text{reject}$ LPA не одразу відхиляє шифрокод, а формує структуру відхилення $E(c_t)$, що відображає відмінність координатних параметрів від очікуваних. У традиційних криптографічних системах подібне відхилення інтерпретується як модифіковане повідомлення. Проте у КК множина відхилень може мати структуровану форму, формально: $E(c_t) = \{e_1, e_2, \dots, e_n\}$, де e_k – відхилення координатного параметра k -го слова від очікуваного значення. Якщо структура відхилень відповідає певному еволюційному правилу R_t , то така подія інтерпретується як імпліцитний сигнал $M_t^{(imp)}$ відповідно до фазового правила інтерпретації відхилень $IC_t: E(c_t) \in R_t \Rightarrow \text{implicit}_{message}, IC_t: E(c_t) \rightarrow M_t^{(imp)}$. Оскільки $|\mathcal{A}_t| \ll |\mathcal{P}_t|$, у моделі КК виникає неявний канал,

індукований структурою відхилень при відхиленні шифрокоду: $V_{\varepsilon_t}(c_t) = 0 \Rightarrow E(c_t) = \{e_1, \dots, e_n\}$.

Оскільки $R_t = f(H_t)$, де H_t – подієва пам'ять обмеженої фазової глибини, стан якої змінюється після кожної події $V_{\varepsilon_t}(c_t) = 1$, то імпліцитний канал (ІК) не має сталої параметризації та не є бітовим [1]. Таким чином правила інтерпретації структурованих відхилень не задаються наперед, а еволюціонують разом із системою. Унаслідок цього формується ІК передачі інформації, як математичний додатковий шар комунікації: $C_{total} = C_{pr} \cup C_{im}$, де C_{pr} – основний канал передачі відкритого тексту, а C_{im} – додатковий ІК передачі інформації через структуровані відхилення. ІК не впливає на пропускну здатність основного каналу – інформація передається через попередньо сформовані R_t , тому ІК не потребує додаткових бітів у шифрокоді. Загальна інформаційна місткість системи подається як [2]:

$$Capacity(C_{total}) = Capacity(C_{pr}) + Capacity(C_{im}).$$

Ймовірність випадкового виникнення структурованої помилки у модифікованому шифрокоді, що відповідає поточному правилу R_t , є надзвичайно малою та задається наперед параметрами безпеки ІК. Якщо припустити, що координатні параметри мають множину можливих значень N , то ймовірність випадкового виконання складного правила оцінюється як $Pr(E(c_t) \in R_t) \approx N^{-k}$, де k – кількість координатних елементів, що беруть участь у правилі. У практичних системах це значення прямує до нуля, тому ІК дозволяють реалізувати додатковий рівень передачі інформації, який не порушує властивостей метаданонейтральності основного каналу та не змінює структуру криптографічного процесу. ІК передають інформацію через структурні властивості координатних відхилень шифрокоду. Такі канали можуть бути визначені як еволюційні імпліцитні канали – новий клас каналів у теорії інформації: Ch_{elc} (evolutionary implicit channels). Інформація не передається через безпосередні бітові значення шифрокоду, тому:

$$I_{struct} = I(E(c_t); R_t), I_{total} = I(C_{primary}) + I(E(c_t); R_t).$$

Декодування: $Decode(c_t) = (D_{primary}(c_t), D_{implicit}(E(c_t)))$, де $D_{primary}$ – декодування основного повідомлення, а $D_{implicit}$ – інтерпретація структури відхилень координатних параметрів. Таким чином один шифрокод може одночасно переносити два незалежні інформаційні повідомлення. Якщо c_t містить n координатних слів, а кожне слово має k допустимих варіантів відхилення, то кількість можливих структур сигналу становить $|E(c_t)| = k^n$. Таким чином простір потенційних каналів Ch_{elc} у координатній криптографії має експоненційну потужність.

Список використаних джерел

1. Simmons G. J. The prisoners' problem and the subliminal channel // *CRYPTO*. – 1983. – P. 51–67.
2. Cover T. M., Thomas J. A. Elements of Information Theory. – Wiley, 2006.

УДК 004.056.55:004.056.53

*Соловей В. А., молодший наук. співробітник**Житомирський військовий інститут ім. С. П. Корольова***ФАЗОВО-ЕВОЛЮЦІЙНІ КРИПТОГРАФІЧНІ СИСТЕМИ:
ФОРМАЛЬНА БЕЗКЛЮЧОВА МОДЕЛЬ**

У роботі розглядається формальна модель нового класу криптографічних систем – фазово-еволюційних криптографічних систем (ФЕКС), що функціонують без використання криптографічних ключів. На відміну від традиційних криптографічних моделей, де безпека визначається секретністю або складністю відновлення ключа, у ФЕКС безпека системи визначається еволюцією її внутрішнього операційного стану [1]. Така модель є фундаментальною для координатної криптографії та інших систем, у яких криптографічні властивості визначаються динамікою внутрішніх процесів системи. У класичній криптографії формування шифротексту описується відображенням виду $c = \text{Enc}(m, k)$, де m – відкрите повідомлення, а k – криптографічний ключ. Формально у ФЕКС процес формування шифрокоду можна подати як $c_t = F(m_t, n_t, \mathcal{E}_t)$, $\mathcal{E}_t$ – операційний стан системи у фазі t , m_t – компонент відкритого тексту, n_t – вектор імітаційних даних $\mathcal{NA}$, F – відображення формування шифрокоду. $\mathcal{NA}$ – це внутрішній ентропійний вектор, що використовується у випадках відсутності відкритого тексту, для маскування структури повідомлення: $n_t \sim \mathcal{D}_{\mathcal{NA}}$, де $\mathcal{D}_{\mathcal{NA}}$ – розподіл ентропійних векторів імітаційних даних [2]. Формально ФЕКС ($\mathcal{C}_{\mathcal{PE}}$) можна визначити як клас систем:

$$\mathcal{C}_{\mathcal{PE}} = \{\text{system} \mid c_t = F(m_t, n_t, \mathcal{E}_t), \mathcal{E}_{t+1} = \Psi(\mathcal{E}_t, c_t), k = \emptyset\}.$$

Це означає, що криптографічне перетворення визначається еволюцією операційного стану системи. Симетрія $\mathcal{E}_t$ та стохастична симетрична еволюція $\mathcal{E}_{t+n}$ комунікуючих систем є необхідною умовою для ФЕКС. Симетрія виникає як властивість еволюції операційного стану систем. Механізмом синхронізації комунікуючих систем є логічна безпарольна автентифікація (LPA) шифрокоду. Формально процедура описується як $V_{\mathcal{E}_t}(c_i) \in \{0,1\}$, де результат 1 означає, що структура шифрокоду узгоджується з поточним операційним станом системи. На відміну від класичних систем автентифікації, не використовує ключі, паролі або цифрові підписи. Якщо дві системи мають симетричні операційні стани, то шифрокод, сформований однією системою, може бути коректно верифікований іншою: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{\mathcal{E}_t}(c) = 1, \forall t$.

Симетрія операційних станів підтримується через послідовну фазову еволюцію систем, та визначається однаковими верифікованими подіями:

$$\mathcal{E}_{t+1}(A) = \Psi(\mathcal{E}_t(A), c_t), \mathcal{E}_{t+1}(B) = \Psi(\mathcal{E}_t(B), c_t).$$

Синхронізація систем не потребує використання криптографічних ключів - роль ключа виконує симетричний операційний стан систем.

Операційний стан $\mathcal{E}_t$ є комплексним параметром системи та включає фазові параметри еволюції, подієву пам'ять обмеженої фазової глибини

H_t , а також координатне представлення криптографічних об'єктів. Кожна подія формування або реконструкції за умови верифікації шифрокоду змінює подальшу траєкторію розвитку системи. Фундаментальною властивістю ФЕКС є унікальність фаз еволюції. Якщо позначити фазовий стан системи через Φ_t , то для будь-яких різних моментів часу виконується $\forall i \neq j: \Phi_i \neq \Phi_j$. Це означає, що операційний стан системи не може бути повторений. Наслідком унікальності фаз є властивість фазової антиколізійності шифрокодів. Для будь-яких двох подій виконується $m_i = m_j \Rightarrow c_i \neq c_j$ та $c_i = c_j \Rightarrow m_i \neq m_j$. Таким чином однакові повідомлення не можуть породжувати однакові шифрокоди, але однакові шифрокоди – як правило сформовані різними текстами, не залежно від їх фазової належності. Саме тому автентифікація автора шифрокоду через механізм ЛБА – виникає як логічний наслідок симетрії фазової еволюції систем, а не як результат використання криптографічних ключів, паролів чи будь-яких інших цифрових ідентифікуючих даних.

Оскільки еволюція операційного стану залежить від історії подій у декількох попередніх фазах, траєкторія еволюції має немарковський характер [1]. Поточний стан системи визначається не лише попереднім станом, а всією історією подій, накопичених у подієвій пам'яті H_t яка не збільшується за розміром, а змінює свій стан. Кожна верифікована подія фази t є безумовною, змінює стан H_t невідкладно, але не впливає на її розмір. Умовні події – навпаки, накопичується у H_t , змінюють її стан тільки після виконання умови, що пов'язана із ймовірнісним очікуванням геометричних параметрів $\mathcal{E}_{t+n}$, де n – невідома: $\exists n \in \mathbb{N}$: умова($\mathcal{E}_{t+n}$).

Кількість попередніх фаз $d_t = |\varphi_i: i < t|$, умови яких зберігаються у H_t обмежена її фазовою глибиною у поточній фазі та може бути змінена. Формально це можна подати як $\mathcal{E}_t = f(\mathcal{E}_{t-1}, H_t)$. Отже поведінка системи визначається накопиченою історією криптографічних подій.

Формально безпеку можна подати як функцію $\mathcal{E}_t$: $Security = f(\mathcal{E}_t) \Rightarrow Security \notin KeySpace$. Криптографічна стійкість є наслідком динаміки внутрішніх процесів та симетричної еволюції операційного стану систем. Конфіденційність, автентифікація та цілісність інформації виникають як внутрішні властивості системи, а не як результат використання зовнішніх криптографічних інфраструктур: $Enc(m, key), Enc(m, \mathcal{E}_t) \Rightarrow key \equiv \mathcal{E}_t$. Дешифрування: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow Dec(F(m_t, \mathcal{E}_t)) = m_t, \mathcal{E}_t \notin KeySpace$.

Стохастична немарковська еволюція $\mathcal{E}_t$ виконує роль динамічного криптографічного параметра, тому: $Security \neq Key$, оскільки ключ формує тільки один операційний стан із всієї множини можливих.

Список використаних джерел

1. Bellare M., Rogaway P. Introduction to modern cryptography // UCSD Notes. – 2005.
2. Cover T. M., Thomas J. A. Elements of Information Theory. – Wiley, 2006.

КООРДИНАТНЕ КОДУВАННЯ У ДИНАМІЧНО ЕВОЛЮЦІОНУЮЧИХ КРИПТОГРАФІЧНИХ ПРОСТОРАХ

У роботі розглядається концепція координатного кодування (Coordinate coding, CC) у динамічно еволюціонуючих криптографічних просторах $\mathcal{E}_t$. CC інтерпретує криптографічний процес як навігацію у внутрішньому координатному просторі GIS_t , який є компонентом $\mathcal{E}_t$. У такій моделі шифрокод є відображенням параметризованих координат деяких обраних об'єктів [1] g_i із визначеної множини. GIS_t формується двома групами об'єктів: активними $\mathcal{A}$ та пасивними $\mathcal{P}$, $\mathcal{A} \cap \mathcal{P} = \emptyset$, $|\mathcal{A}| \ll |\mathcal{P}|$. Активні об'єкти $a_i \in \mathcal{A}$ — асоціюються із певним значенням слова відкритого тексту, тоді як пасивні об'єкти $p_i \in \mathcal{P}$ — ні. Всі об'єкти $g_i \in \mathcal{A} \cup \mathcal{P}$ динамічно переміщуються змінюючи свої координатні параметри. Простір не є статичним: він формується та трансформується [2], утворюючи послідовність унікальних конфігурацій $GIS_t = \{g_1^{(t)}, g_2^{(t)}, \dots, g_N^{(t)}\}$, $N = \text{const}$, $i \neq j$: $GIS_i \neq GIS_j$, $\forall t$: $|GIS_t| = N$, тому $\exists k$: $g_k^{(t+1)} \neq g_k^{(t)}$. Другим компонентом $\mathcal{E}_t$ є Логічний Тунель Часу (LTT) — це локальний контекст криптографічної обробки, що визначає правила асоціації між байтами повідомлення та об'єктами GIS, координатну систему відліку та допустимі операції векторного кодування. Функціональним стан системи $LTT_t := \langle GIS_t, R_t \rangle$, де R_t — множина правил, що визначає логічну структуру та допустимі операції у фазі t , тому: $LTT_{t+1} \neq LTT_t$. Загалом: $\mathcal{E}_t = (GIS_t, LTT_t)$ у якому кожна криптографічна подія змінює подальшу траєкторію розвитку системи.

CC реалізується трьома методами векторно-геометричного кодування (VC). Розглянемо три тригера криптографічних подій: w_1, w_2, w_3 . Нехай семантика цих слів: $\mathcal{M}(w_1) = A$, $\mathcal{M}(w_2) = B$ та $\mathcal{M}(w_3) = D$. Кожне слово має своє правило асоціації $\varphi_t^1(\mathcal{M}(w_1)) = a_t^1$, $a_t^1 = A'$, $\varphi_t^2(\mathcal{M}(w_2)) = a_t^2$, $a_t^2 = B'$, $\varphi_t^3(\mathcal{M}(w_3)) = a_t^3$, $a_t^3 = D'$, тобто $A \leftrightarrow A'$, $B \leftrightarrow B'$, $D \leftrightarrow D'$, та координати: $A' = (x_A, y_A)$, $B' = (x_B, y_B)$, $D' = (x_D, y_D)$. Перший метод (VC_1) базується на прямому кодуванні положення об'єкта A' у GIS_t . Для цього задається початок координат O та нульова вісь, після чого визначається вектор $\overrightarrow{OA'}$. Код VC_1 для слова A визначається параметрами цього вектора [2]: $c_{A'} = (|\overrightarrow{OA'}|, \theta_{OA'})$, де $\theta_{OA'}$ — кут нахилу вектора $\overrightarrow{OA'}$. Шифрокод $c_{A'}$ формується як бінарне представлення параметризованих координат вектора $\overrightarrow{OA'}$. Реконструкція інструкції $c_{A'}$ у симетричному операційному стані однозначно знаходить $A' \Rightarrow \varphi_t^1(\mathcal{M}(w_1)) \Rightarrow A$. Другий метод (VC_2) базується на відносному положенні об'єкта B' відносно A' . Визначається вектор $\overrightarrow{A'B'}$, а відповідний код має вигляд як: $c_{B'} =$

$(|A'B'|, \theta_{A'B'}^B)$. Метод VC_2 застосовується лише за умови верифікації попередньої події, пов'язаної з формуванням $c_{A'}$. Третій метод (VC_3) використовує визначений у фазі t базовий вектор $\overline{XY}$. Код слова D визначається як відношення параметрів вектора $\overline{B'D'}$, до параметрів базового вектора $\overline{XY}$: $c_{D'} = \left(\frac{|B'D'|}{|\overline{XY}|}, \frac{\theta_{A'B'}^B}{\theta_{XY}^D} \right)$. Наявність базового вектора $\overline{XY}$ та верифікація події, пов'язаної з $c_{B'}$, є необхідними умовами застосування методу VC_3 . У результаті формується послідовна залежність криптографічних подій (ефект храпового механізму), незалежно від джерела цих подій $w_i \in UA_t \cup NA_t$:

$$c_t = \mathcal{F}_t \left(VC_3 \left(VC_2 \left(VC_1(\mathcal{M}(w_1)), \mathcal{M}(w_2) \right), \mathcal{M}(w_3) \right), GIS_t, LTT_t \right),$$

де $\mathcal{F}_t$ – відображення формування шифрокоду як бінарного представлення параметрів векторної конфігурації. Після кожної операції кодування конфігурація змінюється: $GIS_{t+1} = \Psi(GIS_t, LTT_t, c_t) \Rightarrow LTT_{t+1} = \Omega(GIS_{t+1}, LTT_t, c_t)$, $\varepsilon_i \neq \varepsilon_j \Rightarrow c_i \neq c_j$. Для коректної комунікації операційні стани систем повинні залишатися симетричними. Тільки верифіковані події c_i опосередковано впливають на траєкторію еволюції системи. Верифікація шифрокоду описується: $V_{\varepsilon_t}(c_t) \in \{0,1\}$. Успішна верифікація: $V_{\varepsilon_t}(c_t) = 1 \Leftrightarrow g_i \in \mathcal{A}_t$, $G(c_t) \subset \mathcal{A}_t$, де $G(c_t) = \{g_{i_1}, \dots, g_{i_k}\}$ – підмножина об'єктів індукована c_t . Верифіковані події є тотожними, траєкторія еволюції симетрична: $\forall t \in N : \mathcal{E}_t^{Alice} = \mathcal{E}_t^{Bob}$.

Таким чином безпека визначається динамікою внутрішнього стану системи, а не секретністю чи складністю криптографічних ключів: $Security = f(GIS_t, LTT_t)$. Тому конфіденційність виникає як наслідок унікальності GIS; автентифікація – як властивість симетричної узгодженості LTT; цілісність – як результат координатної залежності $w_i(g_i)$ криптографічних подій: $w_{i+1} = VC_{i+1}(w_i)$ та $V_{\varepsilon_t}(c_t) = 1$.

У такій моделі криптографічна стійкість виникає як властивість еволюції системи, а не як наслідок секретності ключового простору: $Security \not\subseteq KeySpace$, $KeySpace = \emptyset$. Отже CC слід розглядати не як окремий алгоритм, а як криптографічну модель, у якій криптографічні властивості виникають як наслідок еволюції внутрішнього координатного простору системи. Процес шифрування не зводиться до фіксованого відображення, а визначається динамікою стану, що формує онтологічно замкнений та метаданонейтральний канал зв'язку: $Enc(m, k) \neq F(m, GIS_t, LTT_t)$. Шифрокод не має глобального значення.

Його інтерпретація можлива лише у власному фазовому просторі:

$$Decode_{\varepsilon}(c_t) = g_t \Leftrightarrow \varepsilon = \varepsilon_t.$$

Список використаних джерел

1. Conway J. H., Sloane N. J. A. Sphere Packings, Lattices and Groups. – Springer, 1999.
2. Cover T. M., Thomas J. A. Elements of Information Theory. – Wiley, 2006.

УДК 004.056.55:004.056.53

*Соловей В. А., молодший наук. співробітник**Житомирський військовий інститут ім. С. П. Корольова***ЛОГІЧНА АВТЕНТИФІКАЦІЯ БЕЗ ПАРОЛІВ**

У цій роботі розглядається механізм логічної автентифікації без використання паролів (LPA) у рамках формальної моделі координатної криптографії (КК). Класичні системи автентифікації базуються на секретних ключах, цифрових підписах, паролях [1], ідентифікованих цифрових відбитках тощо. Запропонований підхід верифікує шифрокод за його структурою відносно очікуваної на цей подієвий момент. Зміст відкритого тексту, що пов'язаний із отриманим шифрокодом (c_t), не має значення для функціонування цього механізму. LPA має логічну природу походження, що пов'язана із опосередкованим механізмом встановлення факту симетрії системи отримувача відносно стану системи автора шифрокоду. Операційний стан визначається як $\mathcal{E}_t = (GIS_t, LTT_t)$, де GIS_t – внутрішній координатний простір, що складається з множини динамічних об'єктів g_i із унікальними параметризованими координатами, а LTT_t – логічний тунель часу, який задає правила асоціації, допустимі операції кодування та функціональний контекст у фазі t . Шифрокод формується параметризованими координатами g_i , які визначаються бієктивними правилами асоціації φ_t^i , для кожного слова, між семантикою слова та одним g_i . Нехай $\mathcal{M}$ – семантика слова відкритого тексту w_n , де $n \in N_t$, ініціює процес формування c_t . Кількість подій у фазі t дорівнює кількості слів N_t . Значимо: $\forall w_i, w_j \in N_t, i \neq j$:

$$GIS_t^{(w_i, g_i)} \neq GIS_t^{(w_j, g_j)} \wedge LTT_t^{(\varphi_t^i, \mathcal{M}(w_i))} \neq LTT_t^{(\varphi_t^j, \mathcal{M}(w_j))}, \quad \text{тобто}$$

конфігурації є унікальними для різних слів і відповідних їм семантик.

GIS_t формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset$, $GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри.

Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – підмножина об'єктів координатного простору, індукована c_t , яка відповідає вибору тільки активних об'єктів $a_i \in \mathcal{A}_t$, $G_t^{(c_t)} \subset \mathcal{A}_t$. Тоді шифрокод c_t приймається тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0, 1\}$, $V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція верифікації, а значення 1 відповідає прийняттю. Нехай W^1 – множина можливих значень першого слова тексту довжини m біт, причому $|\mathcal{A}_t^1| = |W^1| = 2^m$, де $\mathcal{A}_t^1 \subset \mathcal{A}_t$. Правило асоціації: $\varphi_t^1: W^1 \rightarrow \mathcal{A}_t^1$ кожному $\mathcal{M}(w_1) \in W^1$ ставить у відповідність єдиний об'єкт $a_i \in \mathcal{A}_t^1$. Тоді для слова W^2 визначається відображення $\varphi_t^2: W^2 \rightarrow \mathcal{A}_t^2$. Кількість елементів a_i^1 у множині $\mathcal{A}_t^1$ дорівнює 2^m . Після першої події усі об'єкти множини $\mathcal{A}_t^1$ втрачають поточне правило асоціації φ_t^1 , змінюють свої координатні параметри стохастичним чином та отримують нове правило асоціації, яке буде

використовуватись у наступній фазі ϕ_{t+1}^i . Тому виконується: $a_i \in \mathcal{A}_t^i \Rightarrow a_i \notin \mathcal{A}_t^j \Rightarrow a_i \notin \mathcal{A}_{t+n}^j, i \neq j$. За умови сталості параметра m виконується: $|\mathcal{A}_t^1| = |\mathcal{A}_t^2| = \dots = |\mathcal{A}_t^i| = 2^m$, для всіх фаз та подій системи. Успішна верифікація шифрокоду забезпечує збереження симетрії у подальшій фазовій еволюції систем:

$$V_{\mathcal{E}_t}(c_t) = 1 \Rightarrow (G_t^{(c_t)} \subset \mathcal{A}_t) \Rightarrow \mathcal{E}_{t+1}^{Alice} = \mathcal{E}_{t+1}^{Bob}, \quad \forall t \in N.$$

Ймовірність P_{err} того, що модифікований шифрокод успішно пройде верифікацію визначається $p_t = \frac{|\mathcal{A}_t|}{|GIS_t|} \Rightarrow P_{err} = \left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)^k$, де k – кількість слів у координатних подіях реконструкції $G_t(c_t) = \{g_1, g_2, \dots, g_k\}$. Якщо кожне слово додає нову координатну подію перевірки, то ймовірність помилкової автентифікації зменшується експоненційно. Інформаційна характеристика LPA – ентропія автентифікації $H_{LA} = -\log P_{err}$, тому: $H_{LA} = k \log \left(\frac{|GIS_t|}{|\mathcal{A}_t|}\right)$. Це означає, що ентропія LPA лінійно зростає зі збільшенням кількості координатних подій перевірки.

Після кожної операції кодування конфігурація змінюється:

$$GIS_{t+1} = \Psi(GIS_t, LTT_t, c_t) \Rightarrow LTT_{t+1} = \Omega(GIS_{t+1}, LTT_t, c_t), \\ \mathcal{E}_{t+1} = (GIS_{t+1}, LTT_{t+1}), \mathcal{E}_i \neq \mathcal{E}_j \Rightarrow c_i \neq c_j.$$

Таким чином ЛБА виконує роль подієвого механізму синхронізації фазової еволюції $\mathcal{E}_t$, без використання секретних ключів або паролів.

Якщо задано допустиму ймовірність помилкової автентифікації δ , то: $P_{err} = \delta, \left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)^k = \delta, \frac{|\mathcal{A}_t|}{|GIS_t|} = \delta^{1/k}$, розмір простору: $|GIS_t| = \frac{|\mathcal{A}_t|}{\delta^{1/k}}$.

Розмір $|GIS_t|$ повинен бути таким, щоб забезпечити задану стійкість.

Якщо шифрокод має k слів та m бітові слова, то $|\mathcal{A}_t| = k 2^m$, тоді:

$$|GIS_t| = \frac{k 2^m}{\delta^{1/k}}. \text{ Але при заданому } |GIS_t| \text{ маємо: } \left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)^k \rightarrow 0 \text{ (} k \rightarrow \infty \text{).}$$

Якщо треба розрахувати k при заданій структурі GIS_t та заданому δ , тоді: $k \geq \frac{\log \delta}{\log \left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)}$ – формула мінімальної довжини шифрокоду.

ЛБА має логічну природу $V_{\mathcal{E}_t}(c_t) = f(GIS_t, LTT_t, c_t)$ залежить виключно від криптографічного стану $\mathcal{E}_t$ та не спирається на семантику відкритого тексту $\mathcal{M}$: $V_{\mathcal{E}_t}(c_t) \not\equiv f(\mathcal{M}), c_t \rightarrow G_t(c_t) \rightarrow V_{\mathcal{E}_t}(c_t) \rightarrow \mathcal{E}_{t+1}$.

ЛБА має історично-залежний характер, тому еволюція $\mathcal{E}_t$ має немарковську властивість. Нехай Φ оператор формування LTT , тоді:

$$LTT_t = \Phi(c_{t-1}, c_{t-2}, \dots) \rightarrow V_{\mathcal{E}_t}(c_t) = f(GIS_t, \Phi(c_{t-1}, c_{t-2}, \dots), c_t), \\ \Rightarrow V_{\mathcal{E}_t}(c_t) \Rightarrow \mathcal{E}_{t+1}. \text{ Висновок: ЛБА є подієвою системою з пам'яттю.}$$

Список використаних джерел

1. Bellare M., Pointcheval D., Rogaway P. Authenticated key exchange secure against dictionary attacks // EUROCRYPT. – 2000.
2. Shannon C. A mathematical theory of communication // Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423.

УДК 004.056.55:004.056.53

*Соловей В. А., молодший наук. співробітник**Житомирський військовий інститут ім. С. П. Корольова***ПАРАДИГМА ФОРМУВАННЯ ЕКСПОНЕНЦІЙНО СТИЙКИХ ШИФРОКОДІВ У КООРДИНАТНІЙ КРИПТОГРАФІЇ**

У роботі розглядається парадигма формування експоненційно стійких шифрокодів (c) у межах Координатної Криптографічної моделі (КК). У класичних криптографічних системах шифротекст є результатом криптографічного перетворення відкритого тексту (w) за допомогою алгоритму та секретного ключа. Шифрокод c_t у КК не містить криптографічно перетвореного тексту, а виступає навігаційною інструкцією, реконструкція якої дозволяє знайти об'єкт g_i у віртуальному просторі. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події – c_t не містить. Знайдений об'єкт належить до визначеної множини, яка за кількістю дорівнює повному алфавіту одного слова тексту. Кількість біт w (алфавіт) система визначає сама. Кожне w , за номером $w_1, w_2, \dots, w_n$ має свою окрему асоційовану множину та унікальне правило асоціації. Якщо хоч одне w_n було відновлено за допомогою одного g_i визначеної множини – правило асоціації нівелюється та всі g_i цієї множини змінюють свої координати.

Криптографічний стан системи визначається як $\mathcal{E}_t = (GIS_t, LTT_t)$, де GIS_t – геометричний координатний стан внутрішнього простору системи у фазі t , а LTT_t – логічний тунель часу, що визначає функціональний контекст системи у цій фазі. $\mathcal{E}_t$ визначає правила формування та реконструкції шифрокоду: $c_t = F_{\mathcal{E}_t}(w_t)$, де $F_{\mathcal{E}_t}$ – унікальна композиція перетворень, що визначається унікальним поточним станом системи. Реконструкція w_t відбувається у два етапи: $c_t \rightarrow G_t(c_t) \rightarrow w_t$, де $G_t(c_t)$ – множина координатних подій реконструкції g_i внутрішнього простору. GIS_t складається з активної та пасивної множини об'єктів: $A_t \cap P_t = \emptyset$,

$GIS_t = A_t \cup P_t$, принципова умова: $|A_t| \ll |P_t|$. Для слова довжини m біт множина можливих значень: $|W| = 2^m$, тому для кожного слова, незалежно від його значення система резервує $A_t^i \subset A_t : |A_t^i| = 2^m$. Правило асоціації бієктивне: $\phi_t^i: W \rightarrow A_t^i$, активний об'єкт a_i має суперпозиційне координатне представлення: $\Sigma_t(o_t) = \{v_t^{(1)}, v_t^{(2)}, \dots, v_t^{(r)}\}$. Суперпозиція координат є властивістю простору, а не повідомлення. Розв'язання суперпозиції визначається відображенням $\psi_t: \Sigma_t(o_t) \rightarrow \{v_t^*\}$.

Координатні параметри v_t^* використовуються для формування бінарного представлення події. Надалі виконується композиція криптографічних перетворень: перестановки, дифузія, XOR-операції тощо. Реконструкція шифрокоду, така, що всі k знайдені об'єкти належать тільки до A_t – та будуть вірно відновлені всі слова тексту – можлива тільки за умови симетрії $\mathcal{E}_t$ у поточній фазі та симетричної

еволюції: $\mathcal{E}_{t+1}^{Alice} = \mathcal{E}_{t+1}^{Bob}$. Шифрокод – це подія, яка не має ніякої семантики окрім навігаційної.

Симетричну еволюцію $\mathcal{E}_t$ забезпечує механізм логічної безпарольної автентифікації (LPA), який через логічний висновок встановлює систему автора – через механізм верифікації отриманого від нього шифрокоду.

Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом, який верифікується як «свій» (інакше – «чужий») тоді і тільки тоді, коли виконується предикат верифікації:

$$V_{\mathcal{E}_t}(c_t) \in \{0,1\}, \quad V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t,$$

де $V_{\mathcal{E}_t}$ – функція LPA, а значення 1 відповідає прийняттю («свій»). LPA не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. c_t може бути верифікований лише системами з симетричним операційним станом: $\mathcal{E}_t(A) = \mathcal{E}_t(B) \Rightarrow V_{\mathcal{E}_t}(c) = 1$, *accept*, що дозволяє зробити логічний висновок про автора шифрокоду.

Визначимо простір всіх можливих операційних криптографічних станів системи: $\mathcal{S} = \{(GIS_t, LTT_t)\}$. Для будь-якого W та будь-якого c_t існує криптографічний стан системи, у якому цей шифрокод може бути згенерований: $\forall w \in W, \forall c \in C \exists \mathcal{E}_t: c = F_{\mathcal{E}_t}(w)$.

У теорії інформації абсолютна криптостійкість досягається у шифрі C одноразового блокнота OTP, визначається: $I(W; C) = 0$.

Якщо $LTT_t = \Phi_t(c_{t-1}, c_{t-2}, \dots) \Rightarrow |LTT| \sim 2^t$, тоді $|S| = |GIS| \cdot |LTT|$ та $|S| \approx |GIS_t|! \cdot |C|^t$ потужність простору значно перевищує простір ключів OTP: $|K_{OTP}| = 2^{|W|} \Rightarrow |S| \gg |K_{OTP}|$.

Оскільки шифрокод C , сформований в межах моделі координатної криптографії - не містить семантики відкритого тексту W , тому взаємна інформація $I(W; C) = 0$ – для зовнішнього спостерігача.

Простір ключів OTP є частковим випадком простору криптографічних станів системи $|S| \gg |K_{OTP}| \rightarrow \boxed{K_{OTP} \subset S}$.

У Координатній криптографії абсолютна криптостійкість виникає як властивість простору операційних криптографічних станів системи. Цю властивість можна інтерпретувати як стан-підсилену абсолютну секретність (state-amplified secrecy). Надійність систем безпеки, що сформовані у межах моделі КК полягає у тому, що у Shannon-моделі: $\forall m, c \exists k$ – потрібен ключ, цій системі: $\forall m, c \exists \mathcal{E}_t$ – ключ не потрібен.

Таким чином КК формує новий клас шифрокодів у яких криптографічна стійкість виникає як властивість немарковської стохастичної еволюції криптографічного стану системи шифрування.

Список використаних джерел

1. Bellare M., Pointcheval D., Rogaway P. Authenticated key exchange secure against dictionary attacks // EUROCRYPT. – 2000.
2. Shannon C. A mathematical theory of communication // Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423.

УДК 004.7

*Дячук О.Ю., ст. викладач
Колощук М.С., ст. викладач*

Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ АЛГОРИТМУ TurboQuant ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ МОНІТОРИНГУ МЕРЕЖЕВИХ ПОДІЙ

У сучасних умовах розвитку інформаційних технологій забезпечення кібербезпеки є одним із ключових завдань функціонування інформаційних систем. Зростання обсягів мережевого трафіку, кількості підключених пристроїв та складності кіберзагроз зумовлює необхідність використання ефективних методів моніторингу та аналізу мережевих подій у режимі реального часу.

Традиційні підходи до аналізу подій безпеки часто характеризуються високими витратами обчислювальних ресурсів, значними затримками обробки та обмеженими можливостями виявлення складних аномалій, що знижує загальну ефективність систем кіберзахисту. У зв'язку з цим актуальним є пошук нових алгоритмічних рішень, здатних забезпечити масштабованість та швидкодію систем моніторингу [1].

Одним із перспективних підходів є використання алгоритму TurboQuant – сучасного методу векторної квантизації, запропонованого дослідниками Google для підвищення ефективності обробки високовимірних даних [1], [2].

Алгоритм TurboQuant забезпечує значне зменшення обсягу пам'яті, необхідної для збереження та обробки даних, зокрема у структурах типу KV-cache, що широко застосовуються у системах аналізу поточкових даних. За рахунок ефективної компресії векторних представлень досягається зменшення використання пам'яті до кількох разів та суттєве прискорення обробки інформації без втрати точності [1], [3].

З технічної точки зору, алгоритм поєднує підходи PolarQuant та Quantized Johnson-Lindenstrauss, що дозволяє мінімізувати похибки квантизації та забезпечити високу якість відновлення даних [2]. Важливою особливістю є те, що TurboQuant наближається до інформаційно-теоретичних меж стиснення, забезпечуючи мінімальні спотворення при максимальному рівні компресії [2].

У контексті систем моніторингу мережевих подій застосування алгоритму TurboQuant забезпечує підвищення ефективності обробки даних, що в свою чергу дозволяє виділити такі основні переваги застосування алгоритму:

- зменшити навантаження на оперативну пам'ять при обробці журналів подій та мережевого трафіку;
- підвищити швидкість аналізу поточкових даних;
- забезпечити масштабованість систем моніторингу;
- підвищити ефективність виявлення аномалій у мережі.

Інтеграція алгоритму у системи класу SIEM та SOAR відкриває можливості для автоматизації процесів аналізу та реагування на інциденти інформаційної безпеки.

У результаті теоретичного аналізу та узагальнення сучасних досліджень встановлено, що застосування алгоритму TurboQuant у системах моніторингу мережевих подій дозволяє:

- зменшити використання обчислювальних ресурсів;
- підвищити швидкість обробки подій;
- знизити затримки у виявленні інцидентів;
- покращити точність виявлення аномалій;
- підвищити рівень автоматизації процесів кіберзахисту.

Таким чином, використання алгоритму TurboQuant дозволяє суттєво підвищити ефективність систем моніторингу мережевих подій за рахунок оптимізації використання обчислювальних ресурсів та прискорення обробки даних.

Запропонований підхід може бути використаний у корпоративних мережах, центрах обробки даних та хмарних інфраструктурах, а також інтегрований у сучасні системи управління інформаційною безпекою.

Окремо слід зазначити, що впровадження подібних алгоритмів має вплив не лише на програмні системи, а й на розвиток апаратного забезпечення та ринку мікропроцесорних технологій [4].

Перспективи подальших досліджень полягають у експериментальній оцінці ефективності алгоритму та його адаптації до різних типів мережевих середовищ.

Список використаних джерел

1. Google Research. TurboQuant: Redefining AI efficiency with extreme compression. 2026. URL: <https://research.google/blog/turboquant-redefining-ai-efficiency-with-extreme-compression/>
2. Zandieh A., Mirrokni V. et al. TurboQuant: Online Vector Quantization with Near-optimal Distortion Rate. arXiv, 2025. URL: <https://arxiv.org/abs/2504.19874>
3. Google TurboQuant та вплив на ринок. URL: <https://mezha.ua/news/google-turboquant-309754/>
4. TurboQuant від Google: вплив на ринок мікросхем. URL: <https://mind.ua/news/20302857-turboquant-vid-google-yak-nova-tehnologiya-shi-sprovokuvala-rozkol-na-rinku-mikroshem>

УДК 004.738.5

*Пятаков О.О., здобувач
Колощук М.С., ст. викладач*

Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОЖЛИВОСТЕЙ GITHUB CODEQL ТА OWASP ZAP В УМОВАХ DEVSECOPS-КОНВЕЄРА

Сучасні веб-додатки постійно зіштовхуються зі зростаючою кількістю кіберзагроз. Ускладнення архітектури програмного забезпечення вимагає переходу до концепції DevSecOps та інтеграції перевірок безпеки на ранніх етапах життєвого циклу розробки (Shift-Left). Існуючі методи тестування, такі як статичний аналіз (SAST) та динамічне сканування (DAST), мають свої переваги та суттєві обмеження при ізольованому використанні: SAST часто генерує хибно-позитивні спрацювання і не аналізує конфігурацію сервера, тоді як DAST не має доступу до вихідного коду і пропускає приховані логічні вразливості.

Метою дослідження є практичний порівняльний аналіз можливостей інструментів GitHub CodeQL (SAST) та OWASP ZAP (DAST), а також дослідження ефективності їх об'єднання в єдиний аналітичний гібридний конвеєр.

В рамках дослідження було використано еталонний вразливий веб-додаток OWASP Juice Shop. У хмарному середовищі GitHub Actions було спроектовано та налаштовано автоматизований CI/CD конвеєр, який включав послідовний запуск інструментів безпеки під час збірки та розгортання коду у Docker-контейнері.

Після успішного налаштування пайплайну (рис. 1), було проведено сканування додатка. Для аналізу та консолідації результатів було розроблено авторський програмний модуль мовою Python. Даний скрипт виконує роль агрегатора: він отримує звіти від SAST та DAST, порівнює їх та усуває дублікати, формуючи зведений звіт.

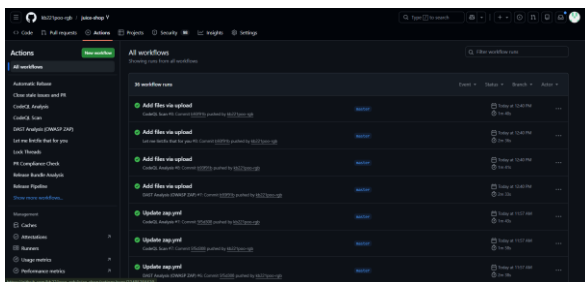
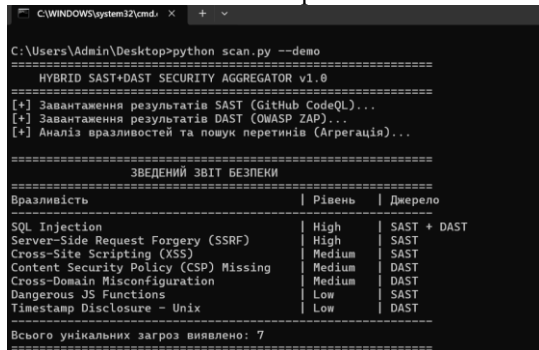


Рисунок 1 – Візуалізація успішного виконання гібридного конвеєра CI/CD

Результати агрегації (рис. 2) наочно демонструють спеціалізацію кожного з інструментів. Інструмент GitHub CodeQL успішно виявив вразливості на рівні коду, такі як Server-Side Request Forgery (SSRF) та Cross-Site Scripting (XSS). Водночас OWASP ZAP ідентифікував проблеми конфігурації веб-сервера: відсутність Content Security Policy (CSP) та Cross-Domain Misconfiguration, які фізично не могли бути виявлені статичним аналізатором.



```

C:\WINDOWS\system32\cmd.exe
C:\Users\Admin\Desktop>python scan.py --demo

=====
HYBRID SAST+DAST SECURITY AGGREGATOR v1.0
=====
[+] Завантаження результатів SAST (GitHub CodeQL)...
[+] Завантаження результатів DAST (OWASP ZAP)...
[+] Аналіз вразливостей та пошук перетинів (Агрегація)...
=====
ЗВЕДЕНИЙ ЗВІТ БЕЗПЕКИ
=====
Вразливість | Рівень | Джерело
-----
SQL Injection | High | SAST + DAST
Server-Side Request Forgery (SSRF) | High | SAST
Cross-Site Scripting (XSS) | Medium | SAST
Content Security Policy (CSP) Missing | Medium | DAST
Cross-Domain Misconfiguration | Medium | DAST
Dangerous JS Functions | Low | SAST
Timestamp Disclosure - Unix | Low | DAST
Всього унікальних загроз виявлено: 7
=====

```

Рисунок 2 – Результат роботи програмного модуля агрегації вразливостей (SAST+DAST)

Найбільш критична уразливість — SQL Injection — була успішно виявлена обома системами, що підтверджується зведеним звітом програмного модуля (рис. 2).

Отже, проведене практичне дослідження підтвердило, що використання лише одного класу сканерів є недостатнім для комплексного захисту. Побудова гібридного CI/CD конвеєра з інтеграцією GitHub CodeQL та OWASP ZAP дозволяє компенсувати недоліки окремих методів та забезпечити максимальне покриття вразливостей згідно з класифікацією OWASP Top 10.

Список використаних джерел

1. OWASP Top 10:2021. URL: <https://owasp.org/Top10/>
2. About CodeQL code scanning in your CI/CD system. URL: <https://docs.github.com/en/code-security/code-scanning>
3. OWASP ZAP - Baseline Scan. URL: <https://www.zaproxy.org/docs/docker/baseline-scan/>

УДК 004.7

Хохлов М.О., аспірант

Державний університет «Житомирська політехніка»

ВИМОГИ СТАНДАРТИЗАЦІЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ МОНІТОРИНГУ СИТУАЦІЙНОГО ЦЕНТРУ

Інформаційно-комунікаційна система моніторингу (далі – ІКСМ) є технічним ядром ситуаційного центру (далі – СЦ) і призначена для збору, передавання, оброблення, зберігання, аналізу та подання даних для оцінювання та моделювання ситуацій з метою забезпечення процесу підготовки і прийняття рішень [1]. В рамках регіонального СЦ така система має функціонувати в умовах багаторівневої архітектури, міжвідомчої взаємодії та постійного надходження по каналах зв'язку різномірної інформації з сенсорних засобів, геоінформаційних ресурсів, статистичних джерел та оперативних повідомлень. Тому, обґрунтування вимог стандартизації такого класу складних систем виступає одною із основних задач структурного і параметричного синтезу ІКСМ регіонального СЦ [2, 3, 4].

Стандартизація ІКСМ повинна починатися з формування базової моделі даних, спільної для всіх підсистем СЦ. У такій моделі мають бути визначені типи інформаційних об'єктів, їх атрибути, правила ідентифікації та зв'язки між ними. Для кожного інформаційного повідомлення необхідно встановити обов'язковий склад полів: ідентифікатор джерела, тип події або стану, часову мітку, просторову прив'язку, набір контрольованих параметрів, ознаку достовірності та режим доступу [4]. Обмін між підсистемами повинен виконуватися через уніфіковані інтерфейси, які регламентують формат повідомлень, порядок підтвердження доставки, оброблення помилок, повторну передачу та зворотну сумісність [5].

Ключовою вимогою є семантична стандартизація, довідники, класифікатори, коди подій, статуси об'єктів, територіальні ознаки та інші словники, що використовуються різними учасниками інформаційної взаємодії, оскільки технічна сумісність без єдиної інтерпретації даних не забезпечує коректної аналітики. Кожний запис повинен супроводжуватись метаданими, які будуть забезпечувати відстеження походження, контроль актуальності та можливість автоматизованої перевірки. Особливу увагу необхідно приділити нормуванню показників якості даних: повноті, достовірності, несуперечності, точності просторово-часової прив'язки та допустимої затримки надходження [6, 7].

Стандартизація ІКСМ також охоплює вимоги захисту й експлуатаційної стійкості системи. Для цього визначено окремі класи інформації, правила та механізми: входу, доступу, логування дій користувачів, контролю цілісності та захисту даних в процесі їх передавання і зберігання. На експлуатаційному рівні регламентується резервування компонентів, моніторинг каналів обміну, відновлення і порядок підключення нових джерел без порушення роботи наявних підсистем.

Таким чином, реалізація вимог стандартизації ІКСМ забезпечить ефективне функціонування СЦ завдяки уніфікації форматів і протоколів обміну, формалізації даних, упорядкуванню міжсистемної взаємодії й запровадженню єдиних вимог до якості, захисту і супроводу інформації, а також створить підґрунтя підготовки управлінських рішень у сфері безпеки й сталого розвитку регіону на основі своєчасного отримання, аналізу, оцінювання, моделювання та прогнозування стану об'єктів моніторингу та своєчасного виявлення і попередження про ризик можливої небезпеки.

Список використаних джерел

1. Бродський Ю. Б., Ковбасюк С. В. Концептуальний підхід до створення ситуаційного центру сталого розвитку регіону. Сучасні інформаційні технології у сфері безпеки та оборони. 2024. Т. 49, № 1. С. 151–159. doi: 10.33099/2311-7249/2024-49-1-151-159.
2. Бродський Ю. Б., Ковбасюк С. В. Кібернетична модель регіонального ситуаційного центру. Технічна інженерія. 2024. № 2(94). С. 81–90.
3. Про стандартизацію : Закон України від 05.06.2014 № 1315-VII // База даних «Законодавство України» / Верховна Рада України.
4. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України.
5. Хохлов М.О., Ковбасюк С.В. Уніфікація протоколів обміну даними інформаційних систем громадського транспорту. Тези XVIII Міжнародної науково-практичної конференції «Інтегровані інтелектуальні роботехнічні комплекси», 20-21 травня 2025 року. Київ : «Київський авіаційний інститут», 2025. С. 389-391.
6. Garcia Alvarez M., Morales J., Kraak M.-J. Integration and Exploitation of Sensor Data in Smart Cities through Event-Driven Applications. Sensors. 2019. Vol. 19, No. 6. Art. 1372. doi: 10.3390/s19061372.
7. Shams F. et al. Integration of heterogeneous information sources for an effective emergency management. International Journal of Emergency Management. 2016. Vol. 12, No. 1. P. 70–94. doi: 10.1504/IJEM.2016.074880.

УДК 004.7

Рудюк Б.М., асистент

Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ GLOBALPROTECT, CISCO SECURE CLIENT ТА FORTICLIENT ДЛЯ ЗАХИЩЕНОГО ВІДДАЛЕНОГО ДОСТУПУ В УМОВАХ КІБЕРЗАГРОЗ

У сучасних умовах гібридної організації праці та стрімкого зростання кіберзагроз, забезпечення захищеного віддаленого доступу стає критичним елементом корпоративної інформаційної безпеки. Традиційні VPN-рішення еволюціонують у бік Zero Trust Network Access (ZTNA), інтеграції з SASE (Secure Access Service Edge) та безперервної оцінки стану кінцевих пристроїв. Провідні рішення ринку – Palo Alto Networks GlobalProtect, Cisco Secure Client (AnyConnect) та Fortinet FortiClient – пропонують комплексні підходи до шифрованого віддаленого доступу, але відрізняються архітектурою, рівнем інтеграції з екосистемою та рівнем акценту на запобігання загроз.

GlobalProtect становить невід'ємну частину екосистеми Palo Alto Networks і забезпечує тісну інтеграцію з міжмережевими екранами наступного покоління (NGFW) та хмарною платформою Prisma Access. Рішення реалізує принципи Zero Trust Network Access (ZTNA 2.0), передбачаючи безперервну верифікацію ідентичності користувача, стану пристрою та контексту доступу. Архітектура базується на компонентах GlobalProtect Portal та GlobalProtect Gateway, що дає змогу здійснювати централізоване й узгоджене керування доступом у гібридних і хмарних середовищах.

Cisco Secure Client належить до найпоширеніших корпоративних клієнтів захищеного доступу. Рішення підтримує сучасні протоколи SSL/TLS та IPsec IKEv2, забезпечуючи високу сумісність із різноманітним мережевим обладнанням Cisco. Ключовою перевагою є глибока інтеграція з платформою Cisco Identity Services Engine (ISE) для оцінки стану пристроїв і динамічного контролю доступу, а також з Cisco Umbrella – для додаткового захисту на рівні DNS навіть поза активним VPN-з'єднанням.

FortiClient від компанії Fortinet позиціонується як уніфікований агент кінцевої точки (Fabric Agent), який поєднує функції захищеного віддаленого доступу, захисту від шкідливого програмного забезпечення та оцінки відповідності вимогам безпеки. Завдяки тісній інтеграції з екосистемою Fortinet Security Fabric рішення забезпечує наскрізну видимість і контроль загроз у гетерогенних ІТ-середовищах, дозволяючи динамічно застосовувати політики доступу.

Таблиця 1. Порівняльна характеристика рішень

	GlobalProtect	Cisco Secure Client	FortiClient
Протоколи	IPsec, SSL/TLS, ZTNA	SSL/TLS, IPsec IKEv2, ZTNA, DTLS	IPsec, SSL/TLS, ZTNA
MFA	SAML, RADIUS, сертифікати	SAML, RADIUS, RSA SecurID, Cisco Duo	SAML, FortiToken, RADIUS, сертифікати
Платформи	Windows, macOS, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android	Windows, macOS, Linux, iOS, Android
Виявлення загроз	Інтеграція з WildFire	Cisco Talos Intelligence	FortiGuard Labs
Інструменти управління	Panorama, Prisma Access	Cisco SecureX, інтеграція з ISE/DNA Center	FortiClient EMS
Ліцензування	Підписка (включено до NGFW / Prisma Access)	Підписка за кількістю користувачів (Advantage / Premier)	Freemium (обмежена версія) + комерційна підписка

Рішення підтримують MFA та інтеграцію з IDP через SAML 2.0. GlobalProtect вирізняється застосуванням профілів стану хоста (HIP), що забезпечує динамічну адаптацію політик доступу на основі безперервного моніторингу кінцевих точок.

У контексті криптографічного захисту GlobalProtect та FortiClient реалізують ZTNA-тунелювання за стандартом TLS 1.3, тоді як Cisco Secure Client використовує протокол DTLS (на базі UDP) для оптимізації затримки та продуктивності.

Ефективність протидії загрозам базується на інтеграції з екосистемами вендорів: GlobalProtect використовує хмарну пісочницю WildFire, Cisco базується на аналітиці Talos Intelligence, а FortiClient акумулює уніфіковану телеметрію в межах Fortinet Security Fabric для наскрізного моніторингу гетерогенних середовищ.

Вибір рішення залежить від існуючої інфраструктури та пріоритетів безпеки. GlobalProtect є оптимальним для організацій, що потребують максимальної видимості трафіку та використовують інструменти аналізу загроз Palo Alto. Cisco Secure Client залишається стандартом для великих корпорацій зі складною мережевою структурою, де критичною є деталізація політик доступу. FortiClient часто представляє найкраще співвідношення "функціональність/вартість" для компаній, які шукають інтегроване рішення, що поєднує VPN та захист кінцевих точок.

Список використаних джерел

1. GlobalProtect. Palo Alto Networks | TechDocs Home. URL: <https://docs.paloaltonetworks.com/globalprotect>
2. Secure Client (including AnyConnect). Cisco. URL: <https://www.cisco.com/site/us/en/products/security/secure-client/index.html>
3. FortiClient 7.4. Fortinet Document Library | Home. URL: <https://docs.fortinet.com/product/forticlient>

УДК 004.7

*Єфіменко А. А., магістрант
Єфіменко А.А., к.т.н., доцент*

Державний університет «Житомирська політехніка»

АДАПТАЦІЯ МЕТОДОЛОГІЇ DEVOPS ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ІОТ-СИСТЕМ

Від «розумних» будинків, що функціонують на основі взаємопов'язаних пристроїв, до промислової автоматизації та концепцій «розумних міст», які базуються на використанні автономних сенсорів, стрімкий розвиток технологій Інтернету речей (IoT) суттєво трансформує сучасні галузі та сприяє формуванню нових бізнес-моделей. Водночас управління такими складними екосистемами пов'язане зі значними викликами. IoT-системи взаємодіють із великою кількістю пристроїв, опрацьовують значні обсяги даних у реальному масштабі часу та вимагають високого рівня надійності, масштабованості й безпеки.

Традиційні підходи до управління життєвим циклом програмного забезпечення, орієнтовані на розробку стандартизованих рішень, виявляються недостатньо ефективними в умовах IoT-середовищ. Це зумовлює необхідність адаптації сучасних інженерних практик, зокрема DevOps, до специфіки таких систем [1].

Методологія DevOps розглядається як сучасна інженерна парадигма, що поєднує процеси розробки та експлуатації програмного забезпечення з метою підвищення рівня автоматизації та скорочення часу доставки змін. Вона застосовується не лише у класичних IT-системах, але й у вбудованих рішеннях, зокрема в робототехніці та системах інтелектуальних агентів. [2] У свою чергу, екосистема IoT подається як набір фізичних пристроїв, таких як датчики та виконавчі пристрої, зінтегрованих в розлогих мережевих структурах, що містять набори серверів та шлюзів, які забезпечують надійне їх підключення та взаємодію.

Аналіз наукових і технічних джерел свідчить, що DevOps-методологія широко застосовується у хмарних і веб-орієнтованих системах, забезпечуючи безперервну інтеграцію, доставку та автоматизацію процесів розробки і експлуатації. Водночас її застосування у сфері IoT залишається обмеженим через низку специфічних факторів, зокрема обмеженість обчислювальних ресурсів пристроїв, гетерогенність апаратного забезпечення, складність реалізації безпечних механізмів оновлення програмного забезпечення (ОТА), а також нестабільність мережевих з'єднань [3]. У науковій літературі недостатньо представлено цілісні підходи до інтеграції

DevOps-практик у життєвий цикл IoT-систем, що враховують зазначені обмеження та забезпечують узгодженість між етапами розробки, тестування, розгортання та моніторингу.

Метою дослідження є формування підходу до адаптації DevOps-методології для IoT-систем, визначення її ключових принципів та розроблення концептуальної моделі, яка забезпечує автоматизацію процесів розробки, тестування, розгортання та супроводу IoT-пристроїв з урахуванням їх специфічних характеристик. Основна ідея дослідження полягає у встановленні відповідності між типовими проблемами IoT-середовищ та можливостями DevOps-практик, а також у формуванні узагальненої моделі, що інтегрує підходи безперервної інтеграції, доставки та моніторингу в єдину систему управління життєвим циклом IoT.

У межах дослідження проведено ідентифікацію основних проблем IoT-систем, зокрема складності архітектури, відсутності автоматизованих процесів розгортання, обмежених можливостей моніторингу та підвищених ризиків інформаційної безпеки. На основі цього здійснено зіставлення зазначених проблем із відповідними DevOps-практиками, включаючи використання CI/CD для автоматизації процесів збірки та розгортання firmware, а також впровадження засобів централізованого моніторингу та управління конфігураціями.

Отримані результати дозволили узагальнити підходи до інтеграції DevOps у IoT-системи та сформулювати концептуальні положення щодо побудови адаптованої DevOps-моделі, яка враховує обмеження IoT-пристроїв та специфіку їх функціонування.

Таким чином, адаптація DevOps-методології до IoT-середовищ може слугувати основою для підвищення ефективності та безпеки функціонування розподілених систем. Перспективи подальших досліджень включають розроблення спеціалізованих DevSecOps-рішень для IoT, інтеграцію механізмів автоматизованого аналізу безпеки.

Список використаних джерел

1. Жовнір , Ю., Грибовський , О., Орлов, М., Дуда, О., & Кунанець, Н. "Методологія розроблення та супроводу інформаційних систем, базованих на технології інтернету речей", Управління розвитком складних систем, (60), 56–70, 2024.
2. LALIT SAINI, Dr. VISHAL SHRIVASTAVA, Dr. KRISHAN KANT LAVANIA, Dr. AKHIL PANDEY, "DevOps in IOT", International Journal of Research Publication and Reviews, vol. 5, no. 4, pp. 297-308, 2024.
3. Georges Bou Ghantous, Asif Qumer Gill, "Evaluating the DevOps Reference Architecture for Multi-cloud IoT-Applications," SN Computer Science, vol. 2, no. 3, pp. 1-12, 2021.

УДК 004:7

*Сердійчук І.С., магістрант
Єфіменко А.А., к.т.н., доцент*

Державний університет «Житомирська політехніка»

АРХІТЕКТУРНІ РІШЕННЯ ДЛЯ МОНІТОРИНГУ ТА РОЗПОДІЛУ РЕСУРСІВ ШЛЮЗІВ БЕЗПЕКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ

Сучасний етап розвитку корпоративних мереж характеризується високим рівнем гетерогенності, об'єднуючи різноманітні класи пристроїв, операційні системи та канали зв'язку. У таких умовах шлюзи безпеки відіграють критичну роль, забезпечуючи автентифікацію, шифрування трафіку та фільтрацію загроз на межі корпоративного периметра. Постійне зростання обсягів переданих даних та збільшення кількості віддалених підключень призводять до значного підвищення вимог до продуктивності та надійності цих вузлів[1].

Аналіз існуючих інфраструктур показує, що традиційна монолітна архітектура шлюзів безпеки часто не здатна впоратися з непередбачуваними піковими навантаженнями. Виконання складних криптографічних операцій швидко виснажує обчислювальні ресурси маршрутизаторів. Наслідком цього стає збільшення кількості втрачених пакетів, зростання джитера та критичне уповільнення часу відгуку корпоративних сервісів. Крім того, у разі апаратного або програмного збою єдиного шлюзу виникає ризик повної зупинки бізнес-процесів підприємства через втрату захищеного зв'язку.

Метою дослідження є розробка архітектурних рішень для ефективного розподілу ресурсів та забезпечення відмовостійкості шлюзів безпеки у гетерогенному мережевому середовищі. Для вирішення визначеної проблеми пропонується впровадження кластерної архітектури з використанням технологій балансування навантаження та забезпечення високої доступності. Запропонована архітектура передбачає розгортання групи шлюзів, що працюють у режимі Active-Active для паралельного та рівномірного оброблення криптографічних потоків, або Active-Passive для миттєвого автоматичного перемикання у разі відмови основного вузла[3].

Ключовим компонентом розробленого рішення є інтеграція централізованої системи моніторингу. Вона має здійснювати безперервний збір телеметричних даних з кожного шлюзу, включаючи метрики завантаження CPU, використання пам'яті, поточної пропускної здатності та затримки пакетів. На основі цих показників алгоритми динамічного розподілу ресурсів здатні автоматично перенаправляти нові сесії на найменш завантажені вузли, уникаючи перевантаження окремих елементів мережі.

За результатами аналізу сформульовано такі рекомендації щодо розподілу ресурсів:

- впровадити відмовостійкі кластери шлюзів безпеки із підтримкою синхронізації станів сесій для усунення єдиної точки відмови[2];
- застосовувати адаптивні алгоритми балансування навантаження, які в реальному часі враховують поточний стан апаратних ресурсів кожного криптографічного шлюзу;
- інтегрувати централізовану систему моніторингу для безперервного аналізу телеметрії та автоматичного перенаправлення трафіку при виявленні перевантажень;
- забезпечити можливість горизонтального масштабування мережевого периметра за рахунок модульного додавання нових вузлів без зупинки роботи корпоративних сервісів.

Таким чином, результати аналітичного дослідження свідчать, що перехід до розподіленої кластерної архітектури з активним моніторингом дозволяє нівелювати ризики відмови мережевого периметра. Запропоноване рішення оптимізує використання апаратних ресурсів, зменшує час затримки при обробці трафіку та суттєво підвищує загальний рівень надійності захищених комунікацій. Перспективним напрямом подальших досліджень є розробка та застосування методів машинного навчання для предиктивного аналізу навантаження та превентивного розподілу ресурсів шлюзів безпеки.

Список використаних джерел

1. Convery S. Network Security Architectures. Indianapolis : Cisco Press, 2004. 792 p.
2. Kopparapu C. Load Balancing Servers, Firewalls, and Caches. New York : John Wiley & Sons, 2002. 224 p.
3. Bourke T. Server Load Balancing. Sebastopol : O'Reilly & Associates, 2001. 192 p.

УДК 004.056.5

Опанасенко Є.Р., магістрантка

Єфіменко А.А., к.т.н., доцент

Державний університет «Житомирська політехніка»

ОЦІНКА ВПЛИВУ АРХІТЕКТУРИ ВЕБ-ДОДАТКУ НА ЧАСТОТУ ХИБНОПОЗИТИВНИХ СПРАЦЮВАНЬ ПРИ СКАНУВАННІ ВРАЗЛИВОСТЕЙ

Сучасні веб-додатки дедалі частіше будуються за принципами розподілених систем: Single Page Applications (SPA), мікрофронтенди, мікросервіси та serverless-архітектури вже стали стандартом для забезпечення масштабованості, гнучкості та швидкої розробки. Водночас інструменти динамічного аналізу безпеки (DAST), такі як OWASP ZAP, Burp Suite, Invicti чи Detectify, залишаються ключовим елементом автоматизованого тестування безпеки. Однак у складних архітектурах традиційні DAST-сканери генерують значну кількість хибнопозитивних (false positive) спрацювань, що призводить до втрати від сповіщень, перевантаження команд безпеки та зниження довіри до автоматизованого сканування[2,3].

Аналіз сучасних джерел та практики використання DAST-інструментів показує, що найбільша кількість хибнопозитивів виникає в архітектурах з високим рівнем динаміки клієнтської частини та розподіленості бекенду.

Найвищий рівень хибнопозитивів фіксується в мікрофронтендах. Фрагментована структура, використання різних фреймворків у межах одного додатка, міждоменна взаємодія та динамічне завантаження компонентів призводять до того, що сканери не можуть правильно побудувати контекст застосування. Це спричиняє дублювання тестів, помилкове трактування безпечного JavaScript-коду як XSS чи IDOR, а також численні хибні спрацювання на контроль доступу[3].

Дуже близьким за проблематикою є SPA (React, Angular, Vue, Svelte тощо). Клієнтська маршрутизація, віртуальний DOM, умовне відображення компонентів та те, що URL не змінюється при переходах між сторінками, — усе це сильно ускладнює нормальне сканування додатка. Традиційні краулери (наприклад, у OWASP ZAP чи Burp) часто зациклюються на станах або пропускають значну частину функціоналу, що генерує повторні та хибні тести на ін'єкції, CSRF чи порушення контролю доступу[2,3].

Третє місце посідають мікросервіси + serverless (FaaS, Lambda, Cloudflare Workers). Тут проблеми пов'язані з великою кількістю

динамічних ендпоінтів, подієво-орієнтованою логікою, стартом функцій «з нуля» та складною міжсервісною автентифікацією (JWT, OAuth). Сканер не здатен підтримувати повний контекст сесії між сервісами, що призводить до помилкових спрацювань на помилки конфігурації, обхід авторизації та API-аномаліях[2].

Деяко менш проблематичними є GraphQL + API-heavy архітектури, де сканери погано моделюють складні схеми запитів, що також підвищує рівень хибних спрацювань. Натомість класичні моноліти та JAMstack/статичні сайти демонструють найнижчий рівень хибних спрацювань завдяки простішій структурі URL та меншій поверхні атаки. SSR/SSG-рішення (Next.js, Nuxt, Remix) займають проміжну позицію — вони кращі за чисті SPA, але все одно генерують більше шуму, ніж моноліти.

Основні причини високого рівня хибнопозитивів: відсутність повного розуміння JavaScript-логіки, проблеми з підтримкою стану сесії, вибухи станів у розподілених системах та недостатня адаптація традиційних DAST-інструментів до сучасних патернів розробки[1].

Перехід до сучасних архітектур суттєво ускладнює ефективність традиційного DAST-сканування через зростання хибнопозитивних результатів. Для зменшення шуму рекомендується використовувати AI-based DAST-інструменти (Invicti, Escape, Checkmarx One), надавати OpenAPI/GraphQL-специфікації, застосовувати аутентифіковане сканування та комбінувати DAST з IAST/RASP. Наразі ключовим напрямком розвитку є перехід до валідації на основі доказів що до вразливостей та інтеграція DAST у CI/CD-процеси з автоматичною фільтрацією false positives[1,2,3].

Список використаних джерел

1. O. Revniuk, N. Zagorodna, R. Kozak, B. Yavorsky DEVELOPMENT OF AN INFORMATION SYSTEM FOR THE QUANTITATIVE ASSESSMENT OF WEB APPLICATION SECURITY BASED ON THE OWASP ASVS STANDARD 2025, № 2 (118), с. 57- 64.

2. SecureSlate Team. The 7 Best DAST Solutions for 2026 — Ranked by Speed and Accuracy [Електронний ресурс] – Режим доступу: <https://getsecureslate.com/blog/the-7-best-dast-solutions-for-2026-ranked-by-speed-and-accuracy>.

Invicti. False Positives in Web Application Security – Facing the Challenge [Електронний ресурс] – Режим доступу: <https://www.invicti.com/white-papers/false-positives-in-application-security-whitepaper>.

УДК 004.056.5

*Опанасенко Є.Р., магістрантка
Бродський Ю. Б., к.т.н., доцент
Росіїнський Ю.М., к.т.н., доцент*

Державний університет «Житомирська політехніка»

АНАЛІЗ ТА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ СКАНЕРА OWASP ZAP НА ПРИКЛАДІ ВЕБ- ДОДАТКУ DVWA

Стрімка цифровізація та міграція бізнес-процесів у веб-середовище загострюють проблему захисту інформаційних ресурсів від кібератак. В умовах, коли ручний пошук вразливостей вимагає значних часових ресурсів, інструменти автоматизації, такі як OWASP Zed Attack Proxy (ZAP), набувають критичного значення. Проте сліпа довіра до автоматичних алгоритмів несе в собі ризики пропуску складних загроз. Дослідження можливостей цього сканера дає змогу сформулювати чітке уявлення про реальну ефективність автоматизованих засобів та визначити оптимальну стратегію їх використання. Отримані результати підтверджують, що успішність аудиту безпеки залежить не стільки від вибору інструменту, скільки від методології його застосування, зокрема поєднання автоматизації з людським інтелектом.

Особливу цінність для розуміння меж можливостей автоматизованих сканерів становить аналіз їх роботи в середовищі DVWA (Damn Vulnerable Web Application). Цей додаток є не просто набором вразливих скриптів, а повноцінним полігоном, що імітує реальні помилки розробників на різних рівнях захищеності. Специфіка DVWA полягає у градації рівнів безпеки («Low», «Medium», «High», «Impossible»), що дозволяє простежити еволюцію коду від повної відсутності захисту до впровадження фільтрації вхідних даних та використання підготовлених запитів. Тестування на такій платформі чітко демонструє момент, коли автоматичний сканер втрачає ефективність: якщо на низькому рівні ZAP легко ідентифікує вразливості за стандартними сигнатурами, то вже на середньому рівні, де застосовуються базові методи санітизації (наприклад, функція `mysql_real_escape_string` або прості регулярні вирази), автоматика часто зазнає невдачі без додаткового налаштування контексту та ручного корегування векторів атаки[3].

Аналіз роботи OWASP ZAP показує, що ефективність сканування прямо пропорційна глибині попереднього налаштування та розумінню природи виявлених загроз. Використання базових автоматичних

режимів дозволяє виявити поверхневі вразливості, покриваючи не більше 60–70% потенційних загроз. Однак практична користь від результатів роботи ZAP значно зростає при детальному розборі звітів. Сканер не лише сигналізує про наявність проблеми, а й надає доказову базу: повний текст HTTP-запиту, використаний шкідливий пейлоад (payload) та відповідь сервера, що підтверджує успішну експлуатацію. Це дає розробникам точні інструкції для відтворення помилки та її виправлення[2].

Ключовим інсайтом роботи є доведення переваги гібридного підходу над суто автоматичним. Експериментальні дані свідчать, що найвищий рівень виявлення вразливостей (до 95%) досягається при використанні OWASP ZAP у режимі перехоплюючого проксі. Це дозволяє поєднувати автоматичний пошук типових помилок із ручним фаззингом (fuzzing) — підстановкою специфічних пейлоадів у місця зі складною бізнес-логікою. Саме такий метод дає змогу обходити фільтри безпеки та виявляти критичні вразливості високого рівня складності, наприклад, збережені XSS або сліпі SQL-ін'єкції, які автоматичні алгоритми часто ігнорують через неможливість коректної інтерпретації відповіді сервера[1,2].

Таким чином, результати дослідження дають підстави стверджувати, що OWASP ZAP є потужним елементом у системі кіберзахисту, проте його роль має зводитися до інструменту підсилення можливостей фахівця, а не повної заміни ручного тестування. Впровадження комплексної методики, де автоматизація пришвидшує рутинні процеси, а ручний контроль забезпечує глибину аналізу, виступає запорукою мінімізації ризиків та підвищення загального рівня захищеності веб-додатків.

Список використаних джерел

1. OWASP Zed Attack Proxy Documentation. OWASP Foundation. [Електронний ресурс]. – Режим доступу: URL: <https://www.zaproxy.org/docs/>
2. Scarfone, K., et al. (2008). Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115.
3. Damn Vulnerable Web Application (DVWA). GitHub Repository. [Електронний ресурс]. – Режим доступу: URL: <https://github.com/digininja/DVWA>

УДК 004.738.5

*Грищенко Д.С., здобувач,
Колошук М.С., ст. викладач,
Окунькова О.О., ст. викладач*

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ІАМ-ПЛАТФОРМ ДЛЯ УПРАВЛІННЯ ДОСТУПОМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Зростання кількості корпоративних інформаційних систем, хмарних середовищ та розподілених користувачів ускладнює контроль доступу до ресурсів організацій, що підтверджується сучасними дослідженнями [1]. Традиційні підходи на основі локальних облікових записів і ручного адміністрування прав є недостатньо гнучкими та схильними до помилок, що зумовлює необхідність використання систем класу Identity and Access Management (IAM).

Метою дослідження є порівняльний аналіз функціональних можливостей та ефективності провідних IAM-платформ для управління доступом у корпоративних інформаційних системах з урахуванням сучасних вимог інформаційної безпеки.

Для досягнення поставленої мети застосовано метод порівняльного аналізу, узагальнення та систематизації функціональних характеристик трьох IAM-платформ – Microsoft Entra ID, Okta та Keycloak – за такими критеріями: підтримка протоколів автентифікації (OAuth 2.0, SAML 2.0, OpenID Connect), реалізація рольової моделі доступу (Role-Based Access Control, RBAC), наявність багатофакторної автентифікації (Multi-Factor Authentication, MFA), функції аудиту та моніторингу подій, а також можливості інтеграції з хмарними і гібридними середовищами.

Таблиця 1 – Порівняльна характеристика IAM-платформ

Платформа	MFA	RBAC	Протоколи	Інтеграція
Microsoft Entra ID	+	+	OAuth 2.0, SAML, OIDC	Висока
Okta	+	+	OAuth 2.0, SAML, OIDC	Висока
Keycloak	+	+	OAuth 2.0, SAML, OIDC	Гнучка

IAM-платформи є комплексними рішеннями, що забезпечують управління цифровими ідентичностями користувачів та контроль їх доступу до інформаційних ресурсів, включаючи автентифікацію, авторизацію, управління ролями, аудит та моніторинг. Централізація управління правами дозволяє адміністратору обслуговувати великі організації з тисячами користувачів з єдиного інтерфейсу, що мінімізує ймовірність помилок та знижує операційне навантаження. Застосування моделі RBAC забезпечує логічний розподіл прав відповідно до функціональної ролі: від базового доступу рядового співробітника до повноважень системного адміністратора [2].

У результаті порівняльного аналізу встановлено, що всі три платформи реалізують ключові функції IAM, однак відрізняються за

моделлю розгортання та гнучкістю налаштування. Microsoft Entra ID є оптимальним рішенням для організацій, що використовують екосистему Microsoft 365, завдяки нативній інтеграції з корпоративними сервісами. Oкта вирізняється широкими можливостями підключення до хмарних застосунків через готові конектори та підтримкою складних сценаріїв федерації ідентичностей. Keycloak як рішення з відкритим кодом забезпечує максимальну гнучкість конфігурації за умови наявності достатніх ресурсів для самостійного розгортання та підтримки. Використання механізму MFA у поєднанні з RBAC суттєво знижує ризики несанкціонованого доступу: за даними галузевих досліджень, впровадження MFA дозволяє заблокувати понад 99,9 % автоматизованих атак на облікові записи [1].

Окрему увагу у дослідженні приділено механізмам аудиту та автоматизації. IAM-системи ведуть журнали подій, у яких фіксуються всі дії користувачів: автентифікаційні спроби, операції зміни прав, доступ до ресурсів. Це забезпечує оперативне виявлення підозрілої активності та відповідає вимогам регуляторних стандартів (ISO/IEC 27001, GDPR). Автоматизація циклу управління обліковими записами (provisioning/deprovisioning) скорочує час реакції на кадрові зміни та унеможливорює збереження надлишкових прав доступу після звільнення працівника.

Наукова новизна роботи полягає у формалізації критеріїв оцінювання IAM-платформ як компонентів корпоративної системи безпеки та встановленні залежності ефективності їх застосування від архітектурної моделі IT-інфраструктури.

За результатами дослідження встановлено, що ефективність IAM-платформи визначається не лише переліком підтримуваних функцій, а й відповідністю архітектурній моделі організації та рівнем зрілості її IT-інфраструктури. Застосування рольової моделі доступу та багатofакторної автентифікації у поєднанні з інструментами аудиту забезпечує комплексний контроль над інформаційними ресурсами. Вибір між комерційними хмарними рішеннями (Entra ID, Oкта) та відкритими самостійно розгорнутими платформами (Keycloak) має здійснюватися з урахуванням масштабу організації, наявних технічних компетенцій та бюджетних обмежень. Впровадження IAM-рішень є доцільним для організацій будь-якого масштабу як ефективний інструмент підвищення рівня кібербезпеки та оптимізації процесів управління доступом.

Список використаних джерел

1. What is Identity and Access Management (IAM)? IBM. URL: <https://www.ibm.com/topics/identity-access-management>.
2. NIST Special Publication 800-63-3: Digital Identity Guidelines. National Institute of Standards and Technology. URL: <https://pages.nist.gov/800-63-3/>.

УДК 004.7

*Млинський Б.М., здобувач,
Дячук О.Ю., ст. викладач,
Колощук М.С., ст. викладач*

Державний університет «Житомирська політехніка»

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ВІДМОВСТІЙКОСТІ В РОЗПОДІЛЕНИХ МЕРЕЖЕВИХ СИСТЕМАХ: АНАЛІЗ ПРОБЛЕМИ SPLIT-BRAIN ТА ПОРІВНЯННЯ З АВТОНОМНИМИ АРХІТЕКТУРАМИ

Сучасні розподілені мережеві системи формуються як розподілені обчислювальні середовища, що складаються з великої кількості взаємопов'язаних вузлів і застосовуються у хмарних інфраструктурах, дата-центрах та сервісно-орієнтованих архітектурах. Однією з ключових вимог до таких систем є забезпечення відмовостійкості (fault tolerance), яка визначає здатність системи зберігати працездатність за умов часткових відмов окремих компонентів.

Метою роботи є аналіз причин виникнення проблеми split-brain у розподілених системах та порівняння підходів до забезпечення відмовостійкості з автономними архітектурами.

На відміну від автономних або централізованих архітектур, де існує єдина точка відмови (single point of failure), розподілені системи орієнтовані на те, що відмови є невід'ємною частиною їх функціонування. Досягнення відмовостійкості базується на використанні надмірності (redundancy), реплікації даних (replication) та механізмів автоматичного відновлення.

Реплікація дозволяє зберігати кілька копій даних на різних вузлах системи, що забезпечує їх доступність навіть у випадку відмови окремих компонентів. При цьому застосовуються різні моделі узгодженості, зокрема strong consistency, коли всі копії даних підтримуються в узгодженому стані в режимі реального часу, та eventual consistency, яка допускає тимчасові розбіжності стану системи з метою підвищення продуктивності та зменшення затримок [3].

Фундаментальним обмеженням розподілених систем є теорема CAP, відповідно до якої система не може одночасно гарантувати consistency, availability та partition tolerance. Оскільки мережеві розділення є неминучими у великих мережах, практичні реалізації змушені обирати компроміс між узгодженістю та доступністю. У цьому контексті виникає проблема split-brain, яка є одним із найбільш небезпечних сценаріїв відмов [3].

Split-brain виникає у випадку мережевого розділення (network partition), коли кластер поділяється на кілька ізольованих частин, кожна

з яких продовжує функціонувати незалежно. У таких умовах може виникнути ситуація з множинними керівними вузлами (multiple leaders), коли кілька вузлів одночасно виконують роль координатора. Це пов'язано з тим, що кожен вузол приймає рішення на основі локального уявлення про стан системи (local view), яке може бути неповним або застарілим через затримки передачі даних або втрату пакетів [5].

Наслідки split-brain є критичними для систем, що працюють з транзакційними або консистентними даними. Незалежна обробка запитів у різних частинах системи призводить до конфліктів запису (write conflicts) та розбіжності даних (data divergence). Після відновлення мережевого з'єднання виникає необхідність узгодження станів (reconciliation), що є складним процесом і може супроводжуватися частковою втратою інформації або порушенням логічної цілісності даних. Для вирішення таких конфліктів використовуються спеціалізовані підходи, включаючи політики на кшталт last-write-wins або більш складні механізми, такі як CRDT, однак вони не завжди гарантують коректність з точки зору прикладної логіки [1].

Для мінімізації ризику виникнення split-brain застосовуються алгоритми досягнення згоди (consensus algorithms), серед яких найбільш відомими є Paxos та Raft. Вони забезпечують узгоджене прийняття рішень між вузлами навіть у разі часткових відмов. Основою їх роботи є використання кворуму (quorum), тобто рішення вважається прийнятим лише за умови підтримки більшістю вузлів. Це дозволяє гарантувати, що лише одна частина системи може виконувати операції запису, тоді як інші вузли переходять у пасивний стан.

Додатково використовуються механізми ізоляції вузлів, зокрема fencing, які запобігають одночасному доступу кількох вузлів до спільних ресурсів. У практичних реалізаціях застосовується підхід STONITH, що передбачає примусове відключення вузла для уникнення конфліктів. Важливу роль також відіграють механізми контролю стану вузлів, зокрема heartbeat, які забезпечують регулярну перевірку доступності компонентів системи. Однак такі механізми не є абсолютно надійними, оскільки не дозволяють точно відрізнити реальну відмову від тимчасових мережових затримок, що може призводити до помилкових рішень [2].

У порівнянні з розподіленими системами, автономні архітектури мають значно простішу структуру. Всі операції виконуються в межах одного вузла або контрольованого середовища, що забезпечує високу узгодженість даних без необхідності складних механізмів синхронізації. Відсутність розподіленої координації спрощує проєктування системи та знижує ризик виникнення логічних конфліктів [4].

Водночас такі системи мають суттєвий недолік у вигляді єдиної точки відмови. У разі виходу з ладу центрального вузла система повністю втрачає працездатність. Навіть при використанні резервних механізмів перемикання можливі затримки у відновленні роботи та ризик втрати даних. Крім того, централізовані системи мають обмежені можливості масштабування, що обмежує їх застосування у великих обчислювальних середовищах [1].

Проведений теоретичний аналіз сучасних підходів до забезпечення відмовостійкості дозволив узагальнити ключові особливості функціонування розподілених систем в умовах мережових розділень.

У результаті проведеного аналізу встановлено, що проблема split-brain є наслідком фундаментальних обмежень розподілених систем, пов'язаних із необхідністю балансування між узгодженістю та доступністю. Порівняння з автономними архітектурами показало, що підвищення відмовостійкості досягається ціною ускладнення механізмів координації та управління даними. Найбільш ефективним підходом до запобігання split-brain є поєднання алгоритмів узгодження, кворумних механізмів та засобів ізоляції вузлів.

Подальший розвиток цієї галузі пов'язаний із дослідженням адаптивних систем, які здатні динамічно змінювати параметри узгодженості залежно від стану мережі, а також із розробкою нових моделей обробки даних, що дозволяють природно обробляти конфлікти без значного ускладнення системи. Це відкриває перспективи створення більш надійних і масштабованих мережових систем, здатних ефективно функціонувати в умовах постійних змін і часткових відмов [1].

Список використаних джерел

1. Assiri B., Sheneamer A. Fault tolerance in distributed systems using deep learning approaches // PLOS ONE. 2024. URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0310657>
1. Sari A., Akkaya M. Fault tolerance mechanisms in distributed systems // International Journal of Computer Applications. 2015. Vol. 8. URL: https://www.researchgate.net/publication/287198069_Fault_Tolerance_Mechanisms_in_Distributed_Systems
2. Fault tolerance in distributed systems: a survey. 2019. URL: https://www.researchgate.net/publication/330123117_Fault_Tolerance_in_Distributed_Systems_A_Survey
3. Liu S. A survey on fault-tolerance in distributed optimization and machine learning. 2021. URL: <https://www.semanticscholar.org/paper/A-Survey-on-Fault-tolerance-in-Distributed-and-Liu/972be47cdd1b43f2f8245a8e34efcd6d7f251c4f>
4. Brewer E. Towards robust distributed systems. 2000. URL: https://www.researchgate.net/publication/221343719_Towards_robust_distributed_systems

УДК 004.8

*Лелета В.Р., здобувачка,
Маєвський О.В., к.т.н., доцент,
Бродський Ю.Б., к.т.н., доцент
Державний університет "Житомирська політехніка"*

ІНТЕЛЕКТУАЛЬНИЙ АГЕНТ ДЛЯ АНАЛІТИЧНОЇ ПІДТРИМКИ СИТУАЦІЙНОГО ЦЕНТРУ В ЗАДАЧАХ МОНІТОРИНГУ НАДЗВИЧАЙНИХ ПОДІЙ

В умовах зростання кількості надзвичайних подій, природних катастроф, техногенних аварій і гібридних загроз особливого значення набуває оперативне отримання, аналіз і узагальнення даних для підтримки прийняття рішень. Ситуаційні центри виконують функцію інформаційно-аналітичного забезпечення управління кризовими подіями, однак їх ефективність значною мірою залежить від швидкості обробки великих масивів різномірної інформації та здатності виявляти критичні закономірності [1]. У зв'язку з цим перспективним є застосування інтелектуальних агентів, здатних автоматизувати процеси збору, структурування та первинної аналітичної обробки даних [1; 2].

Метою дослідження є розробка концепції інтелектуального агента для аналітичної підтримки ситуаційного центру, який забезпечує автоматизований збір даних із різних джерел, їх попередню обробку, аналітичну інтерпретацію та підготовку зведеної інформації для підтримки управлінських рішень. Як приклад предметної області розглядається моніторинг стихійних лих та надзвичайних подій на території України.

Запропонований агент орієнтований не лише на накопичення інформації, а насамперед на її практичне використання в аналітичному контурі ситуаційного центру. Його основними завданнями є: автоматизований збір даних про надзвичайні події; інтеграція статистики з відкритих, офіційних і картографічних джерел; очищення та нормалізація даних; виявлення територіальних, часових і типологічних закономірностей; аналітичне ранжування подій за рівнем ризику; а також формування коротких інформаційно - аналітичних зведень для операторів та аналітиків. Такий підхід дає змогу зменшити навантаження на персонал, скоротити час переходу від даних до висновків і підвищити якість ситуаційної обізнаності [2].

Як приклад прототипу доцільно розглядати моніторинг стихійних лих в Україні, зокрема повеней, пожеж, землетрусів, та інших кризових явищ природного або техногенного характеру. У межах такої задачі агент може здійснювати збір статистики щодо часу, географії, масштабу

та наслідків подій, виявляти регіони з підвищеною концентрацією ризиків та формувати аналітичну основу для оперативного реагування. Практична цінність цього полягає в тому, що ситуаційний центр отримує не набір розрізнених повідомлень, а структуровану інформаційну картину, придатну для оцінювання обстановки, прогнозування та планування дій [3].

Функціонально інтелектуальний агент може бути реалізований як модульна система, що включає підсистеми збору даних, їх нормалізації, аналітичної обробки, інтерпретації та візуалізації результатів. Це особливо важливо з позицій своєчасного попередження про ризикову ситуацію в регіоні.

Оскільки агент функціонує в середовищі, критичному до достовірності й цілісності інформації, його розробка повинна враховувати вимоги кібербезпеки. Йдеться насамперед про захист джерел даних, контроль доступу, аудит дій, перевірку достовірності вхідної інформації та стійкість до маніпуляцій або несанкціонованого впливу на логіку системи.

Отже, розробка інтелектуального агента для аналітичної підтримки ситуаційного центру є перспективним напрямом підвищення ефективності інформаційно-аналітичного забезпечення у сфері попередження ризикових ситуацій. Практичним результатом такої розробки може стати демонстраційний прототип, інтегрований до аналітичної системи ситуаційного центру, який забезпечує збір статистики, формування коротких аналітичних зведень, виявлення ризиків та візуалізацію динаміки подій.

Очікуваний ефект від впровадження такого рішення полягає у підвищенні оперативності, структурованості та аналітичної цінності інформації, що безпосередньо впливає на якість прийняття рішень в умовах кризових ситуацій [1; 3].

Список використаних джерел

1. Kryvonos L., Logvynenko S., Zhurba O. та ін. Digital technologies in the system of state economic security management // Problems and Perspectives in Management. 2026. URL: <https://www.researchgate.net/publication/401879405>
2. Huang K., Huang J., Mehmood Y. et al. AAGATE: A NIST AI RMF-Aligned Governance Platform for Agentic AI // arXiv. 2025. URL: <https://arxiv.org/abs/2510.25863>
3. Korchenko O., Korystin O., Shulha V. та ін. Sustainable development of smart regions via cybersecurity of national infrastructure // Sustainability. 2025. URL: <https://www.mdpi.com/2071-1050/17/19/8757>

УДК 004.9

*Левицька Т. О. канд. техн. наук, доцент
ДВНЗ «Приазовський державний технічний університет»*

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНТЕЛЕКТУАЛЬНИХ АЛГОРИТМІЧНИХ СИСТЕМ У КРИПТОВАЛЮТНОМУ ТРЕЙДИНГУ

Сучасний розвиток цифрових фінансових ринків і стрімке поширення технологій децентралізованих фінансів (DeFi) сприяли появі складних алгоритмічних систем аналізу та прогнозування ринкових даних. У подібних системах дедалі частіше використовуються моделі глибинного навчання, зокрема архітектури Long Short-Term Memory та Gated Recurrent Unit, що дозволяють ефективно працювати з часовими рядами та реалізовувати ринково-нейтральні торгові стратегії. Разом із високою точністю прогнозування виникає проблема забезпечення належного рівня інформаційної безпеки. Недостатній захист API-ключів, можливість модифікації вхідних даних або витік параметрів моделі можуть призвести до значних фінансових втрат і порушення вимог міжнародних регуляторних стандартів, таких як MiFID II [1] та NIST AI Risk Management Framework [2]. У зв'язку з цим актуальним є формування захищеної інфраструктури для систем криптовалютного алгоритмічного трейдингу, що використовують методи машинного навчання.

Об'єктом дослідження є експериментальний прототип торгової системи, який отримує ринкову інформацію з криптовалютної біржі Binance та децентралізованої платформи деривативів dYdX. Методологія роботи ґрунтується на аналізі технічних характеристик блокчейн-протоколів, дослідженні поширених вразливостей екосистеми DeFi [3,4] та застосуванні сучасних підходів до керування секретними даними в хмарних обчислювальних середовищах. Додатково використовуються криптографічні методи автентифікації запитів до зовнішніх сервісів.

У ході дослідження було визначено чотири ключові рівні загроз, які потребують реалізації відповідних механізмів захисту. Перший рівень пов'язаний із зовнішніми джерелами даних. У середовищі DeFi можливі атаки, що базуються на маніпуляції ціновими оракулами [5] або використанні механізмів флеш-кредитування[6], які здатні тимчасово викривляти ринкові котирування. Для зменшення впливу таких атак запропоновано механізм попередньої обробки даних, який передбачає фільтрацію аномальних значень та перевірку котирувань за даними декількох біржових джерел. Другий рівень загроз стосується інфраструктури системи. У запропонованій архітектурі всі програмні

компоненти розміщуються в ізолюваному сегменті хмарної мережі. При цьому жоден із модулів не зберігає конфіденційні параметри локально. Доступ до API-ключів і конфігураційних даних реалізовано через спеціалізовані сервіси керування секретами, наприклад Key Vault або KMS, із використанням механізму керованих ідентифікацій. Третій рівень пов'язаний із виконанням торгових операцій. Для запобігання атакам повторного відтворення запитів застосовується криптографічний підпис на основі алгоритму HMAC-SHA256. Додатково встановлюється обмежене часове вікно дії запиту (30 секунд), що унеможливило використання перехоплених повідомлень[7]. Експериментальні перевірки показали ефективність такого підходу для блокування несанкціонованих транзакцій. Четвертий рівень безпеки стосується безпосередньо моделей машинного навчання та торгової стратегії. Для зниження ризиків впроваджено механізм аварійного зупинення торгівлі («kill-switch»), який працює на основі аналізу зміни статистичних характеристик даних та фінансових показників системи[8-10]. У випадку виявлення значних відхилень у розподілі ознак або перевищення встановлених обмежень ризику система автоматично припиняє торгові операції та деактивує ключі доступу.

Під час апробації системи були отримані наступні науково-практичні результати:

- Ефективність захисту: Впровадження механізму HMAC-SHA256 разом із попсе-валідацією дозволило заблокувати 98,7% спроб атак повторного відтворення (replay attacks) під час стрес-тестування.
- Швидкодія: Додаткова затримка (latency), впроваджена криптографічним підписом та зверненням до KMS, склала лише 12-15 мс, що є прийнятним для середньочастотних стратегій і не впливає на проковзування (slippage).
- Точність Kill-switch: Система детектування аномалій (feature drift) показала detection rate на рівні 94,5% при спробах маніпулювання вхідними ознаками моделі через спотворення цінкових оракулів.

Запропонована архітектура дозволяє підвищити стійкість алгоритмічного торгового контуру до широкого спектра кіберзагроз. Проведене тестування підтвердило ефективність запропонованої архітектури при роботі з реальними торговими API. Поєднання хмарних механізмів безпеки, криптографічних методів захисту та моніторингу стану моделей машинного навчання забезпечує зниження операційних ризиків і сприяє відповідності сучасним вимогам регуляторного середовища щодо надійності алгоритмічних фінансових систем.

Список використаних джерел

1. European Securities and Markets Authority. MiFID II Review Report on Algorithmic Trading. ESMA70-156-4572, 2021. URL: https://www.esma.europa.eu/sites/default/files/library/esma70-156-4572_mifid_ii_final_report_on_algorithmic_trading.pdf (дата звернення: 10.12.2025).
2. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST, Gaithersburg, 2023. DOI: 10.6028/NIST.AI.100-1.
3. Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., & Gervais, A. (2023). SoK: Decentralized Finance (DeFi) Attacks. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 2444–2461). IEEE. <https://doi.org/10.1109/SP46215.2023.10179435>
4. Werner S., Perez D., Gudgeon L., Klages-Mundt A., Harz D., Knottenbelt W. SoK: Decentralized Finance (DeFi). AFT '22: 4th ACM Conference on Advances in Financial Technologies. 2022. P. 30–46. DOI: 10.1145/3558535.3559780
5. Daian P., Goldfeder S., Kell T. та ін. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. 2020 IEEE Symposium on Security and Privacy. IEEE, 2020. DOI: 10.1109/SP40000.2020.00097.
6. Cao S., Huang L., Wang Z. Flashot: A Snapshot of Flash Loan Attack on DeFi Ecosystem. 2021 IEEE International Conference on Blockchain. IEEE, 2021. DOI: 10.1109/Blockchain53845.2021.00060.
7. FICC Markets Standards Board. Emerging themes and challenges in algorithmic trading and machine learning. Spotlight Review, 2020. URL: <https://fmsb.com/wp-content/uploads/2020/04/FMSB-Spotlight-Review-Emerging-themes-and-challenges-in-algorithmic-trading-and-machine-learning.pdf> (дата звернення: 10.12.2025).
8. Yerlikaya F. A., Bahtiyar Ş. Data poisoning attacks against machine learning algorithms. Expert Systems with Applications, 2022, vol. 208, 118101. DOI: 10.1016/j.eswa.2022.118101.
9. Pialla, G., Ismail Fawaz, H., Devanne, M., Weber, J., Idoumghar, L., Muller, P.-A., Bergmeir, C., Schmidt, D. F., Webb, G. I., & Forestier, G. (2025). ime series adversarial attacks: An investigation of smooth perturbations and defense approaches. International Journal of Data Science and Analytics, 19, 129–139. <https://doi.org/10.1007/s41060-023-00438-0>
10. Rigaki, M., & Garcia, S. (2023). A survey of privacy attacks in machine learning. ACM Computing Surveys, 56(4), Article 101, 1–34. <https://doi.org/10.1145/3624010>

УДК 004.7

Колощук М.С., ст. викладач

Дячук О. Ю., ст. викладач

Окунькова О.О., ст. викладач

Державний університет "Житомирська політехніка"

ВИКОРИСТАННЯ АДЕМ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ ТА ПОТЕНЦІЙНИХ КІБЕРЗАГРОЗ У РОЗПОДІЛЕНИХ МЕРЕЖАХ

Сучасні корпоративні мережі зазнали фундаментальної трансформації: масовий перехід на гібридну модель роботи, міграція застосунків у хмарні середовища, розширення мережі філій та зростання кількості мобільних користувачів призвели до того, що мережевий периметр став розмитим, а поверхня атаки — значно ширшою. У таких умовах традиційні підходи до моніторингу мережевої безпеки, орієнтовані на контроль фіксованого периметра, втрачають ефективність. Зловмисники дедалі частіше використовують легітимні канали зв'язку, компрометовані облікові записи та методи латерального переміщення (lateral movement), які важко виявити за допомогою сигнатурних методів або статичних правил.

Традиційні системи моніторингу, зокрема SIEM, IDS/IPS та NMS, мають суттєві обмеження в умовах розподілених мереж. SIEM-системи забезпечують кореляцію подій безпеки, але працюють переважно реактивно, генерують значну кількість хибних спрацювань і потребують постійного ручного налаштування правил кореляції. IDS/IPS-рішення ефективні проти відомих сигнатур атак, проте безсилі перед новими або невідомими загрозами, що використовують легітимні протоколи. Системи мережевого моніторингу (NMS) зосереджені на стані інфраструктурних елементів, а не на користувацькому досвіді чи виявленні загроз, і не забезпечують наскрізної видимості від кінцевого пристрою до застосунку. У зв'язку з цим виникає потреба в проактивних, автономних рішеннях, здатних виявляти аномалії в реальному часі без постійного втручання людини. Саме таким рішенням є Autonomous Digital Experience Management (ADEM) — компонент платформи Prisma SASE від Palo Alto Networks, що використовує штучний інтелект та машинне навчання для безперервного моніторингу розподілених мереж.

На відміну від SIEM, IDS/IPS та NMS, ADEM забезпечує комплексний підхід: він не лише виявляє аномалії, але й автоматично визначає першопричину, оцінює вплив на користувачів та надає рекомендації щодо усунення. ADEM є нативно інтегрованим у SASE-архітектуру Prisma, що дозволяє отримувати телеметрію з усіх сегментів мережі без розгортання додаткових агентів або обладнання.

Порівняльний аналіз традиційних засобів моніторингу та ADEM наведено в таблиці 1.

Таблиця 1 – Порівняння ADEM з традиційними засобами моніторингу

Характеристика	SIEM	IDS/IPS	NMS	ADEM
Метод виявлення загроз	Кореляція подій за правилами	Сигнатурний аналіз	Порогові значення метрик	ML-моделі, аналіз відхилень від baseline
Видимість	Логи, події безпеки	Мережевий трафік	Інфраструктурні пристрої	Наскрізна: від пристрою до застосунку
Проактивність	Низька (реактивний)	Середня	Низька	Висока (прогнозування та автономне усунення)
Інтеграція з SASE	Відсутня або обмежена	Відсутня	Відсутня	Нативна
Автономне усунення	Ні	Частково (блокування)	Ні	Так (guided remediation playbooks)

В основі функціонування ADEM лежить адаптивне базування (adaptive ML baselining) — метод, за якого система безперервно навчається на історичних даних, формуючи динамічний базовий рівень «нормальної» поведінки для кожного сегмента мережі. На відміну від фіксованих порогових значень, ADEM застосовує сегментне оцінювання (segment-wise scoring), коли відхилення вимірюються відносно того, що є нормальним для конкретного сегмента (LAN, ISP, оверлейні тунелі) та конкретної групи користувачів. Крім того, ADEM використовує кластеризацію користувачів (user clustering) за спільними ознаками, такими як провайдер зв'язку, географічне розташування або шлях до шлюзу. Це дозволяє відрізнити локальну проблему одного користувача від системної деградації, що впливає на велику кількість осіб.

Ключовим компонентом є кореляційний рушій (correlation engine), який пов'язує симптоми, підтверджувальні дані та ймовірну першопричину, автоматично формуючи інцидент із рекомендаціями щодо усунення. Такий підхід дозволяє скоротити час виявлення (MTTD) до 95% та час усунення (MTTR) до 77%.

Архітектура ADEM у контексті SASE. ADEM є нативно інтегрованим у три ключові компоненти платформи Prisma SASE. По-перше, агент GlobalProtect на кінцевих пристроях користувачів збирає телеметрію про стан Wi-Fi, завантаження CPU/пам'яті та якість з'єднання. По-друге, пристрої Prisma SD-WAN (ION) у філіях забезпечують моніторинг усіх активних і резервних WAN-шляхів до застосунків, визначаючи базові показники затримки, джиттера та втрат для кожного сегмента. По-третє, хмарні точки присутності Prisma Access виконують синтетичні тести та моніторинг реального трафіку користувачів, забезпечуючи видимість навіть тоді, коли користувачі та застосунки перебувають поза межами корпоративної мережі. Завдяки такій нативній інтеграції ADEM не потребує розгортання додаткових агентів або обладнання, що спрощує впровадження та знижує операційні витрати.

Важливо зазначити, що архітектура ADEM повністю відповідає принципам Zero Trust: система забезпечує повну видимість усього

трафіку, контроль доступу на основі контексту (користувач, пристрій, застосунок, місцезнаходження) та безперервну верифікацію кожного з'єднання. Такий підхід унеможлиблює приховане латеральне переміщення зловмисника всередині мережі.

ADEM може бути використаний для виявлення низки потенційних кіберзагроз у розподілених мережах. Зокрема, латеральне переміщення (lateral movement) — техніка, за якої зловмисник після початкової компрометації переміщується між вузлами мережі в пошуках цінних активів, — може бути виявлене через аномальну зміну затримки або джиттера між внутрішніми сегментами, а також через нехарактерні патерни трафіку між вузлами, які зазвичай не взаємодіють між собою. Крім того, ADEM здатний виявляти аномальний трафік: різке зростання обсягу переданих даних, зміну типових протоколів або портів, підозрілі DNS-запити, що можуть свідчити про витік даних або командно-контрольний трафік (C2). Особливу цінність становить можливість використання відхилень у показниках затримки та джиттера як індикаторів атак: раптове погіршення якості з'єднання може свідчити про атаку типу «людина посередині» (MITM), DDoS-атаку або компрометацію кінцевого пристрою, що генерує аномальний трафік. ADEM дозволяє відстежувати ці показники на кожному сегменті мережі (LAN, інтернет, Prisma Access, застосунок) і виявляти відхилення від встановленого базового рівня.

ADEM є якісно новим підходом до виявлення аномалій у розподілених мережах завдяки поєднанню ML-моделей, адаптивного базування та наскрізної видимості. Інтеграція ADEM у SASE-архітектуру забезпечує безперервний моніторинг від кінцевого пристрою до застосунку, що повністю відповідає принципам Zero Trust та дозволяє виявляти загрози, які залишаються непоміченими традиційними засобами. Використання відхилень у показниках затримки та джиттера як індикаторів кіберзагроз відкриває нові можливості для проактивного виявлення атак типу lateral movement та MITM. Подальші дослідження можуть бути спрямовані на інтеграцію ADEM з XDR-платформами та розробку спеціалізованих моделей машинного навчання для виявлення складних APT-атак у розподілених мережах.

Список використаних джерел

1. Prisma SASE: Autonomous Digital Experience Manager (ADEM). The Network DNA. 2025. URL: <https://www.thenetworkdna.com/2025/10/prisma-sase-autonomous-digital.html>
2. Sharma M. Adaptive ML Baselineing to Detect Network Performance Degradations. Palo Alto Networks Community Blog. 2025. URL: <https://live.paloaltonetworks.com/t5/community-blogs/adaptive-ml-baselineing-to-detect-network-performance/ba-p/1241203>
3. Autonomous Digital Experience Management At a Glance. Palo Alto Networks. 2024. Autonomous DEM Administrator's Guide. Palo Alto Networks. 2024. 28 лют. URL: <https://origin-docs.paloaltonetworks.com/autonomous-dem/autonomous-dem-admin/adem-monitoring-and-tests>

УДК 004.056

*Миколайчук В. В., ст. викладач
Державний університет «Житомирська політехніка»*

DNSSEC ЯК ЗАСІБ ЗАХИСТУ ВІД DNS-СПУФІНГУ В ХМАРНІЙ ПЛАТФОРМІ AZURE

Система доменних імен (DNS) є фундаментальним компонентом мережевої інфраструктури, що забезпечує перетворення доменних імен у IP-адреси. Проте класичний протокол DNS не передбачав механізмів автентифікації відповідей, що робить його вразливим до атак. Однією з найнебезпечніших є атака DNS-спуфінгу (DNS cache poisoning), при якій зловмисник підміняє легітимні DNS-відповіді фальшивими, перенаправляючи користувачів на шкідливі ресурси. У 2008 році Ден Камінський продемонстрував критичну вразливість протоколу DNS, що дозволяла здійснювати масштабні атаки отруєння кешу DNS-серверів [1]. Ця вразливість стала каталізатором впровадження технології DNSSEC.

DNSSEC (Domain Name System Security Extensions) – набір розширень протоколу DNS, стандартизований у RFC 4033–4035, що забезпечує автентифікацію походження DNS-даних та перевірку їх цілісності за допомогою криптографічних підписів [2]. Механізм DNSSEC ґрунтується на ланцюгу довіри (chain of trust) від кореневої зони DNS до конкретного домену. Кожна зона підписує свої ресурсні записи приватним ключем, створюючи записи типу RRSIG. Відкритий ключ зони публікується у записі DNSKEY, а його хеш передається батьківській зоні як запис DS (Delegation Signer), формуючи ієрархічний ланцюг довіри. Для підтвердження відсутності записів використовуються записи NSEC або NSEC3, що унеможливають підробку негативних відповідей.

Все більше організацій розгортають інфраструктуру в хмарних платформах, зокрема Microsoft Azure, що пропонує сервіс Azure DNS для управління DNS-зонами. У лютому 2025 року Microsoft оголосив про загальну доступність (GA) підтримки DNSSEC для публічних зон Azure DNS [3]. Реалізація відповідає стандарту RFC 9824, що визначає вимоги до операційних практик впровадження DNSSEC [4]. Azure DNS автоматично генерує та керує криптографічними ключами зони (ZSK та KSK), виконує підписування ресурсних записів та забезпечує ротацію ключів. Для активації DNSSEC адміністратору достатньо увімкнути функцію для публічної зони та додати запис DS до реєстратора домену.

Впровадження DNSSEC в Azure DNS надає суттєві переваги: захист від DNS-спуфінгу та MITM-атак, оскільки кожна відповідь криптографічно підписана. Це критично для організацій, що мають відповідати стандартам PCI-DSS або ISO 27001. Водночас існують виклики: криптографічні підписи збільшують розмір DNS-відповідей, що може спричинити фрагментацію UDP-пакетів та потребує підтримки EDNS0. Ефективність DNSSEC залежить від повноти впровадження на всіх рівнях ланцюга довіри та підтримки валідації на стороні рекурсивного резолвера [5].

Отже, DNSSEC є необхідним механізмом забезпечення безпеки DNS-інфраструктури в хмарному середовищі Azure. Загальна доступність підтримки DNSSEC для публічних зон Azure DNS свідчить про зрілість технології та готовність платформи Microsoft до відповідності сучасним стандартам безпеки. Автоматизація управління ключами з боку Azure DNS суттєво знижує бар'єр впровадження, роблячи DNSSEC доступним для широкого кола організацій. Подальші дослідження можуть бути спрямовані на аналіз продуктивності DNS-запитів із увімкненим DNSSEC та порівняння реалізацій у різних хмарних провайдерах.

Список використаних джерел

1. Kaminsky D. It's The End Of The Cache As We Know It [Електронний ресурс] – Режим доступу до ресурсу: <https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf>.
2. RFC 4033 – DNS Security Introduction and Requirements [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc4033>.
3. DNSSEC for Azure DNS public zones is now generally available [Електронний ресурс] – Режим доступу до ресурсу: <https://azure.microsoft.com/en-gb/updates?id=479465>.
4. RFC 9824 – DNSSEC Automation [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc9824>.
5. DNSSEC overview [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/azure/dns/dnssec>.

Секція 3 ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

УДК 004.85

*Коротун О.В., к.пед.н., доцент кафедри КН
Чернець К.А., здобувач освіти
Державного університету «Житомирська політехніка»*

ОГЛЯД СУЧАСНИХ КУЛІНАРНИХ РЕКОМЕНДАЦІЙНИХ СИСТЕМ

Стрімкий розвиток інформаційних технологій сприяє інтеграції рекомендаційних систем в усі галузі, в тому числі й у побуті людини. Одним з таких застосувань є кулінарні рекомендаційні системи, які призначені для автоматизованого підбору рецептів і страв відповідно до індивідуальних уподобань користувачів, доступних інгредієнтів, харчових обмежень, контекстних факторів тощо.

Найпростіша кулінарна рекомендаційна система описана в статті [1] на основі гібридної фільтрації з використанням векторизації TF-IDF і машинного навчання. За допомогою контентної фільтрації аналізуються атрибути рецепту, переглянуті користувачем, а за допомогою колаборативної - поведінка користувача (вподобання, оцінки тощо). Ця система демонструє задовільну якість у формуванні рекомендацій, але ще не має зворотного зв'язку та налаштувань користувача.

Схожою системою є [2], проте тут використовується нейронна колаборативна фільтрація. Контентна фільтрація добре працює для текстової релевантності, часто повертає рецепти зі схожими словами, а колаборативна - демонструє кращу персоналізацію та здатність враховувати приховані вподобання користувачів за допомогою неявного зворотного зв'язку.

На відміну від попередніх, система на основі моделі HGAT (Hierarchical Graph Attention Network) [3] враховує зв'язки між сутностями. Для створення потрібно побудувати гетерогенний граф з трьома типами вузлів («Користувач», «Рецепт» та «Інгредієнт») та чотирма типами зв'язків («Інгредієнт - Інгредієнт», «Рецепт - Інгредієнт», «Рецепт - Рецепт», «Користувач - Рецепт»). З цього випливає, що моделювання відношень тут явне, тобто модель не просто шукає схожі рецепти, а навчається розуміти складну мережу

зв'язків між користувачами, рецептами та інгредієнтами, що робить такий підхід більш точним.

З розвитком штучного інтелекту (ШІ) також з'являються рекомендаційні системи з ШІ [4]. Це дозволяє не лише рекомендувати рецепти на основі текстового опису, а й розпізнавати інгредієнти за зображенням страви чи давати поради щодо приготування. Однією з таких систем є KERL [5]. Вона аналізує запит, витягуючи ключові сутності такі, як інгредієнти та вподобання користувача. Потім вона шукає інформацію з графа знань за допомогою LLM і генерує рецепт.

Таким чином, проведений аналіз розглядає переваги різноманітних кулінарних рекомендаційних систем: від базової гібридної фільтрації до складних архітектур на основі великих мовних моделей. Найбільш перспективним напрямом є інтеграція графів знань із LLM, оскільки це використати гнучкість генеративного штучного інтелекту для створення персоналізованого кулінарного досвіду.

Список використаних джерел:

1. Verma V. P. Recipes Recommendation System using Machine Learning. *International Journal for Research in Applied Science and Engineering Technology*. 2025. Vol. 13, no. 5. P. 3583–3587. URL: <https://doi.org/10.22214/ijraset.2025.71001>
2. Widiyanti N. P. T., Suarjaya I. M. A. D., Rusjayanthy N. K. D. Food Recipe Recommendation System with Content-Based Filtering and Collaborative Filtering Methods. *Sinkron*. 2025. Vol. 9, no. 3. P. 1167–1776. URL: <https://doi.org/10.33395/sinkron.v9i3.14778>
3. Recipe Recommendation With Hierarchical Graph Attention Network / Y. Tian et al. *Frontiers in Big Data*. 2022. Vol. 4. URL: <https://doi.org/10.3389/fdata.2021.778417>
4. A M. H. Survey on AI-based Recipe Recommendation, Retrieval, and Generation Systems. *International Journal for Research in Applied Science and Engineering Technology*. 2025. Vol. 13, no. 12. P. 2400–2416. URL: <https://doi.org/10.22214/ijraset.2025.76350>
5. Mohbat F., Zaki M. J. KERL: Knowledge-Enhanced Personalized Recipe Recommendation using Large Language Models. *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, Vienna, Austria. Stroudsburg, PA, USA, 2025. P. 19125–19141. URL: <https://doi.org/10.18653/v1/2025.acl-long.938>.

УДК 004.7

*Галух А. О., магістрант
Бондарчук В. О., магістрант*

*Онищук О. О., кандидат технічних наук, доцент
Волинський національний університет імені Лесі Українки*

ПОРІВНЯННЯ ПРОТОКОЛУ HTTP І ТЕХНОЛОГІЇ WEBSOCKET У СУЧАСНИХ ВЕБСИСТЕМАХ

Актуальність дослідження зумовлена широким використанням веб орієнтованих систем у фінансових сервісах, електронній комерції, онлайн-моніторингу, ігрових платформах та IoT-рішеннях. У таких середовищах критичними є затримка передачі даних, стабільність з'єднання та рівень кіберзахисту. Неправильний вибір протоколу може призвести до перевантаження мережі, зниження продуктивності або зростання ризиків безпеки [1-5].

Метою роботи є порівняння протоколу HTTP та технології WebSocket з урахуванням обсягу переданих даних, швидкодії та кібербезпеки, а також визначення доцільних сфер їх використання [2].

Методика дослідження базується на аналізі архітектурних особливостей протоколів, принципів встановлення та підтримки з'єднання, оцінці накладних витрат на передачу даних і розгляді механізмів захисту інформації.

Результати. HTTP використовує модель «запит–відповідь», за якої кожна взаємодія між клієнтом і сервером потребує окремого запиту. Навіть із застосуванням оптимізацій цей підхід супроводжується передачею службових заголовків, що збільшує трафік і затримки. Така модель є ефективною для систем з помірною інтенсивністю обміну даними.

WebSocket після початкового HTTP-рукошлякування встановлює постійне двостороннє з'єднання, що дозволяє передавати повідомлення без повторних запитів. Це суттєво зменшує затримки та накладні витрати, що є перевагою для систем реального часу (рис.1).

У контексті кібербезпеки HTTP має розвинену інфраструктуру захисту, тоді як WebSocket потребує додаткових механізмів контролю з'єднань і запобігання зловживанням через тривалі сесії. Для HTTP характерна простіша інтеграція з балансувальниками навантаження та кешувальними механізмами, що полегшує горизонтальне масштабування. WebSocket, у свою чергу, потребує підтримки стану з'єднань і додаткових ресурсів сервера, однак забезпечує вищу ефективність у сценаріях з великою кількістю одночасних клієнтів та частими оновленнями даних у режимі реального часу.

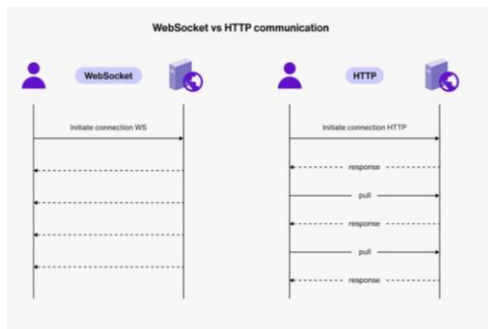


Рис.1 Порівняння WebSocket та HTTP протоколи

Висновки. HTTP доцільно використовувати у вебсистемах із помірними вимогами до швидкодії та підвищеною увагою до стандартних механізмів безпеки. WebSocket є ефективним для застосунків реального часу з інтенсивним обміном даними, проте вимагає ретельного проектування системи кіберзахисту. Вибір технології повинен базуватися на комплексному аналізі вимог до продуктивності, обсягу трафіку та рівня безпеки.

Список використаних джерел:

1. **WebSockets vs HTTP** [Електронний ресурс]. – Ably. – Режим доступу: <https://ably.com/topic/websockets-vs-http>
2. **WebSockets vs HTTP: Key differences explained** [Електронний ресурс]. – Postman Blog. – Режим доступу: <https://blog.postman.com/websockets-vs-http-key-differences-explained/> (дата звернення: 02.03.2026).
3. **WebSockets API Documentation** [Електронний ресурс]. – Mozilla Developer Network. – Режим доступу: https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API
4. **HTTP long polling vs WebSockets** [Електронний ресурс]. – Medium. – Режим доступу: <http://medium.com/@dmosyan/http-long-polling-vs-websockets-dadab8f7f26f>.
5. **WebSocket vs HTTP: What you need to know** [Електронний ресурс]. – Digital Samba Blog. – Режим доступу: <https://www.digitalsamba.com/blog/websocket-vs-http>
6. **What is WebSocket and how it is different from the HTTP** [Електронний ресурс]. – GeeksforGeeks. – Режим доступу: <https://www.geeksforgeeks.org/web-tech/what-is-web-socket-and-how-it-is-different-from-the-http/> (дата звернення: 02.03.2026).

УДК 004.7

Венгловська Ю.В., викладач*Державний університет «Житомирська політехніка»***ВПЛИВ КОМП'ЮТЕРНИХ ІГОР НА КРЕАТИВНІСТЬ**

Швидке зростання популярності комп'ютерних ігор серед молоді та дітей зумовлює необхідність дослідити їх потенційний вплив на різні сфери розвитку особистості, зокрема на креативність.

Креативність – це складне і багатогранне поняття, яке привернуло увагу дослідників з різних дисциплін. В основі творчості лежить генерування нових і корисних ідей, продуктів або рішень проблем. З огляду на її важливість для стимулювання інновацій, вирішення проблем і адаптивності, розуміння природи творчості та факторів, що сприяють її розвитку, стало важливою областю досліджень у психології, освіті та менеджменті [1].

Дослідження в сфері комп'ютерних ігор показують, що мотивація гравців відіграє вирішальну роль у підвищенні креативності. Ігри з відкритим світом зазвичай забезпечують більшу свободу і гнучкість, приваблюючи гравців, які бажають виразити себе. Підкреслюючи роль викликів та автономії, стає очевидним, що ігри, розроблені для просування цих елементів, можуть значно підвищити творчу продуктивність гравців. Ігри з подібним форматом є хорошим прикладом цього, бо вони надають гравцям свободу досліджувати та створювати, що вказує на те, що принципи дизайну ігор можуть ефективно використовувати внутрішні мотивації гравців [2].

Ігри можна вважати штучним середовищем, в якому задоволення гравця є пріоритетом, а не точне відтворення реального світу. Хоча незвичайна або шкідлива поведінка в реальному житті може мати довгострокові, можливо негативні наслідки, ігри надають безпечний простір для експериментів. Ці характеристики створюють середовище, сприятливе для творчості в іграх; можливі взаємодії в іграх визначають діапазон розумових здібностей, які можна розвивати. Різні ігри поєднують стратегічні, експресивні, реактивні або соціальні елементи, кожна з яких має своє особливе поєднання та акцент. Тому вибір гри, яка доповнює поточні здібності та захоплення конкретного гравця, є критично важливим, що дозволяє досягти більш значного зростання або дослідження нових розумових просторів [3].

Результати глобального опитування, що представлені на рис. 1, показують, що більшість респондентів відзначають позитивний вплив комп'ютерних ігор на психоемоційний стан і соціальну взаємодію. Зокрема, 81% опитаних вказують на ментальну стимуляцію, 80% – на

зниження стресу, а 78% — на створення доступного середовища для людей з різними можливостями. Крім того, понад 70% респондентів зазначають підвищення відчуття щастя, зменшення тривожності, можливість відволікання від повсякденних труднощів та налагодження нових соціальних зв'язків.

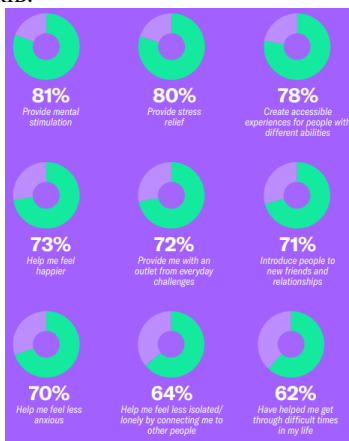


Рис. 1. Результати глобального опитування [4]

Таким чином, отримані дані свідчать про загалом позитивний вплив комп'ютерних ігор на когнітивну, емоційну та соціальну сфери розвитку особистості.

Список використаних джерел:

1. Mercier M., Bourgeois-Bougrine S., Lubart T. Games and Creativity: A Theoretical Framework. *Journal of Intelligence*. 2026. Vol. 14, no. 2. P. 21. URL: <https://doi.org/10.3390/jintelligence14020021>.
2. Cheng Y. The impact of online games on creativity and the role of imagination // *Frontiers in Behavioral Neuroscience*. 2025. Vol. 19. Article 1561548. DOI: 10.3389/fnbeh.2025.1561548.
3. Ganter-Argast C., Schipper M., Shamsrizi M., Stein C., Khalil R. The light side of gaming: creativity and brain plasticity // *Frontiers in Human Neuroscience*. 2024. Vol. 17. Article 1280989. DOI: 10.3389/fnhum.2023.1280989.
4. Entertainment Software Association (ESA). Power of Play: 2025 Global Video Games Report. Washington, D.C.: Entertainment Software Association, 2025. URL: <https://www.theesa.com/wp-content/uploads/2025/09/PoP-2025-v10-web-spreads.pdf>

УДК 005.8:004.4

*Шабуня Д.Є., здобувач,
Шеховцова В.І., к. пед. н., доцент
Харківський національний університет радіоелектроніки*

ПІДХОДИ ДО РОЗРОБКИ ІТ-СЕРВІСУ З ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ЗАХОДІВ ВОЛОНТЕРСЬКОЇ ОРГАНІЗАЦІЇ

Згідно із законодавством України, волонтерська діяльність є добровільною, соціально спрямованою та неприбутковою формою благодійності, що відіграє критичну роль у вирішенні суспільних криз [1]. В сучасних умовах ефективність діяльності волонтерських об'єднань безпосередньо залежить від якості координації людських та матеріальних ресурсів під час реалізації гуманітарних, соціальних чи освітніх проєктів. Процес організації заходів у волонтерському середовищі характеризується високою динамічністю, необхідністю швидкого залучення великої кількості учасників та координації дій у реальному часі. Використання розрізаних інструментів (месенджерів, електронних таблиць) призводить до втрати даних та зниження операційної ефективності, що зумовлює актуальність розробки спеціалізованого ІТ-сервісу для автоматизації життєвого циклу заходів [2]. В основі розробки ІТ-сервісу лежить аналіз бізнес-процесів волонтерської організації, що включає етапи планування, реєстрації, проведення та формування звітності. сервіс проєктованої інформаційної системи (ІС) має забезпечувати рольову модель доступу, де адміністратори керують глобальним календарем, координатори здійснюють розподіл задач, а волонтери отримують персоналізовані сповіщення та доступ до інструкцій. Для вибору оптимальної стратегії автоматизації було проведено порівняльний аналіз методів управління івентами (табл. 1). Архітектурне рішення модуля базується на використанні сучасних веб технологій та клієнт-серверної взаємодії. Для надійного збереження та обробки даних про користувачів та події доцільно використовувати реляційні СУБД (наприклад, Oracle), що гарантують цілісність інформації. Проектування інтерфейсу (Frontend) у середовищі Figma з використанням принципів адаптивного дизайну забезпечує зручність роботи як зі стаціонарних комп'ютерів координаторів, так і з мобільних пристроїв волонтерів «у полі» [3].

Важливим аспектом є інтеграція модуля з хмарними сервісами та зовнішніми API. Використання Google Calendar API дозволяє синхронізувати розклад заходів із особистими календарями учасників, а впровадження системи автоматичних сповіщень через API месенджерів мінімізує ризики низької явки волонтерів [4]. Забезпечення

безпеки персональних даних реалізується через шифрування каналів зв'язку та впровадження механізмів автентифікації, що відповідає вимогам законодавства щодо захисту інформації [5].

Таблиця 1 – Порівняльний аналіз методів управління заходами волонтерської ІС

Параметр порівняння	Ручне управління	Загальні CRM-системи	Спеціалізований модуль
Швидкість обробки заявок	Низька	Середня	Висока (автоматична)
Контроль за волонтерами	Ускладнений	Частковий	Повний (через статуси)
Гнучкість налаштувань	Висока	Низька	Висока (під специфіку ГО)
Можливість аналітики	Відсутня	Обмежена	Повна (KPI заходів)

Очікуваним результатом впровадження розробленого модуля є створення єдиного інформаційного простору для всіх учасників заходу, що дозволяє скоротити час на адміністрування на 30–40% та підвищити прозорість розподілу волонтерських ресурсів. Таким чином, розробка спеціалізованого ІТ-сервісу є необхідним кроком для масштабування діяльності волонтерської організації в умовах сучасних викликів.

Список використаних джерел:

1. Закон України «Про волонтерську діяльність» від 19.04.2011 № 3236-VI. URL: <https://zakon.rada.gov.ua/laws/show/3236-17> (дата звернення: 19.03.2026)
2. Digital Transformation for Nonprofits. TechSoup Europe. URL: <https://www.techsoupeurope.org/digital-transformation-for-nonprofits/> (дата звернення: 19.03.2026)
3. Figma Documentation: Best Practices for UI Design. URL: <https://help.figma.com/> (дата звернення: 19.03.2026)
4. Google Calendar API Guide. URL: <https://developers.google.com/calendar/api/guides/overview> (дата звернення: 19.03.2026)
5. Закон України «Про захист персональних даних». URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 19.03.2026)

УДК 004.5:004.89

*Романенко С.О., старший викладач
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут*

ІНТЕЛЕКТУАЛЬНА АДАПТАЦІЯ ІНТЕРФЕЙСІВ КОРИСТУВАЧА НА ОСНОВІ ПОВЕДІНКОВОЇ АНАЛІТИКИ ТА МЕТОДІВ МАШИННОГО НАВЧАННЯ

Сучасні інформаційні системи відзначаються складністю функціональних можливостей, високою інтеграцією компонентів та різноманіттям користувацьких сценаріїв. Зі збільшенням функціональної насиченості програмного забезпечення ускладнюються інтерфейси користувача. Традиційні статичні інтерфейси, однакові для всіх користувачів, часто не забезпечують достатньої зручності та ефективності взаємодії. Оскільки користувачі відрізняються рівнем підготовки та досвідом роботи з системами, виникає потреба у нових підходах до проектування інтерфейсів. Перспективним є застосування адаптивних інтерфейсів, які змінюють структуру та відображення елементів залежно від поведінки користувача та контексту використання.

У роботі розглянуто підхід до побудови інтелектуальної системи адаптації інтерфейсів користувача на основі аналізу поведінкових даних, що формуються під час взаємодії з програмним середовищем. Запропонована модель передбачає збір і обробку інформації про дії користувача, зокрема частоту використання функцій, тривалість виконання операцій, послідовність навігаційних дій та кількість помилок. Отримані дані використовуються для аналізу поведінки користувачів і визначення типових моделей взаємодії з інформаційною системою. На основі цих результатів формується персоналізований профіль користувача, що відображає його рівень підготовки, типові сценарії роботи та особливості взаємодії із програмним забезпеченням.

Для аналізу поведінкових даних доцільно застосовувати методи машинного навчання, які автоматизують виявлення закономірностей у великих обсягах інформації. Зокрема, використовуються алгоритми кластеризації, класифікації та прогнозування. Кластеризація дозволяє виділяти групи користувачів із подібними моделями поведінки та формувати типові профілі взаємодії, що сприяє оптимізації структури інтерфейсу для різних категорій користувачів. Класифікація визначає тип користувача на основі поточної поведінки, а алгоритми прогнозування передбачають найбільш ймовірні подальші дії у певному

контексті. Використання цих методів дозволяє системі адаптації приймати обґрунтовані рішення щодо модифікації інтерфейсу.

На основі отриманих результатів система адаптації може автоматично змінювати структуру інтерфейсу, оптимізувати порядок відображення елементів, пропонувати користувачу релевантні функції та спрощувати навігацію у програмному середовищі. Зокрема, найбільш використовувані елементи можуть переміщуватися у доступніші області екрана, тоді як рідко використовувані функції — приховуватися або переноситися у додаткові меню. Такий підхід дозволяє зменшити перевантаження інтерфейсу та підвищити швидкість виконання типових операцій.

Запропонований підхід сприяє підвищенню ефективності взаємодії користувачів з інформаційними системами, зменшенню кількості помилок та зниженню когнітивного навантаження. Використання поведінкової аналітики та методів машинного навчання створює передумови для формування інтелектуальних інтерфейсів нового покоління, здатних адаптуватися до індивідуальних потреб користувачів у режимі реального часу. Такі рішення можуть бути застосовані у вебзастосунках, корпоративних інформаційних системах та освітніх платформах.

Подальші дослідження у цьому напрямі можуть бути спрямовані на інтеграцію запропонованої моделі з сучасними вебтехнологіями, хмарними платформами та системами великих даних. Це дозволить забезпечити масштабованість рішень та їх застосування у великих розподілених інформаційних системах. Окрім цього, перспективним напрямом є використання методів глибинного навчання та нейронних мереж для більш точного прогнозування поведінки користувачів і автоматичної оптимізації інтерфейсів у складних програмних середовищах. Також доцільним є дослідження можливостей інтеграції адаптивних інтерфейсів з системами підтримки прийняття рішень та інтелектуальними аналітичними платформами, що відкриває нові перспективи розвитку інтелектуальних інформаційних технологій.

Список використаних джерел:

1. Norman D. A. The Design of Everyday Things. Revised and expanded edition. New York: Basic Books, 2013. 368 p.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge: MIT Press, 2016. 775 p.

УДК 004.8:004.65

Лі Н.Д.
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
Кобилін І.О.
к.т.н., асистент кафедри Інформатики,
Харківський національний університет радіоелектроніки

ГІБРИДНИЙ МЕТОД ВИЯВЛЕННЯ ДУБЛІКАТИВ WORKFLOW ДЛЯ LORA-МОДЕЛЕЙ НА ОСНОВІ СТРУКТУРНОГО ТА ПОВЕДІНКОВОГО АНАЛІЗУ

Активний розвиток генеративних моделей штучного інтелекту, зокрема моделей типу Stable Diffusion та LoRA (Low-Rank Adaptation), призвів до появи великої кількості workflow генерації зображень, що поширюються через різноманітні онлайн-платформи. Workflow таких систем зазвичай представляють собою графи обчислювальних операцій, які описують послідовність обробки даних у системах генерації зображень. Однак значна кількість опублікованих workflow є повними або частковими дублікатами вже існуючих рішень. Це ускладнює навігацію по репозиторіях, знижує якість каталогів моделей та створює проблему ідентифікації оригінальних рішень.

Існуючі підходи до виявлення дублікативного контенту в основному базуються на прямому порівнянні структур даних або на аналізі результатів генерації. Структурні методи аналізують топологію графів workflow, що дозволяє швидко визначати ідентичні або близькі за структурою рішення. Поведінкові методи, у свою чергу, аналізують результати виконання workflow та порівнюють отримані зображення за допомогою методів комп'ютерного зору. Кожен із цих підходів має власні обмеження: структурні методи можуть не враховувати функціональну еквівалентність різних графових структур, тоді як поведінкові методи потребують значних обчислювальних ресурсів.

Метою роботи є розробка гібридного методу виявлення дублікатів workflow для LoRA-моделей, що поєднає структурний аналіз графів та поведінкову оцінку результатів генерації зображень.

На першому етапі workflow, представлені у форматі JSON, перетворюються у орієнтований граф, де вузли відповідають обчислювальним операціям, а ребра — потокам даних між ними. Для забезпечення незалежності від внутрішніх ідентифікаторів вузлів виконується канонізація графової структури, що включає нормалізацію атрибутів вузлів та топологічне сортування графа. Після цього формується структурний відбиток workflow за допомогою

криптографічного хешування (SHA-256) та алгоритму SimHash, що дозволяє виявляти як точні дублікати, так і структурно подібні графи.

На другому етапі здійснюється поведінковий аналіз workflow. Для цього кожен workflow виконується на фіксованому наборі тестових параметрів генерації (prompts та seed). Згенеровані зображення перетворюються у компактні векторні представлення (ембединги) за допомогою моделей візуального кодування, зокрема CLIP. Отримані векторні представлення агрегуються у поведінковий відбиток workflow. Подібність між workflow визначається за допомогою косинусної міри між відповідними векторами ознак.

Список використаних джерел:

1. Hu E. et al. LoRA: Low-Rank Adaptation of Large Language Models // arXiv preprint arXiv:2106.09685.
2. Radford A. et al. Learning Transferable Visual Models From Natural Language Supervision // Proceedings of ICML, 2021.
3. Charikar M. Similarity Estimation Techniques from Rounding Algorithms // Proceedings of STOC, 2002.
4. Cormen T. Introduction to Algorithms. – MIT Press, 2009.

УДК 004

*Хіхло Іван Дмитрович, студент
Кунун Тетяна Василівна, кандидат технічних наук
Національний університет «Одеська Політехніка»*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасному інформаційному суспільстві стрімкий розвиток цифрових технологій сприяв активному впровадженню штучного інтелекту (ШІ) в різні інформаційні системи (ІС). Поширення даних, що генеруються щодня, вимагає нових методологій їх обробки, аналізу та використання. Це підкреслює ключову роль штучного інтелекту в підвищенні ефективності ІС. Його застосування сприяє автоматизації складних процесів, підвищує якість аналізу інформації та прискорює прийняття управлінських рішень.

ШІ визначається як сукупність методів і технологій, що дозволяють комп'ютерним системам імітувати певні аспекти людського інтелекту. Ці можливості охоплюють навчання на основі даних, аналіз і розпізнавання зображень, обробку природної мови, прогнозування та прийняття рішень. У сфері ІС ШІ знаходить застосування в оптимізації продуктивності програмного забезпечення, автоматизації обробки інформації та підвищенні продуктивності різних технологічних процесів.

Машинне навчання є ключовим елементом ШІ. Ця технологія дозволяє ІС аналізувати великі масиви даних, виявляти приховані закономірності та формувати прогнози. Як наслідок, системи мають здатність постійно підвищувати свою продуктивність, що стає можливим завдяки накопиченню досвіду. Алгоритми машинного навчання широко застосовуються для аналізу поведінки користувачів у мережі, прогнозування економічних показників, функціонування систем рекомендацій тощо.

Іншою важливою сферою застосування ШІ в ІС є обробка природної мови. Ці технології дають комп'ютерам можливість аналізувати текстову інформацію, розшифровувати зміст повідомлень та зручно взаємодіяти з користувачами. Ці технології є основою для розробки таких складних інструментів, як чат-боти, голосові помічники, системи автоматичного перекладу та інтелектуальні пошукові системи. Цей розвиток має потенціал значно спростити доступ до інформації та поліпшити взаємодію між людьми та комп'ютерними системами.

Використання ШІ стало поширеним у різних сферах діяльності. У фінансовому секторі впровадження ІС, що використовують ШІ, дозволило аналізувати транзакції та виявляти підозрілі операції, що

сприяє більш ефективному запобіганню шахрайству. У медичній галузі ІІІ використовується для аналізу медичних зображень, підтримки діагностики та прогнозування розвитку захворювань. У промисловому контексті інтелектуальні ІС відіграють ключову роль в оптимізації виробничих процесів, забезпеченні якості продукції та прогнозуванні потенційних технічних несправностей обладнання.

Важливою сферою застосування ІІІ є інформаційна безпека. У сучасному світі, де ІС піддаються безлічі кіберзагроз, використання інтелектуальних алгоритмів стало ключовою стратегією для швидкого виявлення аномальної активності в мережі, комплексного аналізу загроз та проактивного запобігання кібератакам. Очікується, що цей захід підвищить безпеку інформаційних ресурсів та зменшить ризик витоку конфіденційних даних.

Незважаючи на значні переваги, впровадження ІІІ в ІС супроводжується певними проблемами та викликами. Значний виклик стосується сфери захисту персональних даних та конфіденційності інформації. З огляду на поширеність алгоритмів ІІІ в обробці значних обсягів даних, надзвичайно важливо встановити надійні заходи безпеки та дотримуватися етичних стандартів при використанні інформації. Крім того, важливим питанням є прозорість алгоритмів ІІІ. У багатьох випадках складні моделі машинного навчання працюють за принципом «чорного ящика», що ускладнює розуміння процесу прийняття рішень системою. Це може призвести до ускладнень у сферах, де точність і підзвітність результатів ІС є обов'язковими.

Отже, інтеграція ІІІ в сферу ІС стає ключовою областю розвитку сучасних інформаційних технологій. Інтеграція інтелектуальних алгоритмів має потенціал для підвищення ефективності обробки даних, автоматизації складних процесів та створення нових можливостей для розвитку цифрових послуг. Подальший розвиток ІІІ сприятиме створенню більш інтелектуальних, адаптивних та безпечних ІС. Ці системи відіграватимуть важливу роль у розвитку інформаційного суспільства.

Список використаних джерел:

1. Пилипчук В. В., Попов М. О. Напрями використання інструментарію штучного інтелекту для аналізу розвідувальної інформації [Електронний ресурс]. Сучасні інформаційні технології у сфері безпеки та оборони. – 2025.
2. Тимошенко Л. Аспекти використання штучного інтелекту в сучасних інформаційних технологіях і управлінні виробництвом [Електронний ресурс] // Інформаційні технології в металургії та машинобудуванні. – 2024.

УДК 004.02

*Кожанов Андріан Євгенійович, аспірант,
Євланов Максим Вікторович, д.т.н., професор
Харківський національний університет радіоелектроніки*

ВДОСКОНАЛЕННЯ МЕТОДУ СИНТЕЗУ ОПИСУ АРХІТЕКТУРИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Процес управління конфігурацією є одним з найважливіших процесів життєвого циклу інформаційних систем (ІС) управління підприємствами та організаціями. У цьому процесі виділяється задача ідентифікації конфігурації. Вона пов'язана із визначенням системних елементів, які є елементами конфігурації («Configuration item», CI). Рішення цієї задачі встановлюють та підтримують основу для контролю та обліку стану ІС та її CI протягом усіх їхніх життєвих циклів [1].

Теоретичні та прикладні основи систем управління конфігурацією ІС та інших ІТ-продуктів визнано в цілому сформованими [1, 2]. Але ці основи не вільні від недоліків. Головним з них є концептуальність представлення цих основ [1]. Одним із підходів до подолання цього недоліку є пропозиція відмовитися від єдиного опису CI протягом усього життєвого циклу ІС. Ця відмова дає змогу розглядати задачу ідентифікації конфігурації ІС як сукупність таких задач:

- задача ранньої ідентифікації CI (результатом вирішення якої є множина CI як архітектурних сутностей ІС, виділених за результатами аналізу добре сформульованих вимог до цієї системи);
- задача проектної ідентифікації CI;
- задача ідентифікації CI під час реалізації.

В процесі дослідження було вирішено розглядати опис архітектури ІС та сутностей цієї архітектури як результат задачі синтезу варіанта опису раціональної архітектури ІС. Цю задачу у [3] запропоновано описати теоретико-ігровою моделлю вигляду

$$\Gamma_{IS} = \langle \{Pr, U\}, \{X^{\{Pr, U\}}\}, \{f^{\{Pr, U\}}\} \rangle \quad (1)$$

де Γ_{IS} – позначення гри Постачальника та Споживача ІТ-послуг (функцій ІС); $\{Pr, U\}$ – множина гравців, які беруть участь у грі Γ_{IS} (Постачальник та Споживач відповідно); $\{X^{\{Pr, U\}}\}$ – множина стратегій гри Γ_{IS} , яка формується на основі множини варіантів описів архітектури створюваної ІС IT_{act} ; $\{f^{\{Pr, U\}}\}$ – множина функцій виграшу гри Γ_{IS} [3].

Для знаходження результату гри (1) у [3] було запропоновано використовувати метод пошуку рівноваг Неша для біматричної гри в чистих стратегіях. Результатом застосування цього методу є опис архітектури створюваної ІС як множини окремих функцій цієї ІС. Але такий детальний опис архітектури значно ускладнює подальший розподіл опису архітектури ІС між окремими командами Постачальника. Тому необхідно вдосконалити цей метод з метою зменшення кількості СІ в описі архітектури ІС.

Вдосконалений метод передбачає виконання таких етапів.

Етап 1. Виділити окремі архітектурні сутності ІС як результат вирішення задачі кластеризації описів окремих функцій даної ІС.

Етап 2. Сформувати матриці виграшів Споживача й Постачальника.

Етап 2. Відзначити максимальні елементи в кожному стовпці матриці виграшів Споживача. Якщо в деякому стовпці даної матриці кілька максимальних елементів, то необхідно відзначити всі такі елементи.

Етап 3. Відзначити максимальні елементи в кожному рядку матриці виграшів Постачальника. Якщо в деякому рядку даної матриці кілька максимальних елементів, то необхідно відзначити всі такі елементи.

Етап 4. Провести пошук перетинання результатів Етапу 2 і Етапу 3.

Етап 5. Якщо результат виконання Етапу 4 не є порожньою множиною, зафіксувати відповідні варіанти описів архітектури створюваної ІС як описи раціональної архітектури даної ІС. У іншому випадку визнати, що опису раціональної архітектури ІС на чистих стратегіях не існує. Завершити застосування методу.

Список використаних джерел:

1. Quigley J.M., Robertson K.L. Configuration Management, Second Edition: Theory and Application for Engineers, Managers, and Practitioners. New York, 2019. Auerbach Publications. 453 p.
2. Farayola O.A., Hassan A.O., Adaramodu O.R., Fakeyede O.G., Oladeinde M. Configuration management in the modern era: best practices, innovations, and challenges. *Computer Science & IT Research Journal*. 2023. Vol. 4, No 2. P. 140-157.
3. Evlanov M. Development of the model and method of selecting the description of rational architecture of information system. *Eastern-European Journal of Enterprise Technologies*. 2016. Vol. 1, No. 2(79). P. 4–12.
4. Kozhanov A., Ievlanov M. (2026). Definition a clusterization method to solve the task of early identification of IT product configuration elements. *Eastern-European Journal of Enterprise Technologies*. 2026. Vol. 1, No. 2 (139). P. 77–90.

УДК 004.7

Кунун Т.В., к.т.н., ст. викладач,

Сидоров ЮМ., здобувач,

Національний університет «Одеська політехніка»

ADMINISTRATOR UTILITY: УТИЛІТА ЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ СИСТЕМНИМИ ОБМЕЖЕННЯМИ WINDOWS

В роботі розглянута створення прикладної утиліти для системних адміністраторів, яка дозволяє централізовано керувати службами, політиками безпеки та апаратними обмеженнями операційної системи Windows з одного інтерфейсу.

Застосунок має модульну архітектуру, побудовану на розділенні відповідальностей між окремими бібліотеками (assemblies). Кожен модуль відповідає за окремий аспект роботи програми, що спрощує підтримку та розширення функціоналу.

Основні модулі застосунку

AdministratorUtility - основний виконуваний застосунок, що відповідає за ініціалізацію інтерфейсу користувача.

AdministratorUtility.Core - бізнес-логіка, пов'язана з керуванням службами, пристроями та обробкою адміністративних операцій.

AdministratorUtility.Mvvm - інфраструктура MVVM, базові ViewModel, механізми обміну повідомленнями між компонентами.

AdministratorUtility.Windows - інкапсульований доступ до можливостей Windows API.

AdministratorUtility.Storage - робота з локальною базою даних SQLite.

AdministratorUtility.FileStorage - збереження та експорт даних у файлові формати.

AdministratorUtility.Translations - підтримка багатомовного інтерфейсу.

AdministratorUtility.Shared - спільні структури даних та допоміжні утиліти.

Такий розподіл дозволяє ізолювати системну логіку від інтерфейсу користувача та забезпечує чисту архітектуру застосунку.

Для реалізації адміністративного функціоналу застосунок використовує можливості Windows API. Доступ до системних функцій здійснюється через спеціалізований модуль, що дозволяє інкапсулювати виклики API та забезпечити безпечну і контрольовану взаємодію з операційною системою. Застосунок використовує Windows API для: керування станом та типом запуску служб Windows; отримання інформації про апаратні пристрої та їхні класи; увімкнення та вимкнення пристроїв.

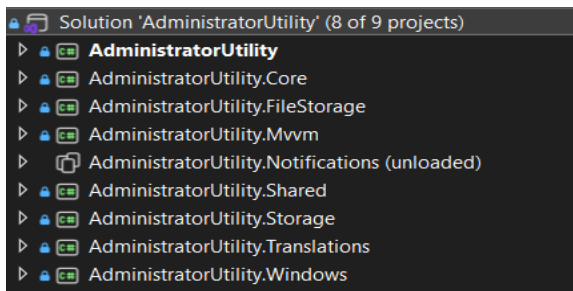


Рисунок 1 – Структура проекту

Такий підхід дозволяє реалізувати необхідний функціонал без прямого втручання користувача в системні інструменти.

Графічний інтерфейс застосунку реалізований з урахуванням зручності та швидкості роботи системного адміністратора. Інтерфейс поділений на вкладки відповідно до типів керованих об'єктів.

Основні вкладки застосунку:

Favorites - швидкий доступ до обраних служб і пристроїв;

Services - керування службами Windows;

Devices - керування пристроями та класами пристроїв;

Logs - перегляд журналу адміністративних дій;

Окремо передбачено вікно налаштувань застосунку (Settings), яке дозволяє адаптувати інтерфейс під потреби користувача.

Користувач може обрати мову інтерфейсу (українська або англійська), а також тему оформлення - системну, світлу або темну.

Застосунок надає можливість перегляду списку системних служб Windows та виконання над ними основних адміністративних дій. Користувач може змінювати стан служб, тип їх запуску або видалити з PC, відкривати розташування служби в реєстрі та файловій системі, а також додавати служби до списку обраних. Інформація про служби може бути збережена у файли різних форматів для подальшого аналізу або звітності.

Застосунок дозволяє переглядати класи пристроїв та пов'язані з ними апаратні компоненти. Передбачено можливість увімкнення та вимкнення пристроїв, перегляду інформації в системному реєстрі, додавання пристроїв до списку обраних та експорту даних у файл.

Список використаних джерел:

1. Griffiths I. Programming C# 10: Build Cloud, Web, and Desktop Applications. Sebastopol : O'Reilly Media, 2022. P. 810.
2. Martin R. C. Clean Architecture: A Craftsman's Guide to Software Structure and Design. Boston : Prentice Hall, 2017. P. 432.
3. Microsoft. .NET documentation [Електронний ресурс]. Режим доступу: <https://learn.microsoft.com/dotnet>

УДК 004.7

Кунун Т.В., к.т.н., ст. викладач,

Білоусов Д.О., здобувач,

Національний університет «Одеська політехніка»

ЕКСПЕРТНА СИСТЕМА ДЛЯ ПРОГНОЗУВАННЯ РІВНЯ ЗАБРУДНЕННЯ ПОВІТРЯ У МІСТІ

Інтенсивний розвиток міської інфраструктури та промисловості створює значне навантаження на екосистему, що безпосередньо загрожує здоров'ю мешканців мегаполісів. Традиційні системи екологічного моніторингу зазвичай фіксують забруднення вже за фактом, тоді як для реального захисту населення необхідне випереджувальне прогнозування. Актуальність дослідження полягає у необхідності переходу від простої фіксації даних до автоматизованого передбачення небезпечних станів атмосфери.

Для вирішення цього завдання запропоновано використання технологій штучного інтелекту, а саме експертної системи. Таке рішення дозволяє обробляти різнотипні вхідні дані та знаходити приховані залежності. Архітектура системи базується на гібридній моделі знань: використання фреймів для опису об'єктів та продукційних правил для побудови логічних висновків.

Метою проекту є створення програмного прототипу, який здатний не лише оцінювати поточний стан повітря, а й прогнозувати його зміни та генерувати попередження для користувачів.

У процесі роботи отримано такі результати:

1. Спроектовано базу знань із правилами для прогнозування небезпеки та надання рекомендацій у різних ситуаціях, наприклад, при смогу чи аваріях;

2. Реалізовано алгоритм, який послідовно аналізує факти про погоду та викиди і автоматично робить висновок про якість повітря;

3. Розроблено веб-сайт, де користувач може побачити прогноз забруднення, дізнатися його причину та отримати інструкцію дій.

Для створення системи використовували такі технології:

Python - основна мова, яку обрали для написання коду проекту.

Experta - бібліотека, що дозволила реалізувати логіку експертної системи.

Streamlit - інструмент для швидкої побудови зручного веб-інтерфейсу.

Pandas - засіб для обробки вхідних даних у форматі CSV.

Система працює як цілісний механізм: користувач вводить дані, машина логічного виведення аналізує їх на основі знань і фактів,

формує результати та рекомендації, а підсистема пояснень демонструє логіку прийнятих рішень. Крім того, запропонована система може бути масштабована для використання у різних містах із урахуванням їхніх специфічних екологічних умов та джерел забруднення. Інтеграція з відкритими метеорологічними сервісами та датчиками якості повітря дозволяє забезпечити постійне оновлення даних і підвищити точність прогнозування. Важливою перевагою є можливість адаптації бази знань шляхом додавання нових правил, що робить систему гнучкою та придатною до подальшого розвитку.

Перспективи вдосконалення проєкту включають використання методів машинного навчання для підвищення точності прогнозів, а також розширення функціоналу за рахунок мобільних застосунків і систем сповіщення в реальному часі. Це дозволить оперативніше інформувати населення про потенційні загрози та сприятиме зменшенню негативного впливу забрудненого повітря на здоров'я людей.

У результаті реалізації проєкту створено інструмент підтримки прийняття рішень, який забезпечує раннє виявлення екологічних загроз. Система дозволяє автоматизувати аналіз даних та надавати своєчасні рекомендації для мінімізації негативного впливу на здоров'я населення.

Список використаних джерел:

1. Ambient (outdoor) air quality [Електронний ресурс] / World Health Organization (WHO). – Режим доступу: [https://www.who.int/news-room/fact-sheets/detail/ambient-\(outdoor\)-air-quality-and-health](https://www.who.int/news-room/fact-sheets/detail/ambient-(outdoor)-air-quality-and-health) (дата звернення 25.01.2025).
2. Expert System [Електронний ресурс] / Encyclopedia Britannica. – Режим доступу: <https://www.britannica.com/technology/expert-system> (дата звернення 25.01.2025).
3. Save EcoBot: Карти якості повітря в Україні [Електронний ресурс] – Режим доступу: <https://www.saveecobot.com/> (дата звернення 25.01.2025).
4. Experta Library for Python [Електронний ресурс] / PyPI Repository. – Режим доступу: <https://pypi.org/project/experta/> (дата звернення 25.01.2025).

УДК 004.4+622.691.2

Воловецький В.Б., доктор філософії, ст.дослідник
«Науково-дослідний інститут транспорту газу» АТ «Укртрансгаз»

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОГНОЗУВАННЯ УСКЛАДНЕНЬ НА ГАЗОСХОВИЩАХ

Під час відбирання газу зі свердловин підземних сховищ газу (ПСГ) можуть виникати різні ускладнення. Одними з них є накопичення рідини на вибої свердловин та у внутрішній порожнині шлейфів. Іншим ускладненням є відкладання гідратів у результаті змінення термодинамічних умов по шляху руху газу з пласта до газозбірному пункту [1, 2]. Ускладнення негативно впливають на забезпечення технологічного режиму експлуатування свердловин і, відповідно, призводять до зниження об'єму відбирання газу. Отже, доцільно застосовувати комплексний підхід, який передбачає детальне вивчення причин виникнення ускладнень, розроблення та уживання ефективних заходів для запобігання їх. Це дасть змогу забезпечувати стабільне експлуатування свердловин газосховищ.

Для контролювання технологічного процесу відбирання газу на газосховищах [3] потрібно розробити програмне забезпечення (ПЗ). У [4] подано розроблену систему прогнозування утворення гідратів на ПСГ з використанням технологій штучного інтелекту. Уживання цього заходу дасть змогу забезпечувати як стабільне експлуатування свердловин, так і газосховища у цілому. У [5] запропоновано ПЗ «Режим ПСГ», за допомогою якого можна забезпечувати розв'язання різних задач для потреб виробництва. У [6] подано розроблену систему прогнозування накопичення рідини у свердловинах та шлейфах на газосховищах. У [7] описано функційні можливості ПЗ «Режим свердловин» для проведення газодинамічних розрахунків за різних умов експлуатування свердловин. Отже, резюмую, що одним із ефективних заходів запобігання можливих ускладнень на газосховищах є впровадження розробленого ПЗ для прогнозування їх. Такий підхід дасть змогу своєчасно виявляти можливі ускладнення і, відповідно, застосовувати методи та заходи для запобігання утворенню їх.

Список використаних джерел:

1. Бугай А., Воловецький В., Пономарьов Ю. Інтелектуальна система контролювання та регулювання режиму експлуатування свердловин газосховищ в умовах гідратоутворення: зб. матеріалів 8-ої Міжнародної науково-технічної конференції "Інформаційні системи та технології ICT-2019" (09-14 вересня 2019 р., Харків). Харків: ХНУРЕ. 2019. С. 26-29.

2. Volovetskyi V.B., Doroshenko Ya.V., Bugai A.O., Kogut G.M., Raiter P.M., Femiak Y.M., Bondarenko R.V. Developing measures to eliminate of hydrate formation in underground gas storages. Journal of Achievements in Materials and Manufacturing Engineering. 2022. Vol.111. No.2. P. 64-77.

3. Воловецький В., Бугай А., Пономарьов Ю. Критерії побудови оптимальної системи прогнозування параметрів роботи підземних сховищ газу: зб. матеріалів 7-ої Міжнародної науково-технічної конференції "Інформаційні системи та технології ICT-2018" (10-15 вересня 2018 р., Харків). Харків: ХНУРЕ. 2018. С. 94-96.

4. Воловецький В., Романишин Ю., Райтер П. Прогнозування гідратуутворення на підземних сховищах газу з використанням технологій штучного інтелекту: зб. матеріалів XII Міжнародної науково-практичної конференції "Інформаційні управляючі системи та технології (ІУСТ-ОДЕСА-2024)" (23-25 вересня 2024 р., Одеса). Одеса: Національний університет "Одеська політехніка". 2024. С. 280-283.

5. Воловецький В., Романишин Ю. Особливості програмного забезпечення для визначення режимів експлуатування підземних сховищ газу: зб. тез VIII Міжнародної науково-практичної конференції "Прикладні інформаційні системи та технології в цифровому суспільстві" (01 жовтня 2024 р., Київ). Київ: Київський національний університет ім. Тараса Шевченка. 2024. С. 46-50.

6. Воловецький В., Фрідман О., Райтер П., Щирба О., Романишин Ю., Прогнозування накопичення рідини в свердловинах та шлейфах на підземних сховищах газу. Інформаційні управляючі системи та технології (ІУСТ-ОДЕСА-2025): зб. матеріалів XII Міжнародної науково-практичної конференції (24-26 вересня 2025 р., Одеса). Одеса: Національний університет "Одеська політехніка". 2025. С. 259-261.

7. Воловецький В., Бугай А., Щирба О., Романишин Ю., Левицький А. Визначення оптимальних режимів експлуатування свердловин підземних сховищ газу засобами програмного забезпечення. Прикладні інформаційні системи та технології в цифровому суспільстві: зб. тез IX Міжнародної науково-практичної конференції (01 жовтня 2025 р., Київ). Київ: Київський національний університет імені Тараса Шевченка. 2025. С. 38-48.

УДК 004.7

*Кунуп Т.В., к.т.н., ст. викладач,
Іванчиков О. І., здобувач,
Національний університет «Одеська політехніка»*

ОСОБЛИВОСТІ ВИКОРИСТАННЯ WMS-СИСТЕМ ДЛЯ ОПТИМІЗАЦІЇ УПРАВЛІННЯ СКЛАДСЬКИМИ ПРОЦЕСАМИ

У сучасних умовах цифрової трансформації підприємств особливого значення набуває автоматизація логістичних процесів. Ефективне управління складськими ресурсами є важливою складовою функціонування підприємств, діяльність яких пов'язана з обробкою значних обсягів товарно-матеріальних цінностей. Одним із ключових інструментів автоматизації складської логістики є системи управління складом класу WMS (Warehouse Management System).

WMS-система являє собою спеціалізований програмний комплекс, призначений для автоматизації та оптимізації процесів управління складськими операціями. Основними функціями таких систем є контроль надходження товарів на склад, управління їх розміщенням, облік запасів, комплектація замовлень, інвентаризація та відвантаження продукції. Використання WMS дозволяє підвищити точність обліку товарних запасів, зменшити кількість помилок під час виконання складських операцій та підвищити ефективність використання складських площ.

Важливою особливістю WMS-систем є можливість оптимізації процесів розміщення та переміщення товарів на складі. Система аналізує параметри продукції, інтенсивність її використання та доступні складські ресурси, що дозволяє формувати оптимальні маршрути переміщення товарів і мінімізувати час виконання логістичних операцій. Крім того, сучасні WMS-рішення підтримують інтеграцію з корпоративними інформаційними системами підприємства, зокрема ERP, CRM та системами управління транспортною логістикою.

Застосування WMS-систем також забезпечує підвищення рівня прозорості складських процесів. Завдяки використанню технологій автоматичної ідентифікації, таких як штрихкодування та RFID, здійснюється оперативний контроль руху товарів і формування актуальної інформації про стан складських запасів у режимі реального часу. Це дозволяє керівництву підприємства приймати обґрунтовані управлінські рішення та підвищувати ефективність логістичної діяльності.

Окрему увагу слід приділити ролі WMS у підвищенні якості обслуговування клієнтів. Завдяки автоматизації процесів комплектації

та відвантаження замовлень зменшується ймовірність помилок, скорочуються терміни доставки та забезпечується точність виконання замовлень. Це сприяє підвищенню рівня задоволеності клієнтів і формуванню конкурентних переваг підприємства на ринку.

Не менш важливим аспектом є економічна ефективність впровадження WMS-систем. Хоча початкові витрати на впровадження можуть бути значними, у довгостроковій перспективі вони окупуваються за рахунок зниження операційних витрат, оптимізації використання ресурсів та підвищення продуктивності праці. Крім того, автоматизація дозволяє зменшити залежність від людського фактору, що є особливо актуальним в умовах нестабільності ринку праці.

Отже, провадження WMS-систем є важливим напрямом підвищення ефективності функціонування складської логістики підприємств. Використання таких інформаційних систем сприяє оптимізації управління запасами, зменшенню операційних витрат та підвищенню рівня автоматизації складських процесів.

Список використаних джерел:

1. Григорак М. Ю. Інтелектуалізація логістичного менеджменту : монографія. Київ : Сік Груп Україна, 2017. С.408.
2. Крикавський Є. В., Чернописька Н. В. Логістичні системи : навч. посіб. Львів : Видавництво Львівської політехніки, 2012. С.312.
3. Посилкіна О. В., Сагайдак-Нікітюк Р. В., Доровський О. В. Складська логістика : навч. посіб. Харків : НФаУ, 2012. С.664.
4. Смерічевський С. Ф., Ткаченко О. С. Автоматизація складської діяльності як чинник підвищення ефективності логістичної системи підприємства. Економіка та суспільство. 2021. Вип. 25. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/264> (дата звернення: 11.03.2026).
5. Чередниченко О. Ю. Роль WMS-систем у цифровій трансформації логістики. Вісник Національного технічного університету «ХПІ». Серія: Економічні науки. 2019. № 2. С. 45–50.
6. Гуменюк В. В. Використання технологій RFID та штрихкування в автоматизації складського обліку. *Інфраструктура ринку*. 2020. Вип. 42. С. 115–120.
7. Терент'єв О. О. Особливості інтеграції WMS та ERP систем на сучасних підприємствах. Причорноморські економічні студії. 2022. Вип. 74. С. 88–93.

УДК 004.9:620.9

*Лисенко А.Я., аспірант,
Грінченко Г.С., к.т.н., доцент,
Харківський національний університет імені В.Н. Каразіна*

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ КВАЛІМЕТРИЧНОГО ОЦІНЮВАННЯ РИЗИКІВ ЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ

Сучасна енергетична інфраструктура є критично важливою складовою функціонування економіки та безпеки держави. Енергетичні об'єкти характеризуються високою складністю, значною кількістю технічних параметрів та підвищеним рівнем потенційних ризиків, що можуть виникати внаслідок технічних порушень функціонування, зовнішніх впливів або людського фактора. У таких умовах особливої актуальності набуває своєчасне та обґрунтоване оцінювання ризиків, яке дозволяє підвищити надійність функціонування енергетичних систем і мінімізувати можливі негативні наслідки.

Одним із перспективних підходів до комплексного аналізу ризиків є кваліметричне оцінювання, що ґрунтується на використанні системи показників якості та їх кількісної інтерпретації, що дає можливість формалізувати процес оцінювання, врахувати вплив різноманітних факторів та отримати інтегральну оцінку рівня ризику енергетичних об'єктів. У зв'язку з цим виникає потреба у створенні спеціалізованих інформаційних систем підтримки прийняття рішень, які забезпечують автоматизацію збору, обробки та аналізу даних, а також допомагають експертам формувати обґрунтовані управлінські рішення. Розробка такої системи сприятиме підвищенню ефективності оцінювання ризиків, оперативності аналізу інформації та загальному рівню безпеки функціонування енергетичних об'єктів.

Запропонований підхід до кваліметричного оцінювання ризиків енергетичних об'єктів ґрунтується на використанні системи ієрархічно структурованих показників, що характеризують технічний стан, надійність, безпеку та експлуатаційні умови функціонування об'єкта. Кожен із показників відображає окремий аспект потенційного ризику та має відповідну вагу, що визначає ступінь його впливу на загальний рівень ризику. У межах підходу здійснюється формування багаторівневої моделі оцінювання, яка включає визначення набору критеріїв, їх нормування, встановлення вагових коефіцієнтів та розрахунок інтегрального показника ризику. Для узагальнення інформації застосовуються методи кваліметрії, що дозволяють поєднати якісні та кількісні характеристики в єдину систему

оцінювання. Це забезпечує можливість порівняння різних енергетичних об'єктів або їх станів за єдиною шкалою ризику.

Інформаційна система підтримки прийняття рішень реалізує зазначену модель у вигляді програмного інструменту, який автоматизує процес введення даних, обробку показників, розрахунок часткових та інтегральних оцінок, а також візуалізацію результатів. Система дозволяє оперативно аналізувати рівень ризику, виявляти критичні фактори та формувати рекомендації щодо підвищення надійності й безпеки функціонування енергетичних об'єктів. Таким чином, запропонований підхід забезпечує комплексне, формалізоване та обґрунтоване оцінювання ризиків, що підвищує ефективність управління станом енергетичної інфраструктури та сприяє прийняттю більш об'єктивних управлінських рішень.

Застосування інформаційної системи дає можливість автоматизувати обробку даних, підвищити оперативність проведення оцінювання та зменшити вплив суб'єктивних факторів під час прийняття управлінських рішень. Крім того, використання кваліметричних методів дозволяє враховувати широкий спектр технічних та експлуатаційних параметрів, що впливають на рівень ризику.

Отримані результати можуть бути використані для підвищення ефективності управління безпекою та надійністю енергетичних об'єктів, а також для підтримки процесу прийняття обґрунтованих рішень у сфері експлуатації та модернізації енергетичної інфраструктури. Перспективи подальших досліджень полягають у розширенні функціональних можливостей системи, інтеграції з іншими інформаційними ресурсами та вдосконаленні методів оцінювання ризиків.

Список використаних джерел:

1. Trishch R., Nechuiviter O., Hrinchenko H., Bubela T., Riabchykov M., Pandova I. Assessment of safety risks using qualimetric methods // *MM Science Journal*. 2023. No. 10. P. 6668. DOI: https://doi.org/10.17973/MMSJ.2023_10_2023021.
2. Peček B., Kovačič A. Methodology of monitoring key risk indicators // *Economic Research – Ekonomska Istraživanja*. 2019. Vol. 32, No. 1. P. 3485–3501. DOI: <https://doi.org/10.1080/1331677X.2019.1658529>.
3. Грінченко Г. С., Кіпоренко О. В., Негодов С. С., Лисенко А. Я., Мазорчук К. К., Нос Р. С. Розвиток нормативного підходу до оцінювання ризиків енергопідприємств // *Машинобудування*. 2024. № 34. С. 17–30. DOI: <https://doi.org/10.26565/2079-1747-2024-34-02>.

УДК 004.46

*Горпініч І.О., студ. гр. КНТ-215м, магістрант,
Зайко Т.А., к.т.н, доцент
Національний університет «Запорізька політехніка»*

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТРАНЗАКЦІЙНИХ ДАНИХ ТА ВИЯВЛЕННЯ ШАХРАЙСТВА

У сучасному світі фінансові транзакції стають дедалі більш цифровими, що призводить до збільшення ризику шахрайських операцій. Виявлення шахрайства є критично важливим для банків та платіжних систем, оскільки шахрайські транзакції призводять до значних фінансових збитків. Класичні методи аналізу, засновані на правилах або статичних моделях, не завжди ефективні через велике розбалансування класів та високу динамічність шахрайських схем. Використання методів штучного інтелекту та глибокого навчання дозволяє автоматично виявляти аномалії та прогнозувати ризик шахрайства з високою точністю [1].

Метою роботи є створення моделі для класифікації транзакцій на нормальні та шахрайські з використанням гібридного підходу, який поєднує можливості автоенкодера [2]-[3] та нейронного класифікатора, а також аномалійно-детекційного методу Isolation Forest [4]–[5]. Використана вибірка Credit Card Fraud Detection [6], яка містить числові ознаки транзакцій та мітки класів.

Основними проблемами було те, що:

- клас шахрайських транзакцій становить приблизно 0.2% від усіх даних;
- модель повинна виявляти аномалії навіть у разі обмежених даних для тренування.

В роботі запропоновано гібридну модель Hybrid Deep Autoencoder Isolation Fraud Detection [7]:

- autoencoder [2]-[3] призначений для навчання компактного представлення нормальних транзакцій. Вхідний вектор приймає 64 нейрони в латентному просторі міститься 16 нейронів в кінці реконструкція вхідних даних. Різниця між вхідними даними та реконструкцією використовується як ознака аномалії;

- нейронний класифікатор (Classifier) приймає латентне представлення та reconstruction error. Складається з одного прихованого шару з 32 нейронами та Dropout для запобігання перенавчанню;

- isolation forest [4]-[5] використовується для оцінки ймовірності аномалії на основі дерева рішень. Додає інформацію про нетипові транзакції для фінальної оцінки;

- фінальна оцінка транзакції обчислюється як середнє значення ймовірності від нейронної мережі та аномальної оцінки Isolation Forest. Порогове значення 0.3, що оптимізовано для балансу precision та recall шахрайських транзакцій.

Модель навчалася 30 епох із використанням оптимізатора Adam та комбінації BCEWithLogitsLoss для класифікації та MSELoss для reconstruction error. В табл.1 представлено результати отримані на тестовій вибірці.

Таблиця 1

Результати на тестовій вибірці

Клас	Precision	Recall	F1-score	Support
Normal(0)	0.86	0.99	0.92	394
Fraud(1)	0.91	0.33	0.48	98

Загальні метрики accuracy 0.86, roc-auc 0.923 [8].

Високий roc-auc 0.92 підтверджує, що модель ефективно відокремлює шахрайські транзакції. Precision шахрайських транзакцій 0.91 означає, що більшість передбачених шахрайських операцій справді є шахрайськими. Recall [8] 0.33 можна покращити за рахунок адаптивного порогу для конкретних бізнес-завдань.

Запропонований гібридний підхід поєднує автоенкодер, нейронний класифікатор та Isolation Forest, що дозволяє ефективно виявляти аномалії та шахрайство.

Використання reconstruction error у поєднанні з латентним представленням покращує розпізнавання складних шаблонів шахрайських транзакцій.

Модель показала високий ROC-AUC [8] 0.92, що свідчить про ефективність алгоритму навіть при сильно розбалансованих даних.

Для практичного застосування можна регулювати поріг класифікації 0.3 – 0.5 для балансування precision та recall залежно від фінансових ризиків.

Список використаних джерел:

- 1 Nasteski V. An overview of the supervised machine learning methods 2017. Vol. 4, №. 51-62. P. 56. URL: https://www.researchgate.net/profile/Vladimir-Nasteski/publication/328146111_An_overview_of_the_supervised_machine_learning_methods/links/5c1025194585157ac1bba147/An-overview-of-the-supervised-machine-learning-methods.pdf
- 2 Misra S. et al. An autoencoder based model for detecting fraudulent credit card transaction / Procedia Computer Science, 2020. Vol. 167, P. 254-262. URL: <https://www.sciencedirect.com/science/article/pii/S1877050920306840/pdf?md5=72e32da2744bcbef307050473d4b8679&pid=1-s2.0-S1877050920306840-main.pdf>
- 3 Fanai H., Abbasimehr H. A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection / Expert Systems with Applications. 2023. Vol. 217, P. 119562 URL: <https://www.sciencedirect.com/science/article/pii/S0957417423000635>
- 4 John H., Naaz S. Credit card fraud detection using local outlier factor and isolation forest / Int. J. Comput. Sci. Eng. 2019. Vol. 7, №. 4. P. 1060-1064. – Access mode: https://www.researchgate.net/profile/Sameena-Naaz-4/publication/335809102_Credit_Card_Fraud_Detection_using_Local_Outlier_Factor_and_Isolation_Forest/links/695e419ea1fd01798911addf/Credit-Card-Fraud-Detection-using-Local-Outlier-Factor-and-Isolation-Forest.pdf
- 5 Ounacer S. et al. Using Isolation Forest in anomaly detection: the case of credit card transactions / Periodicals of Engineering and Natural Sciences. 2018. Vol. 6, №. 2. URL: <https://pen.ius.edu.ba/index.php/pen/article/download/1757/1236>
- 6 Credit Card Fraud Detection URL: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>
- 7 Link to the program code URL: https://github.com/IrinaGorpinich/Hybrid_Fraud_Detection/blob/main/main.py
- 8 Hossin M. A review on evaluation metrics for data classification evaluations / International journal of data mining & knowledge management process. 2015. Vol. 5, №. 2. P. 1. URL: <https://www.academia.edu/download/37219940/5215ijdkp01.pdf>

УДК 004.94:004.89:621.311

*Казначеева Анастасія Василівна, здобувачка поза
аспірантурою, ст. викладач
Державний університет інформаційно-комунікаційних
технологій*

МОДЕЛЬ ОЦІНКИ ТА ПРОГНОЗУВАННЯ ЕНЕРГОСПОЖИВАННЯ ІОТ-ПРИСТРОЇВ З УРАХУВАННЯМ ЗМІН ЗОВНІШНЬОГО СЕРЕДОВИЩА

Енергоефективність є одним з ключових факторів сталого розвитку сучасних інформаційних технологій, зокрема в контексті Інтернету речей (IoT), де пристрої часто функціонують в умовах обмежених енергетичних ресурсів. Розвиток екологічно орієнтованих рішень у сфері IoT передбачає не лише впровадження енергоощадних технологій, але й створення інтелектуальних методів управління енергоспоживанням, здатних адаптуватися до змін зовнішнього середовища [1]. Штучний інтелект та методи машинного навчання дедалі ширше застосовуються для прогнозування споживання енергії та оптимізації роботи пристроїв, що сприяє зниженню вуглецевого сліду та підвищенню автономності систем [2].

Незважаючи на значні успіхи, відомі підходи мають ряд обмежень. Частина моделей орієнтована на аналіз енергоспоживання в статичних умовах, без врахування динамічних змін зовнішніх факторів (температури, вологості, освітленості), що суттєво впливають на роботу IoT-пристроїв [3]. Інші рішення ґрунтуються на даних високочастотних сенсорів, які вимагають додаткового обладнання та збільшують енергетичні витрати, обмежуючи їх застосування у малопотужних або розподілених системах [4]. Підходи з використанням цифрових двійників та нечіткої логіки демонструють потенціал у підвищенні ефективності управління енергією, проте потребують адаптації для роботи з неповними та неоднорідними даними середовищ [5]. Прогнозування на основі традиційних регресійних або стохастичних методів часто виявляється недостатньо точним у випадках складних нелінійних залежностей, властивих енергетичним процесам в IoT [6]. Додатковою проблемою є забезпечення приватності та безпеки даних у розподілених мережах, де використання інформації від численних сенсорів може призводити до витоку конфіденційних відомостей [7].

Отже, виникає необхідність у створенні математичних моделей та відповідних інтелектуальних методів, здатних виконувати оцінку та прогнозування енергоспоживання IoT-пристроїв з урахуванням змін

зовнішнього середовища, працюючи з різнотипними й неповними даними та забезпечуючи високу точність і адаптивність.

Метою даної роботи є розробка математичної моделі енергетичного балансу IoT-пристрою з урахуванням впливу зовнішніх факторів та її реалізація із застосуванням методів штучного інтелекту для підвищення точності прогнозування енергоспоживання та ефективності управління енергорежимами.

Енергоспоживання пристрою у конкретному тижні розглядається як функція багатьох змінних та їх часових лагів. Узагальнене представлення моделі має вигляд:

$$E_t = f(T_t, H_t, I_t, W_t, R_t, L_t, D_t, E_{t-1}, E_{t-2}, \dots, E_{t-q}) + \varepsilon_t, \quad (1)$$

де E_t – споживання енергії у тиждень t (мА·год/тиждень), T_t – середня температура навколишнього середовища (°C), H_t – відносна вологість повітря (%), I_t – інсоляція (середня сонячна потужність на одиницю площі, Вт/м²), W_t – середня швидкість вітру (м/с), R_t – кількість опадів (мм), L_t – тривалість світлового дня (год), D_t – коефіцієнт робочого циклу (частка від 0 до 1), q – глибина використання лагів енергоспоживання (кількість попередніх тижнів, що враховуються у прогнозі), ε_t – стохастичний шум, що враховує невимірювані чинники.

Щоб отримати придатну для реалізації формулу, функцію було апроксимовано комбінацією лінійних і слабо нелінійних взаємодій між змінними. Модель можна записати як:

$$E_t = \beta_0 + \sum_{i=1}^p \beta_i X_{i,t} + \sum_{j=1}^q \gamma_j E_{t-j} + \sum_{k=1}^m \delta_k \cdot \varphi_k(X_t) + \varepsilon_t, \quad (2)$$

де β_0 – вільний член (базовий рівень споживання за нейтральних умов), $X_{i,t}$ – нормалізовані входні ознаки середовища та навантаження у момент часу t , β_i – коефіцієнти впливу окремих ознак у лінійній частині моделі, γ_j – коефіцієнти автокореляційної залежності, що відображають інерційність енергоспоживання, $\varphi_k(X_t)$ – нелінійні перетворення ознак (наприклад, добутки, квадрати або гармонічні функції, що моделюють сезонність), δ_k – вагові коефіцієнти при нелінійних членах, m – кількість таких нелінійних комбінацій.

Така формалізація дозволяє моделі поєднувати:

- лінійні залежності, наприклад пропорційне зростання споживання зі збільшенням коефіцієнта робочого циклу D ;
- автокореляційні ефекти, коли поточне споживання суттєво залежить від рівнів у попередні тижні (E_{t-1} , E_{t-2} , ...);
- нелінійні залежності, як-от вплив температури у вигляді квадратичної залежності (через зростання втрат енергії при екстремальних температурах) або синусоїдальні складові для сезонних ефектів.

Завдяки такій структурі модель здатна відображати як стабільні тренди (базове енергоспоживання при середніх кліматичних умовах), так і різкі коливання, зумовлені короточасними погодними аномаліями чи змінами режиму роботи пристрою.

У публічному доступі відсутні уніфіковані набори, які б одночасно містили детальні метеорологічні параметри та реальні показники споживання енергії IoT-пристроїв із щотижневою роздільною здатністю. Саме тому генерація власного синтетичного набору даних забезпечила повний контроль над його статистичними характеристиками, включно з сезонністю, трендами, амплітудою шуму та моделюванням аномальних подій, що критично важливо для відтворюваності експериментів та коректного порівняння алгоритмів.

Для імітації експлуатаційних умов було згенеровано синтетичний часовий ряд тривалістю 156 тижнів (еквівалент трьох повних календарних років), що дозволило відтворити як короткострокові, так і довгострокові сезонні та трендові закономірності. Кожен тиждень містив дев'ять ключових параметрів, серед яких вісім відображали вплив зовнішнього середовища на роботу пристрою, а дев'ятий – був цільовим показником, що характеризував фактичне енергоспоживання у ват-годинах на тиждень.

До змінних середовища належали: середньотижнева температура повітря ($^{\circ}\text{C}$), відносна вологість (%), рівень сонячної інсоляції ($\text{Вт}/\text{м}^2$), швидкість вітру ($\text{м}/\text{с}$), атмосферний тиск (гПа), інтенсивність опадів ($\text{мм}/\text{тиждень}$), середня тривалість світлового дня (години), а також показник рівня пилу та дрібнодисперсних часток у повітрі ($\text{PM}_{2.5}$, $\text{мкг}/\text{м}^3$). Кожна із цих змінних генерувалася з урахуванням річних і піврічних сезонних циклів, випадкових коливань та імовірнісних екстремальних відхилень, що імітували нетипові погодні або екологічні події.

Реалізація математичної моделі виконана у вигляді програмного комплексу, що поєднує генерацію синтетичних даних, їх попередню обробку, навчання прогнозної моделі та візуалізацію результатів. Обчислювальна основа побудована на лінійно-нелінійній регресійній залежності, де енергоспоживання E_t описується як функція сезонних та випадкових складових, а також впливу параметрів зовнішнього середовища. Формування входних змінних передбачає використання структурованого набору показників: інтенсивності сонячної радіації, температури повітря, відносної вологості, швидкості вітру, концентрації твердих частинок $\text{PM}_{2.5}$, атмосферного тиску, тривалості світлового дня та кількості опадів. На основі цих параметрів моделюється цільова змінна – тижневе енергоспоживання IoT-пристрою у ват-годинах (Wh), що синтезується шляхом поєднання

гармонічних функцій для відтворення сезонних коливань та білого гаусівського шуму для моделювання стохастичних відхилень.

Рис. 1 ілюструє архітектуру програмного комплексу для моделювання та прогнозування тижневого енергоспоживання IoT-пристрою з урахуванням впливу середовищних параметрів. Логіка роботи системи поділена на взаємопов'язані етапи, що забезпечують повний цикл – від генерації вхідних даних до побудови прогнозу та візуалізації результатів.

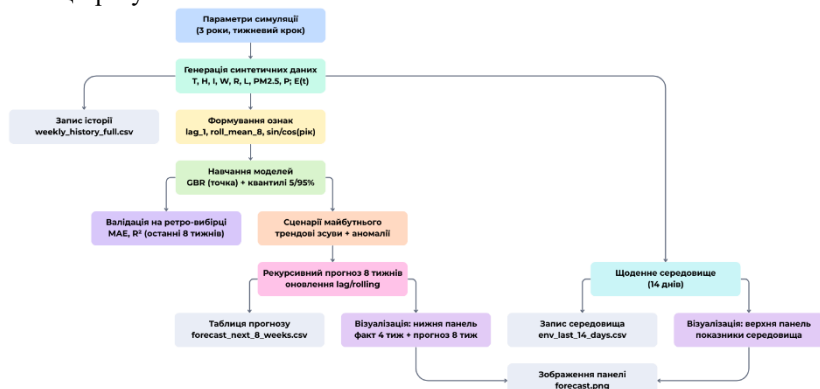


Рис. 1. Архітектура програмного комплексу для генерації синтетичних даних, побудови моделі та прогнозування енергоспоживання IoT-пристрою з урахуванням впливу параметрів зовнішнього середовища

На початковому етапі задаються параметри симуляції (тривалість 3 роки з тижневим кроком), після чого виконується генерація синтетичного датасету, що включає змінні температури (Т), вологості (Н), швидкості вітру (W), інсоляції (R), тривалості світлового дня (L), концентрації твердих частинок PM2.5, атмосферного тиску (P) та цільову змінну – енергоспоживання $E(t)$. Структуровані часові ряди зберігаються у форматі `weekly_history_full.csv` для подальшої обробки.

Далі формується набір ознак, включаючи лагові змінні (lag_1), ковзні середні ($roll\_mean_8$) та тригонометричні перетворення синус/косинус для моделювання сезонності. На основі цих ознак виконується навчання градієнтного бустингу (GBR) для точкових прогнозів та квантильних моделей (5% та 95%) для побудови інтервалів невизначеності. Якість моделі перевіряється на ретроспективній вибірці (останні 8 тижнів) з використанням показників MAE та R^2 .

Після валідації застосовуються сценарії майбутніх змін, що враховують трендові зсуви та аномальні впливи середовища.

Рекурсивний механізм прогнозування на 8 тижнів із оновленням лагових та ковзних характеристик забезпечує динамічну адаптацію моделі. Результати записуються у файл `forecast_next_8_weeks.csv`, а також використовуються для побудови двопанельної візуалізації: верхня панель відображає динаміку параметрів середовища за останні 14 днів, нижня – фактичне енергоспоживання за попередні 4 тижні та прогноз на наступні 8.

Для реалізації комплексу застосовано Python 3.11 з бібліотеками NumPy, Pandas та SciPy для роботи з даними, scikit-learn для машинного навчання, а також Matplotlib та Seaborn для побудови візуалізацій. Така архітектура є доцільною, оскільки забезпечує повний контроль над генерацією даних, дозволяє відтворювати умови для порівняння алгоритмів, а також легко адаптується до реальних промислових датасетів.

На рис. 2 наведено результати моделювання та прогнозування енергоспоживання IoT-пристрою на основі синтетично згенерованих даних середовища. Верхня частина панелі відображає часові ряди ключових вхідних параметрів за останні 14 днів: температуру повітря, відносну вологість, інсоляцію та робочий коефіцієнт `duty cycle`. Кожний показник представлено у вигляді дискретних точкових графіків із часовою розгорткою, що дозволяє відстежувати короткострокову динаміку та взаємозв'язки між змінними. Нижня частина панелі містить поєднану візуалізацію фактичного енергоспоживання за попередні 4 тижні та прогноз на наступні 8 тижнів. Прогноз представлений як середня оцінка (точкова лінія) та інтервал невизначеності у діапазоні квантилів $[q05; q95]$, отриманий за допомогою градієнтного бустингу із квантильними оцінками.

Технічна інтерпретація отриманих результатів свідчить, що модель здатна не лише враховувати короткострокові тренди змін середовища, але й адаптувати прогноз за умов наявності шумових флуктуацій та потенційних аномалій. Наявність широкого інтервалу невизначеності на окремих ділянках прогнозу свідчить про підвищену варіативність зовнішніх факторів у ці періоди, що узгоджується із симульованими сценаріями сезонних зсувів.

Практична значущість отриманих результатів полягає в можливості впровадження системи для автономного моніторингу та прогнозування споживання енергії IoT-пристроями, що критично важливо для оптимізації енергетичних витрат у сільському господарстві, екологічному моніторингу та промислових системах з автономним живленням. Новизна полягає у поєднанні генерації контрольованого синтетичного датасету із можливістю адаптивного прогнозування на короткостроковий період у тижневій дискретизації, що дає змогу точно

оцінювати енергетичні потреби навіть за відсутності історичних польових вимірювань.

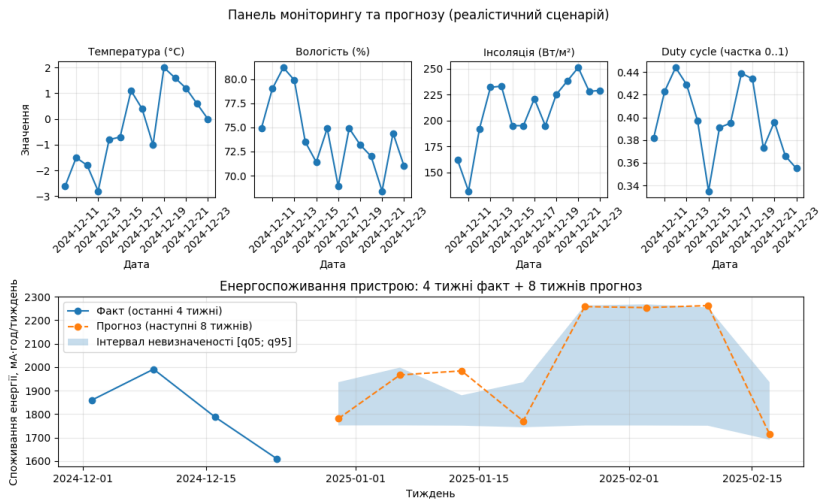


Рис. 2. Панель попередніх показників та прогнозу енергоспоживання IoT-пристрою в умовах змін середовища

Перспективи подальших розробок передбачають розширення моделі для роботи з реальними даними сенсорних мереж, включення алгоритмів адаптивного керування режимами роботи пристрою залежно від прогнозованого енергоспоживання, а також інтеграцію з системами прийняття рішень у реальному часі. Це відкриває можливості для створення інтелектуальних енергоменеджмент-систем, здатних підвищувати ефективність використання автономних IoT-рішень у складних та змінних умовах середовища.

Список використаних джерел:

1. Preethi, Ulla M. M., R. S., Devadas R., Priya, B. J. A. Green IoT: AI-powered solutions for sustainable energy management in smart devices. *Procedia Computer Science*. 2025. Вип. 258. С. 2312-2322. DOI: <https://doi.org/10.1016/j.procs.2025.04.486>
2. Preethi, Ulla M. M., R. S., Devadas R., Hiremani V., N. P. Leveraging machine learning for sustainable IoT: Predictive analytics for energy efficiency. *Procedia Computer Science*. 2025. Вип. 258. С. 2150-2158. DOI: <https://doi.org/10.1016/j.procs.2025.04.465>
3. Macias J. E. Z., Trilles S. Machine learning-based prediction model for battery levels in IoT devices using meteorological variables. *Internet of*

Things. 2024. Вип. 25. Стаття №101109. DOI: <https://doi.org/10.1016/j.iot.2024.101109>

4. Bokstaller J., Cerny M., Schneider J. Calendar-based RUL prediction for batteries: A data-driven approach using IoT device utilization data. Future Batteries. 2025. Вип. 5. Стаття №100046. DOI: <https://doi.org/10.1016/j.fub.2025.100046>

5. Prauzek M., Gaiova K., Kucova T., Konecny J. Fuzzy energy management strategies for energy harvesting IoT nodes based on a digital twin concept. Future Generation Computer Systems. 2025. Вип. 166. Стаття №107717. DOI: <https://doi.org/10.1016/j.future.2025.107717>

6. Balaji S., Karthik S. Energy prediction in IoT systems using machine learning models. Computers, Materials & Continua. 2023. Вип. 75, № 1. С. 443-459. DOI: <https://doi.org/10.32604/cmc.2023.035275>

7. Dai R., Bai G. Distributed context-aware Transformer enables dynamic energy consumption prediction for smart building networks. Digital Communications and Networks. 2025. DOI: <https://doi.org/10.1016/j.dcan.2025.03.006>

УДК 004.8:004.65

*Прасол Н.С., здобувач,**Марчук Г.В., ст. викл.**Державний університет «Житомирська політехніка»*

СЕМАНТИЧНИЙ ПОШУК ВАКАНСІЙ У ВЕБПОРТАЛАХ ПРАЦЕВЛАШТУВАННЯ НА ОСНОВІ AUGMENTED GENERATION

Сучасні вебпортали працевлаштування досі переважно використовують класичний пошук за ключовими словами. Такий підхід не враховує синоніми, контекст і семантичну близькість понять. У результаті кандидати пропускають вакансії, а роботодавці – кваліфікованих спеціалістів.

Щоб вирішити цю проблему, пропонується впровадження семантичного пошуку з використанням архітектури RAG. Архітектура Retrieval-Augmented Generation включає векторний пошук релевантних документів з генерацією відповіді за допомогою великої мовної моделі. На прикладі вебпорталу працевлаштування, користувач вводить запит українською або англійською мовами, система автоматично перетворює його на векторне представлення, знаходить семантично близькі вакансії в базі даних, додає їх до контексту промпту і генерує персоналізовану відповідь зі списком вакансій та поясненнями.

У межах MERN-проекту пропонується інтеграція RAG з використанням вбудованих можливостей MongoDB Atlas Vector Search [3], що дозволяє уникнути зовнішніх сервісів подібних до Pinecone [1]. На першому етапі до схеми Job додається поле embedding типу Array з векторним індексом. При створенні або оновленні вакансії на сервері генерується ембединг опису за допомогою відкритої моделі через API OpenAI [2]. Після цього налаштовується векторний індекс, який дозволяє знаходити вакансії за ступенем їхньої змістовної подібності. Коли користувач вводить свій запит, система створює таке ж математичне представлення запиту і виконує пошук, повертаючи найбільш близькі за змістом вакансії. Знайдені дані форматуються та додаються до промпту мовної моделі, яка генерує список вакансій із коротким описом до кожної. Такий підхід повністю інтегрується в існуючу серверну частину на Express та не вимагає значних змін у клієнтській частині вебзастосунку.

На рис. 1 представлена схема архітектури RAG для семантичного пошуку вакансій в проекті.

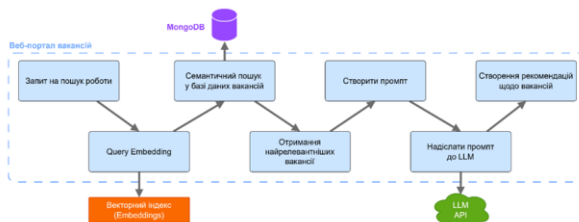


Рис.1. Архітектура RAG для семантичного пошуку вакансій

Запропонована архітектура має низку важливих переваг. По-перше, полегується інтерфейс, оскільки користувачу більше немає потреби заповнювати блоки фільтрації. По-друге, час відгуку залишається меншим за 200 мс для тисяч оголошень про роботу завдяки використанню векторного пошуку MongoDB Atlas [3]. По-третє, система масштабується без витрат на зовнішню векторну базу даних.

Водночас існують певні обмеження. По-перше, при додаванні нових вакансій потрібно додатково обробляти їхній текст, що вимагає додаткових обчислень на сервері. По-друге, відповіді мовної моделі іноді можуть трохи відрізнятися при повторних запитах, тому необхідно витратити час на налаштування моделі так, щоб її результати були максимально стабільними. По-третє, якщо кількість вакансій перевищить 50 тисяч, доцільно застосувати комбінований пошук - одночасно за змістовною подібністю та звичайними ключовими словами.

Таким чином, впровадження семантичного пошуку з використанням RAG перетворює звичайний MERN-портал працевлаштування на сучасну інтелектуальну платформу. Технологія, інтегрується в наявний проект завдяки вбудованому векторному пошуку MongoDB. Запропонований підхід підвищить точність підбору вакансій та покращить користувацький досвід.

Список використаних джерел

1. Pinecone - What is a Vector Database? [Електронний ресурс] / Pinecone Systems Inc. – 2025. – Режим доступу до ресурсу: <https://www.pinecone.io/learn/vector-database/>.

2. OpenAI API Reference - Embeddings [Електронний ресурс] / OpenAI. – 2026. – Режим доступу до ресурсу: <https://platform.openai.com/docs/api-reference/embeddings>.

3. MongoDB Atlas Vector Search Overview [Електронний ресурс] / MongoDB Inc. – 2026. – Режим доступу до ресурсу: <https://www.mongodb.com/docs/atlas/atlas-vector-search/vector-search-overview/>

УДК 004.8: 004.646

Олексюк О.С., магістрант,

Марчук Г.С., ст. викл.

Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ НАВЧАННЯ З ПІДКРІПЛЕННЯМ ДЛЯ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНОГО АВТОПІЛОТА В АВІАСИМУЛЯТОРІ

Розвиток технологій штучного інтелекту відкриває нові можливості для створення автономних систем керування складними динамічними об'єктами. Традиційні методи автоматичного керування, засновані на жорстко запрограмованих правилах або лінійних регуляторах, часто не здатні ефективно діяти в умовах високої невизначеності та нелінійної аеродинаміки. Метою роботи є розробка та теоретичне обґрунтування моделі інтелектуального автопілота для ведення повітряного бою в симуляційному середовищі з використанням методів навчання з підкріпленням.

Задача керування літаком формалізується як Марковський процес прийняття рішень (Markov Decision Process, MDP) і описується п'ятьма базовими компонентами: стани, дії, переходи, винагорода та політика.

Метою агента є максимізація очікуваної сумарної дисконтованої винагороди протягом епізоду взаємодії із середовищем. Процес оптимізації зводиться до пошуку таких вагових коефіцієнтів нейронної мережі, при яких літак надійно відстежує ціль та уникає пошкоджень [1].

Вектор стану агента формується з чотирьох логічних блоків. Блок 1 – параметри власного стану літака. Блок 2 - просторова орієнтація. Блок 3 - відносне положення цілі. Блок 4 - кінематика зближення. Ці параметри консолідуються у єдиний тензор, який обробляється MLP або рекурентною мережею GRU [1].

Керування реалізується через безперервний простір дій у діапазоні $[-1, 1]$, який включає чотири канали: тягу двигуна, крен, тангаж та ристання. Така модель забезпечує плавне і фізично коректне маневрування літака. Правильне проектування функції винагороди є одним із найважливіших етапів навчання агента.

Сумарна винагорода формується як лінійна комбінація зазначених складових, що стимулює агента оптимізувати траєкторії одночасно за декількома критеріями.

Для подолання проблеми «рідкісних винагород» (sparse rewards) в архітектуру агента інтегровано модуль внутрішньої мотивації (Curiosity-driven exploration), який генерує додаткову внутрішню

винагороду за непередбачуваність стану середовища. Це дозволяє агенту освоїти базову фізику польоту ще до моменту, коли він починає регулярно отримувати зовнішню винагороду за перехоплення цілі.

Практичну верифікацію підходу здійснено у власному симуляційному середовищі на базі Unity / ML-Agents. Автопілот на алгоритмі PPO з модулем Curiosity навчався просторовому перехопленню статичних та рухомих цілей. Конвергенція моделі підтверджується чотирма метриками навчання (рис. 1).

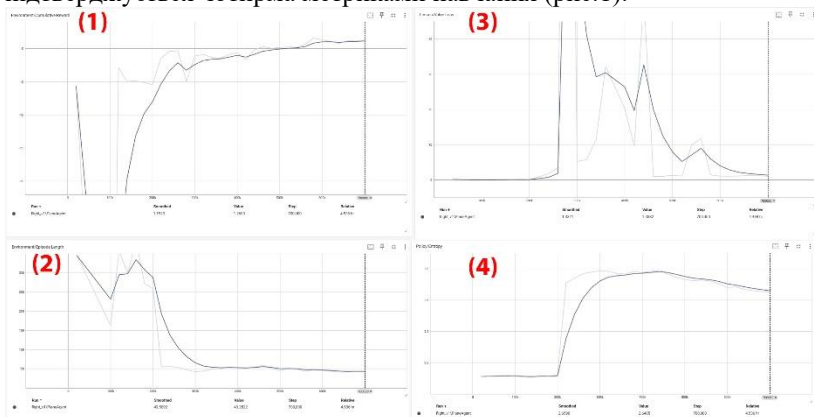


Рис. 1. Динаміка навчання RL-агента (Cumulative Reward, Episode Length, Value Loss та Policy Entropy) у середовищі Unity

Результати дослідження підтверджують ефективність застосування DRL для побудови інтелектуального автопілота. Завдяки ітеративному навчанню у симуляторі алгоритм здійснює керування на мікрорівні з точністю та частотою, недосяжними для людського сприйняття. Запропонований підхід формує потужний фундамент для розробки автопілотів-напарників, здатних брати на себе критичне просторове маневрування та знижувати когнітивне навантаження на пілота. Досягнення цього напрямку знайшли практичне підтвердження у випробуваннях AlphaDogfight (DARPA), де автономні агенти перевершили досвідчених пілотів-людей [2].

Список використаних джерел

1. Hu, D., Yang, R., Zuo, J., Zhang, Z., Wu, J., & Wang, Y. (2021). Application of deep reinforcement learning in maneuver planning of beyond-visual-range air combat. *IEEE Access*, 9, 32282–32297.
2. Bae, J. H., Jung, H., Kim, S., Kim, S., & Kim, Y. D. (2023). Deep reinforcement learning-based air-to-air combat maneuver generation in a realistic environment. *IEEE Access*, 11, 26427–26440.

УДК 004.8

Мандрик О.В., магістрант,

Марчук Г.В., ст. викл.

Державний університет «Житомирська політехніка»

ІГРОВИЙ ШТУЧНИЙ ІНТЕЛЕКТ У СИМУЛЯТОРАХ ДЛЯ МОДЕЛЮВАННЯ РЕАЛІСТИЧНИХ СЦЕНАРІЇВ

Сучасні ігрові симулятори охоплюють широкий спектр сценаріїв - від ведення фермерського господарства до керування транспортом, але можливості штучного інтелекту для реалізації поведінки неігрових персонажів (NPC) використовуються недостатньо.

Метою дослідження є визначення ролі ігрового штучного інтелекту (ШІ) у моделюванні динамічних сценаріїв та оцінка його впливу на когнітивний розвиток гравців. Об'єктом дослідження є симулятори як інтерактивні середовища, а предметом - алгоритми ШІ, що визначають адаптивну поведінку NPC та їхню реакцію на дії користувача.

Однією з ключових проблем ігрового штучного інтелекту є обмеженість його можливостей, що проявляється у передбачуваності поведінки неігрових персонажів, відсутності адаптації до нестандартних дій гравця та використанні суворо заданих сценаріїв. Такі обмеження зумовлені застосуванням спрощених поведінкових моделей, зокрема скінчених автоматів або фіксованих наборів правил, що не враховують складну динаміку взаємодії з гравцем. Як наслідок, NPC часто виконують лише декоративну або вкрай спеціалізовану функцію.

У багатьох ігрових симуляторах NPC узагалі відсутні, оскільки фокус ігрового процесу (наприклад, у таких іграх як Mini Metro, Dorfromantik, Farming Simulator (solo), Euro Truck Simulator, Unpacking тощо) зосереджений на відтворенні єдиної, цілком конкретної функції або процесу, наприклад керуванні транспортним засобом чи виконанні виробничих операцій. Навіть якщо розробник введе у такий ігровий процес NPC, вони не зроблять досвід гравця значно багатшим чи яскравішим. Наявність розвинених неігрових персонажів частіше притаманна для ігор з обмеженими елементами симуляції або таких, що не прагнуть до максимального технічного реалізму, наприклад серії The Sims, де NPC відіграють ключову роль у формуванні ігрового досвіду.

Сучасні ігрові технології активно інтегрують методи машинного навчання та адаптивного AI, що створює передумови для формування більш реалістичних і динамічних ігрових сценаріїв, що створює значний

потенціал для адаптації ігрового процесу до дій гравця та формування більш реалістичних сценаріїв.

На рисунку 1 наведено концептуальний підхід до інтеграції алгоритмів ШІ, машинного навчання та еволюційного моделювання в ігровий процес.

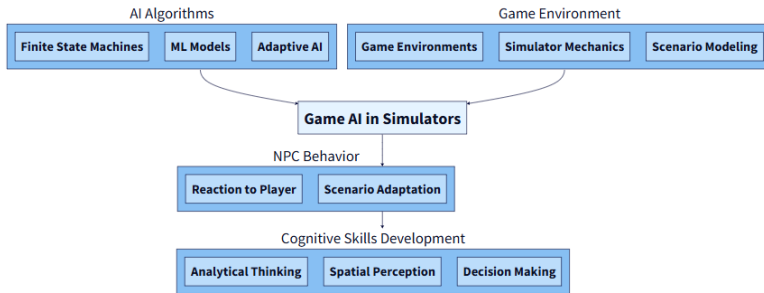


Рисунок 1. - ШІ-алгоритми в ігрових симуляторах

Інтеграція алгоритмів штучного інтелекту в ігрові системи формує нові можливості для створення інноваційних проєктів та проведення досліджень. Використання ШІ для моделювання поведінки ігрових персонажів підвищує реалістичність і якість ігрового контенту [3], що дозволяє ефективніше застосовувати симулятори як засіб навчання, розвитку когнітивних навичок та професійної підготовки фахівців [1, 2].

Отже, ігровий штучний інтелект є важливим чинником підвищення реалістичності та інтерактивності симуляторів. Його використання сприяє розвитку когнітивних навичок користувачів, зокрема аналітичного мислення, просторового сприйняття та прийняття рішень. Подальший розвиток NPC і ШІ-моделей має значний потенціал для ігрової індустрії, а також освітніх і тренувальних середовищ.

Список використаних джерел:

1. Kovtaniuk M.S., Shokaliuk S.V. & Stepanyuk, A.N. Game simulators as educational tools for developing algorithmic thinking skills in computer science education. *CTE Workshop Proceedings*. 2025, 12, pp.19–62.
2. Karaca Y., Derias, D. & Sarsar G. Ai-powered procedural content generation: Enhancing npc behaviour for an immersive gaming experience. *Available at SSRN 4663382*. 2023.
3. Armanto H., & Rosyid H. A. Improved Non-Player Character (NPC) behavior using evolutionary algorithm—A systematic review. *Entertainment Computing*, 2025, 52, 100875.

УДК 004:658.5

*Одарченко Р.С. д.т.н., професор,
Ассаул О.Ю. здобувач,
Іщук К.І. здобувач*

Національний університет «Київський авіаційний інститут»

ОЦІНКА ПІДХОДІВ ДО ОЦІНКИ ЦИФРОВОЇ ЗРІЛОСТІ ПІДПРИЄМСТВ

У сучасній економіці цифрова зрілість виступає не лише мірою впровадження інформаційно-комунікаційних технологій, але й ключовим індикатором здатності підприємства генерувати нову цінність, адаптуватися до ринкових змін та забезпечувати сталий розвиток. Однак, незважаючи на визнану важливість цифрової трансформації, методологія оцінювання її результатів залишається фрагментованою. Існує значна кількість моделей цифрової зрілості (Digital Maturity Models, DMM), які суттєво відрізняються за архітектурою, охопленням та методами розрахунку.

Аналіз провідних світових підходів (зокрема DMAT Європейської Комісії, TM Forum DMM, моделей консалтингових компаній Deloitte, Gartner, McKinsey DQ) дозволяє виокремити шість структурних компонентів, за якими їх доцільно порівнювати: виміри, шкальні елементи, вагові коефіцієнти, рівні зрілості, інструменти оцінки та шлях еволюції. Для підприємств зі складною технологічною інфраструктурою цей перелік необхідно розширити критерієм здатності інтегрувати об'єктивні операційні дані.

Проведена оцінка існуючих підходів виявила низку критичних недоліків. По-перше, близько 72% сучасних DMM мають суто описовий (дескриптивний) характер. Вони фіксують стан «як є», але не містять алгоритмів адаптивного управління для переходу до цільового стану. По-друге, крос-галузеві моделі (наприклад, DMAT або Gartner) застосовують принцип лінійної агрегації або відсутність вагових коефіцієнтів, що ігнорує нерівномірний вплив різних факторів на ефективність виробництва. По-третє, фундаментальною проблемою є домінування методу самооцінювання (self-assessment). Суб'єктивне опитування менеджменту створює ризик значного викривлення результатів, оскільки повністю ігнорує операційний шар даних (Operational Data Layer) – об'єктивні технічні показники ефективності (KPI), такі як час відновлення сервісу (MTTR), доступність мережі чи рівень автоматизації.

Усунення цих недоліків вимагає переходу від статичних анкетних методів до гібридних моделей оцінки. Ефективний підхід має

поєднувати суб'єктивні оцінки організаційно-культурних вимірів із автоматизованим збором технічних KPI безпосередньо з інформаційних систем підприємства (наприклад, OSS/BSS), використовуючи механізми адаптивного зважування.

Зокрема, пропонується використання вдосконаленого інтегрального індексу цифрової зрілості, який обчислюється на основі скоригованих вимірів та галузевого бенчмаркінгу за формулою:

$$D_{\text{enhanced}} = \gamma \times (w_i \times D_i) \times (1 - \gamma) \times B_{\text{overall}}$$

де D_{enhanced} – розширений індекс цифрової зрілості; D_i – значення i -го виміру після коригування на коефіцієнт достовірності (Reliability Factor) та операційні дані; w_i – ваговий коефіцієнт виміру, що визначається специфікою галузі; B_{overall} – нормоване значення, розраховане порівняно з галузевими бенчмарками; γ – коефіцієнт, що визначає ступінь впливу внутрішніх даних порівняно із зовнішнім бенчмаркінгом ($\gamma \in [0;1]$).

Таким чином, оцінка підходів до вимірювання цифрової зрілості доводить необхідність відмови від універсальних дескриптивних моделей на користь галузево-адапованих інструментів. Інтеграція об'єктивних метрик ефективності та механізмів динамічного зважування дозволяє перетворити оцінку цифрової зрілості з інструменту простої фіксації стану на дієвий механізм адаптивного управління цифровою трансформацією підприємства.

Список використаної літератури:

1. Joint Research Centre (JRC). Digital Maturity Assessment Tool (DMAT): Framework and Guidelines for EDIHs. European Commission, 2023. 48 p.
2. Pham M. H., Pham T. T. H. Comprehensive review of Digital Maturity Model and Proposal for a Continuous digital transformation process with Digital Maturity Model integration. IJCSNS International Journal of Computer Science and Network Security. 2022. Vol. 22, no. 1. P. 741–757.
3. Thordsen T., Bick M. A decade of digital maturity models: much ado about nothing?. Information Systems and e-Business Management. 2023. Vol. 21. P. 947–976.
4. Valdez-de-Leon O. A Digital Maturity Model for Telecommunications Service Providers. Technology Innovation Management Review. 2016. Vol. 6, no. 8. P. 19–32.

УДК 004.8:316.472.4:339.138

Мойсеев М.Г., магістр

Національний університет «Одеська політехніка»

МЕТОДИКА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ СОЦІАЛЬНОЇ АКТИВНОСТІ КОРИСТУВАЧІВ ДЛЯ ФОРМУВАННЯ ПЕРСОНІФІКОВАНИХ МАРКЕТИНГОВИХ СТРАТЕГІЙ

Вступ. В умовах глобальної цифровізації соціальні мережі перетворилися на ключове джерело емпіричних даних про поведінку, вподобання та ціннісні орієнтації споживачів. Актуальність дослідження зумовлена необхідністю трансформації традиційних методів маркетингового аналізу в інтелектуальні системи, що здатні опрацьовувати великі масиви неструктурованої інформації в режимі реального часу [1].

Класичні підходи до сегментації аудиторії за демографічними ознаками втрачають ефективність, поступаючись методам аналізу цифрового сліду, які дозволяють прогнозувати споживчий попит на основі соціальної активності (лайків, репостів, коментарів та тривалості перегляду контенту).

Основна частина. Процес аналізу соціальної активності є багатофакторним завданням, що включає моніторинг динаміки залученості, семантичний аналіз текстових повідомлень та дослідження структури соціальних графів.

Складність полягає у високому рівні інформаційного шуму та неоднорідності даних. Запропонована методика базується на комплексному поєднанні алгоритмів обробки природної мови (NLP) та методів кластерного аналізу [2].

Методика реалізується за наступними етапами. На першому етапі проводиться збір даних (data crawling) з відкритих API соціальних платформ.

Отримана інформація проходить етап попередньої обробки: токенизацію, лематизацію та видалення стоп-слів. Важливим аспектом є ідентифікація тональності (sentiment analysis), що дозволяє диференціювати позитивні, негативні та нейтральні реакції користувачів на бренд або продукт.

На другому етапі здійснюється кількісна оцінка соціальної активності через побудову відповідних метрик залученості (Engagement Rate). Проте, на відміну від стандартних підходів, методика передбачає використання вагових коефіцієнтів для різних типів активності, що залежать від маркетингових цілей.

Наприклад, коментарі та поширення мають вищий пріоритет над пасивними переглядами при оцінці лояльності до бренду.

Третій етап полягає у сегментації користувачів за допомогою алгоритмів машинного навчання, таких як k-means або DBSCAN. Це дозволяє виділити мікросегменти аудиторії з подібними поведінковими патернами [3].

Для кожного сегмента автоматично генерується рекомендаційна модель, яка лягає в основу маркетингової стратегії: визначення оптимального часу для публікацій, вибір стилістики контенту та персоналізація рекламних пропозицій.

Інтеграція результатів аналізу в маркетингову стратегію дозволяє компаніям перейти від масового маркетингу до стратегії «one-to-one», мінімізуючи витрати на залучення клієнтів (CAC) та підвищуючи їхній життєвий цикл (LTV).

Практична реалізація методики може бути впроваджена у формі автоматизованого аналітичного модуля для CRM-систем. Це забезпечує високу адаптивність маркетингових інструментів до динамічних змін у споживчих трендах.

Висновки. Розроблена методика аналізу соціальної активності забезпечує глибоке розуміння поведінкових чинників споживачів у цифровому середовищі.

Поєднання інструментів NLP та кластеризації дозволяє не лише оцінювати поточний стан бренду, а й прогнозувати реакцію ринку на нові маркетингові ініціативи, що підвищує загальну конкурентоспроможність підприємства.

Впровадження таких інтелектуальних систем у маркетингову практику мінімізує суб'єктивні ризики при прийнятті рішень та закладає фундамент для переходу до стратегій предиктивного управління клієнтським досвідом.

Список використаних джерел:

1. Smith A., Taylor J. Social Media Analytics and Business Intelligence: A New Paradigm. *Journal of Digital Marketing*. 2022. Vol. 12, No 3. P. 45–52.
2. Wang Y. Machine Learning Techniques for Customer Sentiment Analysis in Social Networks. *International Journal of Information Technology*. 2023. Vol. 15, No 1. P. 88–101.
3. Bondarenko O. Predictive Analytics in Social Media Marketing Strategies. *Computing and Systems*. 2024. Vol. 7, No 2. P. 112–120.

УДК 004.932:004.8

*Лазаренко М.В., здобувач
Рудніченко М.Д., к.т.н., доцент,
Шибасєва Н.О., к.т.н., доцент,
Національний університет «Одеська політехніка»*

АНАЛІЗ ІЄРАРХІЧНИХ АГЕНТНИХ МОДЕЛЕЙ ОБРОБКИ МУЛЬТИМОДАЛЬНИХ ДАНИХ В ПРОЦЕСАХ РОЗПІЗНАВАННЯ ОБРАЗІВ

Вступ. Ієрархічні агентні моделі пропонують архітектурне рішення, що дозволяє розподілити завдання обробки між рівнями агентів із різною спеціалізованою функціональністю, поєднуючи локальні та глобальні стратегії розпізнавання та інтерпретації образів. Актуальність наряду обумовлена складністю сучасних даних, що надходять із різномірних джерел, і потребою синтезувати семантичну інформацію на різних рівнях абстракції. Ієрархічні агентні структури здатні ефективно інтегрувати фрактальні, часові, контекстні і семантичні ознаки, розподіляючи обчислювальні ресурси та забезпечуючи адаптацію процесу обробки залежно від складності вхідних сигналів [1].

Основна частина. Поява мультимодальних даних зумовила потребу розвитку моделей, здатних не лише обробляти окремі потоки інформації, але й інтегрувати зміст з різних сенсорних доменів. Ієрархічні агентні моделі передбачають організацію обчислювальних одиниць (агентів) у багатоетапні структури, де кожен агент або група агентів спеціалізуються на окремих аспектах мультисенсорної обробки. На нижчому рівні такої ієрархії агенти виконують первинну фільтрацію та локальні трансформації даних.

Вищі рівні агентних ієрархій виконують інтеграцію локально оброблених результатів для формування глобальних представлень. Ці рівні включають більш складні когнітивні механізми для семантичної інтерпретації сцен, встановлення причинно-наслідкових зв'язків, виділення об'єктних категорій та контекстних відношень між ними. Комунікація між агентами здійснюється через стандартизовані інтерфейси обміну інформацією, що дозволяє агентам адаптувати свої алгоритмічні стратегії залежно від отриманих контекстних сигнатур [2].

Ієрархічний підхід дозволяє вирішувати ключові проблеми, характерні для обробки мультимодальних даних: узгодження неоднорідних представлень, усунення суперечливих сигналів, інтеграцію інформації різної дискретності, а також адаптацію до динамічних змін контексту. Наприклад, у складних задачах розпізнавання сцен агенти нижчого рівня можуть фокусуватися на

локальних просторових ознаках, тоді як агенти вищого рівня інтегрують ці ознаки для побудови моделі об'єктних взаємозв'язків.

Однією з архітектурних моделей, що знайшла застосування в цій сфері, є багаторівневий агентний граф, де кожен вузол графу представляє окремого агента з певною спеціалізацією. Такі графи можуть бути побудовані за принципом розширеної глибокої ієрархії, в якій інформація просувається вгору по рівнях для агрегування та семантичної інтерпретації, а також назад для уточнення локальних оцінок із урахуванням глобального контексту.

Деякі підходи передбачають використання гібридних структур, де ієрархічні агентні модулі поєднують класичні алгоритми машинного навчання (нейромережі, класифікатори) зі структурованими комунікаційними правилами, що дозволяють оптимізувати процес розпізнавання шляхом узгодження локальних і глобальних оцінок [3].

Серед сучасних розробок у цій сфері – моделі, що поєднують агентні механізми з глибокими гібридними архітектурами для інтеграції візуальних та текстових даних, що суттєво покращує якість семантичного узгодження розпізнаваних об'єктів у мультисенсорних системах. Серед основних тенденцій у розвитку ієрархічних агентних моделей – активне використання механізмів attention-подібних структур, що дозволяють агентам зосереджувати свою увагу на релевантних частинах вхідних даних залежно від поточного контексту.

Висновки. Ієрархічні агентні моделі становлять перспективний напрям у сфері обробки мультимодальних даних завдяки своїй здатності розподіляти завдання між рівнями агентів, інтегрувати неоднорідні сигнали та забезпечувати адаптивність при розпізнаванні складних образів. Аналіз сучасних архітектур свідчить про необхідність подальшого розвитку механізмів комунікації між агентами, інтеграції гібридних методів навчання та адаптації до динамічних контекстів.

Список використаних джерел:

1. Khan S., Hayat M., Bennamoun M., Sohel F. Multimodal Deep Learning for Robust RGB-D Object Recognition. *IEEE Transactions on Image Processing*. 2023. Vol. 32. P. 3175–3187.
2. Guo Y., Wang Y., Wu H., Lin Y. Hierarchical Agent-Based Framework for Multimodal Perception in Autonomous Systems. *Journal of Artificial Intelligence Research*. 2024. Vol. 71. P. 255–284.
3. Zhang Z., Zheng L., Yang Y. Graph Attention Networks for Multimodal Fusion in Object Recognition. *Pattern Recognition*. 2025. Vol. 127. P. 108538–108538.

УДК 004.8:519.6

*Панюшкін А.Ю., здобувач,
Рудніченко М.Д., к.т.н., доцент
Національний університет «Одеська політехніка»*

РОЗРОБКА КОНЦЕПЦІЇ СИСТЕМИ ВИРІШЕННЯ ЗАВДАНЬ НЕЛІНІЙНОЇ ОПТИМІЗАЦІЇ НА БАЗІ АЛГОРИТМІВ РОЙОВОГО ІНТЕЛЕКТУ

Вступ. В умовах високої розмірності афінних і неафінних просторів розв'язання завдань оптимізації класичними детерміністичними алгоритмами часто супроводжується значними обчислювальними витратами та ризиком потрапляння в локальні екстремуми. Підходи, що базуються на ройовому інтелекті як класі природно-натхненних алгоритмічних структур, демонструють здатність забезпечувати децентралізовану координацію «агентів» пошуку для гнучкого балансування між дослідженням та експлуатацією простору рішень [1]. Актуальність розробки концепції системи вирішення завдань нелінійної оптимізації на основі ройових алгоритмів полягає у необхідності системного підходу до організації архітектури таких систем, що дозволить поєднати механізми кооперації агентів з адаптивними стратегіями пошуку в умовах складних обмежень [2].

Основна частина. При формуванні концептуальної системи вирішення нелінійних оптимізаційних задач одним з першочергових етапів є визначення архітектурної структури системи [3]. Архітектура такої системи може бути розглянута як багаторівнева платформа, що складається з кількох функціональних шарів. Перший шар – це шар агентних модулів, де кожний агент реалізує власну локальну логіку ройового алгоритму, наприклад, частинкового росту (PSO), колонії мурах (ACO) чи оптимізації на основі поведінки інших біологічних моделей. Агентні модулі відповідають за локальний пошук, оцінювання функції пристосованості і оновлення свого стану згідно з правилами, заданими для конкретного алгоритму.

Другий шар – це координаційний рівень, на якому агрегується інформація про стан всіх агентів, формується глобальний контекст вирішення задачі та здійснюється міжагентна комунікація для обміну знаннями про знайдені області простору рішень. Така координація дозволяє уникати дублювання пошуку в одному і тому самому регіоні простору і сприяє більш ефективному розподілу обчислювальних ресурсів для розширення дослідження глобального простору. У цьому шарі функціональні механізми синхронізації, адаптації параметрів та контролю «стратегії дослідження–експлуатації» відіграють

визначальну роль, особливо у випадках нелінійних обмежень, які можуть створювати складні ландшафти цільових функцій.

Третій шар архітектури системи – стратегічний рівень, на якому визначаються глобальні політики пошуку, критерії адаптації та оновлення параметрів рою в залежності від характеру задачі та динамічних змін вхідних умов. Цей рівень містить модулі оцінювання ефективності застосованих стратегій, механізми пере-налаштування поведінки агентів і рішення про комбінації алгоритмічних підходів.

Взаємодія між цими шарами здійснюється через стандартизовані інтерфейси обміну даними та керування, що забезпечують гнучкість системи щодо підключення нових алгоритмів чи адаптивних модулів. Такий компонентний підхід до побудови архітектури дозволяє створювати гібридні стратегії оптимізації, де локальні агентні модулі можуть використовувати різні роєві алгоритми залежно від стадії пошуку чи локальної складності проблеми. Одним з ключових архітектурних елементів є модуль адаптивного балансування, що визначає співвідношення між глобальним пошуком та локальними пошуковими процесами, адаптуючи параметри агентів у відповідності до отриманих результатів та змін у зовнішньому середовищі задачі.

Висновки. Запропонована концепція системи вирішення завдань нелінійної оптимізації на базі алгоритмів роєвого інтелекту окреслює багаторівневу архітектуру, що поєднує локальні пошукові модулі, координаційні механізми та стратегічний конт-ролер для адаптивного керування поведінкою агентів. Такий архітектурний підхід дозволяє організувати гнучку, масштабовану систему, здатну ефективно вирішувати складні оптимізаційні задачі з нелійними обмеженнями та цільовими функціями, а також забезпечувати адаптацію параметрів під час процесу пошуку.

Список використаних джерел:

1. Han J. An Advanced Adaptive Group Learning Particle Swarm Optimization Algorithm Based on Symmetry Concepts. *Symmetry*. 2025. Vol. 17, No 5. P. 667–668.
2. Wang C. Chaotic Elite Clone Particle Swarm Optimization for Efficient Industrial Task Allocation. *Scientific Reports*. 2025. Vol. 15, No 19527. P. 2153–2155.
3. Adonin L.S., Vladyko A.G. Swarm Intelligence Algorithms for Optimization Problems in Telecommunication Systems. *Research Journal RCSI*. 2025. Vol. 10, No 3. P. 101–115

УДК 004.94:004.8

*Тимошенко Д.О., здобувач,
Рудніченко М.Д., к.т.н., доцент
Національний університет «Одеська політехніка»*

АНАЛІЗ СУЧАСНИХ МАЛИХ МОВНИХ МОДЕЛЕЙ ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ АСИСТУВАННЯ В ОНЛАЙН- ЗУСТРІЧАХ

Вступ. Серед нових напрямів розвитку штучного інтелекту особливої уваги потребують малі мовні моделі (SLM), що поєднують здатність до глибокого семантичного розуміння та підвищену ефективність обчислень при значно меншій кількості параметрів, ніж великі трансформерні моделі. SLM демонструють потенціал для реального часу автоматизації процесів підсумовування, класифікації, витягнення інформації та інтерактивних діалогових відповідей в умовах обмежених обчислювальних ресурсів, що є критично важливим для інтеграції в сервіси онлайн-зустрічей і корпоративні комунікаційні платформи. Поточні дослідження зосереджують увагу на оптимальному балансі між продуктивністю й ефективністю моделей, структурних компонентах архітектур, адаптації до конкретних доменних задач і впровадженні в продуктивні системи [1].

Основна частина. Початкові дослідження малих мовних моделей концентруються навколо зменшення кількості параметрів при збереженні здатності до природномовних трансформацій. SLM, на відміну від великих мовних моделей з десятками і сотнями мільярдів параметрів, зазвичай мають кількість параметрів від декількох мільйонів до кількох мільярдів, що дозволяє їм ефективно працювати в режимі реального часу на пристроях із обмеженою обчислювальною потужністю або в кейсах, де важлива конфіденційність даних через локальне виконання обчислень.

Класичні архітектури малих мовних моделей часто базуються на трансформерних компонентах зі скороченою глибиною та шириною, що зумовлюється зменшенням кількості шарів уваги і параметрів моделі. Такі архітектурні оптимізації включають методи дистиляції знань, квантування параметрів та відсікання частин моделі, що незначною мірою впливають на якість вихідного контенту, але суттєво знижують розмір і час обчислення [2].

У контексті автоматизації асистування під час онлайн-зустрічей важливим аспектом є підтримка декількох мовних задач: транскрипція мови в текст, тематичне узагальнення обговорень, виділення ключових тез, класифікація сенсу висловлювань та формування релевантних

резюме після завершення події. Архітектурно система, що використовує SLM, може бути побудована як модуль конвеєра даних, де вхідні аудіо- чи відеопотоки спочатку трансформуються в текстовий формат за допомогою систем розпізнавання мовлення, після чого обробка природної мови здійснюється SLM, адаптованою до конкретної доменної області задач і заданих критеріїв якості відповіді чи резюме. У цьому контексті модель може бути навчена на попередньо зібраному корпусі даних, специфічних для онлайн-зустрічей та конференцій, із включенням прикладів структурованих діалогів, презентаційних команд і групових обговорень. Такі моделі можуть бути інтегровані у багатокомпонентну архітектуру, де SLM виступає одним із вузлів, що взаємодіє з компонентами контекстного менеджера й історії діалогу, з можливістю персоналізації відповідей відповідно до ролей учасників, часових обмежень і типу теми обговорення [3].

На відміну від великих моделей, SLM відзначаються значно нижчими вимогами до пам'яті й обчислювальної потужності, що робить їх привабливими для розробки локальних агентів у сервіси онлайн-зустрічей, де темп і масштаб інтерпретації мовної інформації критичні для ефективної підтримки учасників. Архітектурні рішення щодо інтеграції SLM включають розподілені схеми обчислень, де транскрипційний модуль працює автономно, а SLM відповідає за семантичне узагальнення та генерацію висновків у реальному часі..

Висновки. Аналіз сучасних досліджень в області SLM показує, що архітектурні рішення повинні враховувати специфіку домену, потребу в реальному часі та адаптивності до діалогових контекстів. Подальші дослідження можуть спрямовуватися на покращення архітектурних інтеграцій, оптимізацію продуктивності моделей в умовах обмежених ресурсів і тестування в реальних сценаріях онлайн-комунікації..

Список використаних джерел:

1. Pham T.M., Nguyen P.T., Yoon S., Lai V.D., Dernoncourt F., Bui T. SlimLM: An Efficient Small Language Model for On-Device Document Assistance. ArXiv. 2024. P. 1–11.

Xu B., Chen Y., Wen Z., Liu W., He B. Evaluating Small Language Models for News Summarization: Implications and Factors Influencing Performance. Proceedings of the 2025 NAACL-Long. 2025. Vol. 1. P. 4909–4922.

Corradini F. State of the Art and Future Directions of Small Language Models. Information. 2025. Vol. 9, No 7. P. 189–189.

УДК 004.8:336.761:330.43

*Шведов Д.В., аспірант,
Національний університет «Одеська політехніка»*

РОЗРОБКА АЛГОРИТМУ ПОБУДОВИ ГІБРИДНИХ МОДЕЛЕЙ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ФІНАНСОВИХ РИЗИКІВ У СФЕРІ ДОВГОСТРОКОВИХ ІНВЕСТИЦІЙ

Вступ. Актуальність дослідження зумовлена зростанням складності фінансових ринків, посиленням глобалізаційних процесів та підвищенням невизначеності в умовах довгострокового інвестування. Трансформація економічних систем, цифровізація фінансових інструментів і поява нових класів активів формують багатовимірне середовище ризиків, яке не може бути адекватно описане виключно класичними статистичними підходами [1]. Довгострокові інвестиції характеризуються підвищеною чутливістю до макроекономічних коливань, структурних змін, політичних факторів та поведінкових аспектів учасників ринку. У таких умовах традиційні моделі оцінювання ризиків, що базуються на припущеннях нормальності розподілів демонструють обмежену прогностичну здатність [2].

Основна частина. Фінансові ризики довгострокового інвестування мають комплексний характер і включають ринковий, кредитний, ліквідності, інфляційний та системний компоненти. Їх формування відбувається під впливом як кількісно вимірюваних економічних показників, так і якісних факторів, що відображають очікування, поведінкові реакції та інформаційні асиметрії [3]. У зв'язку з цим модель оцінки ризиків повинна інтегрувати різномірні джерела даних, включаючи часові ряди макроекономічних індикаторів, фінансову звітність компаній, біржові котирування та альтернативні сигнали.

Запропонований алгоритм побудови гібридної моделі передбачає поетапну інтеграцію статистичних і машинних методів із забезпеченням їх функціональної узгодженості. На першому етапі здійснюється формування інформаційної бази. Вхідні дані проходять процедури очищення, нормалізації та усунення пропусків. Особлива увага приділяється перевірці стаціонарності часових рядів, виявленню структурних зламів та сезонних компонентів. Для зменшення розмірності простору ознак застосовуються методи головних компонент або автоенкодера.

Другий етап алгоритму пов'язаний із побудовою базової економіетричної моделі, яка відображає фундаментальні взаємозв'язки між ключовими змінними. Такою моделлю може виступати багатофакторна регресія або авторегресійна структура з розподіленими

лагами. Її функція полягає у формуванні первинної оцінки ризику та виділенні систематичних компонентів варіації. Отримані залишки інтерпретуються як нелінійна або стохастична складова, що не пояснюється класичними припущеннями.

На третьому етапі здійснюється застосування методів машинного навчання для моделювання залишкової структури ризику. Використовуються алгоритми ансамблевого типу, нейронні мережі глибинної архітектури або методи градієнтного підсилення. Їх вибір обґрунтовується здатністю виявляти складні нелінійні залежності та взаємодії високого порядку між ознаками. Навчання моделей проводиться на основі крос валідації з урахуванням часової послідовності даних, що запобігає інформаційному витоку та забезпечує коректність прогнозних оцінок.

Гібридизація моделей реалізується шляхом комбінування результатів економетричної та машинної складових. Інтеграція може здійснюватися через адитивну або зважену схему, де вагові коефіцієнти визначаються на основі мінімізації функції втрат. Такий підхід дозволяє зберегти інтерпретованість структурної частини моделі та одночасно підвищити точність прогнозу за рахунок інтелектуальної компоненти. Практична реалізація алгоритму можлива у вигляді програмного комплексу, що інтегрує модулі попередньої обробки даних, моделювання та візуалізації результатів.

Висновки. У результаті дослідження обґрунтовано необхідність використання гібридних моделей інтелектуального аналізу для оцінювання фінансових ризиків у сфері довгострокових інвестицій. Розроблений алгоритм поєднує економетричні методи та інструменти машинного навчання, що забезпечує підвищення точності прогнозування та збереження інтерпретованості результатів.

Список використаних джерел:

1. Kuzmenko O. Intelligent data mining approaches in portfolio risk assessment under economic uncertainty. *Economic Annals-XXI*. 2019. Vol. 178, No 7-8. P. 98–104.
2. Melnyk T. Development of integrated econometric and neural network models for financial risk evaluation in long-term investment strategies. *Financial Markets and Institutions*. 2021. Vol. 10, No 2. P. 142–156.
3. Peujio F. M. Hybrid Machine Learning Models for Long-Term Stock Market Forecasting: Integrating Technical Indicators. *Journal of Risk and Financial Management*. 2025. Vol. 18, No 4. P. 201–201.

УДК 004.932:004.8:534.222

*Шумейко К.П., аспірант,
Національний університет «Одеська політехніка»*

ІНТЕГРАЦІЯ МЕТОДІВ БАГАТОВИМІРНОГО АНАЛІЗУ МУЛЬТИМОДАЛЬНИХ ДАНИХ У ЗАДАЧАХ КЕРУВАННЯ ГІДРОАКУСТИЧНИМИ ПРОЦЕСАМИ

Вступ. Сучасні гідроакустичні системи функціонують у складному динамічному середовищі, що характеризується значною варіативністю параметрів водного середовища, наявністю шумових перешкод та багатоканальністю джерел інформації.

Актуальність дослідження зумовлена необхідністю підвищення ефективності керування гідроакустичними процесами на основі інтеграції різнорідних даних, отриманих із сенсорних систем різної фізичної природи.

Традиційні підходи до обробки сигналів, що ґрунтуються на одновимірних або слабо структурованих моделях, виявляються недостатніми для адекватного врахування складних просторово-часових залежностей [1].

Зростання обсягів мультимодальних даних, що включають акустичні сигнали, параметри середовища, навігаційні характеристики та додаткові контекстні ознаки, формує передумови для застосування методів багатовимірного аналізу.

Основна частина. Гідроакустичні процеси мають складну природу, яка визначається взаємодією хвильових явищ, властивостей середовища та характеристик джерел сигналів.

Формування інформативних ознак у таких системах відбувається на основі даних різної модальності, включаючи часові ряди акустичних коливань, спектральні характеристики сигналів, температурні та гідрологічні показники. Це зумовлює необхідність побудови моделей, здатних одночасно враховувати різнорідність і високий рівень кореляцій між ознаками [2].

Запропонований підхід передбачає багаторівневу обробку мультимодальних даних із використанням методів зниження розмірності, латентного представлення та інтеграції ознак. На початковому етапі здійснюється агрегація даних із різних сенсорних джерел із подальшою синхронізацією у спільному часовому просторі. Важливим аспектом є усунення шумів, компенсація втрат сигналу та нормалізація масштабів вимірювань.

Наступний етап передбачає застосування методів багатовимірного статистичного аналізу для виявлення структурних залежностей.

Зокрема, використовуються методи головних компонент, факторного аналізу та багатовимірного шкалювання, що дозволяють виділити найбільш інформативні компоненти даних та зменшити вплив надлишкових ознак. У випадку нелінійної структури даних доцільним є використання автоенкодерів або інших глибинних моделей представлення.

На рівні моделювання процесів керування застосовуються методи машинного навчання, орієнтовані на роботу з мультимодальними даними. До них належать рекурентні нейронні мережі для обробки часових залежностей, а також гібридні архітектури, що поєднують згорткові та рекурентні компоненти.

Такий підхід дозволяє враховувати як локальні особливості сигналів, так і їх довгострокову динаміку.

Інтеграція результатів різних моделей здійснюється на основі ансамблевих методів або через побудову метамоделей, що узагальнюють інформацію з кількох джерел.

Особливістю запропонованої концепції є орієнтація на адаптивне керування, при якому модель постійно оновлюється на основі нових даних. Це забезпечує підвищення стійкості системи до змін середовища та зменшення похибок прогнозування. Практична реалізація підходу передбачає створення програмно-апаратних комплексів, здатних працювати в режимі реального часу.

Висновки. У роботі обґрунтовано доцільність використання методів багатовимірного аналізу мультимодальних даних у задачах керування гідроакустичними процесами.

Запропонований підхід забезпечує підвищення точності аналізу та прогнозування за рахунок інтеграції різномірних джерел інформації та використання сучасних методів машинного навчання. Отримані результати можуть бути використані при розробці інтелектуальних гідроакустичних систем нового покоління..

Список використаних джерел:

1. Urick R. J. Principles of Underwater Sound. New York: McGraw-Hill, 1983. 423 p.
2. Haykin S. Neural Networks and Learning Machines. 3rd ed. New York: Pearson, 2009. 936 p.
3. Li X., Zhao Y. Multimodal Data Fusion in Underwater Acoustic Signal Processing. IEEE Access. 2023. Vol. 11. P. 45678–45692..

УДК 004.89:004.93

*Зленський А.О., аспірант,
Національний університет «Одеська політехніка»*

МЕТОДОЛОГІЧНІ ПІДХОДИ ПОБУДОВИ АДАПТИВНИХ СИСТЕМ ІНТЕЛЕКТУАЛЬНИХ АГЕНТІВ ДЛЯ ЗАДАЧ АНАЛІЗУ ТА ІДЕНТИФІКАЦІЇ ОБ'ЄКТІВ

Вступ. Розвиток інтелектуальних інформаційних технологій зумовлює зростання ролі агентних підходів у вирішенні задач аналізу та розпізнавання складних об'єктів. Актуальність дослідження визначається необхідністю створення адаптивних систем, здатних функціонувати в умовах невизначеності, неповноти даних і змінності середовища. Традиційні алгоритми класифікації та ідентифікації, що базуються на фіксованих моделях, демонструють обмежену ефективність при роботі з динамічними потоками даних і високою варіативністю ознак [1]. У цьому контексті інтелектуальні агенти розглядаються як автономні програмні сутності, здатні до самонавчання, адаптації та кооперації, що відкриває нові можливості для побудови ефективних систем розпізнавання.

Основна частина. Методологічна основа побудови адаптивних агентних систем передбачає поєднання принципів багаторівневої організації, розподіленої обробки інформації та інтеграції різних методів аналізу даних. Кожен агент у системі виконує спеціалізовані функції, пов'язані з обробкою окремих аспектів вхідної інформації, таких як виділення ознак, попередня класифікація або оцінювання достовірності результатів. Ключовим етапом є формування інформаційного простору ознак, що забезпечує адекватне представлення об'єктів. Для цього застосовуються методи попередньої обробки даних, включаючи нормалізацію, фільтрацію шумів і трансформацію ознак у компактні латентні представлення. Використання методів зниження розмірності дозволяє усунути надлишковість інформації та підвищити обчислювальну ефективність системи [2]. Архітектура агентної системи формується за ієрархічним або мережовим принципом, що забезпечує гнучкість взаємодії між агентами. На нижньому рівні функціонують агенти, орієнтовані на обробку сирих даних і виділення локальних ознак. На вищих рівнях здійснюється інтеграція результатів і прийняття рішень на основі агрегованої інформації. Взаємодія між агентами реалізується через механізми обміну повідомленнями та кооперативного навчання. Важливим методологічним аспектом є організація механізмів прийняття рішень у межах агентної системи з урахуванням

невизначеності та неповноти вхідної інформації. У цьому контексті доцільним є застосування ймовірнісних моделей, байєсівських підходів та нечіткої логіки, що дозволяють формалізувати процеси оцінювання альтернатив і вибору оптимальних рішень. Поєднання детермінованих і стохастичних методів забезпечує підвищення надійності ідентифікації об'єктів у складних умовах функціонування. Крім того, використання механізмів контекстно-орієнтованого аналізу дозволяє агентам враховувати додаткову інформацію про середовище, що суттєво покращує якість розпізнавання та зменшує кількість помилкових класифікацій. Адаптивність системи досягається за рахунок впровадження механізмів самонавчання та оновлення моделей у процесі експлуатації. Для цього використовуються методи машинного навчання, зокрема нейронні мережі, ансамблеві алгоритми та підходи підкріплювального навчання. Важливим аспектом є забезпечення узгодженості рішень, що приймаються різними агентами, шляхом використання стратегій колективного вибору або мета-рівня керування. Особлива увага приділяється здатності системи до узагальнення та перенесення знань між різними задачами ідентифікації. Це досягається через використання спільних представлень ознак і механізмів трансферного навчання. Такий підхід дозволяє підвищити ефективність роботи системи в умовах обмежених навчальних вибірок та змінних характеристик об'єктів.

Висновки. У результаті дослідження сформульовано методологічні засади побудови адаптивних систем інтелектуальних агентів для задач аналізу та ідентифікації об'єктів. Запропонований підхід базується на інтеграції розподіленої обробки даних, методів машинного навчання та механізмів адаптації, що забезпечує підвищення точності розпізнавання і стійкості до змін середовища. Практичне значення результатів полягає у можливості їх застосування при створенні інтелектуальних систем підтримки прийняття рішень.

Список використаних джерел:

1. Wooldridge M. An Introduction to MultiAgent Systems. 2nd ed. Chichester: Wiley, 2009. 484 p.
2. Bishop C. M. Pattern Recognition and Machine Learning. New York: Springer, 2006. 738 p.
3. Zhang Z., Liu H. Adaptive Multi-Agent Systems for Intelligent Recognition Tasks. Expert Systems with Applications. 2022. Vol. 198. P. 116–130.

УДК 004.75

*Голуб Д. К., магістрант,
Вишняк М. Ю., к.т.н., доцент
Харківський національний університет радіоелектроніки*

МЕТОДИ КОРЕЛЯЦІЇ ЗАПИТІВ ТА ВІДПОВІДЕЙ ПРИ АСИНХРОННІЙ ВЗАЄМОДІЇ З APACHE KAFKA

Сучасна розробка програмного забезпечення все частіше базується на мікросервісній архітектурі [1], яка передбачає розбиття системи на набір незалежних сервісів. Ключовим викликом при проектуванні таких систем є організація надійної та ефективної комунікації між ними. Популярним патерном є асинхронний request-reply, який поєднує переваги синхронної взаємодії з перевагами асинхронності. Однак, такі брокери повідомлень як Apache Kafka, не мають нативної підтримки цього патерну, що ускладнює його використання в проектах, де Kafka вже задіяна для інших цілей (наприклад, обробка подій).

Apache Kafka працює за моделлю "publish-subscribe" [2], де споживачі читають повідомлення з топіків у власному темпі, і не передбачає прямого зв'язку між відправником конкретного повідомлення та його отримувачем. Для подолання цього обмеження було розроблено метод, що базується на кількох ключових компонентах.

Основа методу – присвоєння унікального ідентифікатора (UUID v4) кожному вихідному запиту. Цей correlationId додається до заголовків Kafka-повідомлення. Окрім цього, в заголовки додається параметр replyTo, який містить назву топіка, куди сервіс-виконавець має надіслати відповідь. Такий підхід дозволяє будь-якому споживачу, який отримав запит, зрозуміти, куди і з яким ідентифікатором потрібно відправити результат. Структурно механізм взаємодії наведено на рисунку 1 у вигляді UML Sequence Diagram.

Клієнтський компонент ініціює виклик методу service Service A, передаючи необхідні вхідні дані. Після отримання запиту сервіс генерує унікальний ідентифікатор кореляції, який використовується для подальшого зіставлення відповіді із відповідним запитом. Одночасно створюється об'єкт Promise [3], що представляє майбутній результат виконання операції, і посилання на нього зберігається у внутрішній структурі даних типу Map<correlationId, Promise>. Після цього сервіс формує повідомлення-запит, яке містить ідентифікатор кореляції, назву топіка для відповіді та дані запиту, і публікує його до відповідного топіка запитів у брокері повідомлень.

Сервіс Service B у режимі безперервного споживання повідомлень отримує запит із топіка, виконує необхідну бізнес-логіку обробки та формує повідомлення-відповідь, що містить той самий correlationId і результат виконання. Це повідомлення публікується до топіка відповідей. Сервіс Service A, який постійно виконує цикл споживання повідомлень з цього топіка, отримує відповідь, зчитує ідентифікатор кореляції та знаходить відповідний об'єкт Promise у своїй внутрішній структурі. Після цього виконується операція resolve, у результаті чого початковий виклик методу отримує результат виконання запиту. Такий підхід дозволяє поєднати асинхронну взаємодію через брокер повідомлень із семантикою класичної моделі запиту та відповіді, забезпечуючи слабке зв'язування між мікросервісами та ефективну кореляцію повідомлень.

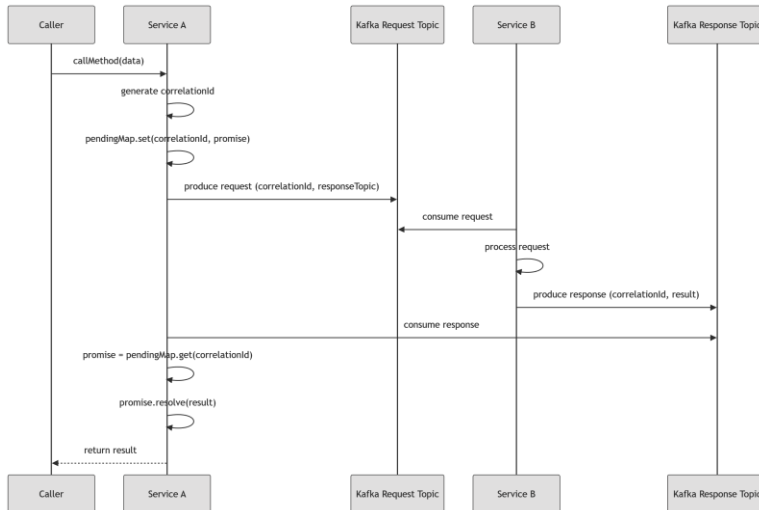


Рис.1. UML Sequence Diagram процесу виконання запиту

Список використаних джерел:

1. Richards M., Ford N. Fundamentals of Software Architecture. Sebastopol : O'Reilly Media, 2020. 383 с.
2. Documentation for Apache Kafka. URL: <https://kafka.apache.org/41/getting-started/introduction/> (дата звернення: 14.03.2026).
3. Pasquali S. Mastering Node.js. Birmingham : Packt Publishing Ltd., 2013. 347 с.

УДК:004.67

Коротун О.В., к. т. н., доцент

Пасічник В.О., магістрант

Державний університет «Житомирська політехніка»

СУЧАСНІ ПІДХОДИ ТА ТЕХНОЛОГІЇ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ АНАЛІЗУ ФІЗИЧНОГО СТАНУ ЛЮДИНИ

Стрімкий розвиток технологій моніторингу та біометричних сенсорів дозволив змінити підходи до аналізу показників фізичного стану людини [1]. Масова доступність цифрових інструментів для відстеження активності, зокрема підрахунку кількості пройдених кроків та спалених калорій, надала користувачам можливість самостійно накопичувати та аналізувати персональні дані без обов'язкового супроводу фахівців. Унаслідок цього в сучасному світі спостерігається зростання зацікавленості у регулярному контролі власних фізичних показників. За статистикою, кількість людей віком від 16 до 35, які виконують фізичні навантаження, значно зросла протягом останніх років [2]. У зв'язку з цим зростає потреба в об'єктивних підходах до оцінювання фізичного стану та аналізу індивідуальних показників здоров'я.

Метою дослідження є системний аналіз наявних технологічних рішень та методів побудови системи, призначених для класифікації та порівняльного оцінювання індивідуальних фізичних параметрів.

Об'єктом дослідження є процеси інтелектуального збору, оброблення, візуалізації та класифікації даних про фізичні параметри людини, а предметом дослідження - алгоритмічні підходи до зіставлення персональних показників із референтними значеннями, методи візуалізації залежностей між складом тіла та показниками здоров'я. У межах роботи застосовано методи антропометричного аналізу, порівняльно-типологічний підхід та метод узагальнення технічних характеристик сучасних інтелектуальних систем.

Під час дослідження було проведено комплексний огляд архітектурних рішень, у яких ключовим функціоналом є порівняння індивідуальних показників із нормативними значеннями відповідно до вікової категорії. Аналіз показав, що аналітична складова сучасних систем базується на механізмі зіставлення фактичних параметрів користувача з показниками, що встановлюються міжнародними та національними організаціями охорони здоров'я на основі масштабних наукових досліджень. Такі системи не виконують діагностичну

функцію, а слугують інструментом для порівняльного аналізу та інформаційної підтримки користувача.

Використання інтелектуальних систем для візуалізації та порівняння фізіологічних параметрів розглядається як засіб підвищення обізнаності користувачів щодо власного стану здоров'я. Результати огляду наукових джерел свідчать, що візуалізація динаміки змін індивідуальних параметрів у форматі порівняння «до» та «після» сприяє підвищенню мотивації до покращення фізичного зовнішнього вигляду та подальшого контролю антропометричних характеристик [3].

Теоретична значущість полягає у систематизації підходів до побудови недіагностичних систем моніторингу фізичних показників, а практична - у формулюванні бази для розробки інтерфейсів та алгоритмів, що забезпечують коректне порівняння фізичних параметрів та нормативних значень.

Перспективним напрямом подальших досліджень є впровадження інтелектуальних алгоритмів для поглибленого аналізу фізичних показників та розширення інструментарію візуалізації для наочного відображення м'язових та функціональних параметрів з урахуванням вікових груп.

Список використаних джерел:

1. Piwek L., Ellis D. A., Andrews S., Joinson A. The Rise of Consumer Health Wearables: Promises and Barriers. PLOS Medicine. 2016. Vol. 13, No. 2. e1001953. (дата звернення: 15.02.2026)

URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC4737495/>

2. Gen Z and Millennial Fitness Report 2023 : Understanding the future of fitness. Les Mills International. 2023. (дата звернення: 16.02.2026)

URL: <https://ru.scribd.com/document/685199762/les-mills-international-2023-gen-z-fitness-cracking-the-code-en-hr>

3. Дяченко А., Кульчицька І., Антонюк А. Підвищення мотивації до занять руховою активністю студентів на основі використання фітнес-додатків // ТОВ «ТВОРИ». 2021. (дата звернення: 20.02.2026)

URL: <https://dspace.vspu.edu.ua/items/5a986f9f-f79a-49d9-ac46-5725dce65446>

УДК:004.67

Коротун О.В., к. т. н., доцент

Пасічник В.О., магістрант

Державний університет «Житомирська політехніка»

ПРОЄКТУВАННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ АНАЛІЗУ ФІЗИЧНОГО СТАНУ ЛЮДИНИ

В умовах зростання інтенсивності повсякденної діяльності особливої актуальності набуває підтримання належного рівня фізичної форми людини. Водночас ведення здорового режиму та профілактика захворювань сприяють підвищенню якості життя [1], що, у свою чергу, формує підвищений попит на програмні рішення у сфері моніторингу здоров'я [2]. Такі системи мають забезпечувати можливість самостійного та регулярного оцінювання показників фізичної форми організму без необхідності постійного залучення вузькопрофільних спеціалістів.

Актуальність роботи зумовлена потребою у зручних програмних інструментах, що забезпечують автоматизований збір, збереження, обробку та аналіз антропометричних даних із можливістю їх порівняння з нормативними значеннями.

Мета дослідження полягає у розробленні архітектури та програмного продукту для комплексного аналізу й моніторингу фізичного стану людини, що забезпечує автоматизоване порівняння отриманих показників з еталонними даними та візуалізацію динаміки змін основних фізичних параметрів. Об'єктом дослідження є процес моніторингу фізичного стану людини із використанням інформаційних технологій.

Предметом дослідження є методи, алгоритми та програмні засоби обробки даних, реалізовані з використанням сучасних мов програмування та відповідних бібліотек, що забезпечують функціонування системи аналізу антропометричних параметрів людини.

У роботі використано методи описової статистики та кореляційного аналізу для оцінки взаємозв'язків між антропометричними показниками, методи часових рядів для аналізу динаміки змін, а також методи візуалізації даних для інтерпретації результатів аналізу.

Програмна реалізація розробленої системи базується на використанні екосистеми Python, що забезпечує гнучкість, масштабованість та можливість інтеграції сучасних інструментів обробки даних. Архітектура системи є модульною та включає

підсистему введення і попередньої обробки даних, модуль автоматизованого порівняння індивідуальних антропометричних показників з нормативними значеннями [3] на основі статистичних критеріїв, модуль побудови графічних візуалізацій, а також підсистему автоматизованої генерації аналітичних звітів. Система здійснює виявлення статистичних закономірностей, зокрема кореляційних залежностей між динамікою маси тіла та об'ємними антропометричними показниками, а також реалізує прогнозування показників на основі аналізу накопиченої історії вимірювань.

Передбачається, що використання інтелектуальної системи автоматизованого порівняння антропометричних показників із нормативними значеннями сприятиме підвищенню об'єктивності інтерпретації результатів та створенню умов для підвищення мотивації користувача.

Теоретична значущість полягає в обґрунтуванні моделі інтелектуального аналізу антропометричних даних. Практична значущість роботи у можливості використання системи як інструмент самоконтролю та допоміжного засобу аналізу даних.

Перспективи подальших досліджень пов'язані з розширенням функціональних можливостей системи шляхом інтеграції з API пристроїв для моніторингу показників організму, а також впровадженням більш складних моделей машинного навчання для прогнозування тенденцій фізичного розвитку.

Список використаних джерел:

1. Mangra M. G., et al. The role of physical activity opportunities and local environments in promoting health and longevity // Healthcare. – 2025. – Vol. 13, No. 17. – Article 2110. (дата звернення: 20.02.2026)
URL: <https://www.mdpi.com/2227-9032/13/17/2110>
2. Digital Health Monitoring Solutions Market Growth 2025: Trends, Consumer Demand / OpenPR — 2025. (дата звернення: 20.02.2026)
URL: <https://www.openpr.com/news/4119677/digital-health-monitoring-solutions-market-growth-2025>
3. Mopidip: a modular real-time pipeline for machinery diagnosis and prognosis based on deep learning algorithms // Journal of Big Data. — 2025. (дата звернення: 21.02.2026)
URL: <https://link.springer.com/article/10.1186/s40537-025-01123-8>

УДК 004.42

*Картамишев Д.О., к.т.н., асистент
Донбаська державна машинобудівна академія*

МОВА ПРОГРАМУВАННЯ GO У ЗАДАЧАХ АВТОМАТИЗАЦІЇ ІНФРАСТРУКТУРНИХ ПРОЦЕСІВ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Зростання складності сучасних програмних систем безпосередньо впливає на підходи до управління обчислювальною інфраструктурою. У хмарних середовищах та мікросервісних архітектурах кількість взаємодіючих компонентів може вимірюватися сотнями сервісів, що значно ускладнює ручне адміністрування та підтримку систем. За таких умов автоматизація операційних процесів поступово переходить із допоміжного інструмента у необхідну складову функціонування інформаційної інфраструктури.

У контексті розробки інфраструктурного програмного забезпечення особливу увагу привертає мова програмування Go. Її архітектура формувалася з урахуванням потреб створення мережових сервісів та системного програмного забезпечення. Поєднання відносно простого синтаксису з компільованою моделлю виконання дозволяє досягати продуктивності, характерної для системних мов програмування, зберігаючи при цьому зручність розробки.

Однією з ключових особливостей Go є підтримка конкурентних обчислень. Механізм goroutines забезпечує можливість створення великої кількості паралельних процесів виконання з мінімальними накладними витратами. На відміну від традиційних потоків операційної системи, goroutines реалізуються у межах власного планувальника середовища виконання Go, що дозволяє більш ефективно використовувати обчислювальні ресурси під час обробки великої кількості подій.

Подібний підхід особливо добре проявляє себе у системах, де одночасно виконуються операції моніторингу, обробки запитів та управління конфігураціями сервісів. Передача даних між процесами за допомогою channels формує зрозумілу модель взаємодії компонентів та дозволяє уникнути складних механізмів синхронізації, які часто використовуються у традиційному багатопотоковому програмуванні.

Поширення Go у сфері автоматизації інфраструктури підтверджується її використанням у низці сучасних технологічних платформ. Зокрема, такі системи як Docker, Kubernetes, Prometheus та Terraform реалізовані із застосуванням цієї мови. Зазначені проєкти виконують задачі контейнеризації, оркестрації сервісів та збору

телеметричних даних, що передбачає обробку значних обсягів подій у режимі реального часу.

Окремої уваги заслуговує і процес розгортання програм, написаних на Go. Після компіляції формується автономний виконуваний файл, який містить усі необхідні залежності. Такий підхід значно спрощує розгортання програмних компонентів у контейнерних та кластерних середовищах, що є типовими для сучасних інформаційних систем.

У межах проведеного дослідження було проаналізовано підходи до побудови сервісів автоматизованого моніторингу та керування інфраструктурою із використанням Go. Запропоновано архітектурну модель сервісу збору подій, що базується на асинхронній обробці повідомлень та використанні конкурентних механізмів мови. Така модель дозволяє зменшити затримки обробки подій і водночас підвищити ефективність використання обчислювальних ресурсів.

Отримані результати свідчать, що використання Go у задачах автоматизації інфраструктури є доцільним для систем, у яких важливими є висока пропускна здатність, ефективна обробка подій та простота розгортання програмних компонентів.

Варто також зазначити, що застосування Go у задачах автоматизації часто поєднується з подієво-орієнтованими архітектурами. У таких системах обробка подій відбувається асинхронно, а окремі компоненти взаємодіють через повідомлення або черги. Подібна модель дозволяє зменшити зв'язність між сервісами та підвищити стійкість системи до відмов окремих компонентів. У практичних реалізаціях це означає, що система здатна продовжувати роботу навіть у випадку часткових збоїв інфраструктури.

З технічної точки зору Go добре підходить для реалізації подібних механізмів. Вбудовані бібліотеки мови забезпечують зручні засоби для роботи з мережевими протоколами, обробки HTTP-запитів та створення сервісів, що працюють у режимі постійного обміну даними. Крім того, стандартна бібліотека містить інструменти профілювання та моніторингу продуктивності, що значно спрощує аналіз поведінки системи під навантаженням.

Список використаних джерел:

1. Donovan A. A., Kernighan B. W. The Go Programming Language. – Boston : Addison-Wesley Professional, 2016. – 380 p.
2. Pike R. Go at Google: Language Design in the Service of Software Engineering [Electronic resource]. – 2012. – Available at: <https://go.dev/talks/2012/splash.article> (accessed: 16.03.2026).

УДК: 004.62:005.52:336

*Гладченко О.В., к.пед.н., доцент
Коваленко К.А. здобувачка вищої освіти
Державний податковий університет*

СИСТЕМНИЙ АНАЛІЗ ВЕЛИКИХ ДАНИХ У ФІНАНСОВОМУ СЕКТОРІ

Однією з найперспективніших технологій автоматизації фінансового аналізу сьогодні є обробка великих даних. Найчастіше її застосовують для роботи з так званими альтернативними даними – тобто інформацією, що використовується у фінансовому аналізі, але отримується нетрадиційними способами і не надходить безпосередньо від підприємства чи з офіційних джерел. Наразі налічується понад тисячу різноманітних джерел альтернативних даних [2].

Системний аналіз – це процес дослідження, оцінювання, опису та вдосконалення складних систем. Під системами розуміють широкий спектр об'єктів — від технічних і організаційних до соціальних і природних структур. Основне завдання системного аналізу полягає у виявленні взаємозв'язків між елементами системи, що забезпечує її ефективне та узгоджене функціонування [4].

Розглядаючи поняття Big Data (або великих даних) у банківському секторі, варто розуміти, що це передусім колосальні обсяги різноманітної інформації – як чітко структурованої, так і неструктурованої, – яка перебуває у стані безперервного оновлення. Завдяки впровадженню цих технологій фінансові установи отримують потужний інструмент не лише для безпечного накопичення та зберігання масивів даних, але й для їхньої глибокої обробки, що допомагає виявляти приховані закономірності та будувати точні аналітичні прогнози.

Завдяки оперуванню величезними масивами інформації банківська сфера стала одним із лідерів у впровадженні новітніх технологій, що відкриває широкі перспективи для її розвитку. Водночас ефективне використання таких ресурсів потребує переходу до швидкої автоматизованої обробки, оскільки традиційний ручний аналіз у сучасних умовах є практично неможливим.

У практиці банків великі дані найчастіше застосовуються для аналізу чинних і потенційних клієнтів. Зокрема, обробляється інформація про покупки, активність у соціальних мережах, фінансові операції та транзакції. Це дає змогу формувати персоналізовані пропозиції, зменшувати ризики співпраці з ненадійними клієнтами та, як наслідок, підвищувати прибутковість банку [1].

Одним із ключових аспектів, що пояснює необхідність аналізу даних у фінансовій сфері, є:

1. Аналіз реалізації фінансових продуктів. Для підвищення рівня продажів і збільшення ймовірності позитивного рішення клієнта важливо запропонувати послугу саме в той момент, коли вона є найбільш актуальною. На основі аналізу поведінки клієнтів система формує узагальнений профіль потенційного споживача (клієнта або позичальника) та створює для нього індивідуалізовані пропозиції.

2. Антифрод-система. Це сучасний напрям застосування великих даних, спрямований на виявлення шахрайських операцій і схем. У разі фіксації нетипових дій клієнта банк може тимчасово зупинити транзакцію. При цьому аналізуються різні показники та поведінкові моделі, що свідчать про можливу підозрілу активність, зокрема раптове зростання сум переказів або здійснення платежів на нові реквізити [3].

Використання Big Data у фінансовій сфері суттєво підвищує ефективність аналізу, управління ризиками та прийняття управлінських рішень. Поєднання технологій великих даних із системним аналізом забезпечує комплексний підхід до дослідження банківської діяльності, дозволяє враховувати взаємозв'язки між її елементами та підвищує обґрунтованість фінансових рішень. Це сприяє зростанню конкурентоспроможності та стабільному розвитку банківських установ.

Список використаних джерел:

1. Big Data в банках: що це таке й у чому користь для банківського сектору. URL: <https://hub.kyivstar.ua/articles/big-data-v-bankah-shho-cze-take-j-u-chomu-koristi-dlya-bankivsikogo-sektoru>

2. Берко А., Одрехівський М., Яромич М. Інформаційні технології фінансового аналізування. *Вісник Хмельницького національного університету. Серія: Технічні науки*. 2024. № 4. С. 35–42. URL: <https://heraldts.khmnu.edu.ua/index.php/heraldts/article/download/186/321/1047>

3. Для чого потрібен аналіз даних у фінансовій сфері: три приклади. Незалежний громадський портал. URL: <https://ngr-ua.info/2023/09/67597>

4. Системний аналіз: необхідна навичка для кожного IT-спеціаліста. URL: <https://dan-it.com.ua/uk/blog/sistemnij-analiz-neobhidna-navichka-dlja-kozhnogo-it-specialista/>

УДК 004.45:004.65

*Сокорчук І.П., ст. викладач**Харківський національний університет радіоелектроніки*

ЕФЕКТИВНЕ ВИКОРИСТАННЯ СТАНДАРТНИХ УТИЛІТ LINUX ДЛЯ ПОШУКУ ДУБЛІКАТІВ ФАЙЛІВ

Пошук дублікатів файлів є актуальним завданням адміністрування комп'ютерних систем, оптимізації використання дискового простору та підвищення ефективності зберігання даних. Наявність дубльованих файлів призводить до нераціонального використання ресурсів, ускладнює резервне копіювання та знижує продуктивність обробки інформації. У зв'язку з цим важливим є застосування ефективних інструментів і методів для виявлення та аналізу однакових файлів у файлових системах.

Одним із найбільш гнучких підходів є використання стандартних засобів операційної системи Linux у поєднанні з командним інтерпретатором Bash. Зокрема, ефективним є комбінування утиліт `find`, `xargs`, `md5sum`, `sha256sum`, `sort` та `uniq`. Такий підхід дозволяє формувати масштабовані рішення без необхідності встановлення додаткового програмного забезпечення. Основна ідея полягає у генерації контрольних сум файлів і подальшому групуванні результатів для виявлення збігів.

Для автоматизації обробки великої кількості файлів доцільно застосовувати пакетну передачу аргументів через `xargs`. Ця утиліта забезпечує ефективне використання системних ресурсів за рахунок обробки даних блоками, а також підтримує обмежене розпаралелювання через параметр `-P`. Використання значення `$(nproc)` дозволяє задіяти всі доступні обчислювальні ядра, що суттєво підвищує продуктивність у багатоядерних системах. Разом із тим, `xargs` має обмежені можливості балансування навантаження і не забезпечує гнучкого керування процесами.

Альтернативним інструментом є утиліта `GNU parallel`, яка реалізує більш досконалі механізми паралельного виконання. Вона дозволяє автоматично розподіляти завдання між ядрами процесора, задавати кількість паралельних процесів і забезпечує впорядковане виведення результатів. Крім того, підтримується виконання завдань на віддалених вузлах, що розширює можливості застосування у розподілених системах. Недоліками є підвищене споживання ресурсів та необхідність попереднього встановлення.

Для формування контрольних сум можуть використовуватися алгоритми MD5, SHA-256 та SHA-512. Алгоритм MD5

характеризується високою швидкістю, проте має нижчу криптографічну стійкість. Алгоритми SHA-256 та SHA-512 забезпечують більшу надійність і точність ідентифікації файлів, хоча потребують більше обчислювальних ресурсів. Вибір конкретного алгоритму визначається співвідношенням вимог до швидкодії та достовірності результатів.

Спеціалізовані утиліти, такі як `fdupes` та `rdfind`, надають готові рішення для пошуку дублікатів. Вони поєднують використання контрольних сум із побайтовим порівнянням, що дозволяє зменшити кількість хибних збігів. Перевагою таких утиліт є простота використання, проте їх функціональність є менш гнучкою порівняно з комбінованими рішеннями на основі стандартних інструментів.

Додатковим підходом є застосування скриптів мовою Python із використанням бібліотеки `hashlib`. Це дозволяє реалізувати складні алгоритми фільтрації, оптимізації та обробки результатів. Такий підхід є доцільним у випадках, коли стандартні утиліти не забезпечують необхідної функціональності.

На рівні файлових систем також можливе використання вбудованих механізмів дедуплікації, зокрема у файловій системі `btrfs`. У цьому випадку усунення дублювання відбувається автоматично без участі користувача, що є ефективним для великих сховищ даних.

Таким чином, вибір методу пошуку дублікатів файлів залежить від обсягу даних, апаратних ресурсів та вимог до продуктивності. Для простих задач доцільно використовувати `xargs` у поєднанні зі стандартними утилітами. Для високонавантажених систем більш ефективним є застосування `GNU parallel`. У випадках, що потребують максимальної гнучкості, доцільно використовувати програмні рішення на Python або вбудовані можливості файлових систем.

Список використаних джерел:

1. GNU Findutils Manual [Електронний ресурс]. – Режим доступу: <https://www.gnu.org/software/findutils/manual/> (дата звернення: 03.03.2025).
2. Kerrisk M. `xargs(1)` – Linux man-pages project [Електронний ресурс] / M. Kerrisk. – Режим доступу: <https://man7.org/linux/man-pages/man1/xargs.1.html> (дата звернення: 03.03.2025).
3. GNU Coreutils Manual [Електронний ресурс]. – Режим доступу: <https://www.gnu.org/software/coreutils/manual/> (дата звернення: 03.03.2025).
4. GNU Parallel Manual [Електронний ресурс]. – Режим доступу: <https://www.gnu.org/software/parallel/> (дата звернення: 03.03.2025).

УДК 004.8

*Батраченко С.М., студент,
П'ятаченко В.Ю., PhD., асистент
Сумський державний університет*

ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ АНАЛІЗУ ХАРЧОВИХ ЗВИЧОК НА ОСНОВІ ANDROID-ДОДАТКА

Рациональне харчування є важливим чинником підтримання здоров'я, однак сучасні харчові звички часто характеризуються надлишком калорій і дефіцитом корисних компонентів [1]. У зв'язку з цим зростає потреба в інструментах, що дозволяють користувачам аналізувати раціон і контролювати споживання поживних речовин.

Мобільні застосунки для харчування розглядаються як ефективний інструмент формування здорових звичок. Дослідження[2,3] показують, що вони можуть покращувати харчову поведінку користувачів, зокрема підвищувати споживання корисних продуктів і рівень самоконтролю. Водночас більшість рішень орієнтована на зниження ваги, а не на детальний аналіз харчових звичок [3].

Серед поширених аналогів можна виділити MyFitnessPal, YAZIO та FatSecret, які забезпечують облік калорій і макронутрієнтів, а також додаткові функції, зокрема сканування штрихкодів і елементи автоматизованого аналізу (AI). Водночас ці застосунки орієнтовані на масового користувача та зосереджені переважно на контролі калорій і ваги, що обмежує можливості детального аналізу харчових звичок.

Запропоновано інформаційну систему аналізу харчових звичок у вигляді Android-застосунку на основі Flutter/Dart. Застосунок, на відміну від багатьох комерційних аналогів, забезпечує локальний розрахунок енергетичної цінності продуктів і вмісту вітамінів та орієнтований на автономну роботу без серверного середовища.

Система реалізована за модульним принципом і включає, зокрема, модулі автентифікації користувача та калькулятори поживних речовин (рис. 1). Для забезпечення безпеки використовується хешування паролів за алгоритмом SHA-256 із випадковою сіллю. Модуль розрахунку калорій і макронутрієнтів забезпечує пошук продуктів за назвою, задання їх маси та обчислення калорійності, білків, жирів і вуглеводів. Калькулятор вітамінів реалізовано у двох режимах: для окремого продукту та добового раціону з оцінкою їх вмісту відносно рекомендованих норм.

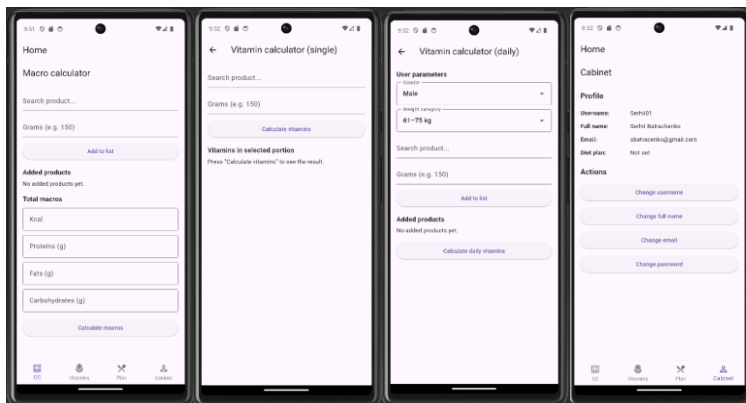


Рис.1. Інтерфейси основних екранів застосунку: головний екран, калькулятор калорій, калькулятори вітамінів, кабінет користувача

Архітектура системи є багатoshаровою: інтерфейс користувача взаємодіє із сервісним шаром, який працює з DAO та локальною базою SQLite. Використано підхід offline-first, за якого основні операції виконуються локально без залежності від зовнішнього сервера. База даних містить інформацію про користувачів, продукти, вітаміни та їх зв'язки. Такий підхід забезпечує автономність і спрощує розгортання.

Застосунок має практичну цінність як інструмент аналізу харчових звичок і може слугувати основою для створення повноцінної системи підтримки прийняття рішень. Перспективи розвитку включають персоналізовані рекомендації, автоматичне формування раціону, розширення бази даних і інтеграцію з хмарними сервісами.

Список використаних джерел:

1. Healthy diet. World Health Organization (WHO). URL: <https://www.who.int/news-room/fact-sheets/detail/healthy-diet> (date of access: 20.03.2026).
2. Seid A., Fufa D. D., Bitew Z. W. The use of internet-based smartphone apps consistently improved consumers' healthy eating behaviors: a systematic review of randomized controlled trials. *Frontiers in Digital Health*. 2024. Vol. 6. DOI:10.3389/fdgth.2024.1282570
3. Smartphone applications for nutrition Support: A systematic review of the target outcomes and main functionalities / D. Pala et al. *International Journal of Medical Informatics*. 2024. Vol. 184. P. 105351. DOI:10.1016/j.ijmedinf.2024.105351

УДК 004.93:681.883.41

*Шумейко К.П., аспірант,
Національний університет «Одеська політехніка»*

ВИКОРИСТАННЯ FUSION-МОДЕЛІ ДЛЯ АНАЛІЗУ МУЛЬТИМОДАЛЬНИХ ДАНИХ

Вступ. В умовах розвитку сучасних інтелектуальних систем особливої актуальності набуває задача спільного аналізу даних, що надходять із різних джерел. На практиці такими джерелами можуть бути зображення, часові ряди, сигнали датчиків, текстові описи та інші типи інформації, які відрізняються за структурою, розмірністю та фізичною природою. Використання лише одного каналу спостереження не завжди забезпечує отримання повного й стійкого уявлення про об'єкт дослідження, оскільки окреме джерело даних може містити шуми, пропуски або обмежений набір інформативних ознак. У зв'язку з цим значний інтерес становить застосування fusion-моделей, призначених для об'єднання різнорідних даних у межах єдиної аналітичної системи [1], [2].

З методичної точки зору fusion-моделі можуть реалізовуватися на різних рівнях обробки інформації. Найпоширенішими є об'єднання на рівні вихідних даних, на рівні ознак і на рівні рішень. Вибір конкретної схеми залежить від структури вхідної інформації, ступеня узгодженості використовуваних джерел і вимог прикладної задачі. Загалом fusion-підхід дає змогу враховувати взаємодоповнювальні властивості різних каналів спостереження і тим самим підвищувати точність, стійкість та інформативність підсумкового аналізу [1], [2].

Основна частина. Одним із перспективних напрямів застосування fusion-моделей є розпізнавання об'єктів у підводному середовищі. У межах цієї задачі найбільший практичний інтерес становить спільне використання відеоданих і даних сонара, оскільки зазначені джерела формують різний, але взаємодоповнювальний опис однієї й тієї самої сцени. Відеокамера забезпечує отримання детального візуального представлення об'єкта, що дає змогу аналізувати його форму, контури, текстурні особливості та, за достатньої якості зображення, колірні характеристики. Водночас ефективність оптичного каналу в підводних умовах істотно знижується внаслідок поглинання і розсіювання світла, зменшення контрасту, кольірних спотворень та обмеженої дальності видимості [3], [4].

На відміну від відеоканалу, сонар зберігає працездатність в умовах низької прозорості води, слабкого освітлення та на значних відстанях. Проте сонаРНі дані, як правило, характеризуються меншою візуальною деталізацією, підвищеним рівнем шумів і обмеженою виразністю ознак, безпосередньо пов'язаних із зовнішнім виглядом об'єкта. Таким чином,

використання лише одного із зазначених джерел не дає змоги забезпечити стійке розпізнавання в усьому діапазоні умов спостереження. Об'єднання відеоданих і даних сонара в межах fusion-моделі є обґрунтованим, оскільки дає змогу компенсувати обмеження кожної з модальностей і сформуванати більш повний опис підводної сцени [3], [5].

З точки зору побудови системи розпізнавання об'єднання відеоінформації та сонарних даних може здійснюватися на кількох рівнях. На рівні вихідних даних можливе спільне використання синхронізованих кадрів після виконання калібрування та просторового вирівнювання сенсорів. На рівні ознак доцільним є спільне використання візуальних характеристик зображення та акустичних структурних ознак, що відображають форму, положення й дистанційні особливості об'єкта. На рівні рішень можуть об'єднуватися результати незалежних моделей, які функціонують окремо для кожного каналу спостереження. Подібна багаторівнева організація дає змогу обирати найефективнішу стратегію fusion залежно від доступності узгоджених наборів даних, обчислювальних обмежень і вимог до точності розпізнавання [1], [2].

Для задач підводного розпізнавання об'єктів особливе значення має здатність fusion-моделі адаптуватися до зміни умов спостереження. У ситуаціях, коли якість відеоданих залишається достатньою, система може більшою мірою спиратися на детальні візуальні ознаки. У разі погіршення прозорості води, зниження освітленості або появи виражених оптичних спотворень зростає значущість сонарного каналу, який дає змогу зберігати інформацію про наявність об'єкта, його просторове положення та загальну структуру. Отже, fusion-підхід забезпечує більш стійке функціонування системи розпізнавання порівняно з використанням лише оптичних або лише акустичних даних [3], [5].

Водночас практична реалізація fusion-моделей для підводного розпізнавання пов'язана з низкою труднощів. До них належать відмінність фізичної природи відеоданих і даних сонара, відсутність прямої попиксельної відповідності між ними, необхідність часової синхронізації, різниця просторової роздільної здатності, наявність шумів, а також обмеженість відкритих узгоджених наборів даних, придатних для навчання і тестування двоканальних моделей [3], [5], [6]. У зв'язку з цим найважливішими етапами побудови подібних систем є калібрування сенсорів, просторово-часове узгодження модальностей, формування спільного простору ознак і розроблення механізмів адаптивного врахування внеску кожного джерела даних у підсумкове рішення.

Таким чином, застосування fusion-моделі для об'єднання відеоданих і даних сонара слід розглядати як перспективний напрям підвищення ефективності підводного розпізнавання об'єктів. Використання цього підходу дає змогу перейти від ізолюваного аналізу окремих каналів спостереження до формування більш цілісного та стійкого уявлення про підводну сцену. Найперспективнішими є архітектури, що забезпечують спільне навчання ознак, міжмодальну взаємодію та адаптивний перерозподіл значущості вхідних даних залежно від умов спостереження [3], [5].

Висновки. Використання fusion-моделей є перспективним підходом до аналізу різномірних даних, що забезпечує підвищення точності та стійкості інтелектуальних систем за рахунок об'єднання інформації з кількох джерел. У задачах підводного розпізнавання об'єктів особливу практичну значущість має спільна обробка відеоданих і даних сонара. Відеоканал дає змогу отримувати детальний семантичний опис сцени, тоді як сонар зберігає працездатність в умовах поганой видимості та на значних відстанях. Їх об'єднання в межах fusion-моделі дає змогу компенсувати обмеження кожного окремого каналу та підвищити надійність розпізнавання об'єктів у складних умовах підводного середовища.

Перспективи подальших досліджень пов'язані з удосконаленням методів калібрування й узгодження модальностей, розширенням узгоджених наборів даних, а також розробленням адаптивних fusion-архітектур, здатних ефективно функціонувати в режимі реального часу на борту підводних робототехнічних платформ.

Список використаних джерел:

1. Hall D. L., Llinas J. An Introduction to Multisensor Data Fusion. Proceedings of the IEEE. 1997. Vol. 85, No 1. P. 6–23.
2. Castanedo F. A Review of Data Fusion Techniques. The Scientific World Journal. 2013. Vol. 2013. Article 704504.
3. Kim H. G., Seo J., Kim S. et al. Underwater Optical-Sonar Image Fusion Systems. Sensors. 2022. Vol. 22, No 21. Article 8445.
4. Er M. J., Wang Y., Zhu L. et al. Research Challenges, Recent Advances, and Popular Datasets in Deep Learning-Based Underwater Marine Object Detection: A Review. Journal of Marine Science and Engineering. 2023. Vol. 11, No 2. Article 327.
5. Li Y., Wang B., Sun J., Wu X., Li Y. RGB-Sonar Tracking Benchmark and Spatial Cross-Attention Transformer Tracker. arXiv. 2024. Article 2406.07189.
6. Negahdaripour S., Sekkati H., Pirsiavash H. Opti-acoustic Stereo Imaging: On System Calibration and 3-D Target Reconstruction. IEEE Transactions on Image Processing. 2009. Vol. 18, No 6. P. 1203–1214.

УДК 004.89:005.2(043.2)

Єдкін Д.Я., здобувач

Сябрук І. М., старший викладач

Державний університет «Київський авіаційний інститут»

ІНТЕЛЕКТУАЛЬНА CRM-СИСТЕМА ПІДТРИМКИ ВЕТЕРИНАРНОГО ПРИЙОМУ З АВТОМАТИЧНОЮ РЕКОМЕНДАЦІЮ ПРЕПАРАТІВ ЗА ДІАГНОЗОМ

У умовах діджиталізації медичних та сервісних процесів, актуальності зараз набуває автоматизація діяльності ветеринарних клінік. Значна частина роботи ветеринарного закладу пов'язана з веденням карток клієнтів і тварин, фіксацією анамнезу, діагнозів, призначень, результатів досліджень, препаратів для лікування та контролем повторних прийомів. Виконання цих процесів вручну або за допомогою розрізних програмних засобів призводить до дублювання інформації, збільшення часу обслуговування та підвищення ризику помилок під час прийняття рішень.

Існуючі CRM-системи здебільшого орієнтовані на загальний облік клієнтів і фінансових операцій, однак не враховують специфіку ветеринарного прийому, де важливими є історія лікування тварини, зв'язок симптомів із діагнозами, вибір препаратів, дозувань і схем лікування. У зв'язку з цим актуальним є створення інтелектуальної CRM-системи, яка не лише зберігає та структурує дані, а й підтримує ветеринарного лікаря під час прийому шляхом автоматичного формування рекомендацій щодо препаратів на основі встановленого діагнозу за допомогою штучного інтелекту.

Метою роботи є розробка інтелектуальної CRM-системи підтримки ветеринарного прийому з автоматичною рекомендацією препаратів за діагнозом із використанням методів штучного інтелекту, на основі попередніх прийомів тварин. Така система має забезпечувати централізоване ведення інформації про клієнтів, пацієнтів, прийоми, послуги, дослідження та лікування, а також допомагати лікарю у виборі релевантних лікарських засобів на основі накопичених клінічних даних.

Запропонована система будується за модульним принципом. До її складу входять модуль керування даними про клієнтів і тварин, модуль ветеринарного прийому, модуль діагностики, модуль складського обліку препаратів, модуль фінансового супроводу та аналітичний модуль рекомендацій. Цей принцип може запропонувати абсолютно будь-яке CRM рішення, проте основною фішкою є окремий сервіс зі штучним інтелектом, який підключається до CRM бази та проводить під час прийому рекомендацій, на основі вхідних даних лікаря.

Під час формування рекомендацій система може враховувати вид тварини, породу, вік, масу, супутні симптоми, результати лабораторних досліджень, протипоказання та попередні схеми лікування. У результаті лікар отримує перелік найбільш доречних препаратів із можливістю подальшого коригування відповідно до клінічної ситуації. Таким чином, штучний інтелект у системі виконує роль інтелектуального асистента, а остаточне рішення залишається за фахівцем.

Для реалізації програмного засобу було використано сучасний веб орієнтований стек технологій. Серверна частина реалізована на базі *NestJS* із використанням *TypeORM* та реляційної бази даних *PostgreSQL*, що забезпечує структуроване зберігання взаємопов'язаних сутностей. Клієнтська частина може бути побудована як веб інтерфейс для персоналу клініки, що надає швидкий доступ до картки пацієнта, історії прийомів, призначень і рекомендацій. Такий підхід дозволяє інтегрувати в єдину систему як операційні процеси клініки, так і інтелектуальну підтримку прийняття рішень.

Важливою перевагою системи є накопичення якісно структурованих даних про реальні клінічні випадки. Надалі це створює основу для вдосконалення моделей штучного інтелекту, зокрема для підвищення точності рекомендацій, виявлення типових схем лікування та побудови прогнозних моделей у ветеринарній практиці. Чим більший обсяг валідованих даних накопичується в системі, тим вищою стає практична цінність інтелектуального модуля.

Під час тестування системи можуть бути перевірені сценарії створення нового прийому, внесення симптомів і діагнозу, автоматичного підбору препаратів, збереження історії лікування, формування фінансових записів та повторного звернення пацієнта. Очікувані результати полягають у зменшенні часу на оформлення прийому, підвищенні повноти ведення медичних записів, зниженні ймовірності пропуску важливих даних та покращенні підтримки ветеринарного лікаря під час вибору лікування.

Практичне значення роботи полягає в можливості навчання штучного інтелекту, на основі, розробленої інтелектуальної CRM-системи ветеринарами, задля можливості в майбутньому використати його в майбутніх технологіях. Як наприклад, при створенні чіпу чи імпланту, який буде знаходити та виявляти симптоми в тілі тварини, дозволить до цього підключити штучний інтелект, який буде збирати аномалії тіла та повертати діагноз. Після чого, якщо діагноз не критичний, надсилати список рекомендованих ліків до власника тварин, при цьому не буде втручання ветеринара та проведення прийому. В іншому випадку, якщо тварина має критичний діагноз з загрозою життя, то автоматично викликати групу ветеринарів на дім.

Список використаних джерел:

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – 4th ed. – Pearson, 2021.
2. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. – 3rd ed. – O'Reilly Media, 2022.
3. Bishop C. M. Pattern Recognition and Machine Learning. – Springer, 2006.
4. Sarker I. H. Machine Learning: Algorithms, Real-World Applications and Research Directions. – Springer, 2021.
5. Gamma E., Helm R., Johnson R., Vlissides J. Design Patterns: Elements of Reusable Object-Oriented Software. – Addison Wesley, 1994.
6. Newman S. Building Microservices. – 2nd ed. – O'Reilly Media, 2021.
7. Evans E. Domain-Driven Design: Tackling Complexity in the Heart of Software. – Addison-Wesley, 2003.
8. Grinberg M. Flask Web Development. – 2nd ed. – O'Reilly Media, 2018.
9. Banks A., Porcello E. Learning React. – 2nd ed. – O'Reilly Media, 2020.
10. Kleppmann M. Designing Data-Intensive Applications. – O'Reilly Media, 2017.
11. McCaffrey J. Machine Learning Using Python. – Microsoft Press, 2018.
12. Chollet F. Deep Learning with Python. – 2nd ed. – Manning Publications, 2021.

УДК 658:5:004

*Гладченко О.В., к.пед.н., доцент,
Цикулова А.Е. здобувачка
Державний податковий університет*

АВТОМАТИЗАЦІЯ ВИРОБНИЧИХ ПРОЦЕСІВ ЯК ФАКТОР ПІДВИЩЕННЯ КОНКУРЕНТОСПРОМОЖНОСТІ МАЛОГО БІЗНЕСУ

Сучасний розвиток технологій зумовлює активне впровадження цифрових рішень та автоматизації у діяльність підприємств. Для малого бізнесу автоматизація виробничих і бізнес-процесів є важливим чинником підвищення ефективності, оскільки сприяє зменшенню витрат, підвищенню продуктивності та покращенню якості продукції і послуг. Водночас, незважаючи на наявність розвинутого ІТ-сектору, цифрова трансформація економіки України відбувається відносно повільними темпами, що підтверджують міжнародні рейтинги цифрового розвитку, де країна переважно займає середні позиції [1].

Упровадження ІКТ, автоматизація бізнес-процесів і використання онлайн-платформ відкривають для підприємств можливість підвищення ефективності діяльності та розширення ринків збуту. Однак малий бізнес часто стикається з низкою перешкод: обмеженим доступом до фінансування; недостатнім рівнем цифрових навичок; нестачею ІТ-фахівців. Тому дослідження автоматизації виробничих процесів є актуальним, оскільки її впровадження сприяє підвищенню конкурентоспроможності підприємств в умовах розвитку цифрової економіки [2].

У сучасних умовах розвитку економіки важливу роль у підвищенні ефективності діяльності підприємств відіграє впровадження цифрових технологій та автоматизованих систем управління. Автоматизація виробничих процесів дозволяє оптимізувати використання ресурсів, скоротити витрати часу на виконання операцій, зменшити вплив людського фактору та підвищити якість продукції. Особливо актуальним це питання є для малого бізнесу, який змушений працювати в умовах обмежених ресурсів та високої конкуренції. Використання сучасних програмних рішень і технологічних платформ сприяє ефективнішому управлінню виробництвом, контролю за процесами та прийняттю обґрунтованих управлінських рішень. Саме тому впровадження інструментів автоматизації є важливим чинником підвищення конкурентоспроможності підприємств [3].

З метою узагальнення сучасних рішень у сфері цифровізації виробництва доцільно розглянути найбільш поширені інструменти

автоматизації, які використовуються підприємствами для оптимізації виробничих процесів.

Таблиця 1

Популярні інструменти для автоматизації виробничих процесів

Інструмент	Основні можливості	Вартість	Цільова аудиторія
Odoo ERP	Автоматизація виробництва, управління запасами, планування ресурсів підприємства (ERP), інтеграція з бухгалтерією	Від \$20/міс.	Малий та середній бізнес
SAP Business One	Управління виробничими процесами, фінансами, складом, планування виробництва	Від \$100/міс.	Підприємства малого та середнього бізнесу
Zoho Creator/ Zoho One	Автоматизація бізнес-процесів, створення корпоративних додатків, управління замовленнями	Від \$30/міс.	Стартапи, малий бізнес
Siemens MindSphere	IoT-платформа для моніторингу виробництва, аналіз даних обладнання, оптимізація процесів	Індивідуальна	Виробничі підприємства

Джерело: сформовано автором на основі [3]

Використання сучасних інструментів автоматизації виробничих процесів сприяє підвищенню ефективності діяльності підприємств, оптимізації використання ресурсів та покращенню управління виробництвом. Для малого бізнесу впровадження таких технологій є важливим чинником підвищення конкурентоспроможності, оскільки дозволяє зменшити витрати, підвищити продуктивність та забезпечити швидку адаптацію до змін ринкового середовища.

Стратегії цифрової трансформації підприємств дедалі частіше розглядаються як невід’ємний елемент загальної стратегії розвитку бізнесу. Це пояснюється тим, що впровадження сучасних цифрових технологій впливає не лише на окремі операційні процеси, а й змінює підходи до управління підприємством у цілому. Цифровізація дозволяє оптимізувати виробничі та управлінські процеси, підвищити швидкість обробки інформації, зменшити витрати та покращити якість прийняття управлінських рішень. У результаті підприємства отримують нові можливості для зміцнення своїх конкурентних позицій, підвищення ефективності діяльності, а також здатності швидко реагувати на зміни зовнішнього середовища [4].

У сучасних умовах цифрова трансформація сприяє формуванню нових бізнес-моделей, розширенню каналів взаємодії з клієнтами та вдосконаленню систем управління ресурсами. Використання цифрових технологій, таких як автоматизація процесів, аналітика великих даних, хмарні сервіси та інструменти штучного інтелекту, дозволяє підприємствам підвищувати продуктивність праці, покращувати якість продукції та послуг, а також більш ефективно планувати свою діяльність.

Підприємства, які успішно впроваджують цифрову трансформацію та зміцнюють власні конкурентні позиції, характеризуються насамперед здатністю швидко реагувати на зміни зовнішнього середовища. Це досягається завдяки активному використанню сучасних цифрових технологій та інструментів. Йдеться не лише про автоматизацію бізнес-процесів, а й про застосування інноваційних методів аналізу даних, використання технологій штучного інтелекту для прогнозування ринкового попиту, а також впровадження персоналізованих рішень для покращення взаємодії з клієнтами. Важливу роль відіграють і хмарні технології, які дозволяють підприємствам гнучко масштабувати свою діяльність та швидко адаптуватися до нових умов. Не менш значущим аспектом є підвищення рівня кібербезпеки, що забезпечує захист важливої комерційної інформації. Крім того, сучасні компанії активно використовують цифрові платформи для інтеграції у міжнародні ланцюги створення вартості, що сприяє розширенню ринків збуту, підвищенню продуктивності праці та скороченню операційних витрат [2].

Цифрова трансформація для українських підприємств передусім підвищує ефективність внутрішніх процесів, що безпосередньо впливає на конкурентоспроможність. Оптимізація робочих процесів і скорочення витрат на адміністрацію, логістику та внутрішню комунікацію дозволяють компаніям швидше виводити нові продукти та послуги на ринок і оперативніше реагувати на зміни в попиті.

Водночас трансформація стимулює інноваційний розвиток, оскільки вимагає перегляду бізнес-моделей та відкриває можливості для впровадження нових продуктів і розширення каналів продажу. Завдяки сучасним методам аналітики та прогнозування на основі великих даних підприємства можуть приймати більш обґрунтовані рішення щодо поведінки споживачів та ринкових тенденцій, що скорочує час і ресурси, необхідні для аналізу інформації вручну [1].

Крім того, цифрові інструменти покращують взаємодію з клієнтами, підвищуючи їхню задоволеність та лояльність, що особливо важливо для розширення експортного потенціалу українських компаній. Автоматизовані системи обліку та контролю підвищують

інформаційну прозорість і зменшують вплив людського фактору, що формує більшу довіру з боку партнерів і клієнтів.

Впровадження цифрових технологій та автоматизації створює нові можливості для стратегічного розвитку підприємств. Завдяки аналітиці даних, штучному інтелекту та інтеграції в цифрові платформи підприємства можуть прогнозувати потреби ринку, оцінювати ефективність виробничих процесів і своєчасно коригувати стратегію розвитку. Це дозволяє малому бізнесу не лише підвищувати оперативну ефективність, а й формувати стійкі конкурентні переваги, адаптуючись до швидких змін у зовнішньому середовищі та розширюючи можливості для виходу на нові ринки [4].

Автоматизація виробничих та бізнес-процесів виступає важливим чинником підвищення ефективності та конкурентоспроможності малого бізнесу в Україні. Впровадження цифрових технологій дозволяє оптимізувати внутрішні процеси, скоротити витрати, підвищити продуктивність і покращити якість продукції та послуг. Крім того, цифрова трансформація сприяє інноваційному розвитку, розширенню каналів продажу, покращенню взаємодії з клієнтами та зміцненню довіри партнерів. Таким чином, активне використання сучасних цифрових інструментів забезпечує малим підприємствам гнучкість, адаптивність та стабільне зміцнення конкурентних позицій на ринку.

Список використаних джерел:

1. Кайда І.В. Цифрова трансформація як ключовий фактор підвищення конкурентоспроможності українського бізнесу. *Економіка та суспільство*. 2025. № 72. URL: <https://economyandsociety.in.ua/index.php/journal/article/download/5761/5703/>
2. Попов О.С., Макаров С.А. Сучасні особливості впровадження цифровізації у малому бізнесі у сфері торгівлі. *Економіка та управління національними господарствами. Проблеми економіки*. 2025. № 2 (64). С. 67-76. DOI: <https://doi.org/10.32983/2222-0712-2025-2-67-76>
3. Юрченко Я.В. Автоматизація бізнес – аналітики за допомогою штучного інтелекту. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2025. №45. С. 733-740. URL: <https://nzlubp.org.ua/index.php/journal/article/download/1865/1646/>
4. Пархуць Е.Д., Огданська О.Д. Забезпечення конкурентоспроможності підприємства на основі моделей цифрової трансформації. *European Journal of Management Issues*. 2025. Vol. 33(2). С. 75-87. URL: <https://philarchive.org/archive/DOERFZ>

УДК 519.8:623.3

*Гітис В.Б., к.т.н., доцент,
Флюд Д.В., здобувач*

Донбаська державна машинобудівна академія

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ КЕРУВАННЯ ГРУПАМИ РОЗМІНУВАННЯ

Сучасні операції гуманітарного розмінування вимагають ефективного планування маршрутів та розподілу ресурсів. Основною проблемою є облік не лише географічної відстані, а й рельєфу місцевості, що впливає на час та безпеку пересування саперів.

В роботі [1] була запропонована математична модель, яка дозволяє оптимізувати ці процеси за допомогою алгоритмів обчислення вартості шляху з урахуванням висотних перепадів.

Вхідними параметрами моделі є:

- $S = \{s_1, s_2, \dots, s_m\}$ – множина саперів (їхні координати у форматі широти та довготи);
- $Z = \{z_1, z_2, \dots, z_n\}$ – множина зон розмінування;
- $h(z)$ – висота над рівнем моря в точці z .

Основне завдання полягає в оптимальному розподілі зон між саперами та побудові маршрутів із мінімальною загальною вартістю переміщення, що враховує не лише географічну відстань, а й складність рельєфу. Для врахування складності рельєфу вводиться поняття вартості переміщення між двома точками A і B .

Загальна вартість переходу визначається як сума географічної відстані та додаткового «штрафу». Чим більша різниця висот, тим вища вартість проходження цієї ділянки.

Розподіл зон між саперами відбувається на основі мінімальної вартості переміщення, а не мінімальної географічної відстані. Для кожної зони $z \in Z$ визначається сапер $s(z)$ який має мінімальну вартість переміщення до цієї зони. Це означає, що кожна зона буде обслуговуватися тим сапером, для якого сумарна вартість шляху є найменшою, що дозволяє врахувати особливості рельєфу та уникнути перевантажених маршрутів.

Після розподілу зон кожен сапер повинен обійти всі призначені йому зони, дотримуючись мінімальної вартості переміщення.

На основі математичної моделі був розроблений програмний застосунок, приклад роботи якого щодо побудови шляхів саперів представлений на рис. 1.

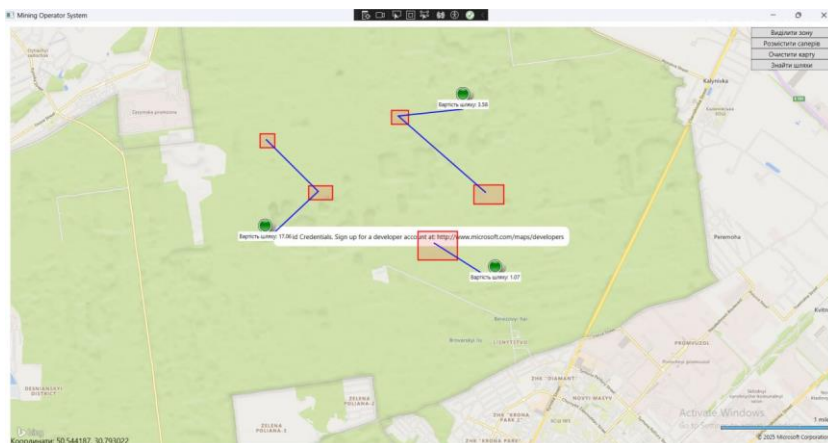


Рис. 1. Шляхи, побудовані для саперів.

На рис. 2 наведений приклад виведення підсумкового розподілу саперів у форматі таблиці для звітності.

Сапер / Зона	Зона 1	Зона 2	Зона 3	Зона 4	Зона 5	Вартість шляху
Сапер 1	✓	✓				17.06
Сапер 2			✓	✓		3.58
Сапер 3					✓	1.07

Рис. 2. Підсумкова таблиця розподілу саперів.

Запропонована інформаційна система для оптимізації роботи саперів за допомогою алгоритмів пошуку шляху та врахування рельєфу місцевості дозволить підвищити ефективність та безпеку процесів гуманітарного розмінування.

Список використаних джерел:

1. Гітіс В.Б., Флюд Д.В. Оптимізаційна модель роботи саперного оператора // Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі: матеріали X Міжнародної науково-практичної конференції. / М-во освіти і науки України; Київ. нац. ун-т культури і мистецтв. Київ : Видавничий центр КНУКіМ, 2025. – С. 43-45.

УДК 004.7

*Леус В. О., здобувач,
Савіцький Р. С., ст. викладач, аспірант
Державний університет «Житомирська політехніка»*

МЕТОДИ СТРУКТУРИЗАЦІЇ ТА ЗБЕРЕЖЕННЯ ДАНИХ У СИСТЕМАХ ВІЗУАЛЬНОГО КОНСТРУЮВАННЯ ВЕБРЕСУРСІВ

Стрімкий розвиток платформ для створення вебресурсів сильно змінив підхід до розробки ПЗ. Сучасні редактори дозволяють користувачам без навичок програмування створювати складні інтерфейси за допомогою механізмів Drag&Drop. Проте для реалізації потрібно вирішити нетривіальну архітектурну задачу: як ефективно структурувати / зберігати створений динамічний контент, структура якого заздалегідь невідома та може змінюватися в будь-який момент.

Традиційний підхід, за яким контент зберігається як готова HTML-розмітка, є неприйнятним для NoCode систем. Збереження HTML у чистому вигляді призводить до втрати семантичного зв'язку елементів, що ускладнює редагування блоків та унеможливорює зміну глобального дизайну сайту надалі. Альтернативою є збереження структури інтерфейсу у вигляді серіалізованого дерева об'єктів (подібного до AST), де кожен вузол є окремим функціональним блоком (текст, зображення, форма) з власними властивостями.

Використання деревоподібних структур висуває специфічні вимоги до бази даних. Класичні реляційні бази даних (SQL) вимагають жорстко заданих схем таблиць. Спроба нормалізувати динамічне дерево блоків у реляційній моделі призводить до використання антипатерну Entity-Attribute-Value, що знижує продуктивність системи через необхідність виконувати велику кількість складних операцій JOIN під час завантаження однієї сторінки.

З іншого боку, документо-орієнтовані бази даних (NoSQL) ідеально підходять для збереження ієрархічних JSON-структур. Однак конструктори містять сутності зі строгою реляційною природою: облікові записи користувачів, права доступу, платежі, зв'язки між сайтами. Застосування виключно NoSQL підходу ускладнює забезпечення транзакційної цілісності для цих критичних даних.

Оптимальним архітектурним рішенням для NoCode платформ є використання гібридної моделі збереження даних на базі сучасних реляційних СУБД (MySQL версії 8.0+), які мають нативну підтримку типу даних JSON [1].

У межах такої моделі архітектура бази даних розділяється. Статичні сутності (користувачі, сайти) зберігаються у класичних реляційних таблицях, що гарантує цілісність даних та каскадне видалення. А динамічна структура сторінки (дерево блоків) зберігається в полі типу JSON. Кожен об'єкт у цьому масиві містить ідентифікатор типу компонента, його унікальний ключ, параметри стилізації та безпосередньо контент.

Переваги такого підходу для систем візуального конструювання є очевидними.

Однією з переваг є швидкодія читання, тому що вся конфігурація сторінки завантажується з бази даних одним запитом без об'єднань, незалежно від кількості блоків або рівня їх вкладеності.

Також гнучкість інтерфейсу дозволяє додавати нові типи блоків до редактора і не потребує міграції або змін схем бази даних на сервері, що значно прискорює подальшу розробку.

Підтримка цілісності системи дає можливість використовувати зовнішні ключі для з'єднання сторінок із сайтами та їх власниками.

Для клієнтського застосунку збережена JSON-структура є декларативною схемою [2]. Під час завантаження сторінки модуль рендерингу парсить JSON-дерево і рекурсивно перетворює кожен вузол у відповідний компонент, передаючи збережені властивості як параметри. Це відокремлює дані від логіки відображення [3].

Ефективне функціонування сучасних NoCode платформ неможливе без оптимізації зберігання даних. Відмова від збереження готового HTML на користь серіалізованих JSON-дерев об'єктів дозволяє реалізувати повноцінний компонентний підхід, а використання гібридної моделі зберігання в реляційній базі даних надає оптимальний баланс між гнучкістю, необхідною для збереження довільних структур інтерфейсу, та транзакційною цілісністю, що є критичним для управління даними користувачів та бізнес-логікою системи.

Список використаних джерел:

1. MySQL 8.0 Reference Manual. The JSON Data Type. URL: <https://dev.mysql.com/doc/refman/8.0/en/json.html> (дата звернення: 09.03.2026).
2. Brooks R. A Deep Dive into Airbnb's Server-Driven UI System. Airbnb Engineering. URL: <https://medium.com/airbnb-engineering/a-deep-dive-into-airbnbs-server-driven-ui-system-842244c5f5> (дата звернення: 11.03.2026).
3. Thinking in React. The Official React Documentation. URL: <https://react.dev/learn/thinking-in-react> (дата звернення: 11.03.2026).

УДК 004.7

*Кунуп Т.В., к.т.н., ст. викладач,
Савранський Р.В., здобувач*

Національний університет «Одеська політехніка»

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА АРХІТЕКТУРНІ РІШЕННЯ У СИСТЕМАХ СПОРТИВНОГО МЕНЕДЖМЕНТУ

Розвиток цифрових технологій суттєво трансформує підходи до управління організаціями, зокрема у сфері спортивного менеджменту. Зростання обсягів даних і необхідність їх оперативної обробки вимагають впровадження ефективних інформаційних систем, побудованих із використанням сучасних технологій та архітектурних рішень.

Метою дослідження є аналіз інформаційних технологій та архітектурних підходів до побудови систем спортивного менеджменту, а також обґрунтування ефективних рішень для підвищення їх масштабованості, надійності та продуктивності.

Об'єктом дослідження є процеси автоматизації управління діяльністю спортивних організацій. Предметом дослідження є інформаційні технології та архітектурні рішення побудови систем спортивного менеджменту.

У ході дослідження проаналізовано основні функціональні компоненти систем спортивного менеджменту, до яких належать: модулі управління даними спортсменів і тренерів, планування тренувального процесу, організація змагань, облік результатів та формування аналітичної звітності. Визначено, що ефективність таких систем значною мірою залежить від правильного вибору технологічного стеку та архітектури програмного забезпечення.

Розглянуто сучасні інформаційні технології, що застосовуються при розробці інформаційних систем. Для реалізації клієнтської частини доцільним є використання веб-орієнтованих технологій та сучасних JavaScript-фреймворків, що забезпечують адаптивність і інтерактивність інтерфейсу користувача. Серверна частина може бути реалізована із застосуванням платформ Node.js або Python, що дозволяє створювати масштабовані веб-застосунки з підтримкою RESTful взаємодії. Для зберігання даних використовуються як реляційні, так і NoSQL бази даних залежно від структури та обсягів інформації.

Особливу увагу приділено аналізу архітектурних рішень. Обґрунтовано доцільність використання багаторівневої архітектури, що передбачає розподіл системи на рівні представлення, бізнес-логіки та доступу до даних. Такий підхід забезпечує модульність, спрощує

супровід та підвищує масштабованість системи. Додатково розглянуто застосування мікросервісної архітектури, яка дозволяє розподілити функціональність системи на незалежні сервіси, що взаємодіють через API, забезпечуючи гнучкість і відмовостійкість.

У процесі дослідження також проаналізовано підходи до управління розробкою програмного забезпечення. Визначено, що використання гнучких методологій, зокрема Scrum, забезпечує ітеративність розробки, можливість швидкого реагування на зміну вимог та підвищення якості кінцевого продукту. Важливим аспектом є інтеграція процесів тестування на всіх етапах життєвого циклу, включаючи модульне, інтеграційне та системне тестування.

Наукова новизна отриманих результатів полягає у комплексному обґрунтуванні доцільності поєднання багаторівневої та мікросервісної архітектури при розробці інформаційних систем спортивного менеджменту, що дозволяє підвищити гнучкість, масштабованість і ефективність обробки даних у таких системах.

Таким чином, застосування сучасних інформаційних технологій та раціонально обраних архітектурних рішень є ключовим фактором створення ефективних систем спортивного менеджменту. Запропоновані підходи можуть бути використані при розробці інформаційних систем для автоматизації діяльності спортивних організацій різного рівня.

Список використаних джерел:

1. Гришук В. Г. Інформаційні системи та технології в управлінні організаціями : навч. посіб. Київ : Видавництво НаУКМА, 2020. С.352.
2. Дубас Р. Г., Олійник А. В. Спортивний менеджмент: теорія та практика : монографія. Тернопіль : Економічна думка, 2018.С. 280.
3. Литвин В. В., Пасічник В. В. Проектування інтелектуальних систем : навч. посіб. Львів : Новий Світ-2000, 2021. С. 412.
4. Ньюмен С. Створення мікросервісів : пер. з англ. Київ : Діалектика, 2019. С. 304.
5. Ткаченко О. С., Серов Ю. О. Застосування гнучких методологій Scrum та Kanban у розробці складних програмних рішень. Комп'ютерні науки та інформаційні технології. 2022. Вип. 12. URL: <http://it-journal.org.ua/article/view/2022-12-05>.
6. Шевченко О. В. Порівняльний аналіз сучасних JavaScript-фреймворків для розробки клієнтської частини веб-застосунків. Вісник Національного технічного університету «ХПІ». Серія: Системний аналіз. 2021. № 1. С. 112–118.
7. Якименко І. В., Козлов П. А. Особливості використання Node.js та NoSQL баз даних у високонавантажених системах. Сучасна інженерія та ІТ-технології. 2020. Вип. 15. С. 45–52.

УДК 004.7

*Корецький Ю.І., здобувач,
Савицький Р.С., аспірант, ст. викладач
Державний університет «Житомирська політехніка»*

ПОРІВНЯЛЬНИЙ АНАЛІЗ АРХІТЕКТУРНИХ ПАТЕРНІВ ІЗОЛЯЦІЇ ДАНИХ У МУЛЬТИТЕНАНТНИХ ХМАРНИХ ЗАСТОСУНКАХ

Питання про те, як розмежувати дані між клієнтами в спільній системі, постає перед розробниками SaaS-застосунків набагато раніше, ніж більшість інших архітектурних рішень. Мультитенантність – це не просто технічна деталь реалізації, а фундаментальний вибір, що визначає подальшу форму всього продукту. Від моделі ізоляції залежить і те, як система поводитиметься під навантаженням, і те, наскільки складно буде її супроводжувати через рік. Існуючі підходи, а саме від виділеної бази на кожного клієнта до спільних таблиць із безпекою на рівні рядків (Row-Level Security, RLS), добре описані в загальних рисах [1], проте їх систематичне порівняння в контексті сучасних реляційних СУБД із підтримкою RLS залишається недостатньо опрацьованим.

Тема мультитенантності має помітну дослідницьку історію. Chong et al. [1] запропонували одну з перших класифікацій SaaS-архітектур, де рівень зрілості системи безпосередньо пов'язується зі ступенем спільного використання ресурсів. Пізніше Bezemer та Zaidman [2] детально розібрали технічні труднощі, з якими стикаються команди при переході на мультитенантну модель, зокрема складність міграцій і гарантування ізоляції. Kabbedijk та Jansen [3] узагальнили патерни варіативності на основі аналізу реальних промислових застосунків. Попри це, питання інтеграції RLS-механізмів реляційних СУБД з ORM-шаром практично не розглядалося.

Для порівняння взято три моделі ізоляції, що найчастіше зустрічаються на практиці. Database-per-Tenant дає кожному клієнту повністю ізольований екземпляр бази даних, але при кількох сотнях тенантів перетворюється на операційний тягар [2]. Schema-per-Tenant розміщує всіх у спільній базі, виділяючи кожному власний namespace [3]. Shared Schema з RLS розміщує всі тенанти в одних таблицях, а розмежування закладено в політики самої СУБД [4].

Моделі оцінювалися за чотирма атрибутами якості згідно ISO/IEC 25010: ізоляція тенантів, масштабованість, ресурсоемність інфраструктури та складність супроводу схем. Паралельно проводилося прототипування на стеку PostgreSQL + Prisma ORM.

Schema-per-Tenant добре справляється до кількох тисяч тенантів і при цьому не вимагає складної логіки на рівні запитів. Міграції є проблемними, тому будь-яка зміна схеми має бути застосована до кожної схеми окремо, що при великій кількості тенантів суттєво збільшує час розгортання [3].

Shared Schema з RLS – найбільш масштабована модель і при цьому найменш витратна в обслуговуванні. PostgreSQL забезпечує надійну ізоляцію через RLS-політики безпосередньо на рівні СУБД, що знімає цей обов'язок з прикладного коду. Додаткова складність виникає при використанні Prisma ORM, який не підтримує RLS нативно, тому контекст доводиться встановлювати вручну через Prisma Client Extensions або прями SQL-виклики.

Модель ізоляції даних – це рішення, прийняте на старті, визначає, як система буде поводитися під навантаженням, скільки коштуватиме її обслуговування і наскільки болісними виявляться міграції. Кожна з трьох розглянутих моделей є обгрунтованою відповіддю на різні набори вимог, але жодна не є універсально кращою.

Для більшості масштабованих SaaS-продуктів модель Shared Schema з RLS є найраціональнішим вибором. При роботі з Prisma ORM це означає явну реалізацію механізму встановлення та скидання RLS-контексту, оскільки нативної підтримки бібліотека не надає.

Список використаних джерел:

1. Chong F., Carraro G., Wolter R. Multi-Tenant Data Architecture. MSDN Library. Microsoft, 2006. URL: <https://learn.microsoft.com/en-us/azure/architecture/guide/multitenant/overview> (дата звернення: 10.03.2026).
2. Bezemer C.-P., Zaidman A. Multi-tenant SaaS applications: maintenance dream or nightmare? Proceedings of the Joint ERCIM Workshop on Software Evolution, 2010. P. 88–92.
3. Kabbeldijk J., Jansen S. Variability in Multi-Tenant Environments: Architectural Design Patterns from Industry. Advances in Conceptual Modeling, Lecture Notes in Computer Science. Springer, 2011. Vol. 6999. P. 151–160.
4. PostgreSQL Global Development Group. Row Security Policies. PostgreSQL 16 Documentation. 2023. URL: <https://www.postgresql.org/docs/current/ddl-rowsecurity.html> (дата звернення: 10.03.2026).

УДК 004.7

*Минець О.Р., здобувач,
Калита Н.І., к.т.н., професор
Харківський національний університет радіоелектроніки*

ІГРОВИЙ DISCORD-БОТ З АВТОМАТИЗОВАНОЮ СИСТЕМОЮ МОНЕТИЗАЦІЇ ТА УПРАВЛІННЯМ ІЄРАРХІЄЮ КОРИСТУВАЧІВ

Платформа Discord [1] є провідним середовищем для формування закритих та відкритих ком'юніті, де ключовим фактором життєздатності групи є ефективна модерация та внутрішня гейміфікація.

Соціальна взаємодія та економічне регулювання всередині цифрової платформи у Discord ґрунтується на принципах:

- а) соціальна ієрархія та рольова модель доступу;
- б) цифрова мікроекономіка спільнот;
- в) монетизація цифрових послуг.

Управління великою кількістю користувачів базується на розподілі ролей, які визначають права доступу до текстових та голосових каналів. Проблема стандартних засобів платформи полягає у відсутності інструментів для динамічного та автоматизованого створення таких ролей самими користувачами.

Цифрова мікроекономіка включає механізми конвертації часу, проведеного у голосових каналах, у віртуальну валюту або статус. Це вимагає точного обліку активності та запобігання зловживанням.

Монетизація цифрових послуг здійснюється через оренду статусів, інвестиції у створення власних "приватних зон" (категорій) та торгівлю між учасниками, що формує стійку внутрішню економіку сервера.

Розроблений ігровий бот базується на мові програмування Python [2] та бібліотеці discord.py, що дозволяє обробляти події платформи в асинхронному режимі, запобігаючи блокуванню основного потоку виконання. Архітектура боту побудована на базі SQLite з використанням бібліотеки aiosqlite, що забезпечує неблокуючу взаємодію з БД для кожного окремого сервера (guild-based database isolation). Структура бази даних містить таблиці для обліку балансу користувачів, рівнів, досвіду, ієрархії ролей та детальної історії транзакцій.

Особливістю розробки є надання користувачам можливості створювати власні ролі, інвестуючи ігрову валюту. Система автоматично створює відповідні категорії та канали з налаштованими правами доступу, що реалізує динамічну модель RBAC (Role-Based Access Control). Приклад асинхронної реалізації створення ієрархічної

структури в коді бота: `category = await guild.create_category(name=f'{role.name}', overwrites=overwrites)`. Бот підтримує не лише створення, а й перепродаж ролей у внутрішньому магазині, де творець ролі може отримувати відсоток від кожної покупки, реалізуючи механізм пасивного доходу.

Гейміфікація реалізована через систему активності у голосових каналах. Бот використовує фонові задачі (`tasks.loop`) для циклічного нарахування досвіду та монет користувачам, враховуючи стан мікрофона та навушників (`self_deaf`). Для оптимізації навантаження на БД застосовано механізм RAM-сесій (`voice_sessions`), де накопичується час перебування до моменту синхронізації з постійним сховищем.

Кожна зміна балансу супроводжується записом у таблицю транзакцій, що дозволяє проводити аудит дій через адміністративну панель. Система також підтримує автоматичне відкликання прав доступу після завершення терміну оренди ролі. Це реалізовано через функцію `check_role_expiration`, яка щохвилини перевіряє `expiration_date` у БД. У разі завершення терміну, бот видаляє роль. Для запобігання втрати даних при раптовій зупинці сервера реалізовано обробник сигналів, який ініціює коректне завершення процесів та збереження активних сесій.

Використання компонентів `discord.ui` (`Modal`, `Select`, `Button`) дозволяє інтегрувати бота в сучасний інтерфейс Discord. Це значно покращує користувацький досвід, оскільки складні дії (переказ монет, вибір кольору ролі, налаштування цін) виконуються через графічні елементи, а не через запам'ятовування складних текстових синтаксисів. Модальні вікна дозволяють збирати структуровані дані від користувача, мінімізуючи помилки вводу.

Розроблений програмний продукт автоматизує складні процеси управління ігровою спільнотою, поєднуючи соціальні та економічні механіки. Використання асинхронного підходу забезпечує стабільну роботу системи на серверах з великою кількістю активних учасників. Перспективою подальшого розвитку є впровадження зовнішніх платіжних систем та розширення ігрових механік (квестів, аукціонів).

Список використаних джерел:

1. Офіційна документація Discord Developer Portal : вебсайт. URL: <https://discord.com/developers/docs> (дата звернення 20.03.2026).
2. Офіційний посібник Python з асинхронного програмування : вебсайт. URL: <https://docs.python.org/3/library/asyncio.html> (дата звернення 20.03.2026).

УДК 004.4:004.738.5

*Берник А. О., здобувачка,
Гришанович Т. О., к.ф-м.н., доцент
Волинський національний університет імені Лесі Українки*

РОЗРОБКА ВЕБОРІЄНТОВАНОЇ СИСТЕМИ БРОНЮВАННЯ ЗАЛІЗНИЧНИХ КВИТКІВ НА ОСНОВІ КЛІЄНТ–СЕРВЕРНОЇ АРХІТЕКТУРИ

У сучасних умовах цифровізації транспортної галузі особливої актуальності набуває автоматизація процесів бронювання та продажу квитків. Залізничні перевезення залишаються одним із ключових видів транспорту в Україні, що обумовлює необхідність створення ефективних інформаційних систем для обслуговування пасажирів.

Метою дослідження є проектування та розробка інформаційної системи бронювання залізничних квитків, яка забезпечує автоматизацію процесів пошуку маршрутів, вибору місць та оформлення електронних квитків. Об'єктом дослідження виступають процеси автоматизації бронювання, а предметом – методи та засоби створення відповідних інформаційних систем.

У роботі проаналізовано основні підходи до побудови інформаційних систем та визначено ключові вимоги до систем бронювання: функціональність, продуктивність, безпека, зручність інтерфейсу та здатність працювати в режимі 24/7. Особливу увагу приділено клієнт–серверній архітектурі, яка забезпечує централізоване зберігання даних, масштабованість і ефективність обробки запитів користувачів.

У ході дослідження проведено аналіз існуючих систем бронювання квитків, що дозволило виявити їхні переваги та недоліки, зокрема проблеми з продуктивністю, синхронізацією даних та обмеженим функціоналом. Це стало підґрунтям для формування вимог до власної системи.

Результатом роботи стала розробка програмного засобу «Railbooker», архітектура якого базується на патерні Model-View-Template. Система реалізована з використанням мови програмування Python та фреймворку Django, що дозволило забезпечити модульність, безпеку та швидкість розробки. Для зберігання даних використано СУБД PostgreSQL, а взаємодія з користувачем реалізована за допомогою вебтехнологій HTML, CSS та JavaScript. Застосування інкрементної моделі розробки дозволило поетапно реалізовувати

функціональні компоненти системи та оперативно вносити зміни відповідно до уточнених вимог.

Функціональні можливості системи включають реєстрацію та авторизацію користувачів, пошук маршрутів (як прямих, так і з пересадками), вибір місць у вагоні, формування замовлення та здійснення онлайн-оплати. Важливим компонентом є алгоритм пошуку маршрутів, який враховує часові обмеження пересадок і забезпечує ефективний підбір варіантів поїздки.

У системі реалізовано рольову модель доступу, що дозволяє розмежувати права користувачів (пасажир, касир, провідник, адміністратор), а також механізми захисту даних відповідно до сучасних стандартів інформаційної безпеки. Для забезпечення безпечних фінансових операцій інтегровано платіжний сервіс, який не передає чутливі дані карток на сервер.

Тестування програмного засобу підтвердило коректність роботи основних функцій, зокрема уникнення подвійного бронювання, правильність обробки запитів та стабільність платіжного модуля.

Розроблена система може бути використана як основа для впровадження у сфері пасажирських перевезень. Подальший розвиток передбачає оптимізацію алгоритмів пошуку, розширення функціоналу та інтеграцію додаткових сервісів, що дозволить створити універсальну платформу для планування подорожей.

Упровадження подібних інформаційних систем сприяє не лише підвищенню якості обслуговування пасажирів, але й оптимізації внутрішніх процесів транспортних компаній. Автоматизація дозволяє зменшити навантаження на персонал, мінімізувати кількість помилок, пов'язаних із людським фактором, та забезпечити оперативний доступ до актуальної інформації про рейси і наявність місць. Це, у свою чергу, підвищує конкурентоспроможність перевізника та рівень задоволеності користувачів сервісу.

Список використаних джерел:

1. Спіцина А. Інформаційні технології системи управління персоналом транспорту як провідної галузі національної економіки України. Modeling the development of the economic systems. 2024. № 1. С. 228–232.
2. Якість програмного забезпечення (за ISO/IEC 25010:2011). QALight. URL: <https://qalight.ua/baza-znaniy/yakist-programnogo-zabezpechennya-za-iso-iec-250102011/> (дата звернення: 01.12.2025).

UDC 004.9

**Pototskyi Maksym, Postgraduate Student,
Gamayun Igor, D.Sc., Professor,
Kopp Andrii, Ph.D., Associate Professor**
National Technical University «Kharkiv Polytechnic Institute»

FRAMEWORK FOR TESTING SMALL LANGUAGE MODELS ABILITY TO ASSESS BPMN QUALITY

Business process modeling using BPMN (Business Process Model and Notation) is a fundamental technique for analyzing and designing information systems. The quality of such models affects the correctness of decisions and the efficiency of workflows. Building BPMN models requires knowledge of the domain and the modeling rules. Recent studies show that large language models are capable of generating BPMN from natural language [1]. At the same time, evaluating the quality of such models remains an open problem. Existing approaches often do not consider a full set of quality criteria or rely on the language models themselves as evaluators [1]. The paper BEF4LLM proposes a multidimensional evaluation that includes syntactic, semantic, and pragmatic aspects, as well as validity [1]. Other studies [2] explore intelligent approaches to BPMN evaluation based on model element features. However, the role of Small Language Models (SLM) [3] in this problem has been scarcely investigated. The aim of this work is to develop a framework for testing the ability of small language models to evaluate BPMN quality.

The proposed framework (Fig. 1) is based on the step-by-step processing of a BPMN model and the generation of a structured representation for analysis. In the first step, the model in XML format is broken down into elements. Tasks, events, and gates are identified. A set of features is generated for each element. These features represent both structural properties and textual labels. Next, a generalized representation of the model is created in the form of a TOON (Token-Oriented Object Notation) [4], which is compact and suitable for processing by language models. Small models have limited resources, so it is important to provide them with data in a compressed form. This reduces computational costs and ensures consistent results.

Then each SLM receives the same TOON-based representation and the system prompt. The evaluation is focusing on identifying business process model tasks following the rule [1]:

$$|in(t) = 1| \wedge |out(t) = 1|.$$

Here $in(t)$ and $out(t)$ are sets of incoming and outgoing sequence flows of a task $t \in T$, while T is a set of tasks defined in the BPMN model.

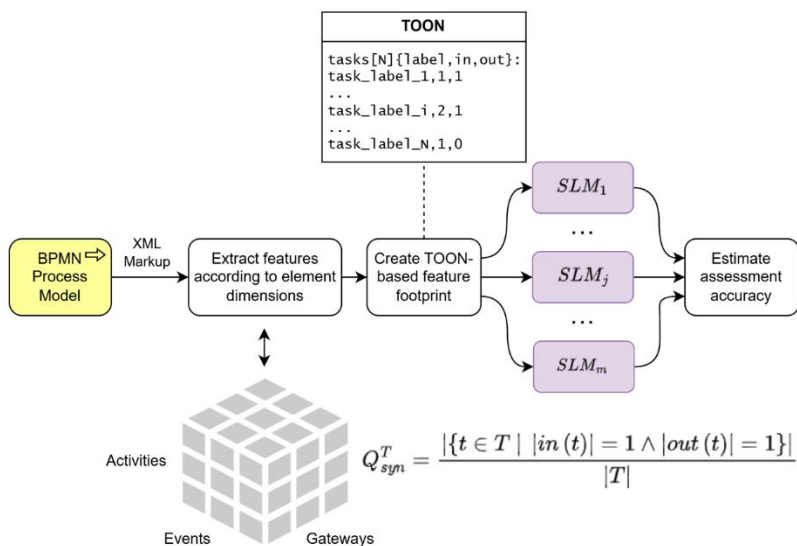


Fig. 1. Proposed framework for testing SLMs ability to assess Q_{syn}^T

The syntactic quality of tasks Q_{syn}^T is computed by dividing the number of tasks following the rule, introduced above, by the total number of tasks. Then estimates obtained using SLMs are compared with the reference value calculated according to the formalized BPMN modeling rules [1].

References:

1. Lauer C., Pfeiffer P., Rombach A., Mehdiyev N. Assessing the Business Process Modeling Competences of Large Language Models [Electronic resource]. – Access: <https://arxiv.org/abs/2601.21787>
2. Yanholenko O., Kopp A., Godlevskiy M., Orlovskiy D., Khatsko N. Towards information technology for BPMN models quality assessment based on intelligence theory [Electronic resource]. – Access: <https://ceur-ws.org/Vol-4004/paper7.pdf>
3. Johnson J. Small Language Models (SLM): A Comprehensive Overview [Electronic resource] / J. Johnson // Huggingface.co. – 2025. – Access: <https://huggingface.co/blog/jjokah/small-language-model>
4. What Is TOON: the Compact Data Format for LLMs and AI [Electronic resource]. – 2023. – Access: <https://openapi.com/blog/what-the-toon-format-is-token-oriented-object-notation>

УДК: 004.94:004.65

*Гладченко О.В. к.пед.н., доцент
Мітла М.О. здобувачка вищої освіти
Державний податковий університет*

МОДЕЛЮВАННЯ ПРОЦЕСІВ ОБРОБКИ ДАНИХ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації суспільства значно зростає роль інформаційних систем, які забезпечують ефективне збирання, зберігання, обробку та аналіз великих обсягів даних. Практично всі сфери діяльності людини – економіка, наука, освіта, державне управління, медицина, транспорт і промисловість – активно використовують інформаційні системи для підтримки прийняття управлінських рішень. У зв'язку з цим особливого значення набуває моделювання процесів обробки даних, що дозволяє досліджувати функціонування складних інформаційних систем, прогнозувати їх поведінку та оптимізувати використання ресурсів.

Моделювання розглядається як ключовий метод наукового пізнання, що передбачає створення формалізованого представлення об'єкта з метою аналізу його властивостей. У сфері інформаційних систем воно дозволяє досліджувати інформаційні потоки, алгоритми обробки та взаємодію компонентів. За твердженням Б. Мельника, застосування моделювання сприяє підвищенню ефективності обробки даних і оптимізації інформаційних процесів [1, с. 417].

Сучасні інформаційні системи характеризуються складною структурою та обробкою значних обсягів даних у реальному часі. Основні етапи обробки включають збирання, первинну обробку, зберігання, аналіз і представлення результатів [2, с. 207]. Моделювання на цих етапах забезпечує визначення оптимальних параметрів функціонування системи ще на стадії її проектування. У наукових дослідженнях застосовуються математичні, імітаційні та концептуальні моделі. Вони дозволяють описувати закономірності функціонування систем, відтворювати їх поведінку та аналізувати структуру й взаємозв'язки. Як зазначає В. Варенко, моделювання інформаційних процесів підвищує ефективність аналітичної діяльності у сфері обробки даних [3, с. 115].

Важливою тенденцією є використання розподілених і хмарних технологій, що забезпечують масштабовану обробку великих масивів даних. У цьому контексті моделювання дозволяє оптимізувати розподіл ресурсів і навантаження. Дослідження А. Миргородського та О. Романюка підтверджують, що застосування моделей у розподілених

системах підвищує продуктивність і ефективність використання ресурсів [4, с. 288].

Інтеграція технологій штучного інтелекту та машинного навчання розширює можливості обробки даних, забезпечуючи адаптивність і точність аналізу. Зокрема, у роботах Т. Носенко та І. Машкіної показано ефективність моделей обробки екологічних даних у системах моніторингу з використанням безпілотних технологій [5, с. 112].

Таким чином, моделювання процесів обробки даних є важливим інструментом дослідження та проектування сучасних інформаційних систем. Використання різних типів моделей дозволяє аналізувати структуру інформаційних процесів, оптимізувати алгоритми обробки даних, підвищувати ефективність використання обчислювальних ресурсів і забезпечувати високу якість інформаційного забезпечення управлінських рішень.

Список використаних джерел:

1. Мельник Б.Є. Моделювання інформаційних збурень та їх виявлення в інтерактивних інформаційних системах підприємств. *Вісник студентського наукового товариства «ВАТРА» Вінницького торговельно-економічного інституту ДТЕУ*: матеріали XIV Всеукр. студ. наук.-практ. конф. (17 квіт. 2025 р.). Вінниця. 2025. Випуск 203. С. 415–423. URL: <http://www.vtei.com.ua/doc/2025/nauka/zbirnyk3.pdf#page=415>
2. Ткаченко О., Ткаченко К., Піддубченко М. Аналіз сучасних тенденцій розробки інформаційних систем. *Кібербезпека: освіта, наука, техніка*. 2024. № 4 (24). С. 205–220. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/595>
3. Варенко В. Моделювання інформаційних процесів в аналітичній діяльності. *Український журнал з бібліотекознавства та інформаційних наук*. 2023. № 11. С. 112–124. URL: <https://librinfosciences.knukim.edu.ua/article/view/282669>
4. Миргородський А., Романюк О. Аналіз динамічних моделей забезпечення узгодженості даних у розподілених системах керування базами даних. *Measuring and computing devices in technological processes*. 2025. № 3. С. 285–292. URL: <https://vottp.khmnu.edu.ua/index.php/vottp/article/view/584>
5. Носенко Т., Машкіна І. Моделювання процесів обробки екологічних даних для систем мобільного моніторингу на основі БпІА та методу IDW. *Кібербезпека: освіта, наука, техніка*. 2025. № 2(30). С. 110–124. URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/955>

УДК 004.85:004.62

Савчук О. І., магістрант

Житомирський державний університет імені Івана Франка

СУЧАСНІ ПІДХОДИ ТА ВИКЛИКИ У ВИКОРИСТАННІ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ДАНИХ

В умовах сучасного цифрового суспільства більшість користувачів взаємодіє з технологіями, які узагальнено називають штучний інтелект, що не повною мірою відображає складність і різноманітність всіх можливостей цих технологій. Наприклад, популярні системи, такі як: ChatGPT, Gemini, Claude, Grok та інші, належать до класу великих мовних моделей (LLM, Large Language Models), – які є лише одним із підвидів технологій у межах машинного навчання (machine learning). Їх функціонування ґрунтується на відповідних алгоритмах і принципах, що є логічним продовженням розвитку підходів машинного навчання. Водночас LLM становлять лише частину широкого спектра сучасних рішень у галузі штучного інтелекту

Машинне навчання виступає складовою ширшої концепції штучного інтелекту та охоплює різноманітні методи і підходи. Однією з ключових сфер його застосування є аналіз великих обсягів даних, де автоматизовані алгоритми дозволяють ефективно обробляти інформацію, яка є надто масштабною для ручного опрацювання.

Практичне застосування машинного навчання в аналізі даних базується на використанні конкретних алгоритмів, кожен із яких орієнтований на вирішення певного класу задач. Залежно від мети аналізу (класифікації, прогнозування чи виявлення закономірностей) обирається відповідний підхід і модель.

Цей вибір безпосередньо залежить від формату моделі. Кожен формат має свої специфіки та розгалуження, до прикладу, різні варіанти «навчання» моделі: навчання без учителя широко використовується для виявлення прихованих закономірностей у даних, тоді як навчання з учителем – для класифікації та прогнозування. У межах задач класифікації використовуються різні алгоритмічні підходи, зокрема логістична регресія, дерева рішень і метод k-найближчих сусідів. Практичне застосування цих алгоритмів охоплює, наприклад, визначення чи є лист спамом, оцінювання кредитного ризику клієнтів. Це дозволяє не лише підвищити ефективність, але й отримати конкурентну перевагу на ринку.

Однак разом із перевагами існують і суттєві проблеми, виклики. Один із ключових – це якість даних, адже результати роботи моделей безпосередньо залежать від даних, на яких вони навчаються. Неповні,

зашумлені або упереджені дані [1] можуть призвести до некоректних результатів. Алгоритми можуть відтворювати або навіть посилювати існуючі соціальні думки, якщо вони присутні в навчальних даних [3]. Тому розробники повинні враховувати аспекти справедливості, прозорості та відповідальності при створенні систем.

Додатковою проблемою є обмежена інтерпретованість складних моделей, зокрема глибоких нейронних мереж (DNN, Deep Neural Network) і великих мовних моделей. Їх функціонування часто є непрозорим для користувача, що ускладнює розуміння механізмів отримання результатів, а також оцінювання їхньої достовірності [2]. Це створює труднощі у довірі до таких систем та їх впровадженні в критично важливі процеси.

Також варто згадати про технічні обмеження, зокрема високі вимоги до обчислювальних ресурсів. Навчання складних моделей потребує значних потужностей, що може бути недоступним для малих компаній або окремих дослідників. Разом з цим, збільшення потужностей прямопропорційно впливає на збільшення витрат підтримки життєдіяльності систем штучного інтелекту, що з часом може критично вплинути на навколишнє середовище [4].

Попри це, перспективи машинного навчання залишаються значними, а його інтеграція в різні сфери відкриває нові можливості для розвитку. Водночас ключовим є забезпечення відповідального та обґрунтованого використання цих технологій. Отже, сучасні підходи до застосування машинного навчання демонструють суттєвий прогрес, але потребують комплексного врахування як технічних, так і етичних аспектів для ефективного використання їх потенціалу.

Список використаних джерел:

1. Data Cleaning. Definition, types, and examples. Julius. URL: <https://julius.ai/glossary/data-cleaning> (дата звернення: 22.03.2026).
2. Columbia Journalism Review. AI Search Has a Citation Problem. Columbia Journalism Review. URL: https://www.cjr.org/tow_center/we-compared-eight-ai-search-engines-theyre-all-bad-at-citing-news.php (дата звернення: 22.03.2026).
3. What is AI bias? | SAP – System Analysis Program Development. URL: <https://www.sap.com/resources/what-is-ai-bias#top> (дата звернення: 22.03.2026).
4. Science Feedback. How much electricity do data centers use, and can they run on renewables?. Science Feedback. URL: <https://cutt.ly/ytl6B4W3> (дата звернення: 22.03.2026).

УДК 004.89

*Селіванов М. В., аспірант,
Пархоменко А. В., к. т. н., доцент,
Національний університет «Запорізька політехніка»*

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ТА ЗАСОБИ ПРОЄКТУВАННЯ ІНТЕРФЕЙСІВ КОМП'ЮТЕРНИХ СИСТЕМ

Технології на основі штучного інтелекту (ШІ) сьогодні активно використовуються при проєктуванні інтерфейсів комп'ютерних систем (ІКС). Однак питання удосконалення ІКС для покращення досвіду користувачів залишаються предметом чисельних досліджень [1-2].

В роботах [3-4] було доведено актуальність використання методів та засобів генеративного ШІ для розробки структури, генерації текстового контенту, зображень та надання рекомендацій щодо удосконалення ІКС. Проте, актуальною задачею залишається підвищення ефективності їх застосування, оскільки розробнику часто доводиться використовувати окрім професійного середовища розробки цілий набір додаткових інструментів на основі ШІ, що не є зручним та потребує додаткових витрат часу.

Метою роботи є інтеграція засобів генеративного ШІ в єдиному програмному середовищі, що забезпечить централізований доступ до інструментів розробника для підвищення ефективності процесу проєктування ІКС.

Розроблена архітектура середовища включає інтерфейсний модуль; модуль керування запитами; API-інтеграційний модуль; модуль обробки та трансформації результатів; модуль збереження стану та контексту.

Програмний застосунок реалізовано для платформи Figma з використанням стеку технологій на основі JavaScript, HTML, CSS, OpenAI API та Figma API.

Програмний застосунок працює за принципом «єдиної точки входу» до ШІ-функціоналу. Методика використання наступна.

Крок 1. Користувач формує запит у межах плагіна.

Крок 2. Запит стандартизується та передається до відповідного API.

Крок 3. Отриманий результат обробляється та адаптується до структури Figma.

Крок 4. Згенерований контент автоматично інтегрується в поточний макет.

Отже усувається потреба переходу між різними вебсервісами, копіювання даних та ручної адаптації результатів.

Розроблений програмний застосунок підтримує наступний функціонал:

- модифікація текстового блоку (зміна тону, скорочення, розширення, персоналізований запит);
- генерація зображень на основі промту користувача;
- чат «ШІ-користувач»;
- організація робочого простору в файлі проєкта Figma (перейменування шарів, створення базової дизайн системи, створення палітри кольорів за принципом Google Design Material);
- аналіз дизайн-макетів користувача з наданням результатів аналізу та поради для покращення від GPT моделі.

Практичне впровадження розробленого програмного застосунку підтвердило значне скорочення часу на виконання типових задач з розробки ІКС. Завдяки інтеграції застосунку в професійне середовище Figma, де виконується основна робота над проєктуванням інтерфейсу, зростає ефективність роботи, оскільки реалізований функціонал дозволяє заощаджувати час на відкриття, перемикання, копіювання, тощо.

В подальшій роботі планується розширення та вдосконалення поточного функціоналу застосунку, зокрема інтеграція більшої кількості API різних моделей генеративного ШІ та тестування застосунку широким колом розробників.

Список використаних джерел:

1. Evaluating and eliciting design requirements for an improved user experience in live-streaming commerce interfaces / [Shin, H., Oh, C., Kim, N. et al.] // *Computers in Human Behavior*. - 2023. - Vol.150. - P. 20-31.
2. Розроблення підходів до вибору методології проєктування інтерфейсу смартсистем / [Г. І. Липак, Т. А. Липак, Н. Е. Кунанець та ін.] // *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*". - 2025. - № 60. - С. 190–199.
3. Селіванов, М.В. Дослідження методів та засобів проєктування інтелектуального інтерфейсу комп'ютерних систем / М.В. Селіванов, А.В. Пархоменко // *Наукові праці ДонНТУ. Серія: Інформатика, кібернетика та обчислювальна техніка*. – 2025. – № 1(40). – С. 97-105.
4. Селіванов, М.В. Інтеграція засобів ШІ для проєктування інтелектуального інтерфейсу комп'ютерних систем / М.В. Селіванов, А.В. Пархоменко // *Друга міжнародна науково-практична конференція «Штучний інтелект та інформаційні технології»*, Київ, 3–4 червня 2025 р.: тези доповідей. – Київ: НУХТ. – 2025. – С.78-81.

УДК 623.1/.7

*Фриз С. П., д.т.н., професор,
Авсієвич Р.О., доктор філософії, доцент,
Дацько Д.В., курсант
Житомирський військовий інститут ім.С.П. Корольова*

КОМПЛЕКС МУЛЬТИСЕНСОРНОЇ РОЗВІДКИ В УМОВАХ РОЗУМНОГО ПОЛЯ БОЮ

Сучасні бойові дії характеризуються переходом до концепції «розумного поля бою», де ключову роль відіграють системи моніторингу, вони являють собою мультисенсорні комплекси, які включають радіолокаційні, оптико-електронні, лідарні, акустичні та радіотехнічні засоби розвідки. Можуть розгортатись на наземних, повітряних, морських та космічних платформах і функціонувати як єдина інформаційна система.

В умовах активного застосування противником засобів маскування, радіоелектронної боротьби та дезінформації, ефективність традиційних систем знижується. Тому інтеграція технологій штучного інтелекту (ШІ) у системи управління боєм є критично важливою для підвищення швидкості, точності та обґрунтованості управлінських рішень.

На сьогодні активно впроваджуються автоматизовані системи ситуаційної обізнаності, що забезпечують збір, передачу та часткову обробку даних у реальному часі. У провідних країнах в тому числі в Україні застосовуються елементи ШІ для аналізу відеопотоків, виявлення цілей та підтримки прийняття рішень.

В Україні спостерігається розвиток подібних систем, зокрема інтеграція безпілотних платформ, геоінформаційних систем та базових алгоритмів машинного зору, що формують основу для подальшого впровадження повноцінних ШІ-рішень.

Основною проблемою є перевантаження систем управління великими обсягами різномірної інформації, яка надходить від численних сенсорів. Дані часто є неповними, суперечливими або зашумленими внаслідок впливу радіоелектронної боротьби та застосування противником хибних цілей.

Існуючі системи не забезпечують достатнього рівня автоматизації аналізу, що призводить до збільшення часу прийняття рішень і зростання навантаження на операторів. Також відсутня ефективна інтеграція даних з різних джерел та механізми достовірної фільтрації хибної інформації.

У результаті знижується точність виявлення та класифікації цілей, що негативно впливає на ефективність бойового застосування сил і засобів.

Підвищення ефективності систем моніторингу поля бою можливе шляхом комплексного впровадження технологій ШІ та побудови інтегрованих мультисенсорних систем.

Основні напрямки які варто розвивати:

застосування алгоритмів комп'ютерного зору (YOLO, CNN) для автоматичного виявлення та класифікації цілей;

використання методів злиття даних (Kalman Filter, Bayesian Networks) для формування єдиної картини поля бою;

впровадження алгоритмів виявлення аномалій для фільтрації хибних цілей та протидії РЕБ;

застосування моделей прогнозування (LSTM, Particle Filter) для оцінки поведінки противника;

використання методів підкріплювального навчання (Reinforcement Learning) для підтримки прийняття рішень та оптимізації бойових дій.

Перспективною є побудова ієрархічної системи, що включає сенсорні вузли, передові пости спостереження, командно-спостережні пункти та центри обробки даних, об'єднані в єдину інформаційну мережу з використанням ШІ.

Реалізація таких підходів дозволить підвищити точність розвідки, скоротити час прийняття рішень та забезпечити ефективне використання наявних ресурсів у сучасних бойових умовах.

Список використаних джерел:

1. Гуржій С. В. Тенденції застосування технологій штучного інтелекту у військово-технічній сфері. Інформація і право. 2024. № 3(50).
2. Лисецький Ю. М. Основи та складові штучного інтелекту // Military Strategy and Technology. 2025. № 1.
3. Боровик Д. О., Зарецький М. О. Використання дронів та штучного інтелекту у військовій стратегії України // Вісник Херсонського національного технічного університету. 2025. № 3
4. Трофименко О. Г., Дика А. І., Логінова Н. І. та ін. Штучний інтелект у військових навчальних симуляторах // Інформаційні технології та суспільство. 2024. № 2(13).

УДК 004.65:004.032.2

**Бабарицький Д. О., здобувач,
Білова Т. Г., к.т.н., доцент**

Харківський національний університет радіоелектроніки

ФОРМУВАННЯ СИСТЕМИ АНАЛІТИЧНИХ ПОКАЗНИКІВ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ПУБЛІЧНИХ ЗАКУПІВЛЯХ

Ефективність цифрових публічних закупівель безпосередньо залежить від своєчасного виявлення ризикових тендерів та системного проведення моніторингу [1]. Головною проблемою автоматизації аналізу тендерів у системі публічних закупівель «Prozorro» залишається різноманітність даних: поєднання значного обсягу неструктурованих текстових описів із кількісними ознаками, що унеможливорює пряме алгоритмічне порівняння лотів і ускладнює пошук аномалій. Також ідентичні товари в різних тендерах можуть відображатися як унікальні об'єкти, що приховує штучне завищення цін.

Для вирішення проблеми запропоновано ієрархічну систему показників та процедуру їх динамічної агрегації для приведення даних до спільного математичного простору. Завдяки цьому пошук прихованих цінових аномалій відбувається всередині автоматично сформованих однорідних за описом підгруп, що дозволяє порівнювати однакові за предметом закупівель тендери.

Схему ієрархічної структури показників та процесу їх обробки представлено на рисунку 1.



Рис.1. Ієрархічна структура аналітичних показників та процедура їх агрегації для виявлення аномалій

Згідно з принципами моніторингу складних інформаційних систем [2], розроблена система будується за ієрархічним принципом і передбачає динамічне агрегування даних з нижчого рівня управління на вищий.

На початковому етапі збору інформації через API «Prozorro» формується масив базових показників: фактичний обсяг, очікувана вартість, наявність ПДВ та місяць оголошення. Далі ці кількісні метрики агрегуються, утворюючи похідні показники, зокрема, ціну за одиницю товару. З метою усунення статистичного шуму та зменшення впливу викидів застосовується логарифмічне згладжування цих показників.

Проблема неструктурованих описів вирішується шляхом введення групи семантичних показників. Текстові дані проходять очищення, лематизацію та векторизуються за алгоритмом TF-IDF. Оскільки кількість підгруп наперед невідома, для агрегації семантичних показників у вищі класифікаційні групи використовується алгоритм K-Means. Він автоматично розбиває векторний простір на підгрупи, де оптимальна кількість категорій визначається динамічно за критерієм максимізації коефіцієнта силуету.

Процес перетворення показників повинен контролювати втрату інформації. Для цього до багатовимірного простору похідних та семантичних показників застосовується метод головних компонент. Він дозволяє знизити розмірність даних із мінімізацією втрати дисперсії.

На фінальному етапі прийняття рішень щодо ризиковості тендеру розгортається щільніший алгоритм DBSCAN. Він оцінює агреговані показники всередині кожної категорії, маркуючи як аномальні ті лоти, що демонструють нетипове співвідношення показників.

Отже, розроблена ієрархічна система аналітичних показників дозволяє формалізувати процес моніторингу закупівель. Застосування алгоритмів NLP, K-Means, PCA та DBSCAN для агрегації аналітичних показників дозволяє контролювати втрату інформації та автоматично дозволяється виявляти приховані цінові відхилення, формуючи обґрунтовані рішення для аудиторів.

Список використаних джерел:

1. Fazekas M., Tóth I. J., King L. P. An objective corruption risk index using public procurement data // *European Journal on Criminal Policy and Research*. 2016. Vol. 22, No. 3. P. 369–397. DOI: <https://doi.org/10.1007/s10610-016-9308-z>
2. Білова Т. Г., Ярута В. О., Побіженко І. О. Формування ієрархічної структури показників моніторингу складної інформаційної системи // *Системи обробки інформації*. 2015. № 12(137). С. 78–80.

УДК 004.05

*Любиченко О.В., здобувач
Горобець С.М., к. пед. н., доцент
Житомирський державний університет імені Івана Франка*

МЕТОДИ ПІДВИЩЕННЯ ДОСТОВІРНОСТІ ОЦІНОК В СИСТЕМАХ РЕЙТИНГУВАННЯ

Сьогодні рейтингові системи використовуються практично в усіх цифрових сервісах: соціальних мережах, інтернет-магазинах, стрімінгових платформах, електронних каталогах тощо. Рейтинги дозволяють користувачам проводити оцінку контенту та впливати на популярність того чи іншого інформаційного продукту. Проте спосіб обчислення рейтингу може суттєво впливати на кінцевий результат оцінювання. Через це одна й та сама сукупність оцінок може бути представлена по-різному залежно від обраного методу.

Найпростіший варіант – це обчислення середнього арифметичного значення оцінки, яке визначається за формулою:

$$R = \frac{1}{n} \sum_{i=1}^n r_i \quad (1)$$

де r_i – окрема оцінка; n – кількість оцінок.

Такий підхід часто використовують на практиці, але він має недолік: результат легко зміщується навіть через невелику кількість нетипових оцінок. Наприклад, кілька дуже високих або дуже низьких значень можуть помітно занизити чи завищити загальний рейтинг.

Через це на практиці все частіше використовують більш стійкі до нетипових оцінок методи рейтингування. Зокрема, байесівські підходи (Bayesian approaches) дозволяють враховувати не тільки самі оцінки, їхню кількість (достовірність), а й враховувати середні показники рейтингів подібних об'єктів оцінювання. Цікавим прикладом складного підрахунку рейтингів є система Ело, яка спочатку використовувалась у іграх з нульовою сумою, наприклад, у шахах, але з часом почала застосовуватися і в інших сферах [1].

Окремо варто згадати метод агрегації рангів. Агрегація потрібна тоді, коли використовують кілька різних алгоритмів і є необхідність отримати один загальний список. При порівнянні різних підходів, зокрема методів Борда (Borda count), Кемени-Янга (Kemeny-Young's method) та Коупленда (Copeland's method) було виявлено, що вирішальним фактором є не складність методу, а попередня нормалізація значень. Після нормалізації оцінок навіть прості способи рейтингування дають досить адекватні результати [2].

Окрему увагу потрібно приділяти шкалі оцінювання. Якщо шкала оцінок має великий крок, наприклад, має лише три значення, то результати рейтингування можуть сильно «стрибати». Цей недолік може сильно спотворювати результати для багатокритеріальних систем оцінювання. Тому на практиці зазвичай використовують більш деталізовані шкали, які мають хоча б 5 – 7 рівнів оцінки [3].

У простих системах часто застосовується обчислення рейтингів за допомогою середнього значення. Через це виникає проблема неадекватного рейтингування нових об'єктів оцінювання у випадках, коли ці об'єкти мають лише кілька оцінок. Один із поширених способів уникати такі ситуації – це метод Байєсівського середнього:

$$R_{bayes} = \frac{C \cdot m + \sum_{i=1}^n r_i}{m + n}, \quad (2)$$

де r_i – оцінка; n – кількість оцінок; C – середня оцінка по всій системі; m – кількість штучно доданих оцінок. Поки оцінок мало, рейтинг прив'язується до середнього у групі, а з часом реальні оцінки вже його корегують. Крім цього, важливо зменшити можливі зовнішні навмисні впливи на результати рейтингування. У великих системах це робиться через обмеження в правилах голосування та через аналіз поведінки користувачів. Наприклад, якщо несподівано з'являється багато однакових оцінок, їх можуть частково ігнорувати.

Отже, можна зазначити, що для підвищення адекватності рейтингів потрібно використовувати методи оцінювання стійкі до нетипових оцінок, наприклад, засновані на Байєсівському підході чи на методі агрегації рангів. В майбутньому, ці методи можуть комбінуватись із адаптивними алгоритмами машинного навчання.

Список використаних джерел:

1. Olesker-Taylor S., Zanetti L. An analysis of Elo rating systems via Markov chains. *Advances in Neural Information Processing Systems*. 2024. Vol. 37.
2. Bałchanowski M., Boryczka U. A comparative study of rank aggregation methods in recommendation systems. *Entropy*. 2023. Vol. 25, № 1. DOI: <https://doi.org/10.3390/e25010132>
3. Zhao S., Dong Y., He Y. The reliability analysis of rating systems in decision making: when scale meets multi-attribute additive value model. *Decision Support Systems*. 2020. Vol. 138. DOI: <https://doi.org/10.1016/j.dss.2020.113384>

УДК 004.89

*Поздняков О. А., аспірант,
Пархоменко А. В., к. т. н., доцент,
Національний університет «Запорізька політехніка»*

ОЦІНЮВАННЯ НЕВИЗНАЧЕНОСТІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ПРИ ГЕНЕРАЦІЇ МІГРОВАНОГО КОРИСТУВАЦЬКОГО АВАР-КОДУ

Інтелектуальний реінжиніринг складних комп'ютерних систем (КС), зокрема міграція користувацького АВАР-коду при переході з застарілої версії SAP ERP 6.0 на нову версію SAP S/4HANA, є одним із ключових завдань цифрової трансформації сучасних підприємств [1].

Дослідження [2, 3] показали ефективність використання методів та засобів генеративного штучного інтелекту для автоматизації цього процесу. Разом з тим, залишається невирішеним питання довіри до результатів, оскільки велика мовна модель (LLM) може генерувати некоректний код без явних ознак помилки (hallucinations), що є критичною проблемою у корпоративних системах. Проблематика оцінювання невизначеності (Uncertainty Quantification, UQ) для LLM є предметом активних досліджень [4, 5], проте її застосування в задачах міграції користувацького коду залишається недостатньо вивченим, що обумовлює актуальність цієї роботи.

Метою роботи є розробка методу оцінювання невизначеності LLM при генерації мігрованого користувацького АВАР-коду для підвищення ефективності процесу інтелектуального реінжинірингу КС.

Розроблюваний метод складається з трьох етапів.

Перший етап передбачає введення метрики Confidence Score (CS) на основі ентропії розподілу токенів при генерації:

$$CS = 1 - \frac{H(p)}{\log|V|},$$
 де $H(p)$ – ентропія розподілу ймовірностей наступного токена, $|V|$ – розмір словника моделі. Висока ентропія сигналізує про невизначеність моделі під час генерації коду.

Другий етап базується на стохастичному семплюванні (Stochastic Sampling, SS): для одного вхідного фрагмента виконується N прогонів генерації з ненульовою температурою, що дозволяє отримати кілька варіантів коду. Варіативність результатів генерації σ_{SS} відображає невизначеність моделі.

Третій етап полягає в інтеграції отриманих показників із метрикою якості IAQS [3] у розширену метрику IAQS⁺ за формулою: $IAQS^+ = \alpha \cdot IAQS + \beta \cdot CS + \gamma \cdot (1 - \sigma_{SS})$, де σ_{SS} – нормована варіативність результатів стохастичного семплювання; α , β , γ – вагові коефіцієнти

($\alpha + \beta + \gamma = 1$), що визначаються експертно або методом аналізу ієрархій.

За результатами оцінювання IAQS+ фрагменти мігрованого користувацького коду автоматично розподіляються на три категорії: «прийнято» ($\text{IAQS+} > 0.75$), «потребує перевірки» ($0.5 \leq \text{IAQS+} \leq 0.75$) та «відхилено» ($\text{IAQS+} < 0.5$). Остаточне калібрування порогів планується за результатами експерименту. Така тривівнева класифікація суттєво скорочує обсяг ручної верифікації порівняно з повним переглядом усього мігрованого користувацького коду фахівцем.

Експериментальну перевірку методу заплановано на вибірці користувацького АВАР-коду з використанням моделі Qwen 2.5 Coder 14B. Очікується суттєве скорочення частки хибно прийнятих фрагментів мігрованого коду порівняно з використанням лише IAQS.

Розроблюваний метод оцінювання невизначеності LLM забезпечить формалізований контроль генерації мігрованого користувацького АВАР-коду. У подальшому планується його інтеграція в процес інтелектуального реінжинірингу КС.

Список використаних джерел:

1. Поздняков О. А. Міграція користувацького коду на нові версії складних комп'ютерних систем з використанням методів і моделей інтелектуального реінжинірингу / О. А. Поздняков, А. В. Пархоменко // Наукові праці ДонНТУ. Серія «Інформатика, кібернетика та обчислювальна техніка». — 2025. — № 2(41). — С. 86–98.
2. Поздняков О. А. Дослідження та вибір великих мовних моделей для автоматизації міграції АВАР-коду / О. А. Поздняков, А. В. Пархоменко // Управління розвитком складних систем. — 2025. — № 63. — С. 191–200.
3. Pozdnyakov O. A. Evaluation and quality assurance of migrated ABAP code using an integral metric and generative artificial intelligence models / O. A. Pozdnyakov, A. V. Parkhomenko // Computer Science. Software Engineering. — 2026. — № 1. — P. 80–89.
4. Detecting hallucinations in large language models using semantic entropy / [S. Farquhar, J. Kossen, L. Kuhn, Y. Gal] // Nature. — 2024. — Vol. 630. — P. 625–630.
5. Look before you leap: An exploratory study of uncertainty analysis for large language models / [Y. Huang, J. Song, Z. Wang et al.] // IEEE Transactions on Software Engineering. — 2025. — Vol. 51, № 2. — P. 413–429.

УДК 004

*Бадігон В.О., здобувач,
Петросян А.Р., аспірант,
Державний університет «Житомирська політехніка»*

РОЗРОБКА БІОМЕТРИЧНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА БАЗІ АРХІТЕКТУРИ EDGE-TO-CLOUD

Сучасні системи контролю доступу все частіше інтегруються з IoT-пристроями [1, 2] та біометричними модулями [3]. Однак більшість існуючих рішень або є закритими пропріетарними платформами (Kisi), або орієнтовані на B2C-сегмент без належної підтримки біометрії, або вимагають глибокої кастомізації з нуля, наприклад, Home Assistant. Крім того, критичною проблемою залишається захист біометричних даних – передача та зберігання зображень обличчя створює ризики витоку персональної інформації. Тому актуальним є проектування власної системи, яка поєднує розподілену обробку даних із вбудованими механізмами конфіденційності.

В основі запропонованого рішення лежить архітектурний підхід Edge-to-Cloud, який передбачає чіткий розподіл функціональних обов'язків між периферійними пристроями та серверною частиною системи. Як показано на діаграмі розгортання (рис. 1), до складу інфраструктури входять інтелектуальні хаби, сервер обробки запитів та база даних. Така організація дозволяє оптимізувати обробку даних і підвищити загальний рівень безпеки. Ключовою особливістю архітектури є винесення процесів біометричної ідентифікації на рівень edge-пристроїв. Smart Hub виконує захоплення зображення, його обробку за допомогою нейромережових алгоритмів та формування векторного представлення обличчя користувача. При цьому первинні зображення не передаються до мережі, що повністю відповідає принципам концепції Privacy by Design. На сервер передається лише ідентифікатор користувача та ідентифікатор замка, що суттєво знижує ризики компрометації персональних даних.

Серверна частина системи реалізована з використанням модульної архітектури і виконує функції валідації доступу, керування правами та ведення журналу подій. Відповідно до діаграми розгортання, сервер взаємодіє з базою даних, у якій зберігаються списки контролю доступу (ACL), конфігурації пристроїв і журнали аудиту. Перевірка прав доступу здійснюється шляхом виконання цільового запиту до колекції ACL за параметрами `userId` та `lockId`. Такий підхід дозволяє отримати рішення про доступ за один запит до бази даних, що є критичним для систем реального часу.

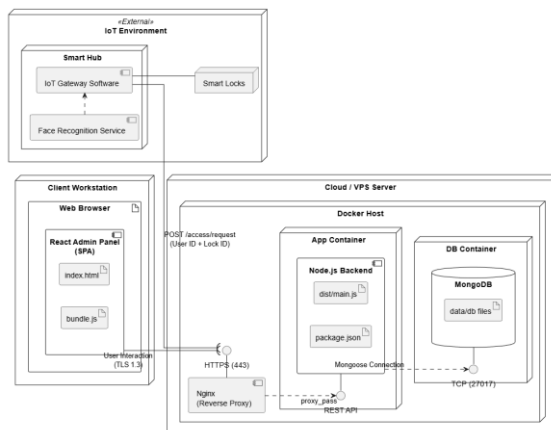


Рис. 1. Діаграма розгортання системи

Безпека системи забезпечується комплексом архітектурних рішень, які також відображено на діаграмі розгортання. Зокрема, реалізовано підхід Zero-Trust, відповідно до якого кожен пристрій автентифікується при кожному запиті до сервера. Додатково застосовано ізоляцію біометричних даних, оскільки сервер не зберігає зображення облич, а оперує лише їхніми векторними представленнями.

Таким чином, запропонована система поєднує розподілену обробку даних, високий рівень безпеки та ефективні механізми управління доступом. Використання підходу Edge-to-Cloud дозволяє досягти балансу між продуктивністю, масштабованістю та захистом персональних даних, що робить систему придатною для впровадження в сучасних корпоративних середовищах.

Список використаних джерел:

1. Ahsan M. S., Pathan A.-S. K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. *IoT*. 2025. Vol. 6, no. 1. P. 9. URL: <https://doi.org/10.3390/iot6010009>.
2. Петросян А. Р., Петросян Р. В., Колос К. Р. Розробка платформи віддаленого управління інфраструктурою Інтернет речей. *Технічна інженерія*. 2021. № 1(87). С. 73–80. URL: [https://doi.org/10.26642/ten-2021-1\(87\)-73-80](https://doi.org/10.26642/ten-2021-1(87)-73-80).
3. Biometric-Based Access Control Systems with Robust Facial Recognition in IoT Environments / B. V. Satish Babu et al. 2024 *Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Krishnankoil, Virudhunagar district, Tamil Nadu, India, 14–16 March 2024. 2024. URL: <https://doi.org/10.1109/incos59338.2024.10527499>.

УДК 004.93:004.8

*Штиль М.Р., здобувач,
Петросян Р.В., ст. викладач
Державний університет «Житомирська політехніка»*

ІНТЕЛЕКТУАЛЬНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОБЛИЧ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

Сучасні системи контролю доступу (СКД) все частіше інтегруються в IoT-екосистеми [1, 2], що потребує автономної роботи на вбудованих пристроях з обмеженою обчислювальною потужністю та енергоспоживанням. Використання хмарних API для розпізнавання облич створює ризики щодо конфіденційності біометричних даних і затримок передачі. Тому актуальною є розробка локальної нейромережевої моделі FaceID, оптимізованої для роботи на мікрокомп'ютерах типу Raspberry Pi у складі розподіленої IoT-системи.

Мета роботи – розробити та дослідити інтелектуальну СКД на основі згорткової нейронної мережі з метричним навчанням, що забезпечує ідентифікацію особи в реальному часі на малопотужному периферійному пристрої з подальшою інтеграцією в архітектуру Edge-to-Cloud.

Запропоновано модульну архітектуру, що включає:

- IoT-вузол збору даних – камера на базі мікроконтролера ESP32, яка фіксує зображення та передає його на хаб;
- обчислювальний Smart Hub (на базі Odroid або інший аналога Raspberry Pi) – виконує локальну детекцію обличчя, попередню обробку та нейромережеву ідентифікацію;
- модуль прийняття рішень – порівнює отриманий вектор з базою даних і надсилає сигнал на виконавчий пристрій (електронний замок).

Центральним аналітичним ядром системи є нейромережева модель, яка отримує необроблені дані, проводить вирівнювання та генерує унікальний 512-вимірний вектор обличчя. Для цього обрано архітектуру ResNet18 (18 шарів з залишковими зв'язками), що дозволяє уникнути деградації градієнтів при глибокому навчанні. Такий баланс між точністю та обчислювальною складністю є критичним для роботи на вбудованих пристроях.

Для навчання використано функцію втрат ArcFace, яка проектує вектори ознак на гіперсферу та максимізує кутову відстань між різними класами (особами). На відміну від стандартного Softmax, ArcFace дозволяє отримувати дискримінативні компактні ембедінги, що значно

зменшує розмір вихідного шару і є критичним для ідентифікації серед сотень співробітників.

Попередня обробка зображень включає: детекцію обличчя за допомогою MediaPipe Face Mesh, знаходження ключових точок, афінне перетворення для корекції нахилу, масштабування та центрування. Фінальне зображення приводиться до розміру 96×112 пікселів. Це дозволяє стандартизувати вхідні дані, зменшити вплив фону та освітлення, а також підвищити швидкість інференсу.

Для навчання використано відкритий датасет CASIA-WebFace (478 332 зображення, 10 572 особи) з характерним «довгим хвостом» розподілу. Реалізовано конвеєр даних для паралельної обробки. Застосовано стратегію поетапного навчання: значення кутового штрафу m лінійно зростає від 0.1 до 0.35 протягом 10 епох, що забезпечує стабільну збіжність. Адаптивне зниження швидкості навчання активується лише після стабілізації m . Для запобігання перенавчанню використано L2-регуляризацию, шари Dropout, а також змішану точність (mixed precision) тощо.

Оцінка якості моделі проводилася за метриками loss, асигасу на тренувальній та валідаційній вибірках (10% від датасету). Динаміка навчання показала відсутність критичного перенавчання (після 12-ї епохи валідаційна точність стабілізується). У сценарії верифікації 1:1 емпірично визначено оптимальний поріг косинусної подібності – 0.45.

Вимірювання швидкодії проводилися на CPU AMD Ryzen 5 7500F. Стабільний час інференсу на кадр після розігріву становить 43 мс, що відповідає ≈ 23 FPS. Враховуючи, що цільовою платформою є мікрокомп'ютер Odroid з апаратним прискорювачем NPU, очікувана затримка після оптимізації буде аналогічною.

Список використаних джерел:

1. Ahsan M. S., Pathan A.-S. K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art. IoT. 2025. Vol. 6, no. 1. P. 9. URL: <https://doi.org/10.3390/iot6010009>.
2. Петросян А. Р., Петросян Р. В., Колос К. Р. Розробка платформи віддаленого управління інфраструктурою Інтернет речей. Технічна інженерія. 2021. № 1(87). С. 73–80. URL: [https://doi.org/10.26642/ten-2021-1\(87\)-73-80](https://doi.org/10.26642/ten-2021-1(87)-73-80).

UDC 004.9

Otreshko Ivan, Postgraduate Student,
Luchnoi Roman, Postgraduate Student,
Litvinova Uliya, Ph.D.,
Kopp Andrii, Ph.D., Associate Professor
National Technical University «Kharkiv Polytechnic Institute»

DATA-DRIVEN APPROACH TO SYNTACTIC GATEWAY QUALITY ANALYSIS OF BUSINESS PROCESS MODELS

Quality of BPMN models determines the accuracy of their interpretation and subsequent use in IT systems. Syntactic quality is of main importance, as errors at this level lead to incorrect process execution logic. Gateways, which determine the branching and merging of sequence flows, play a crucial role. A mismatch between the split and join gateways leads to structural defects in the BPMN model. The paper [1] investigates the ability of language models to analyze BPMN, confirming the relevance of automated approaches. Work [2] proposes intelligent methods for evaluating model quality. However, the problem of formalizing the syntactic gateway quality using BPMN models' data remains relevant. Thus, the aim of this study is to develop a data-driven approach to analyzing the syntactic gateway quality of BPMN models.

The syntactic gateway quality is defined as the average proportion of gateways in the BPMN model that correctly implement business process branching (splits) or merging joins) using the following formula:

$$Q_{syn}^G = \frac{1}{|G|} \left(\sum_{g \in G} \mathbf{1}_S(g) + \sum_{g \in G} \mathbf{1}_J(g) \right),$$

$$\mathbf{1}_S(g) = \begin{cases} 1 & |in(g)| = 1 \wedge |out(g)| > 1, \\ 0 & \text{else} \end{cases},$$

$$\mathbf{1}_J(g) = \begin{cases} 1 & |in(g)| > 1 \wedge |out(g)| = 1, \\ 0 & \text{else} \end{cases},$$

where:

$in(g)$ and $out(g)$ – are the sets of incoming and outgoing sequence flows of a gateway $g \in G$;

G – is the set of gateways defined in the BPMN model;

$\mathbf{1}_S(g)$ – is the indicator function, which takes 1 for split gateways $S \subseteq G$ and 0 for all the other gateway elements;

$\mathbf{1}_J(g)$ – is the indicator function, which takes 1 for join gateways $J \subseteq G$ and 0 for all the other gateway elements.

If the gateways are defined incorrectly (i.e. neither splits nor joins), the Q_{syn}^G value decreases. Thus, the metric Q_{syn}^G reflects the structural consistency level of a business process model.

The proposed data-driven approach is demonstrated in Fig. 1.

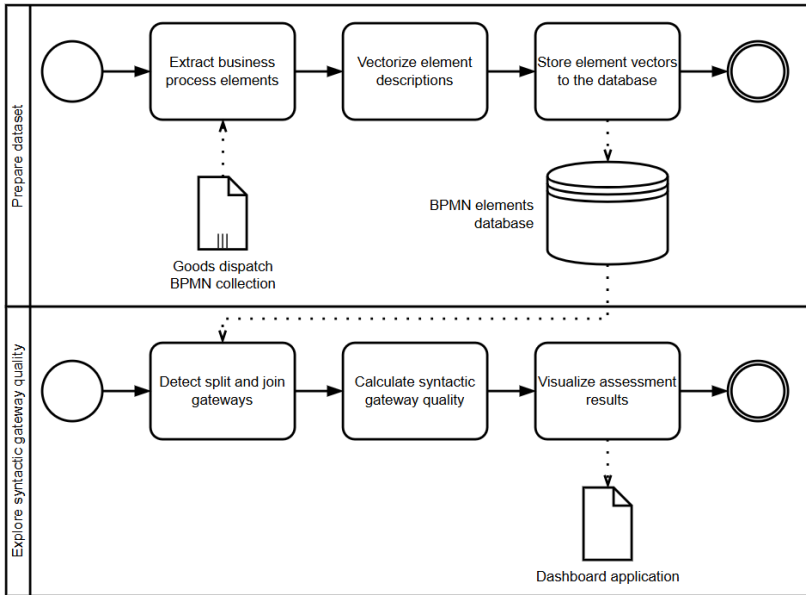


Fig. 1. Data-driven approach to syntactic gateway quality analysis

BPMN elements are extracted and converted into a vector representation, which is then stored in a database. The syntactic quality is calculated as an aggregated metric across all model gateways, reflecting the level of structural consistency. Then, analysis results are visualized using a dashboard and can be used for the further training of an intelligent BPMN evaluation system.

References:

1. Lauer C., Pfeiffer P., Rombach A., Mehdiyev N. Assessing the Business Process Modeling Competences of Large Language Models [Electronic resource]. – Access: <https://arxiv.org/abs/2601.21787>
2. Yanholenko O., Kopp A., Godlevskiy M., Orlovskiy D., Khatsko N. Towards information technology for BPMN models quality assessment based on intelligence theory [Electronic resource]. – Access: <https://ceur-ws.org/Vol-4004/paper7.pdf>

УДК 004.912:005.8:001.89

*Гладич Р. І., науковий співробітник НДУ
Житомирський військовий інститут імені С. П. Корольова*

ЦИФРОВІЗАЦІЯ ПРОЦЕСІВ УПРАВЛІННЯ ТА СУПРОВОДУ НАУКОВОЇ ДІЯЛЬНОСТІ В УМОВАХ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Ефективність сучасного наукового менеджменту безпосередньо залежати від швидкості обробки даних та прозорості моніторингу науково-дослідних робіт (НДР). Традиційні підходи до супроводу наукової діяльності часто страждають від розрізненості інформаційних потоків, що призводить до дублювання звітів та втрати актуальних даних на різних етапах життєвого циклу проекту. Трансформація цих процесів у єдине цифрове середовище дозволяє створити наскрізну систему контролю: від моменту реєстрації ідеї до фіксації кінцевого наукового результату [3].

Запропонована інформаційна система (ІС) реалізує концепцію повного супроводу шляху розробки НДР. В основі архітектури лежить модульний принцип, де кожен етап дослідження формує валідний набір даних для наступних кроків [1]. На стадії планування система автоматизує подачу заявок, перевірку їхньої відповідності пріоритетним напрямам та формування електронних календарних графіків. Це забезпечує вихідну точку для подальшого порівняльного аналізу планових та фактичних показників. Важливим аспектом є інтеграція підсистеми валідації, яка на етапі ініціації проекту проводить автоматизований пошук за внутрішньою базою розробок задля уникнення дублювання тематик та забезпечення унікальності наукового запиту.

Протягом виконання НДР система функціонує як засіб операційного моніторингу. Всі наукові результати – опубліковані статті, отримані патенти, участь у конференціях чи впровадження у виробництво – інтегруються в єдиний цифровий профіль проекту. Такий підхід дозволяє уникнути ручного збору інформації під час проміжних перевірок. Використання веб-орієнтованої платформи забезпечує доступ до актуального стану розробки для всіх учасників процесу: від виконавців до адміністративних підрозділів, що суттєво підвищує якість координації робіт [4]. Додатково впроваджено блок управління ресурсами, що дозволяє відстежувати завантаженість наукового обладнання та ефективність використання бюджетних або грантових коштів у реальному часі.

З технічної точки зору система базується на сервіс-орієнтованій архітектурі, що забезпечує гнучкість при масштабуванні функціональних можливостей. Реалізація централізованого сховища даних дозволяє зберігати не лише текстову звітність, а й первинні цифрові результати досліджень (масиви даних, протоколи експериментів, програмні коди), що є ключовим для верифікації наукових здобутків. Інтерфейсна частина побудована з використанням адаптивних технологій, що надає можливість доступу до аналітичних панелей системи з будь-яких пристроїв, забезпечуючи мобільність наукових керівників при прийнятті управлінських рішень.

Ключовим результатом цифровізації є автоматизація формування звітної документації. Агреговані системою дані дозволяють генерувати підсумкові звіти, мінімізуючи часові витрати на бюрократичні процедури. Це виключає людський фактор при підготовці статистичної звітності для державних органів та внутрішніх структур закладу [2]. Система базується на ролевій моделі доступу, що гарантує цілісність інформації та захист інтелектуальних здобутків наукового колективу. Особливу увагу приділено механізмам верифікації завантажених даних, де кожен результат наукової діяльності проходить стадію цифрового затвердження відповідальною особою, що формує юридично значущий ланцюг доказів виконання робіт.

Впровадження цифрового супроводу змінює логіку управління наукою, роблячи процес розробки НДР контрольованим та прогнозованим. Інтеграція подібних систем у загальне інформаційне середовище установи дозволяє накопичувати базу знань, необхідну для стратегічного планування науково-технічного розвитку та оцінки ефективності використання наукового потенціалу.

Список використаних джерел:

1. Скрипник Г. В., Тютюнник В. М. Цифрова трансформація систем управління науково-технічною діяльністю: архітектурний підхід. *Економіка, управління та адміністрування*. 2023. № 2 (64). С. 45–52.
2. Про наукову і науково-технічну діяльність : Закон України від 26.11.2015 № 848-VIII. URL: <https://zakon.rada.gov.ua> (дата звернення: 24.03.2026).
3. Цифровізація наукової діяльності в Україні: виклики та можливості / О. В. Петренко та ін. *Економіка та держава*. 2021. № 4. С. 12–18.
4. Інформаційні системи та технології в управлінні проектами : монографія / за ред. О. В. Резнікової. Київ : Наукова думка, 2022. 284 с.

УДК 004.89:005.2(043.2)

*Лебедев О.Є, здобувач,
Глазок О.М., к.т.н., доцент
Державний університет «Київський авіаційний інститут»*

ПРОГРАМНИЙ ЗАСІБ АВТОМАТИЗОВАНОГО КОМЕНТУВАННЯ У TELEGRAM-КАНАЛАХ

У сучасному інформаційному середовищі соціальні мережі та месенджери відіграють ключову роль у комунікації між користувачами. Однією з найбільш популярних платформ є Telegram, який активно використовується для ведення інформаційних каналів, поширення новин та взаємодії з аудиторією [1]. Зростання кількості контенту та підписників обумовлює необхідність автоматизації процесів взаємодії, зокрема коментування публікацій.

Ручне коментування повідомлень у Telegram-каналах потребує значних витрат часу та не забезпечує оперативної реакції на нові пости. Існуючі програмні рішення часто мають обмежену гнучкість, складні налаштування або не враховують специфіку конкретного каналу, що знижує їх практичну цінність [2]. Це обумовлює актуальність створення спеціалізованого програмного засобу автоматизованого коментування.

Метою роботи є розробка програмного засобу автоматизованого коментування у Telegram-каналах, який забезпечує автоматичне створення та публікацію коментарів до нових повідомлень. Для реалізації використано мову Python та бібліотеку Telethon [5], що надає засоби взаємодії з Telegram API і підтримує обробку подій у режимі реального часу.

Запропонований програмний засіб побудовано за модульним принципом. До його складу входять модуль моніторингу нових повідомлень, модуль вибору коментаря, модуль надсилання відповіді та модуль логування. Така структура забезпечує гнучкість, спрощує тестування окремих компонентів і дозволяє розширювати функціональність без суттєвих змін у базовій архітектурі.

Алгоритм роботи передбачає відстеження появи нових публікацій у визначеному каналі, аналіз події та формування відповіді за наперед заданими правилами. Для уникнення шаблонності реалізовано механізм випадкового вибору коментарів із підготовленого набору, що підвищує природність взаємодії та зменшує ймовірність повторення однотипних повідомлень.

Важливим аспектом розробки є використання асинхронного програмування, яке дозволяє системі обробляти декілька подій одночасно та забезпечує високу швидкодію в умовах постійного

оновлення контенту [3]. Подієво-орієнтований підхід є доцільним для систем реального часу, оскільки дає змогу мінімізувати затримки та зберігати стабільність роботи навіть за збільшення навантаження.

Сучасні дослідження підтверджують ефективність автоматизації взаємодії у соціальних мережах і вказують на важливість адаптивних механізмів реагування [2, 4]. З огляду на це в роботі передбачено можливість подальшого розширення системи за рахунок інтеграції з аналітичними сервісами, які дозволять оцінювати активність аудиторії, визначати результативність опублікованих коментарів та коригувати параметри роботи програмного засобу.

Під час тестування перевірено роботу системи у різних сценаріях: обробка поодиноких повідомлень, реакція на серію нових публікацій, надсилання коментарів з різних наборів шаблонів. Отримані результати засвідчили коректність функціонування основних модулів, своєчасність публікації коментарів і стабільність роботи протягом тривалого часу.

Практичне значення роботи полягає у можливості використання розробленого програмного засобу для автоматизації ведення Telegram-каналів у сфері медіа, маркетингу та інформаційних технологій. Отже, запропонований підхід дозволяє оптимізувати процес взаємодії з аудиторією, зменшити навантаження на адміністратора та підвищити ефективність комунікації.

Список використаних джерел:

1. Telegram. Official website. URL: <https://telegram.org> (дата звернення: 24.03.2026).
2. Zeng X., Chen L. Social media automation and user interaction: A survey. *IEEE Access*. 2021. Vol. 9. P. 82412–82430.
3. Shahriar H., Haddad R. Event-driven programming for real-time applications. *Journal of Systems Architecture*. 2020. Vol. 107. Article 101729.
4. Kumar S., Gupta A. Automated communication systems in social networks. *International Journal of Information Management*. 2022. Vol. 64. Article 102456.
5. Telethon Documentation. URL: <https://docs.telethon.dev> (дата звернення: 24.03.2026).

УДК 004.9

Мельников О.Ю., к.т.н., доцент

Пархоменко Ю.Д., студент

Донбаська державна машинобудівна академія, м. Краматорськ,

Україна

РОЗРОБКА МОДУЛЬНОЇ СИСТЕМИ КЕРУВАННЯ ПОВЕДІНКОЮ КАМЕРИ В СЕРЕДОВИЩІ UNITY

У сучасних ігрових проєктах, що розробляються в середовищі Unity, система камери є одним із ключових компонентів, що безпосередньо впливає на зручність взаємодії користувача з грою [1]. У більшості випадків реалізація поведінки камери виконується як монолітний скрипт, що ускладнює його розширення, повторне використання та підтримку при зростанні складності проєкту [3]. Це особливо актуально для ігор, у яких камера повинна підтримувати декілька режимів роботи, таких як слідування за об'єктом та вільне переміщення.

Було поставлено й вирішено задачу розробки модульної системи поведінки камери, яка дозволяє гнучко комбінувати різні режими роботи, джерела вхідних даних та алгоритми руху. Запропонований підхід базується на принципах компонентної архітектури та розділення відповідальностей [3-4]. Система включає окремі модулі для визначення режиму роботи камери, отримання вхідних даних користувача та цільових позицій, а також обчислення кінцевого положення камери у просторі.

Однак при розробці такої системи виникає наступне завдання: забезпечити універсальний механізм взаємодії між різними режимами камери, зберігаючи при цьому простоту використання та розширення. Формально це можна описати як задачу побудови абстрактного інтерфейсу ICameraMode, що визначає базові операції керування станом камери, а також набору допоміжних інтерфейсів для джерел даних (позиція цілі, користувацький ввід) та алгоритмів переміщення [4].

Запропонована архітектура передбачає розділення системи на три основні компоненти: режими камери (Follow, Free Move), постачальники даних (Input Provider, Target Provider) та модулі руху (Mover). Кожен режим визначає логіку високого рівня, використовуючи відповідні джерела даних і алгоритми обчислення позиції. Це дозволяє легко додавати нові режими або змінювати поведінку існуючих без модифікації інших частин системи [3, 5].

Пропонується наступний алгоритм функціонування системи. На кожному кадрі активний режим камери отримує необхідні дані

(позицію цілі або напрямок руху), передає їх у модуль обчислення руху, після чого застосовує результат до трансформа камери. Перемикання між режимами здійснюється через централізований контролер, що забезпечує коректну ініціалізацію та завершення роботи кожного режиму [1-2].

Використаємо наступні допущення:

- камера розглядається як об'єкт із позицією та орієнтацією у тривимірному просторі;
- вхідні дані користувача нормалізовані та не залежать від конкретного пристрою введення;
- цільова позиція для режиму слідування визначається або через Transform, або як фіксована точка у просторі.

У подальшому необхідно реалізувати запропоновану модель у середовищі програмування та оцінити її ефективність з точки зору масштабованості, зручності використання та продуктивності [5-6].

Список використаних джерел

1. Unity Technologies. Unity User Manual. URL: <https://docs.unity3d.com/Manual/index.html> (дата звернення: 24.03.2026).
2. Unity Technologies. Cinemachine Documentation. URL: <https://docs.unity3d.com/Packages/com.unity.cinemachine@latest> (дата звернення: 24.03.2026).
3. Robert C. Martin Clean Architecture: A Craftsman's Guide to Software Structure and Design. – Boston: Prentice Hall, 2017. – 432 с.
4. Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides Design Patterns: Elements of Reusable Object-Oriented Software. – Boston: Addison-Wesley, 1994. – 395 с.
5. Jason Gregory Game Engine Architecture. – Boca Raton: CRC Press, 2018. – 1136 с.
6. Ian Millington Game Physics Engine Development. – Boca Raton: CRC Press, 2010. – 512 с.

УДК 004.7

*Шкільнюк Д.О., здобувач,
Коротун О.В., к.пед.н., доцент
Державний університет «Житомирська політехніка»*

ОГЛЯД РІЗНОВИДІВ МІНІ-ІГОР

Сучасна індустрія відеоігор стрімко розвивається, охоплюючи різні жанри, платформи та формати взаємодії з користувачем. Одним із важливих елементів багатьох цифрових продуктів є міні-ігри. Це невеликі за обсягом інтерактивні ігрові механіки, які інтегруються в більші проекти або існують як самостійні продукти. Вони дозволяють підвищити залученість користувачів, урізноманітнити геймплей та спростити сприйняття складної інформації. Крім того, міні-ігри активно застосовуються у сфері освіти, маркетингу та гейміфікації.

Метою роботи є огляд основних різновидів міні-ігор, їх класифікація та аналіз особливостей використання в сучасних цифрових продуктах.

Міні-ігри можна визначити як короткі, завершені ігрові сценарії з простими правилами та обмеженою тривалістю проходження. Згідно з підходами до класифікації ігор, навіть невеликі ігрові механіки можуть належати до різних жанрів залежно від їх геймплейних особливостей.

Відповідно до аналізу наукових джерел, популярність різних жанрів ігор змінюється з часом, проте деякі з них залишаються базовими для створення міні-ігор. Основні різновиди міні-ігор:

1) *Аркадні міні-ігри* - це найпоширеніший тип міні-ігор, який характеризується простою механікою, швидким темпом та необхідністю реакції. Прикладом можуть бути ігри на ухилення, збір предметів або подолання перешкод. Такі ігри легко інтегруються в мобільні додатки та часто використовуються для коротких сесій.

2) *Головоломки (Puzzle)* - міні-ігри орієнтовані на логічне мислення користувача, включають задачі на відповідність, сортування, складання або пошук рішень. Згідно з проведеним аналізом, головоломки є одними з найбільш досліджуваних жанрів у літературі.

3) *Казуальні міні-ігри* характеризуються доступністю для широкої аудиторії та відсутністю складного навчання. Вони часто поєднують елементи різних жанрів і використовуються у соціальних та мобільних іграх.

4) *Симуляційні міні-ігри* відтворюють певні реальні процеси у спрощеній формі. Наприклад, керування ресурсами, вирощування рослин або приготування їжі. Такі міні-ігри часто використовуються у навчальних цілях.

5) *Реакційні (Reflex-based)* - ці міні-ігри перевіряють швидкість реакції користувача. Вони можуть включати натискання кнопок у правильний момент або виконання швидких дій у відповідь на події.

Таблиця 1

Порівняльна характеристика міні-ігор

Тип міні-ігри	Основна мета	Тривалість	Складність
Аркадні	Швидка реакція	Коротка	Низька
Головоломки	Логічне мислення	Середня	Середня
Казуальні	Розвага	Коротка	Низька
Симуляційні	Моделювання процесів	Середня	Середня
Реакційні	Швидкість дій	Дуже коротка	Низька

Міні-ігри активно застосовуються у різних сферах: у відеоіграх - як додаткові активності для урізноманітнення геймплею; у мобільних додатках - для підвищення утримання користувачів; в освіті - як інструмент гейміфікації навчання; у маркетингу - для взаємодії з аудиторією.

Згідно з проведеним аналізом, ключовими характеристиками успішної гри, зокрема і міні-ігор, є зрозумілі правила, зворотний зв'язок та баланс складності. Встановлено, що міні-ігри є важливим елементом сучасних цифрових продуктів. Вони класифікуються за жанровими особливостями, серед яких найпоширенішими є аркадні, головоломки, казуальні, симуляційні та реакційні ігри.

Міні-ігри забезпечують підвищення залученості користувачів, спрощують сприйняття інформації та можуть ефективно використовуватися у різних сферах – від розваг до освіти. Подальші дослідження можуть бути спрямовані на аналіз впливу міні-ігор на поведінку користувачів та їх ефективність у навчальних середовищах.

Список використаних джерел:

1. The Relative Popularity of Video Game Genres in the Scientific Literature: A Bibliographic Survey / Jakub Swacha, 2025. URL: <https://www.mdpi.com/2414-4088/9/6/59>
2. Fundamentals of Game Design – 3rd edition / Ernest Adams, 2010. URL: https://www.academia.edu/81247135/Fundamentals_of_game_design

УДК 004.7

**ДУНАЙ Д.А., магістрант,
 НІКУЛІНА О.М., д.т.н., професор**
*Національний технічний університет «Харківський політехнічний
 інститут»*

ІНТЕГРАЦІЯ ФІЗИКО-ІНФОРМОВАНИХ НЕЙРОННИХ МЕРЕЖ В АРХІТЕКТУРУ ІОТ-СИСТЕМ У КОНТЕКСТІ СТРАТЕГІЇ GREEN IT

У сучасних умовах глобальної енергетичної нестабільності концепція Green IT стає фундаментом стратегічного розвитку інформаційних технологій на рівні підприємства. Ефективне управління енергоспоживанням вимагає розробки прецизійних цифрових двійників, здатних функціонувати у режимі реального часу. Проте класичні методи інтелектуального аналізу даних, що базуються виключно на статистичних моделях, демонструють низьку стійкість до інтермітуючої телеметрії та стохастичних завад, притаманних IoT-сенсорам. Це призводить до генерації фізично інконсистентних прогнозів, що нівелює їхню цінність для прийняття стратегічних рішень. Використання фізико-інформованих нейронних мереж (PINN) дозволяє змінити парадигму моделювання, інтегруючи фундаментальні диференціальні рівняння безпосередньо в обчислювальний граф архітектури.

Концептуалізація архітектурного підходу, в якому PINN-структура інтегрується як центральне аналітичне ядро IoT-інфраструктури підприємства, забезпечує системну імплементацію принципів сталого розвитку та детерміновану оптимізацію енергоефективності. Традиційні стратегії переважно оперують дезинтегрованими доменами, розглядаючи цифрову інфраструктуру та фізичні активи як гетерогенні сутності. Запропонований підхід базується на функціональній конвергенції цих доменів у межах єдиного когнітивного простору, де PINN-модель виконує роль інваріантного ядра, здійснюючи фізично обґрунтовану інтерпретацію сигналів IoT-периферії. На відміну від суто емпіричних моделей типу “black box”, PINN базується на фізично-регуляризованому функціоналі втрат, що враховує нев'язку нелінійних диференціальних операторів:

$$L_{total} = w_d \frac{1}{N} \sum_{i=1}^N |u_i - \hat{u}_i|^2 + w_p \frac{1}{N_f} \sum_{j=1}^{N_f} |F(\hat{u}_j)|^2$$

де оператор $F^{(ii)}$ представляє фундаментальні закони збереження (наприклад, рівняння теплопровідності або балансу потужностей), обчислені через механізм автоматичного диференціювання. У такій архітектурі IoT-сенсори виступають постачальниками динамічних граничних умов, тоді як PINN-ядро гарантує достовірність моделі у стаціонарних та перехідних режимах роботи системи. Це дозволяє досягти стабільного показника апроксимації ($R^2 \approx 0.99$) навіть за умов високого рівня адитивного шуму в каналах зв'язку.

Впровадження фізико-інформованого ядра безпосередньо реалізує стратегію Green IT: обмеження простору пошуку параметрів нейронної мережі фізичними константами призводить до прискорення збіжності градієнтного спуску, що радикально знижує енерговитрати на навчання моделі. Соціальний аспект дослідження реалізується через підвищення інтерпретованості системи: прогноз підтверджується фізичними закономірностями, що знімає проблему соціальної недовіри до автоматизації. Таким чином, інтеграція PINN як аналітичного центру трансформує архітектуру IoT на стратегічний актив екологічного менеджменту, мінімізуючи техногенне навантаження на довкілля. Подальші дослідження будуть спрямовані на аналіз стійкості моделі.

Список використаних джерел:

1. Raissi M., Perdikaris P., Karniadakis G. E. Physics-informed neural networks: A deep learning framework for solving forward and inverse problems. *Journal of Computational Physics*. 2019. Vol. 378. P. 686–707.
2. Hossain S. et al. Interpretable Physics-Informed Neural Networks for energy consumption prediction using IoT sensors. *Array*. 2025. Vol. 28. Art. 100552.
3. Almonier H. A. M. Physics-Informed Neural Networks for Predictive Modeling of Energy Dissipation Pathways in IoT-Integrated Smart Solar Grids. *Albahit Journal of Applied Sciences*. 2025. Vol. 4, No 1. P. 182–194.

УДК 004.7

*Немеровський А.О., здобувач,
Коротун О.В., к.пед.н., доцент
Державний університет «Житомирська політехніка»*

ОПИС ТЕХНОЛОГІЙ ЖАНРУ TOWER DEFENSE

Жанр tower defense зберігає актуальність завдяки поєднанню простої базової логіки та глибоких стратегічних рішень. Такі ігри легко адаптуються до мобільних, веб- і ПК-платформ, їхня механіка добре підходить для коротких сесій і повторного проходження. Тема є важливою через технологічну складність його реалізації. Для якісного tower defense потрібні сіткова карта, система маршрутів, хвильовий спавн ворогів, ефективне оновлення великої кількості об'єктів та зрозумілий інтерфейс.

Найпоширенішою основою рівнів є сіткова або вузлова карта. Гравець розміщує вежі на визначених клітинках, а вороги рухаються вздовж маршруту. Така структура спрощує перевірку колізій і робить розроблення рівнів передбачуваним. Для побудови маршруту застосовують алгоритми пошуку шляху, насамперед A*. У простих проєктах шлях фіксований, а у складніших – оновлюється після встановлення нових перешкод. Це дозволяє гнучко реагувати на дії гравця.

Ключову роль відіграє система хвиль, що задає темп гри, наростання складності та зміну типів супротивників. Хвильова логіка формує відчуття прогресу й дозволяє балансувати рівні без зміни основної карти. Для продуктивності важливим є object pooling – повторне використання снарядів, ворогів і візуальних ефектів. У жанрі, де одночасно активні десятки об'єктів, цей підхід зменшує навантаження на пам'ять і процесор.

Інтерфейс у tower defense повинен швидко передавати гравцеві критичну інформацію: вартість веж, радіус дії, шкоду, швидкість атаки, кількість ресурсів і напрямок руху ворогів. Тому підсвічування зон, індикатори та інформаційні панелі є не декоративними, а функціональними елементами.

У таблиці 1 представлено основні технології зазначеного жанру.

Tower defense – це жанр, у якому технологічна реалізація безпосередньо впливає на якість геймплею, де найбільш значущими компонентами є сіткова структура карти, алгоритми маршрутизації, хвильова система та оптимізаційні методи. Огляд показав, що успішний проєкт жанру будується на поєднанні простої візуальної моделі, передбачуваної логіки ворогів і зручного інтерфейсу. Саме завдяки цьому tower defense залишається ефективною моделлю для навчальних

та комерційних ігор. На практиці технології жанру використовують не лише в розважальних іграх, а й у навчальних симуляторах, де важливо наочно показати принципи планування ресурсів, оцінки ризиків і пріоритетів. Tower defense зручний як модель для експериментів із геймдизайном.

Таблиця 1

Основні технології жанру

Технологія	Функція	Ефект
Сіткова карта	Розміщення веж і маршрутів	Спрощує логіку рівня
A* / pathfinding	Побудова шляху ворогів	Гнучка реакція на перешкоди
Wave system	Керування хвилями супротивників	Формує темп і складність
Object pooling	Повторне використання об'єктів	Зменшує навантаження на систему

Платформна адаптація залежить від вибраних рішень. Для мобільних версій доцільно спрощувати візуальні ефекти та частоту оновлення, для ПК-версій можна збільшувати кількість ворогів, різноманітність веж і глибину балансування.

Отже, технологічний стек tower defense можна розглядати як компактну модель сучасної ігрової архітектури: карта, шлях, хвилі, інтерфейс і оптимізація працюють як єдина система.

Найтипівішими проблемами жанру є надмірна однотипність рівнів, слабка варіативність ворогів і перевантаження інтерфейсу великою кількістю параметрів. Через це важливо поєднувати зрозумілу схему гри з поступовим ускладненням механік.

Подальше вдосконалення tower defense пов'язане із застосуванням процедурної генерації, адаптивного балансу, розумнішого AI та гнучкішої системи апгрейдів. Саме такі рішення дозволяють підтримувати інтерес гравця без втрати доступності.

Список використаних джерел:

1. Salen K., Zimmerman E. *Rules of Play: Game Design Fundamentals*. — Cambridge, MA : MIT Press, 2004. — 672 p.
2. Unity Technologies. *Unity Manual: Object Pooling and Pathfinding* [Електронний ресурс]. — Режим доступу: <https://docs.unity3d.com>

УДК 004.9

*Базалей В.А., здобувач**Харківський національний університет радіоелектроніки*

ВИКОРИСТАННЯ ПРОСТОРОВО-СТАТИСТИЧНОГО ПІДХОДУ ДЛЯ ОЦІНКИ ПАСАЖИРОПОТОКУ ПІД ЧАС АВТОБУСНИХ ПЕРЕВЕЗЕНЬ

У сучасному світі сфера автобусних перевезень відіграє важливу роль у забезпеченні мобільності населення та розвитку міст. Зі зростанням пасажиропотоку й динамічними змінами транспортного попиту актуальним стає створення інформаційних систем для його аналізу. Такі системи дозволяють автоматизувати обробку даних, отримувати статистику пасажиропотоку та підтримувати прийняття управлінських рішень.

Існуючі підходи до аналізу попиту на автобусні перевезення базуються або на статистичних моделях окремих зупинок, або на прогнозуванні доходів від продажу квитків. У роботі [1] запропоновано просторово-статистичний підхід до оцінки пасажиропотоку з використанням GIS-даних, який враховує відстані між зупинками та характеристики території (приклад на рисунку 1).

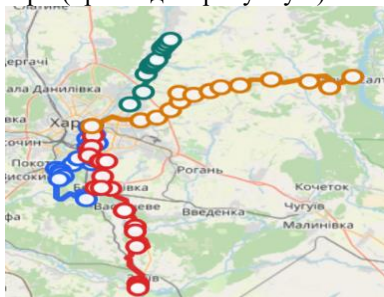


Рис.1. Фрагмент використання GIS-даних

У дослідженні [2] показано, що методи машинного навчання та аналізу часових рядів дозволяють прогнозувати тарифні надходження транспорту. Однак результати таких досліджень часто не інтегруються у єдині інформаційні системи, що ускладнює їх практичне використання.

Метою роботи є створення інформаційної системи для управління та аналізу попиту на автобусні перевезення, яка об'єднує сховище даних та веб-застосунок. Система дозволяє збирати, обробляти дані про продаж квитків, маршрути, зупинки та розклад руху, формуючи єдине інформаційне середовище.

У рамках роботи виконано аналіз структури даних, визначено основні атрибути попиту (час поїздки, маршрут, зупинки, тип квитка, канал продажу) та спроектовано багатовимірну модель даних. На її основі реалізовано сховище даних, оптимізоване для аналітичних запитів, а також веб-інтерфейс для фільтрації, агрегації, візуалізації та редагування інформації.

Побудова сховища даних передбачає використання ETL-процесів для очищення, перевірки та уніфікації даних із різних джерел. Дані агрегуються до рівнів, необхідних для аналізу (доба, рейс, зупинка), що забезпечує можливість оцінки пасажиропотоку та завантаженості маршрутів. Такий підхід відповідає сучасним принципам побудови аналітичних систем у транспортній галузі.

Розроблений веб-застосунок надає користувачу інструменти для перегляду статистики перевезень, завантаженості маршрутів, оцінки попиту на окремих зупинках та порівняння показників різних маршрутів і рейсів. Дані відображаються у вигляді таблиць і графіків, що спрощує їх інтерпретацію.

Запропонована система не виконує автоматичних прогнозів, а забезпечує зручне подання та структурування даних для подальшого використання логістом. На основі отриманої інформації можна оптимізувати розклад руху, коригувати маршрутну мережу та приймати обґрунтовані управлінські рішення.

Отже, поєднання сховища даних та веб-застосунку є ефективним підходом до створення інформаційних систем відображення та аналізу попиту на автобусні перевезення. Розроблена система забезпечує багатовимірне відображення даних та створює основу для подальшого розвитку.

Список використаних джерел:

1. Montero-Lamas Y., Fernández-Casal R., Varela-García F.-A. A spatial statistical approach to estimate bus stop demand using GIS-processed data. *Journal of Transport Geography*, 2024. URL: <https://www.sciencedirect.com/science/article/pii/S0966692324001157> (дата звернення: 23.01.2025).

2. Krembsler J., Spiegelberg S., Hasenfelder R. Fare revenue forecast in public transport: A comparative case study. *Research in Transportation Economics*, 2024. URL: <https://www.sciencedirect.com/science/article/pii/S0739885924000404> (дата звернення: 23.01.2025).

УДК 004.04: 004.02

**Жданюк М.Р., магістрант,
Марчук Г.В., ст. викл.**

Державний університет «Житомирська політехніка»

АДАПТИВНА ПСЕВДОВИПАДКОВА ГЕНЕРАЦІЯ У ІГРАХ ЯК ІНСТРУМЕНТ КЕРУВАННЯ ІГРОВИМ ДОСВІДОМ

У сучасних ігрових застосунках генератори випадкових значень (Random Number Generator, RNG) застосовуються від процедурної генерації рівнів до визначення розкиду пострілів. Оскільки досягнення справжньої фізичної випадковості в програмних системах є технічно нетривіальним завданням, у переважній більшості ігор використовуються псевдовипадкові генератори (Pseudo-Random Number Generator, PRNG) [1].

Метою дослідження є порівняльний аналіз існуючих методів контролю PRNG в іграх та обґрунтування доцільності адаптивного підходу до генерації випадкових подій у іграх жанру Roguelike. Об'єктом дослідження є Roguelike-ігри як середовище активного використання стохастичних механік. Предметом дослідження є методи псевдовипадкової генерації даних та їх вплив на балансування ігрового процесу і задоволеність гравців.

PRNG базується на початковому значенні (seed), що гарантує відтворюваність для тестів, але робить систему передбачуваною. Навпаки, фізичні генератори (True Random Number Generator, TRNG) абсолютно випадкові, проте некеровані, що заважає реалізації ігрової «справедливості». Тому на практиці обидва типи коригуються спеціальними правилами розподілу (табл. 1).

Таблиця 1

Основні методи контролю RNG

Метод	Принцип	Приклад реалізації
Зважена випадковість	Кожен варіант має вагу, що визначає частоту появи.	The Binding of Isaac (4 рівні рідкісності предметів з різними вагами у пулі)
Випадковість, що базується на правилах	Є чіткий набір правил, які визначають оптимальний результат.	Hades (взаємовиключні благословення богів; шанс повторного благословення зростає після пропуску).
Випадковість, що базується на станах	Розподіл коригується залежно від поточного стану гравця.	Left 4 Dead - AI Director (динамічна поява ворогів і ресурсів на основі показників команди).

Roguelike [2] обрано як основне середовище дослідження через поєднання кількох властивостей таких, як перманентний програвш, повторні проходження, залежність результату від сформованої комбінації покращень (білду) та щільний зв'язок ігрового процесу з RNG. Жанр охоплює різні піджанри: карткові ігри (Slay the Spire), слешери (Hades), метроїдванії (Dead Cells), двостічні шутери (The Binding of Isaac). Саме ця різноманітність унаочнює універсальність проблеми балансування стохастики.

Жанрова дилема полягає у пріоритеті суб'єктивного відчуття справедливості над математичною випадковістю. Баланс між нудьгою та фрустрацією зазвичай підтримується статичними методами (табл. 1), проте вони ігнорують індивідуальний стиль гри та поведінку користувача.

Адаптивний RNG розвиває ідею станової випадковості, впроваджуючи безперервний аналіз ігрової сесії для динамічного коригування генерації. Система реагує на дії гравця за принципами:

- систематичні поразки від конкретного ворога → зниження вірогідності його появи (без повного вилючення з пулу) з поступовим відновленням до базового значення;
- надлишкова частота певного предмета → тимчасове зменшення його ваги у пулі;
- висока майстерність гравця → поступове збільшення частоти появи складних ворогів;
- блокування прогресу → підвищення вірогідності генерації «підказуючих» предметів і маршрутів.

На відміну від стандартних підходів, ця адаптація непомітна та персоналізована: гравці з різним досвідом бачать різний розподіл подій навіть за однакових налаштувань. Це автоматично балансує складність, усуваючи потребу в ручному коригуванні параметрів.

Аналіз підтверджує, що традиційні методи RNG (табл. 1) ефективні лише в статистиці. Адаптивний RNG, що базується на поведінці гравця, є перспективним для підвищення лояльності аудиторії Roguelike. Наступним кроком є формалізація архітектури системи та її перевірка на практичному прототипі.

Список використаних джерел:

1. Лайтарук І.Ф. Дослідження процедурної генерації світу на основі розробки комп'ютерної гри з аналізом поведінки гравця. MS thesis. *Волинський національний університет імені Лесі Українки*, 2025.
2. Cartlidge J. Genre, Prototype Theory and the Berlin Interpretation of Roguelikes. *Game Studies*. 2024, 24 (3).

УДК 004.7

Білокур С.Р., здобувач*Національний університет «Київський авіаційний інститут»*

ХМАРНІ ТЕХНОЛОГІЇ У ПОБУДОВІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Зростання обсягів корпоративних даних є однією з ключових проблем сучасного управління підприємством. Хмарні обчислення визначаються як модель надання зручного мережевого доступу до спільного пулу конфігурованих обчислювальних ресурсів [1]. Традиційні КІС, побудовані на локальній інфраструктурі, не здатні ефективно впоратися з нерівномірними і постійно зростаючими потоками даних: розширення сховищ потребує часу і значних витрат, а пікові навантаження – наприклад, під час закриття звітного кварталу – паралізують роботу системи. Дослідження бізнес-перспективи хмарних технологій підтверджує, що перехід до хмарної моделі суттєво змінює структуру витрат підприємства: капітальні вкладення в обладнання замінюються операційними витратами за фактичне споживання [2]. Саме нездатність локальної інфраструктури масштабуватися під реальні потреби бізнесу є тією науково-практичною проблемою, вирішення якої досліджується у цій роботі.

Хмарні платформи забезпечують динамічне масштабування ресурсів і балансування навантаження, використовуючи контейнери та оркестраційні системи (Kubernetes). Це дозволяє КІС адаптуватися до пікових навантажень і працювати без простоїв [3]. Окрім масштабованості, хмарна архітектура усуває іншу хронічну проблему КІС – розрізненість даних. У традиційних системах кожен підрозділ вів свої записи у власному форматі, в результаті дані дублювались і були важко співставимі [4]. Централізоване хмарне сховище реалізується через єдину базу даних або Data Lake, доступну всім підрозділам через API та веб-інтерфейси. Дані зберігаються у структурованому та стандартизованому форматі, а механізми синхронізації та транзакцій забезпечують їхню актуальність у режимі реального часу.

Питання безпеки та доступу у хмарних КІС вирішується на рівні провайдера: дані шифруються при зберіганні та передачі (AES-256, TLS 1.2/1.3), застосовується багатофакторна автентифікація (MFA) та SSO, автоматично виявляються підозрілі активності, а резервне копіювання виконується регулярно [4]. Підприємство зберігає контроль над доступом через RBAC, а сервіси можна ізолювати за допомогою контейнерів і оркестраційних платформ (Kubernetes).

Залежно від даних підприємство обирає одну з моделей хмари. IaaS надає контроль над віртуальними машинами, мережами та сховищами (Block/Object Storage) із масштабуванням та автоматизацією розгортання (Terraform, CloudFormation). PaaS оптимальна для розробки корпоративних застосунків із CI/CD та інтеграцією з базами й аналітикою (Azure App Service, Google App Engine). SaaS дозволяє швидко використовувати готові програми через веб/мобільний інтерфейс із масштабуванням і API [2, 4]. Для чутливих даних актуальна гібридна модель, що поєднує приватну хмару для конфіденційної інформації та публічну для загальних процесів, з безпечним підключенням (VPN/Direct Connect) і балансуванням навантаження через Azure Arc, AWS Outposts або Google Anthos.

Таким чином, впровадження сучасних хмарних рішень сприяє підвищенню конкурентоспроможності підприємства, покращенню якості аналітики та забезпеченню надійності зберігання інформації, що є ключовими факторами успішного функціонування бізнесу в умовах цифрової трансформації. Наприклад Unilever після переходу на SAP S/4HANA Cloud скоротила час підготовки фінансової звітності з 5 днів до 2 годин, а кількість помилок у даних впала на 60% [3]. Крім того, хмарні рішення забезпечують швидку обробку великих обсягів даних у режимі реального часу, автоматизацію ключових бізнес-процесів та гнучке масштабування. Отже, Cloud Computing стає не лише інструментом оптимізації IT, а й стратегічним ресурсом для розвитку сучасного бізнесу.

Список використаних джерел:

1. Ware B., Mercy R. Cloud Computing 2025 and Beyond: Trends, Obstacles, and New Possibilities. ResearchGate. 2025. DOI: 10.20944/preprints202503.0724.v1. URL: https://www.researchgate.net/publication/389790981_Cloud_Computing_2025_and_Beyond_Trends_Obstacle_s_and_New_Possibilities
2. Sydor K., Shcherbyna Y. Cloud Computing Technology: Architecture, Models and Information Security Aspects. 2025. Vol. 18, No 2. P. 184–191. DOI: 10.23939/sisn2025.18.2.184.
3. Unilever and SAP S/4HANA Cloud: digital transformation success story/SAPSE.2022. URL: <https://vods.dm.ux.sap.com/s4hana/pdfs/unilever-improving-information-access-and-streamlining-business-processes-with-the-sap-hana-platform-pdf.pdf> (дата звернення: 24.03.2026).
4. Tsai Y.-C., Singh S., Sanchez R. R., Monroe G. T. Cloud Computing and Enterprise Digital Transformation. Research Paper. 2025. DOI: 10.13140/RG.2.2.17677.04329.

УДК 004.414

*Боданов Є.С., здобувач,
Глазок О.М., к.т.н., доцент
Національний університет «Київський авіаційний інститут»*

МАСШТАБУВАННЯ В KUBERNETES НА ОСНОВІ СПЕЦІАЛІЗОВАНОГО ІНТЕЛЕКТУАЛЬНОГО ОПЕРАТОРА

Сучасні багатокористувацькі платформи програмного забезпечення, що надають послуги за моделлю SaaS, стикаються з рядом викликів ефективності. Метою таких платформ є забезпечити неперервні, високопродуктивні послуги для різних категорій клієнтів, одночасно зберігаючи операційну ефективність та масштабованість. Зокрема, одна з проблем пов'язана з обмеженнями стандартного автоматичного масштабування Kubernetes, оскільки воно спирається на реактивні показники інфраструктури (CPU/RAM), яких недостатньо для суворого дотримання кількісних цілей щодо рівня обслуговування (SLO – Service Level Objective). Ціль рівня обслуговування (SLO) у Kubernetes – це вимірювана ціль для певного аспекту продуктивності сервісу, яку команда зобов'язується досягти. Прикладами можуть бути величина затримки, доступність, рівень надійності або коефіцієнт помилок. Типовий робочий процес включає вимірювання метрики за допомогою Prometheus, OpenTelemetry або іншого стеку моніторингу та порівняння метрики з визначеним SLO. Якщо SLO порушується, система запускає сповіщення, коригує ресурси або ініціює інше відповідне реагування на інциденти.

Автоматичне масштабування в Kubernetes було активною темою досліджень в останні роки. Існуючі підходи можна розділити на три основні категорії: розширення власних механізмів Kubernetes, навчання з підкріпленням та методи на основі часових рядів або машинного навчання.

У роботі [1] представлено фреймворк, який виконує автоматичне масштабування на основі затримки, довжини черги та використання ресурсів. Основним обмеженням цього підходу є його зосередженість на кожному робочому навантаженні: він оптимізує кожну послугу окремо та не враховує конкуренцію між орендарями різних рівнів за умови дефіциту ресурсів у кластері.

У роботі [2] автори пропонують методологію балансування затримки SLO та вартості інфраструктури. Автори описують Custom Pod Autoscaler, який обчислює бажану кількість реплік, використовуючи зважені коефіцієнти. Подібно до попередньої роботи, цей підхід виконує оптимізацію для кожного розгортання, ігноруючи

багатокористувацьку оренду та необхідність глобальної пріоритезації трафіку за умови насичення кластера.

У статті [3] пропонується багатокористувацька SaaS-архітектура, покращена на основі штучного інтелекту, яка забезпечує інтелектуальну ізоляцію ресурсів за допомогою динамічного масштабування. Обмеження включають залежність від точних прогнозів попиту, додаткову складність компонентів штучного інтелекту та оцінку, обмежену певними робочими навантаженнями та хмарними середовищами.

Стандартні засоби автоматичного масштабування ігнорують бюджетні обмеження та пріоритети клієнтів. Це призводить до затримки масштабування, порушень SLO та неконтрольованих витрат на інфраструктуру. У цій роботі було розроблено та впроваджено спеціалізований оператор Kubernetes для заміни стандартних механізмів масштабування інтелектуальним конвеєром прийняття рішень. Рішення інтегрує бізнес-контекст безпосередньо в цикл управління через спеціальне визначення ресурсів (CRD). Було впроваджено інтелектуальні механізми випередження та скидання навантаження для захисту високопріоритетних рівнів за умови дефіциту ресурсів, а також стратегію розміщення подів з урахуванням витрат для оптимізації витрат на інфраструктуру. Експеримент показує, що розроблена система зменшує пікову затримку приблизно в 3,8 раза (з 17,07 с до 4,5 с) порівняно зі стандартним базовим рівнем HPA. За критичної нестачі ресурсів кластера оператор надає пріоритет продуктивності вищого рівня за рахунок нижчих рівнів, що дозволяє провести контрольовану деградацію замість колапсу продуктивності всього кластера.

Список використаних джерел:

1. An SLO driven and cost-aware autoscaling framework for Kubernetes. / V. Punniyamoorthy, B. Kumar, S. Saha, L. Butra, M. Palanigounder, A. K. Agarwal, and K. Kannan. //arXiv preprint: arXiv:2512.23415, December 2025. URL: <https://arxiv.org/pdf/2512.23415>.
2. Marchese A., Tomarchio O. SLO and Cost-Driven Container Autoscaling on Kubernetes Clusters. /15th Int. Conf. on Cloud Computing and Services Science: proceedings. 2025. Pp. 72-79. DOI: 10.5220/0013482100003950.
3. Ravi Chandra Thota. Intelligent Orchestration for Performance-Tuned Multi-Tenant Cloud Systems /Int. J. of Scientific Research in Engineering and Management. December 2025. Vol. 09(12). Pp. 1-9. DOI: 10.55041/IJSREM55464.

УДК 004.75:004.415

*Гаврилюк А.Р., студентка**Державний університет інформаційно-комунікаційних технологій*

ОЦІНКА ПРОДУКТИВНОСТІ РОЗПОДІЛЕНИХ CLOUD-EDGE АРХІТЕКТУР

Стрімкий розвиток цифрових технологій, Інтернету речей та інтелектуальних сервісів спричиняє значне зростання обсягів даних і підвищення вимог до швидкості їх обробки. Традиційні централізовані хмарні системи не завжди здатні забезпечити необхідні показники затримки, пропускну здатності та масштабованості, що є особливо критичним для додатків реального часу. У зв'язку з цим активно розвивається концепція розподілених обчислювальних середовищ, які поєднують можливості хмарних дата-центрів із ресурсами периферійних вузлів мережі. Такі системи формують cloud-edge континуум, що дозволяє розподіляти обчислювальні задачі між різними рівнями інфраструктури залежно від вимог до продуктивності та доступних ресурсів [3].

Розподілені cloud-edge архітектури застосовуються в інтелектуальних транспортних системах, промисловому Інтернеті речей, автономних системах та мультимедійних сервісах. Ефективність їх функціонування значною мірою залежить від механізмів розподілу задач, управління ресурсами та здатності системи адаптуватися до змін навантаження. Тому актуальним завданням є дослідження методів оцінки продуктивності таких систем та визначення факторів, що впливають на ефективність їх роботи [4]. Системи є багаторівневою обчислювальною інфраструктурою, у якій ресурси розташовані як у хмарних дата-центрах, так і на периферійних вузлах мережі. Така архітектура дозволяє виконувати попередню обробку даних ближче до джерела їх генерації, що зменшує затримку передачі та навантаження на центральні сервери. Основними показниками продуктивності таких систем є час відгуку, затримка обробки запитів, пропускна здатність та ефективність використання ресурсів.

Ефективність cloud-edge систем значною мірою залежить від механізмів планування задач. Сучасні алгоритми планування враховують обчислювальні ресурси вузлів, мережеві затримки та пріоритетність сервісів, що дозволяє оптимізувати використання ресурсів і мінімізувати час виконання задач [3]. Перспективним напрямом є застосування методів штучного інтелекту, зокрема алгоритмів глибинного підкріплювального навчання, для адаптивного розподілу задач між вузлами мережі [4]. Використання периферійних

обчислень дозволяє зменшити затримку передачі даних і підвищити стабільність роботи сервісів у порівнянні з централізованими моделями обчислень [2]. Важливими характеристиками cloud-edge інфраструктур також є масштабованість та відмовостійкість, які забезпечуються механізмами динамічного розподілу ресурсів і автоматичного виявлення збоїв [1].

Розподілені cloud-edge архітектури є перспективним напрямом розвитку сучасних інформаційних систем, оскільки поєднують переваги хмарних і периферійних обчислень. Ефективність їх функціонування залежить від оптимального планування задач, ефективного використання ресурсів та мінімізації мережових затримок. Застосування інтелектуальних алгоритмів управління ресурсами дозволяє підвищити продуктивність розподілених систем і забезпечити їх адаптивність до змін навантаження. Подальші дослідження можуть бути спрямовані на розроблення нових методів оптимізації розподілу задач і вдосконалення алгоритмів управління ресурсами у cloud-edge середовищах.

Список використаних джерел:

1. Enhancing performance of machine learning tasks on edge-cloud infrastructures: a cross-domain internet of things based framework / O. Almurshed et al. Future generation computer systems. 2024. P. 107696. URL: <https://doi.org/10.1016/j.future.2024.107696>.
2. Mahjoubi A., Ramaswamy A., Grinnemo K.-J. Deadline-Aware service scheduling via multi-head MARL in device–edge–cloud environments. Computer networks. 2026. P. 112019. URL: <https://doi.org/10.1016/j.comnet.2026.112019>.
3. Performance of distributed multiparty online gaming over edge computing platforms / D. Oliaro et al. Computer communications. 2025. P. 108378. URL: <https://doi.org/10.1016/j.comcom.2025.108378>.
4. Pulse: Multi-objective scheduling of service-based applications in multi-cluster cloud–edge–IoT infrastructures / M. Etheredge et al. Journal of network and computer applications. 2026. Vol. 248. P. 104439. URL: <https://doi.org/10.1016/j.jnca.2026.104439>.

УДК 004.89:656.13

Шевчук О.О., студент

Гаврилюк А.Р., студентка

Державний університет інформаційно-комунікаційних технологій

МЕТОДИ ОПТИМІЗАЦІЇ МАРШРУТІВ ДОСТАВКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЛОГІСТИКИ

Стрімкий розвиток електронної комерції, цифрових платформ і транспортно-логістичних сервісів спричиняє зростання обсягів перевезень та підвищує вимоги до ефективності управління логістичними процесами. У цих умовах особливого значення набуває оптимізація маршрутів доставки, яка дозволяє скоротити транспортні витрати, зменшити час перевезень і підвищити ефективність використання транспортних ресурсів. Інформаційні системи логістики відіграють важливу роль у підтримці прийняття управлінських рішень щодо планування перевезень, використовуючи алгоритмічні методи оптимізації для визначення раціональних маршрутів руху транспортних засобів.

Задача оптимізації маршрутів доставки належить до класу складних комбінаторних задач і розглядається як узагальнення задачі маршрутизації транспортних засобів (Vehicle Routing Problem). Для її розв'язання застосовуються різні алгоритмічні підходи, серед яких важливе місце займають метаевристичні методи оптимізації [1]. Такі алгоритми дозволяють ефективно здійснювати пошук рішень у складних багатопараметричних задачах і знаходити близькі до оптимальних маршрути перевезень.

Перспективним напрямом оптимізації логістичних процесів є використання методів штучного інтелекту, зокрема штучних нейронних мереж [4], які дозволяють аналізувати значні обсяги даних та враховувати динамічні фактори транспортної системи під час планування маршрутів доставки.

Поширеним підходом до розв'язання задач маршрутизації є використання еволюційних алгоритмів. Генетичні алгоритми [5] забезпечують пошук оптимальних маршрутів шляхом ітеративного вдосконалення множини можливих рішень та ефективно застосовуються в умовах великої кількості обмежень.

У задачах оптимізації транспортних маршрутів також широко застосовуються алгоритми ройового інтелекту, зокрема алгоритм мурашиної колонії [3]. При моделюванні реальних логістичних процесів додатково враховуються часові інтервали доставки, послідовність завантаження та розвантаження транспортних засобів, що

реалізується у моделях маршрутизації типу Pickup and Delivery Problem with Time Windows [2].

Сучасні інформаційні системи логістики використовують широкий спектр алгоритмічних підходів до оптимізації маршрутів доставки. Найбільш перспективними серед них є метаевристичні алгоритми, еволюційні методи та алгоритми штучного інтелекту, що дозволяють підвищити ефективність планування логістичних операцій. Подальші дослідження доцільно спрямувати на інтеграцію алгоритмів оптимізації з програмними системами управління логістикою та використання інтелектуальних методів аналізу даних для підтримки прийняття управлінських рішень.

Список використаних джерел:

1. Gu Y. Logistics route optimization based on improved shark optimization algorithm. *Procedia computer science*. 2025. Vol. 262. P. 1322–1328. URL: <https://doi.org/10.1016/j.procs.2025.05.177>.
2. Hu L. Logistics vehicle optimization scheduling based on multi constraint PDPTW algorithm. *Procedia computer science*. 2025. Vol. 262. P. 438–447. URL: <https://doi.org/10.1016/j.procs.2025.05.072>.
3. Wang H. Dynamic path optimization of cold chain logistics based on improved ant colony algorithm from a low-carbon perspective. *Sustainable operations and computers*. 2025. URL: <https://doi.org/10.1016/j.susoc.2025.10.001>.
4. Wang L., Han Y., Xu X. Logistics distribution transportation vehicle route decision-making based on artificial neural network algorithm. *ICT express*. 2025. URL: <https://doi.org/10.1016/j.ict.2025.11.012>.
5. Yuan H., Yang X. A design method for agricultural product logistics cold chain distribution routes based on a genetic algorithm. *Green technologies and sustainability*. 2026. P. 100335. URL: <https://doi.org/10.1016/j.grets.2026.100335>.

УДК 004.738.5

Бондар В.С., здобувач

Усата О.Ю. к.пед.н., доцент

Житомирський державний університет імені Івана Франка

ЗАСТОСУВАННЯ ФРЕЙМВОРКУ NEXT.JS ДЛЯ РОЗРОБКИ СИСТЕМИ РЕКОМЕНДАЦІЙ ВІДЕОКОНТЕНТУ

Цифрова трансформація впливає на усі напрями життєдіяльності суспільства, у тому числі й на збільшення обсягу відеоконтенту. Через стрімке інформаційне перевантаження користувачів, ефективна машинна фільтрація контенту стає ключовим фактором утримання аудиторії [1]. Саме тому системи рекомендацій стали важливим ядром будь-якої успішної медіаплатформи. Традиційні алгоритми часто спираються або на історію взаємодій користувача, або на характеристики контенту. Проте, використання лише одного з цих методів призводить до помилок, таких як проблема «холодного старту» для нових користувачів. Вирішенням цієї проблеми є впровадження гібридних моделей персоналізації, які органічно поєднують обидва підходи [2]. Проте інтеграція складних математичних моделей у вебсередовище вимагає використання передових технологій. Для забезпечення швидкої роботи платформи та безперебійного рендерингу рекомендацій вибір архітектури відіграє вирішальну роль.

Зважаючи на безперервну еволюцію цифрових медіа, створення конкурентоспроможного продукту вимагає адаптації передових технологічних рішень, якими вже користуються світові лідери індустрії. Відповідно, головним вектором цієї роботи є імплементація гібридної системи рекомендацій за допомогою фреймворку Next.js. Такий підхід дозволяє перейняти найкращі практики проектування архітектури та наблизити швидкодію вебплатформи до актуальних стандартів.

Архітектура продукту базується на інтеграції великих зовнішніх баз даних медіаконтенту та обробці сесій авторизованих користувачів. Гібридна модель рекомендацій формується за рахунок поєднання структурних метрик відео (жанри, хронометраж, роки випуску) із механізмами колаборативної фільтрації, що спираються на збережену історію взаємодій. Такий підхід дозволяє динамічно генерувати персоналізовані вибірки контенту, уникаючи при цьому необхідності ресурсомісткого аналізу описів чи застосування важких нейромереж [3].

Проте, математичний розрахунок релевантної вибірки – це лише бекенд-складова завдання. Критичним інженерним викликом є оптимізація процесу рендерингу та доставки цих даних на пристрій користувача. Класичні вебзастосунки типу Single Page Application (SPA), побудовані виключно на базовій бібліотеці React.js,

передбачають клієнтський рендеринг. У такій архітектурі браузер спочатку отримує практично порожній HTML-документ і змушений завантажувати об'ємний JavaScript-бандл. Лише після ініціалізації скриптів клієнт робить асинхронні запити до API для отримання масиву рекомендацій. Це створює так званий ефект «водоспаду» мережових запитів, що призводить до погіршення досвіду взаємодії з платформою.

Для нівелювання описаних проблем у розробці застосовується фреймворк Next.js. Як показує практика використання React у поєднанні з можливостями Next.js дозволяє зменшити час завантаження сторінок, що є критичним для застосунків із великим обсягом медіаданих [4].

Завдяки підтримці рендерингу на стороні сервера, коли користувач відкриває вебплатформу, сервер самостійно звертається до гібридної моделі, отримує персоналізований список рекомендацій та генерує HTML-сторінку. Користувач миттєво бачить контент, що покращує показник Time-to-First-Byte та загальну продуктивність ресурсу.

Крім того, фреймворк Next.js має вбудовану систему маршрутизації. Це дозволяє розмістити логіку обробки даних користувачів та маршрутизацію запитів до алгоритмів персоналізації в межах одного фулстек-застосунку. Відпадає необхідність підтримувати окремий бекенд-сервер для операцій передачі даних, що робить архітектуру платформи більш лаконічною для подальшого масштабування [5].

Розробка конкурентоспроможної відеоплатформи є складним технічним завданням. Застосування гібридної моделі персоналізації підвищує релевантність рекомендацій, а використання Next.js забезпечує ефективну технічну реалізацію. Поєднання серверного рендерингу (SSR), гнучкої архітектури API та високої швидкодії робить Next.js оптимальним інструментом для створення інформаційних систем, що працюють з мультимедійними даними у реальному часі.

Список використаних джерел:

1. Литвин В. В. Технології розроблення інтелектуальних систем : навч. посіб. Львів : Видавництво Львівської політехніки, 2016. 308 с.
2. Burke R. Hybrid Recommender Systems: Survey and Experiments. User Modeling and User-Adapted Interaction. 2002.Vol.12, No4. P.331–370.
3. Adomavicius G., Tuzhilin A. Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions IEEE Transactions on Knowledge and Data Engineering. 2005. Vol. 17, No 6. P. 734–749.
4. React – A JavaScript library for building user interfaces. Official React Documentation. URL: <https://react.dev/> (дата звернення: 20.03.2026).
5. API Routes. Next.js. URL: <https://nextjs.org/docs/pages/building-your-application/routing/api-routes> (дата звернення: 20.03.2026)

УДК 004.9

Богачкін Ф.О., магістрант

Державний університет інформаційно-комунікаційних технологій

РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ МОНІТОРИНГУ ЗАЙНЯТОСТІ СТОЛІВ НА ОСНОВІ ІОТ ТА ВІДЕОАНАЛІТИКИ

Постановка завдання

Ефективне управління простором закладу та оптимізація використання посадкових місць є важливими чинниками підвищення якості обслуговування клієнтів і збільшення прибутковості у ресторанному бізнесі. Однією з поширених проблем є відсутність оперативної інформації про зайнятість столів, що ускладнює роботу персоналу, особливо у періоди високого навантаження. Традиційні методи контролю, які ґрунтуються на спостереженні персоналу або ручному веденні обліку, можуть бути неточними та потребують значних часових витрат. У зв'язку з цим актуальним є використання інтелектуальних інформаційних систем, що поєднують технології Інтернету речей (ІоТ) та відеоаналітики для автоматичного моніторингу стану столів у режимі реального часу.

Мета дослідження

Дослідити можливості створення інтелектуальної системи моніторингу зайнятості столів у ресторані на основі інтеграції технологій ІоТ та відеоаналітики, а також визначити її потенціал для підвищення ефективності управління обслуговуванням клієнтів.

Результат дослідження

Інтелектуальні системи моніторингу зайнятості столів базуються на використанні сенсорних пристроїв та алгоритмів відеоаналізу, що дозволяють автоматично визначати наявність відвідувачів у зонах ресторану. Датчики присутності, руху або тиску фіксують факт зайняття столу, а відеоаналітика забезпечує перевірку та уточнення отриманих даних.

Ключовим елементом архітектури є периферійний обчислювальний пристрій Raspberry Pi, який виконує функції edge-вузла: обробку відеопотоку та збір даних із сенсорів через GPIO. Такий підхід реалізує концепцію edge computing, забезпечуючи обробку даних безпосередньо біля джерела. Загальна архітектура системи представлена на рис. 1.

Використання Raspberry Pi зменшує затримки, знижує навантаження на сервер і підвищує автономність системи. Оброблені дані передаються на сервер або у веб-додаток для подальшого аналізу,

збереження та візуалізації. Архітектура є масштабованою та дозволяє розширювати систему новими вузлами.



Рис. 1. Архітектура системи

Висновки та перспективи

Розробка інтелектуальної системи моніторингу зайнятості столів на основі IoT та відеоаналітики підвищує ефективність управління рестораном. Автоматичний збір і аналіз даних дозволяє отримувати актуальну інформацію про стан посадкових місць, оптимізувати роботу персоналу та покращити обслуговування клієнтів.

Подальший розвиток таких систем пов'язаний із удосконаленням алгоритмів відеоаналізу, розширенням можливостей інтеграції з іншими інформаційними системами закладу та використанням сучасних методів машинного навчання для прогнозування завантаженості ресторану. Це відкриває перспективи створення комплексних інтелектуальних платформ управління ресторанною інфраструктурою.

Список використаних джерел:

1. Asif Khan M., Menouar H., Hamila R. Revisiting crowd counting: state-of-the-art, trends, and future perspectives. Journal of image and vision computing. 2022. URL: <https://doi.org/10.48550/arXiv.2209.07271>.
2. A recurrent neural network architecture for accurate people counting / L. Massa et al. Computer vision and pattern recognition. 2020. URL: <https://doi.org/10.48550/arXiv.2004.09672>.
3. Benchmark data and method for real-time people counting in cluttered scenes using depth sensors / S. Sun et al. Journal of latex class files. 2018. Vol. 14, no. 8. URL: <https://doi.org/10.48550/arXiv.1804.04339>.

УДК 004.8:004.932:616-073.75

*Прокоп'єв Д.М., магістрант,
Тітов С.В., к.т.н., доцент*

Харківський національний університет радіоелектроніки

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДЛЯ ДІАГНОСТИКИ ТА МОНІТОРИНГУ СТАНУ ПАЦІЄНТА

Сучасна медицина характеризується стрімким зростанням обсягів даних, що потребують оперативного аналізу для прийняття життєво важливих рішень. Традиційні методи діагностики, хоча і є надійними, часто залежать від суб'єктивного фактору та кваліфікації лікаря, що створює ризики людської помилки. Впровадження інтелектуальних систем, заснованих на алгоритмах машинного навчання та нейронних мережах, дозволяє автоматизувати процес моніторингу та підвищити точність виявлення патологій на ранніх стадіях.

Мета роботи – розробка та дослідження компонентів інтелектуальної системи, що інтегрує методи аналізу фізіологічних сигналів (ЕКГ), візуальних даних та клінічних параметрів для комплексної діагностики та прогнозування стану пацієнта.

Запропонована система має модульну структуру, що забезпечує гнучкість та можливість повторного використання компонентів:

- Модуль збору та попередньої обробки даних: виконує агрегацію даних із різних джерел (архівів ЕКГ, результати аналізів, зображення) та їх нормалізацію для подальшого аналізу.

- Діагностичний модуль: базується на ансамблях моделей машинного навчання (Random Forest, Gradient Boosting) та нейронних мережах для ідентифікації критичних станів, таких як інфаркт міокарда.

- Модуль моніторингу та прогнозування: використовує гібридні моделі (згорткові нейронні мережі та мережі глибинного навчання) для прогнозування розвитку хронічних захворювань, наприклад, стадій цукрового діабету або ретинопатії.

- Система підтримки прийняття рішень: використовує алгоритми нечіткої логіки для обробки невизначеності в медичних даних та надання рекомендацій лікарю.

Інтеграція різних архітектур глибинного навчання у єдину модель дозволяє значно підвищити точність діагностики на основі візуальних даних (наприклад, оптичної когерентної томографії). Для оцінки точності використовуються метрики Dice Coefficient та AUC. Моніторинг стресових станів: Система включає компоненти для розпізнавання психофізіологічного стану пацієнта (стресу), що є важливим для профілактики серцево-судинних ускладнень.

Експериментальні дослідження показали, що використання гібридних моделей забезпечує високу точність класифікації станів пацієнта. Зокрема, моделі дерев рішень дозволяють ефективно виділяти найбільш значущі ознаки (вік, рівень холестерину, артеріальний тиск) для прогнозування ризиків. Програмна реалізація системи виконана мовою Python з використанням бібліотек Scikit-learn та TensorFlow, що забезпечує високу швидкість обробки даних.

Під час експериментальних досліджень було проведено порівняльний аналіз класифікаторів. Моделі градієнтного бустингу (Gradient Boosting) показали кращі результати на табличних даних (анамнез, аналізи). У задачах розпізнавання стресових станів на основі варіабельності серцевого ритму було досягнуто точності 94% при використанні Random Forest. Дані пацієнтів проходять процедуру деідентифікації перед відправкою на сервер. Також розглядається використання Federated Learning – методу навчання моделей на місцях (у лікарнях) без передачі персональних даних у центральне сховище. Запропонована інтелектуальна система демонструє високу ефективність як інструмент «другої думки» для лікаря. Вона дозволяє мінімізувати пропуски критичних станів та оптимізувати робочий час медичного персоналу. Подальші дослідження будуть спрямовані на інтеграцію з державними реєстрами медичних даних та розширення переліку нозологій, які система здатна розпізнавати в автоматичному режимі.

Розроблена інтелектуальна система дозволяє скоротити час на встановлення діагнозу та забезпечити безперервний моніторинг стану пацієнта. Використання комбінованого підходу (ML + нечітка логіка + DL) робить систему адаптивною до різних типів медичних даних, що є критично важливим для клінічної практики та покращення якості надання медичної допомоги.

Список використаних джерел:

1. Коваленко С. О. Діабетична ретинопатія: сучасні методи діагностики та лікування: монографія. Київ: Здоров'я, 2020. 250 с.
2. Шевченко М. О. Машинне навчання в медичних дослідженнях: основи та застосування. Львів: Львівський національний університет, 2021. 330 с.
3. Тітов С. В., Тітова О. В., Чорна О. С. Метод знаходження апроксимацій приблизних множин з використанням систем числення. Системи обробки інформації. 2023. № 2 (173). С. 58-62. <https://doi.org/10.30748/soi.2023.173.07>

УДК 528.9:004.9:656.1

*Данишина С. Ю., д.т.н., професор
Національний аерокосмічний університет
«Харківський авіаційний інститут»*

ГЕОПРОСТОРОВИЙ АНАЛІЗ ТРАНСПОРТНОЇ АВАРІЙНОСТІ

В Україні проблема забезпечення транспортної безпеки населення є однією з найгостріших. Це пов'язано з різким збільшенням кількості транспортних засобів, а також зі зростанням інтенсивності дорожнього руху за умов недостатньо розвиненої транспортної інфраструктури. Додатковим чинником стають демографічні зміни, зокрема збільшення частки вразливих учасників дорожнього руху (пішоходів, велосипедистів, осіб похилого віку). У результаті спостерігається зростання кількості дорожньо-транспортних пригод (ДТП), що створює серйозні ризики для життя та здоров'я людей, особливо в межах міських територій. Отже, завдання зниження рівня аварійності та травматизму на дорогах України є надзвичайно актуальним [1].

У сучасних дослідженнях розглядають різні аспекти аварійності на транспорті, що охоплюють його технічний стан, вплив людського фактора, якість дорожньої інфраструктури та ефективність нормативно-правового регулювання. Ці фактори стають передумовами виникнення ДТП, що потребує застосування сучасних методів їх ідентифікації, оцінювання та мінімізації. У зв'язку з цим особливу увагу приділяють удосконаленню методів аналізу причин ДТП, зокрема з використанням геопросторового аналізу, який дозволяє системно досліджувати просторові закономірності аварійності та враховувати широкий спектр чинників, які впливають на неї [1, 2].

Для розроблення ефективних заходів щодо зменшення аварійності необхідно дослідити взаємозв'язок між кількістю ДТП і просторово-часовими параметрами їх виникнення. З цією метою, використовуючи ГІС-засоби, проаналізуємо наявні статистичні дані про ДТП, приділяючи особливу увагу їх просторовій прив'язці (рис. 1):

- позначимо на карті місця, де зафіксовано ДТП;
- із застосуванням інструменту Hot Spot Analysis виявимо кластери – території з підвищеною концентрацією ДТП;
- проаналізуємо просторовий зв'язок виявлених кластерів з елементами дорожньої інфраструктури міста.

Таким чином знайдемо ділянки, де наявні системні проблеми, що сприяють виникненню дорожньо-транспортних пригод.

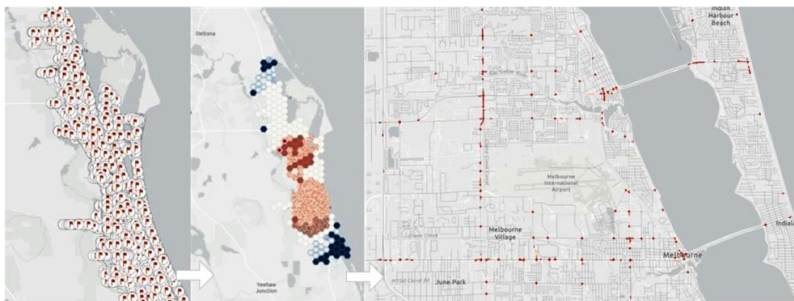


Рис. 1. Геопросторовий аналіз дорожньої інфраструктури міста для виявлення проблем, що сприяють виникненню ДТП

Аналізуючи рис. 1, зазначимо, що просте відображення «точок» ДТП на карті не дає змоги виявити проблемні місця. Лише покроковий аналіз кожного перехрестя з порівнянням кількості ДТП на ньому із сусідніми кварталами та середнім показником по місту дозволяє визначити ділянки з підвищеною аварійністю (позначені червоним кольором). Саме в таких місцях слід шукати системну проблему – погану розмітку, несправний світлофор, небезпечний поворот тощо. ДТП тут не є випадковими, тут слід вживати певні інженерні заходи.

Додатковою перевагою такого підходу є можливість урахувувати «вагу» ДТП, коли до бази даних внесено додаткові атрибути (тяжкість наслідків, кількість учасників, дата та час події). У цьому разі, наприклад, перехрестя, де сталася аварія з тяжкими наслідками, буде позначене інтенсивнішим червоним кольором порівняно з іншими місцями. Додавання часових параметрів дає змогу виявляти ділянки з найбільшою ймовірністю ДТП у певні періоди – у години пік, узимку або під час несприятливих погодних умов.

Отже, саме геопросторовий аналіз є ефективним інструментом для виявлення системних проблем, що дозволяє попереджувати ДТП, зменшувати їх кількість та мінімізувати наслідки.

Список використаних джерел:

1. Дослідження аварійності автотранспорту в аспекті соціальної безпеки / В. О. Карашук, Д. А. Іванченко, О. В. Кіріцева, О. В. Джус. *Наука та транспорт*. 2025. Вип. 29, С. 145 – 155. DOI: 10.31498/2522-9990292025330274.
2. Руденко, Д. В. Оцінка впливу дорожніх умов на аварійність із застосуванням багатофакторної моделі / Д. В. Руденко, А. А. Ренкас, В. І. Товарнянський. *Вісник ЛДУБЖД*. 2021. №. 24, С. 33 – 39. DOI: 10.32447/20784643.24.2021.04.

УДК 004.7+004.415.2

*Попко А. К., здобувач,
Ніколаєнко А. Ю., к.т.н., асистент
Київський національний університет імені Тараса Шевченка*

АРХІТЕКТУРА ПРОГРАМНОЇ СИСТЕМИ МОНІТОРИНГУ ПРОМИСЛОВОГО ОБЛАДНАННЯ

Вступ. Сучасні підприємства експлуатують обладнання від різних виробників із власними закритими системами моніторингу. Наслідком цього є фрагментація даних, що ускладнює комплексний аналіз виробничих процесів. Крім того, більшість наявних рішень функціонує реактивно, фіксуючи лише факт несправності. Такий підхід унеможливило запобігання аваріям і призводить до непередбачуваних простоїв та фінансових втрат.

Метою роботи є проєктування архітектури універсальної програмної системи моніторингу, яка забезпечить централізовану агрегацію телеметрії з різних виробничих вузлів і використання предиктивної аналітики для завчасного виявлення аномалій та ймовірних відмов [1].

Архітектура запропонованої IoT-системи базується на розділенні потоків обробки даних (рис. 1). Високочастотна телеметрія від сенсорів надходить через брокер повідомлень (Mosquitto) за протоколом MQTT до бекенду (ASP.NET Core API). Оскільки синхронний запис посекундних даних з багатьох вузлів генерує критичне навантаження на базу даних (PostgreSQL), застосовано патерн пакетної буферизації. Дані тимчасово накопичуються в пам'яті сервера та записуються об'ємними транзакціями, що суттєво підвищує пропускну здатність системи.

Проте такий підхід створює затримку, неприпустиму для критичних інцидентів, коли параметри виходять за межі норми. Для нівелювання цього недоліку паралельно працює подієво-орієнтований маршрут (Fast Path). У разі фіксації аномалії система ігнорує буфер, миттєво записує події в базу та ініціює Push-сповіщення на фронтенд (Angular/React) через SignalR з нульовою затримкою реакції.

Накопичений масив даних використовується для предиктивної аналітики (Slow Path) [2]. Оскільки використання необробленої телеметрії містить багато шуму і призводить до перенавчання моделей, система попередньо агрегує дані за допомогою ковзних часових вікон. Замість абсолютних значень обчислюються статистичні ознаки (дисперсія, тренди, ковзні середні), які надають можливість модулю ML.NET розпізнавати поступову фізичну деградацію механізмів.

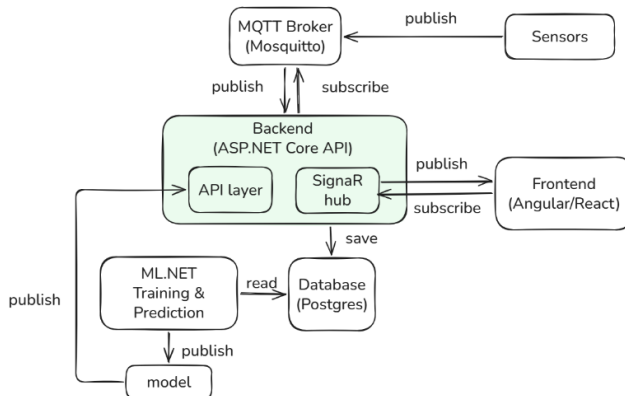


Рис. 1. Структурна схема маршрутизації та обробки даних

Для класифікації ймовірності відмов вибрано алгоритм градієнтного бустингу (LightGBM) [3]. Щоб інженери не лише бачили факт можливої поломки, а й розуміли її причину, впроваджено концепцію Explainable AI. Модель розраховує внесок кожної ознаки у фінальний прогноз, і ці метадані зберігаються в PostgreSQL у неструктурованому форматі JSONB. Така денормалізація усуває потребу в складних зв'язках (JOIN) на рівні бази даних та дає змогу гнучко відображати кореневі причини аномалій в інтерфейсі.

Висновки. Створений прототип IoT-системи вирішує проблему консолідації телеметрії з різнотипного обладнання. Гібридна архітектура з розділенням потоків (Fast/ Slow Path) забезпечує баланс між пропускну здатністю та оперативністю критичних сповіщень. Інтеграція машинного навчання з Explainable AI формує інтерпретовані прогнози відмов, що створює надійне підґрунтя для переходу підприємств до предиктивного обслуговування.

Список використаних джерел:

1. Zonta T., da Costa C. A., da Rosa Righi R., De Lima M. J., Da Trindade E. S., Li G. P. Predictive maintenance in the Industry 4.0: A systematic literature review. Computers & industrial engineering. 2020. Vol. 150:106889. <https://doi.org/10.1016/j.cie.2020.106889>.
2. Mihigo I. N., Zennaro M., Uwitonze A., Rwigema J., Rovai M. On-Device IoT-Based Predictive Maintenance Analytics Model: Comparing TinyLSTM and TinyModel from Edge Impulse. Sensors, 2022. Vol. 22, No 14:5174. <https://doi.org/10.3390/s22145174>.
3. LightGBM. URL: <https://github.com/microsoft/LightGBM> (дата звернення: 03.03.2026 р.)

УДК 004.414.2:004.77

*Камишан П.С., здобувач
Кобилін І.О., к.т.н., викладач*

Харківський національний університет радіоелектроніки

МОДЕЛІ БАГАТОКРИТЕРІАЛЬНОГО РАНЖУВАННЯ РЕЛЕВАНТНОСТІ ІНФОРМАЦІЙНИХ БЛОКІВ У МОБІЛЬНИХ СИСТЕМАХ СУПРОВОДУ

Розвиток інтелектуальних сервісів потребує впровадження адаптивних механізмів управління контентом для забезпечення релевантної взаємодії користувача з оточенням у реальному часі. Проблема реалізації таких систем на мобільних пристроях полягає у візуальній надмірності, коли в обмежене поле зору сенсора одночасно потрапляє декілька об'єктів, що претендують на активацію інформаційного супроводу. Традиційні методи, що базуються на статичних тригерах, часто виявляються неефективними, оскільки не враховують ієрархічну значущість об'єктів та динаміку зміни фокусу уваги користувача [3]. Це обумовлює необхідність розробки моделей багатокритеріального ранжування для автоматизації пріоритезації інформаційних блоків та суттєвого мінімізації когнітивного навантаження на оператора системи.

Запропонована методологія базується на обчисленні інтегрального показника релевантності R_j для кожного j -го об'єкта. На відміну від класичних систем, багатокритеріальний підхід дозволяє розглядати детекцію як елемент структурованої моделі, де пріоритетність визначається адитивною згортою нормалізованих параметрів:

$$R_j = \alpha \cdot A_j + \beta \cdot C_j + \gamma \cdot S_j,$$

де A_j – нормалізована площа об'єкта (відносно кадру), C_j – показник центральності (інверсована відстань до оптичної осі), S_j – семантична вага об'єкта у базі знань. Для забезпечення математичної коректності моделі виконується умова нормування вагових коефіцієнтів:

$$\alpha + \beta + \gamma = 1, \text{ а всі вхідні змінні приведені до діапазону } [0, 1].$$

Процес ранжування інтегрується як логічний шар між модулем комп'ютерного зору та підсистемою видачі контенту [2]. Параметри ефективності наведено у таблиці 1.

Застосування багатокритеріального ранжування усуває конфлікти при груповій ідентифікації об'єктів та забезпечує логічну послідовність подачі матеріалу [4].

Таблиця 1

Критерії оцінки релевантності об'єктів у реальному часі

Критерій ранжування	Методологічне обґрунтування	Результат для системи
Геометрична площа (A_j)	Оцінка розмірів релевантної області	Виділення домінантного об'єкта
Показник центральності (C_j)	Аналіз відхилення від центру кадру	Фокусування на об'єкті уваги
Семантичний пріоритет (S_j)	Вага об'єкта в інформаційній моделі	Врахування значущості
Стабільність детекції	Часова фільтрація візуальних завад	Усунення хибних спрацювань

Такий підхід трансформує систему в інтелектуальний асистент, здатний до автономного прийняття рішень на основі багатовимірного аналізу вхідних даних. Перспективи подальшого впровадження методу пов'язані з оптимізацією обчислювальних витрат алгоритму для підтримки високої продуктивності (FPS) на мобільних пристроях з обмеженими ресурсами. Крім того, моделі є необхідним фундаментом для покращення якості інформаційного супроводу в сучасних системах доповненої реальності та навігаційних сервісах нового покоління.

Список використаних джерел:

1. Redmon J. et al. 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.
2. Shi B. et al. An End-to-End Trainable Neural Network for Image-based Sequence Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, vol. 39, no. 11, pp. 2298-2304.
3. Hwang C. L., Yoon K. Multiple Attribute Decision Making: Methods and Applications. Springer-Verlag, Berlin, 1981.
4. Belton V., Stewart T. J. Multiple Criteria Decision Analysis: An Integrated Approach. Kluwer Academic Publishers, 2002.
5. Gonzalez R. C., Woods R. E. Digital Image Processing. Pearson, 2018.

УДК 004.7

Kaimachnikova V. S., 3rd-year student
Taras Shevchenko National University of Kyiv

SOFTWARE MODELING OF IN-MEMORY VECTOR INDEXING PERFORMANCE FOR RETRIEVAL-AUGMENTED GENERATION (RAG) SYSTEMS

The rapid development of Large Language Models (LLMs) has made Retrieval-Augmented Generation (RAG) an essential architecture in contemporary commercial information systems. According to a recent study [1], the RAG architecture was able to resolve the very significant issue of LLM hallucinations since it relied on knowledge bases containing domain-specific knowledge. However, there are several computational challenges with this architectural design. This is especially true for the semantic retrieval of relevant contextual information from training datasets consisting of millions of high-dimensional vectors, which is a significant retriever performance bottleneck. Highly optimized in-memory vector indexing techniques are required to efficiently handle such massive data amounts and ensure system scalability.

A Python software testing environment was created using the numpy and faiss modules in order to assess retrieval performance empirically. In order to simulate executing 100 concurrent queries against in-memory Vecto databases growing from 10k embeddings to 500k embeddings, the experimental configuration had a dimensionality of 128. CMA computes the cosine similarity metric (arithmetically determines mathematical closeness) for each separated database vector V with respect to a query vector Q in the baseline methodology of the previously mentioned precise search (Brute Force) method topology. This metric can be calculated using any standard formula depending on the user use-case.

$$similarity = \cos(\theta) = \frac{Q \cdot V}{\|Q\| \cdot \|v\|} = \frac{\sum_{i=1}^n Q_i \cdot V_i}{\sqrt{\sum_{i=1}^n Q_i^2} \sqrt{\sum_{i=1}^n V_i^2}}$$

For high-dimensional retrieval, using the HNSW [1] implemented in FAISS [2], making it essentially moves from linear scan to log-based graph traversal for searching.

The HNSW (Hierarchical Navigable Small World) algorithm builds a multi-layer navigable graph as compared to standard linear search algorithms. The search starts at the highest sparse layer and uses a greedy routing algorithm to quickly drop into lower, denser layers until it reaches the nearest neighbor. Note that this approach has some trade-offs:

1. Index creation cost (Index Build Time): Needs to be preconstructed before querying

2. Memory overhead: uses extra RAM to maintain the graph connections between nodes

That said, these architectural compromises are completely made up for by the unheard of execution speed attained during the query processing (i.e. inference) phase. Both the exact search and approximate FAISS HNSW algorithms were executed simultaneously during the simulation to fetch top-5 nearest vectors for each query. Pure execution latency (in milliseconds) was the main evaluation metric, enabling a direct comparison in terms of computational overhead as dataset volume increased.

Table 1 shows a summary of the findings from the combined software profiling; and these data are depicted graphically in Figure 1. Our real world data shows a clear linear performance degradation of the exact Brute Force. Latency for processing a query batch (3564.85 ms) was much longer than acceptable requirements for real time usage because of the database having 500,000 vectors. FAISS (HNSW), on the other hand, managed to do the same operation in 7.84 ms with a little computational overhead by using its own hierarchy of graphs achieving near-constant retrieval time, thus obtained an acceleration factor over 450x[110]! And remember also about a trade-off of basic architecture: there is always some degradation of gaining power on retrieval accuracy especially in Recall metric going from exact search (Brute-Force) method to Approximate Nearest Neighbor (ANN). However, this accuracy loss does not go above 1-2% according to empirical modeling for the selected HNSW graph parameters [10]. For LLM generating tasks, this variation is statistically and semantically insignificant, but the search execution time is improved by more than 45,000%.

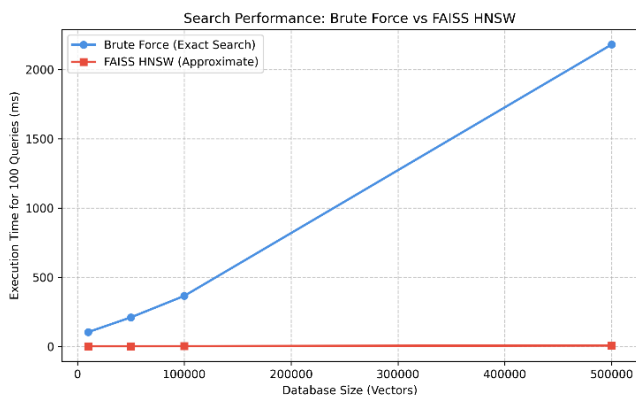


Fig.1. Search performance evaluation: Brute Force vs. FAISS HNSW across scaling database sizes.

Table 1

Comparative analysis of execution time (ms) for exact and approximate vector search algorithms

Database Size (Vectors)	Brute Force (ms)	FAISS HNSW (ms)
10,000	104.50	0.00
50,000	325.67	4.03
100,000	622.24	6.04
500,000	3564.85	7.84

The software models are built where when the vector database has larger volumes, it is computationally unfeasible to run exact Semantic search (Brute Force). Exhaustive search techniques are therefore not feasible for real-time business applications, as the time taken to process these cases expands exponentially. All current state-of-the-art Retrieval-Augmented Generation (RAG) pipelines must instantiate estimated vector indices such as FAISS HNSW in order to avoid this basic bottleneck [3]. This improves high throughput instructions by orders of magnitude in latency while maintaining the information system as sequential and persistent as possible for speed. Although there is a little accuracy penalty associated with switching to approximation retrieval, the 450x speedup factor finally makes it feasible to create scalable, on-demand semantic search infrastructure. Lastly, the synthesis process of LLM assures that the tiny loss of retrieval accuracy is statistically and semantically minor, making this approach intrinsically acceptable to enterprise AI organizations.

List of references

1. Dimitrova M. Retrieval-Augmented Generation (RAG): Advances and Challenges. 2025. URL: <https://doi.org/10.7546/PECR.83.25.03> Date of access 20.03.2026.
2. Sathyavageeswaran R. Designing vendor-neutral semantic search pipelines using open-source embedding models and FAISS. 2026. URL: <https://doi.org/10.30574/wjaets.2026.18.3.0038> Date of access 21.03.2026.
3. Li Y., Jin Y., Tian B., Zhang H., Gao M. ANSMET: Approximate Nearest Neighbor Search with Near-Memory Processing and Hybrid Early Termination. ISCA '25: Proceedings of the 52nd Annual International Symposium on Computer Architecture. 2025. P. 1093–1107. URL: <https://doi.org/10.1145/3695053.3731013> Date of access 24.03.2026.

УДК 004.89

Остапець Я.Д., аспірант

Український державний університет науки і технологій

ОГЛЯД ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ НА ЗАЛІЗНИЧНИХ СТАНЦІЯХ

Ефективність функціонування залізничного транспорту значною мірою визначається якістю управління технологічними процесами на залізничних станціях. Традиційні детерміновані алгоритми не враховують стохастичний характер даних і змінність умов експлуатації, що знижує ефективність прийняття рішень [1]. В умовах обмеженого часу на прийняття рішень та високих вимог до надійності виникає потреба у впровадженні інтелектуальних методів управління.

На думку автора, до основних груп таких інтелектуальних методів доцільно віднести:

- Методи машинного навчання;
- Еволюційні методи;
- Методи колективного інтелекту;
- Нечіткі та гібридні методи.

Одним із ключових напрямів є використання машинного навчання для прогнозування параметрів роботи станції. ML-моделі здатні виявляти закономірності у великих масивах даних, що дозволяє прогнозувати затримки поїздів, оптимізувати маневрову роботу та планувати технічне обслуговування. Особливо актуальною є задача прогнозування часу прибуття вантажних поїздів, яка ускладнюється впливом випадкових факторів. Дослідження показують, що ансамблеві методи, зокрема градієнтний бустинг, забезпечують високу точність прогнозування [2]. Аналіз часових рядів дає змогу передбачати завантаженість колій і конфліктні ситуації, що сприяє прийняттю превентивних рішень.

Для задач оперативного управління ефективними є методи навчання з підкріпленням, які формують оптимальні стратегії в умовах невизначеності. Використання графових нейронних мереж дозволяє враховувати топологію станції як складної мережевої структури. Зокрема, алгоритми типу DQN (Deep Q-Network) демонструють кращі результати у задачах формування та розформування поїздів порівняно з класичними методами, оскільки враховують динаміку системи та можливі майбутні події [3, 4].

Важливими є задачі оптимізації маневрової роботи, формування поїздів і розподілу вагонопотоків. У цих випадках ефективними є

еволюційні методи, зокрема генетичні алгоритми, які дозволяють знаходити рішення у задачах великої розмірності та з багатьма критеріями. Вони успішно застосовуються для складання графіків руху та оптимізації експлуатаційних витрат [5]. Особливістю таких алгоритмів є можливість роботи з багатокритеріальними функціями придатності, де одночасно враховуються експлуатаційні витрати, час доставки вантажу та надійність графіка. Поєднання таких методів із машинним навчанням формує гібридні підходи, здатні враховувати як історичні дані, так і поточний стан системи.

У складних транспортних вузлах перспективним є застосування мультиагентних систем, де елементи інфраструктури моделюються як автономні агенти. Це забезпечує децентралізоване управління, підвищує гнучкість і стійкість системи. Методи ройового інтелекту ефективні для задач маршрутизації та логістики; зокрема, сучасні алгоритми, такі як «Pigeon-Inspired Optimization», демонструють швидку збіжність при високій ефективності [6].

Окрему роль відіграють методи, орієнтовані на роботу в умовах невизначеності та неповноти інформації. Зокрема, використання нечіткої логіки та інтерпретованих моделей дозволяє формалізувати експертні знання та забезпечити прозорість процесу прийняття рішень. Наприклад, у задачах управління гальмівними позиціями сортувальних гірок нечіткі регулятори дозволяють враховувати невизначеність ходових характеристик відцепів та відхилення натискної сили самих уповільнювачів.

Гібридні інтелектуальні системи, що поєднують кілька методів, демонструють кращі результати порівняно з однорідними підходами. Наприклад, нейро-нечіткі системи типу ANFIS (Adaptive Neuro Fuzzy Inference System) поєднують адаптивність нейронних мереж з інтерпретованістю нечіткої логіки. Математична структура ANFIS дозволяє системі самостійно коригувати параметри функцій належності на основі вхідних даних, що забезпечує мінімальну похибку управління.

Таким чином, проведений огляд підтверджує, що гібридні інтелектуальні системи є найбільш перспективним напрямом для управління технологічними процесами на залізничних станціях, оскільки поєднують адаптивність, точність і здатність працювати в умовах невизначеності.

У рамках подальшого розвитку дослідження пропонується розробка системи керування швидкістю скочування вагонів на сортувальних гірках на основі нейро-нечіткої мережі ANFIS з інтегрованим цифровим двійником об'єкта керування. Така архітектура забезпечить самоадаптацію системи при зміні ключових параметрів (зокрема, кута нахилу гірки) та своєчасне коригування управляючих впливів. Це

дозволить підвищити надійність і точність управління в умовах реальної експлуатації.

Список використаних джерел:

1. Жуковицький І. В. Цифрові системи управління швидкістю скочування відчепів на сортувальних гірках : монографія. Дніпропетровськ : Маковецький Ю. В., 2012. 203 с.

2. Minbashi N., Zhao J., Dick C. T., Bohlin M. Enhancing freight train delay prediction with simulation-assisted machine learning. IET Intelligent Transport Systems. 2024. URL: <https://doi.org/10.1049/itr2.12573> (дата звернення: 20.03.2026).

3. Peer E., Menkovski V., Zhang Y., Lee W.-J. Shunting Trains with Deep Reinforcement Learning. 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC) : conference proceedings, Miyazaki, Japan, 07-10 Oct. 2018. IEEE, 2018. URL: <https://doi.org/10.1109/SMC.2018.00520> (дата звернення: 20.03.2026).

4. Optimization of shunting operation plan in large freight train depot based on DQN algorithm / J. Qiu et al. PLoS One. 2025. Vol. 20, no. 4. e0320762. URL: <https://doi.org/10.1371/journal.pone.0320762> (дата звернення: 20.03.2026).

5. A Genetic Algorithm for Railway Scheduling Problems / P. Tormos et al. Metaheuristics for Scheduling in Industrial and Manufacturing Applications. Berlin ; Heidelberg : Springer-Verlag, 2008. (Studies in Computational Intelligence ; vol. 128). P. 255–276. URL: https://doi.org/10.1007/978-3-540-78985-7_10 (дата звернення: 20.03.2026).

6. Zhang X., Wei Y., Hashim Z. Improvement of Swarm Intelligence Algorithm and Its Application in Logistics Network Routing. Journal of Network Intelligence. 2023. Vol. 8, no. 4. P. 1077–1094. URL: <https://bit.nkust.edu.tw/~jni/2023/vol8/s4/02.JNI-S-2023-04-014.pdf> (дата звернення: 20.03.2026).

УДК 004.7

*Бондарев Андрій Сергійович, аспірант,
П'ятченко Владислав Юрійович, асистент
Сумський державний університет*

АНАЛІЗ МЕТОДІВ ОБРОБКИ НЕПОВНИХ ДАНИХ ДЛЯ ВЕБОРІЄНТОВАНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Актуальність проблеми. Системи підтримки прийняття рішень (СППР) на основі машинного навчання активно використовуються у різних сферах діяння, зокрема в освіті. Однією з критичних проблем при цьому є неповнота даних. Для веборієнтованої СППР для оцінювання освітнього контенту за оцінками експертів проблема проявляється вигляді порожніх полів. Подібна неповнота призводить до зміщення розподілу навчальних даних, погіршення точності передбачень і некоректних висновків.

1. У статті «The impact of imputation quality on machine learning classifiers for datasets with missing values» досліджено взаємозалежність між якістю відновлення пропущених значень і точністю класифікаторів, а також порівняно методи для відновлення даних. Встановлено, що найбільший вплив на якість класифікації має частка пропущених значень у тестовій вибірці, а не лише у навчальній. Автори пропонують новий клас метрик якості імпутації на основі відстані Васерштейна, який значно краще відображає збереження реального розподілу даних порівняно із традиційними метриками. Результати демонструють, що некоректна імпутація погіршує точність та інтерпритованість моделей.

2. У статті від Yoon, Jordon, van der Schaar (2018) розглянуто чи можна оцінити пропущені значення на основі спостережуваних даних за допомогою нейромережевого підходу, що навчається відтворювати справжній розподіл даних.

Автори запропонували метод відновлення пропущених значень на основі генеративно-змагальної мережі. Генератор відновлює пропуски з урахуванням наявних значень, тоді як дискримінатор визначає для кожної ознаки – чи є значення реальним чи відновленим. Таким чином, GAIN демонструє принципову перевагу GAN-підходу над статистичними методами.

3. Автори у роботі «Generative Adversarial Networks for Imputing Sparse Learning Performance» (ICPR) вирішують задачу наступну задачу: є матриця оцінок, де рядки - суб'єкти, стовпці - дисципліни, а більша частина клітинок порожня, бо не кожен студент виконував кожне завдання. Автори адаптують GAN-підхід для таких матричних даних,

додаючи CNN-шари для вловлювання залежностей між сусідніми дисциплінами. Метод валідовано на шести реальних навчальних датасетах і перевершує методи матричної факторизації та оригінальний GAIN. Це безпосередньо обґрунтовує застосування GAN-підходу для відновлення неповних експертних оцінок у веборієнтованій СППР, де природа розрідженості це відсутність предметної компетентності окремих.

Проектне рішення для системи. На основі проведеного аналізу обґрунтовано архітектурне рішення для веборієнтованої СППР. Запропонований pipeline обробки неповних даних включає: (1) визначення механізму пропуску та аналізу патернів відсутності – з урахуванням специфіки предметної галузі, де пропуск зумовлений відсутністю компетентності експерта оцінити дисципліну, а не випадковим фактором; (2) відновлення пропущених значень методом GAIN з CNN-розширенням для матричних даних або MICE як статистичною альтернативою при малій частці пропусків; (3) оцінку якості відновлення за метрикою на основі відстані Васерштейна, що забезпечує контроль збереження розподілу даних;

Висновки. У розглянутій задачі відсутність оцінки зумовлена браком компетентності експерта. Застосування GAN-підходу, адаптованого для матричних освітніх даних, у поєднанні з метричним контролем якості відновлення є перспективним напрямом для побудови інтелектуальної системи підтримки прийняття рішень з неповною визначеністю даних.

Список використаних джерел:

1. The impact of imputation quality on machine learning classifiers for datasets with missing values / T. Shadbahr, M. Roberts, J. Stanczuk et al. *Communications Medicine*. 2023. Vol. 3, art. 139. DOI: <https://doi.org/10.1038/s43856-023-00356-z> (дата звернення: 24.03.2026).
2. Yoon J., Jordon J., van der Schaar M. GAIN: Missing Data Imputation using Generative Adversarial Nets. *Proceedings of the 35th International Conference on Machine Learning (ICML 2018)*. 2018. Vol. 80. P. 5689–5698. URL: <https://arxiv.org/abs/1806.02920> (дата звернення: 24.03.2026).
3. Generative Adversarial Networks for Imputing Sparse Learning Performance / L. Zhang, H.-Y. Shum, V. Shute, F. Wang. *Proceedings of the 27th International Conference on Pattern Recognition (ICPR 2024)*. 2024. URL: <https://arxiv.org/abs/2407.18875> (дата звернення: 24.03.2026).

УДК 004.738.5

Катюха А.А., здобувач

Житомирський державний університет імені Івана Франка

ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ВЕБЗАСТОСУНКУ ДЛЯ ПРОСУВАННЯ ВІДЕОІГОР

Актуальність і мета роботи. На сьогодні ігрова індустрія досягла масштабів, що зумовлюють надзвичайно високий рівень конкуренції на ринку. Для успішного релізу відеогри недостатньо лише якісного геймплею – критично важливим етапом є ефективна маркетингова стратегія та правильне позиціонування продукту. Створення професійного вебзастосунку є одним із ключових інструментів залучення аудиторії, що дозволяє не лише презентувати графічний контент, а й розкрити специфічні особливості проєкту. Метою роботи є проєктування та технічна реалізація адаптивного вебзастосунку, спрямованого на популяризацію ігрового продукту та взаємодію з потенційними користувачами.

Аналіз подібних рішень. Під час дослідження було проаналізовано сучасні промо-сайти успішних ігрових проєктів. Більшість існуючих рішень фокусуються на використанні динамічних елементів та інтерактивності для утримання уваги. Проте часто спостерігається проблема надмірної ваги сторінок, що негативно впливає на швидкість завантаження. У даній роботі враховано цей досвід, тому основний акцент зроблено на балансі між візуальною привабливістю та високою продуктивністю, що відповідає сучасним стандартам вебюзабіліті [1].

Обґрунтування технічних рішень. Для реалізації проєкту було обрано класичний стек технологій: HTML5, CSS3 та JavaScript, що відповідають актуальним специфікаціям W3C [3]. Вибір зумовлений необхідністю забезпечення максимальної швидкості роботи та кросбраузерності. Для створення динамічних ефектів використано бібліотеку анімацій, що дозволяють зробити інтерфейс живим, не перевантажуючи систему складними фреймворками, де це не є доцільним.

Результати проєктування та UX/UI концепція. На етапі проєктування особливу увагу було приділено UI/UX-дизайну як фундаментальному елементу користувацького досвіду [2]. Розроблено інтуїтивно зрозумілу навігацію та естетичне графічне оформлення. Архітектура застосунку передбачає повну адаптивність, що гарантує коректне відображення контенту як на стаціонарних моніторах, так і на мобільних пристроях. Функціональні вимоги включали створення

системи зворотного зв'язку та інтерактивних галерей для демонстрації ігрового світу.

Отримані результати. У ході розробки було реалізовано багатофункціональний вебзастосунок, що поєднує в собі маркетинговий інструмент та платформу для дистрибуції відеоігор. До складу системи увійшли наступні модулі:

Інтерактивна вітрина товарів – головна сторінка, що містить динамічні банери, систему фільтрації та актуальні ігрові пропозиції для швидкого привернення уваги відвідувачів;

Інформаційний блок продукту – деталізована сторінка кожної гри, що включає опис ігрових механік, технічні характеристики, системні вимоги та оптимізовану мультимедійну галерею;

Система управління замовленнями – реалізовано функціонал «Кошика» для формування замовлень та механізм «Списку бажаного» (Wishlist) для персоналізації користувацького досвіду та утримання аудиторії.

Висновки та перспективи подальших досліджень. Розроблений вебзастосунок підтверджує ефективність поєднання маркетингових інструментів та функцій електронної комерції для просування відеоігор. Запропонована структура вітрини, інтеграція кошика та списку бажаного дозволяють не лише презентувати ігровий контент, а й безпосередньо стимулювати продажі. Створення персоналізованих функцій є критично важливим фактором для утримання аудиторії в умовах високої конкуренції.

Список використаних джерел:

1. Krug S. Don't Make Me Think: A Common Sense Approach to Web Usability. New Riders Publishing, 2014.
2. Garrett J. The Elements of User Experience: User-Centered Design for the Web. New Riders, 2011.
3. W3C. HTML Standard. URL: <https://html.spec.whatwg.org/>

УДК 004.738.5

*Шкаруба А.В., здобувач**Житомирський державний університет імені Івана Франка*

ОНЛАЙН СЕРВІС ДЛЯ ДИНАМІЧНОЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

В епоху стрімкого зростання обсягів цифрової інформації, здатність швидко аналізувати дані й робити правильні висновки з них стає надзвичайно важливим для прийняття швидких рішень в багатьох галузях. Це пов'язано з тим, що вони безперервно надходять від багатьох джерел, наприклад від систем моніторингу за промисловими об'єктами; сенсорів, що керують життєдіяльністю будівель; програм для опрацювання фінансових звітностей тощо. Звичайно ж текст або набір таблиць не дуже сприяють усвідомленому опрацюванню їх людиною. Тож розробка інтерактивних онлайн-сервісів, здатних візуалізувати у динаміці інформацію, є досить актуальним завданням. Основний проблемний момент при розробці таких вебсистем полягає в тому, щоб представляти графічно числові залежності у зручному для користувача вигляді і при цьому зберігати зручність роботи користувача з великими обсягами вхідних даних досить складно.

У цьому контексті, **метою** дослідження є описати ефективну програмну архітектуру для спеціалізованого веб-сервісу, який забезпечує швидке завантаження, попередню обробку та інтерактивне відображення динамічної графічної інформації.

Для досягнення поставленої мети було представлено наступну клієнт-серверну архітектуру системи, що чітко розділяє процеси на обробку даних та їх фінальну візуалізацію.

Зазвичай основним джерелом вхідної інформації для сервісу виступають структуровані текстові формати, зокрема файли формату CSV. Також треба зважати й на те, що пряме завантаження та обробка таких числових масивів відбувається безпосередньо на стороні клієнта, що призводить до перевантаження оперативної пам'яті та зависання сторінки браузера. Щоб цього уникнути, варто зробити основний акцент на правильному розподілі обчислювального навантаження. Весь процес первинної обробки варто перенести на серверну частину. Вона може бути реалізована на базі середовища Node.js. У такому випадку сервер здійснює асинхронне читування файлів, не блокуючи роботу системи. Після цього він фільтрує інформацію і перетворює її у структурований формат (JSON), який є оптимальним для передачі по мережі.

Важливою складовою надійності системи є використання суворої типізації за допомогою TypeScript. Завдяки цьому на етапі підготовки даних на сервері формуються чіткі об'єкти, які відповідають очікуванням та вимогам клієнтського інтерфейсу. Такий підхід дозволяє браузеру не витратити ресурси та час на складну обробку, перевірку чи сортування файлу. Натомість клієнтська частина миттєво розпочинає відображення графічної інформації одразу після отримання готового пакета даних від сервера. [2]

Отримавши підготовлений та типізований масив даних, клієнтська частина приділяє увагу виключно на візуалізацію та забезпечення взаємодії з користувачем. Оскільки браузер звільнений від великих обчислень, інтерфейс може швидко реагувати на дії користувача і при цьому відображати складні залежності між наборами даних. Це дозволяє реалізувати плавні анімації, зручне масштабування окремих ділянок графіка для детального аналізу, а також динамічне виведення додаткової інформації при наведенні курсору на конкретні точки. Крім того, така оптимізація процесу відображення значно зменшує вимоги до обчислювальної потужності пристрою користувача. Завдяки цьому з аналітикою можна працювати не лише на сучасних комп'ютерах, але й на звичайних офісних ноутбуках чи мобільних пристроях. [1]

Крім того, така модульна архітектура дозволяє підвищити гнучкість та масштабованість розробленого онлайн-сервісу. У разі виникнення потреби підключити нові джерела інформації або обробляти ще більші обсяги даних, то основні зміни будуть лише на сервері. Клієнтський інтерфейс при цьому не буде потребувати великих змін, що робить створену систему універсальним інструментом, простим у підтримці та подальшій модернізації.

Підводячи короткий **підсумок** зазначимо, що запропонований архітектурний підхід дозволяє ефективно вирішити проблему відображення великих масивів інформації у веб-середовищі. Чіткий розподіл завдань між сервером та браузером, перенесення важкої обробки CSV-файлів на серверну сторону (Node.js) та використання суворої типізації даних забезпечують швидку, стабільну та зручну роботу веб-сервісу. У майбутньому планується розширити функціонал системи, додавши нові типи графіків та можливість автоматичного оновлення інформації в режимі реального часу.

Список використаних джерел:

1. Mardan A. Full Stack JavaScript: Learn Backbone.js, Node.js and MongoDB. - New York: Apress, 2015. - 287 p.
2. Zammetti F. Modern Full-Stack Development: Using TypeScript, React, Node.js, Webpack, and Docker. - Berkeley: Apress, 2020. - 374 p.

УДК 004.896:616-07

*Петрівський В.Я., PhD, асистент**Мельник М.О., аспірант**Київський національний університет імені Тараса Шевченка*

ШТУЧНИЙ ІНТЕЛЕКТ У МЕДИЧНІЙ ДІАГНОСТИЦІ

Вступ. Трансформація сучасної медицини в умовах зростання обсягів біомедичних даних обумовлює перехід від традиційних емпіричних методів до автоматизованих систем інтелектуального аналізу. У цьому контексті медична діагностика постає як критична область застосування методів штучного інтелекту, де складність об'єктів дослідження та висока ціна помилки вимагають впровадження прецизійних алгоритмічних рішень. Необхідність оперативної обробки гетерогенної інформації та виявлення прихованих закономірностей у клінічних показниках робить актуальним застосування систем підтримки прийняття рішень, що базуються на математичній формалізації діагностичного процесу.

Основна частина. З точки зору теорії інформаційних систем, процес медичної діагностики піддається суворій формалізації. Його можна представити як багатопараметричну задачу відображення простору вхідних ознак у множину дискретних класів або неперервних значень ймовірності захворювань. Вхідний вектор при цьому формується з гетерогенних джерел, що включають результати лабораторних аналізів, цифрові сигнали біомедичного походження, текстові записи електронних медичних карт та багатовимірні структури медичних зображень. Математична постановка задачі передбачає побудову оптимальної апроксимуючої функції, яка мінімізує помилку класифікації при одночасному врахуванні стохастичної природи біологічних процесів, наявності шумів у вимірювальних каналах та неповноти вихідної інформації. Ефективне розв'язання окресленої задачі забезпечується використанням широкого спектра алгоритмів машинного навчання [1]. Для роботи зі структурованими даними традиційно застосовуються методи опорних векторів, байесівські мережі та ансамблеві моделі, такі як градієнтний бустинг або випадкові ліси, що демонструють високу стійкість до перенавчання. Проте справжній технологічний прорив спостерігається у сфері глибинного навчання. Згорткові нейронні мережі стали стандартом де-факто для аналізу візуальної діагностичної інформації, оскільки вони здатні автоматично виділяти ієрархічні ознаки з зображень КТ, МРТ та рентгенографії, часто перевершуючи досвідчених радіологів за показниками чутливості та специфічності. Водночас рекурентні

архітектури та механізми самоуваги в трансформерних моделях дозволяють здійснювати глибинний аналіз динамічних послідовностей, що критично важливо для інтерпретації електрокардіограм та моніторингу пацієнтів у реальному часі.

Технологічна інтеграція інтелектуальних алгоритмів у медичну інфраструктуру вимагає створення складних програмно-апаратних комплексів, що функціонують на засадах функціональної сумісності та інтероперабельності. Забезпечення обміну даними між різними ланками системи охорони здоров'я реалізується через впровадження міжнародних стандартів, що гарантує цілісність інформаційного поля. Поряд із технічними аспектами, першочергового значення набувають питання кібербезпеки та етики. Оскільки медичні дані є критично конфіденційними, архітектура діагностичних систем повинна передбачати багаторівневий захист від несанкціонованого доступу, включаючи методи знеособлення даних та використання захищених протоколів обробки, що безпосередньо впливає на топологію та складність розроблюваних рішень [2-3].

Висновки. Трансформація медичної діагностики в задачу штучного інтелекту є закономірним етапом цифрової трансформації галузі. Це мультидисциплінарний напрям, що синтезує досягнення обчислювальної математики, великих даних та клінічної медицини. Подальші перспективи розвитку вбачаються у створенні гібридних інтелектуальних систем, які поєднують потужність нейромережових обчислень із формалізованими медичними знаннями та етичними стандартами. Реалізація цього потенціалу дозволить суттєво оптимізувати діагностичні процеси, забезпечивши персоналізований підхід до лікування та значне підвищення ефективності охорони здоров'я в цілому на глобальному рівні.

Список використаних джерел:

1. Kaul V., Enslin S., Gross S. A. History of artificial intelligence in medicine. *Gastrointestinal Endoscopy*. 2020. Vol. 92, no. 4. P. 807–812. URL: <https://doi.org/10.1016/j.gie.2020.06.040>.
2. Hou H., Zhang R., Li J. Artificial intelligence in the clinical laboratory. *Clinica Chimica Acta*. 2024. P. 119724. URL: <https://doi.org/10.1016/j.cca.2024.119724>.
3. Rabbani, N., Kim, G. Y., Suarez, C. J., & Chen, J. H. (2022). Applications of machine learning in routine laboratory medicine: current state and future directions. *Clinical Biochemistry*, 103, 1–7. URL: <https://doi.org/10.1016/j.clinbiochem.2022.02.011>.

УДК 004.021:004.272.2:004.67

*Krasnokutska I.V., PhD, Assoc. Prof.
Hatsenko D.O., undergraduate
Yuriy Fedkovych Chernivtsi National University*

HIGH-PERFORMANCE DATA PROCESSING TECHNOLOGIES IN MODERN INFORMATION SYSTEMS BASED ON GPU

The rapid development of information systems and the exponential growth of data volumes in resource-intensive applications have created a critical need for high-performance data processing technologies. Modern information systems operating in big data environments require efficient The rapid development of information systems and the exponential growth of data volumes in resource-intensive applications have created a critical need for high-performance data processing technologies. Modern information systems operating in big data environments require efficient computational solutions to ensure high performance and scalability. Among contemporary approaches, the CUDA architecture developed by NVIDIA occupies a prominent place as a platform for implementing highly parallel computations on graphics processing units (GPUs). CUDA provides a programming model that enables the utilization of thousands of parallel threads, significantly increasing data processing performance compared to traditional CPU-oriented approaches. The memory hierarchy and thread management mechanisms allow optimization of data access, reduction of latency, and improvement of throughput, which are crucial for information systems dealing with large-scale datasets.

Sorting, as a fundamental data processing operation, is widely used in information systems, particularly in indexing, searching, and analytical data processing. Classical algorithms such as bubble sort, insertion sort, and quicksort are characterized by different computational complexities and performance levels. In particular, bubble sort has a complexity of $O(n^2)$ and is inefficient for large datasets, whereas algorithms with $O(n \log n)$ complexity are more suitable for practical applications. However, as data volumes increase, sequential implementations significantly decrease in performance. The use of GPUs helps overcome these limitations through massive parallelism, where data processing is performed simultaneously by many threads. To experimentally validate the effectiveness of the proposed approaches, a comparative analysis of sequential and parallel implementations of bitonic and bubble sort was conducted. Each experiment was performed ten times for different array sizes, and the average execution time was calculated. The results for bitonic sorting show a significant increase in efficiency of the GPU implementation with larger input data. For an array of size 2^{15} , execution time was 9.73 ms on the CPU and 3.82 ms on

the GPU. For size 2^{19} , these values were 412.75 ms and 14.04 ms, respectively, and for 2^{20} , 1012.52 ms and 21.75 ms. The largest tested array (2^{21}) showed times of 2262.45 ms on the CPU and 39.80 ms on the GPU. With increasing data size, speedup exceeds fifty times, indicating high scalability of GPU processing. Bubble sort shows a more complex performance pattern: for small arrays (2^{12}), the CPU may outperform due to parallelization overhead, but for 2^{15} speedup is $\sim 5\times$, and for 2^{16} , more than twelve times.

Among algorithms designed for parallel processing, bitonic sort demonstrates high efficiency due to its regular computational structure and the possibility of independent element processing. This makes it well-suited for high-performance information technologies. Efficiency in parallel environments depends not only on asymptotic complexity but also on the degree of parallelization and memory access patterns. The obtained results indicate that the efficiency of data processing technologies depends on both hardware features and algorithm choice. Bitonic sort, due to its structure, is more suitable for GPU implementation, whereas bubble sort remains limited due to high computational complexity. In conclusion, using CUDA in information systems opens significant opportunities for improving large-scale data processing. Future research should focus on memory optimization, adaptive parallel algorithms, and integrating GPU computing into modern information systems, contributing to efficient solutions of complex applied problems.

References:

1. Ala'anzy M. A., Tolendi N., Baubek B., Algarni A. Performance evaluation of GPU-based parallel sorting algorithms // PLOS ONE. – 2026. – Vol. 21, No. 2. – e0342167. – DOI: 10.1371/journal.pone.0342167.
2. Yazici A., Gokahmetoglu H. Implementation of sorting algorithms with CUDA: An empirical study // International Journal of Applied Methods in Electronics and Computers. – 2016. – DOI: 10.18100/ijamec.53457.

УДК 004

*Розбицький Р.Е., магістрант**Петросян Р.В., с.т. викладач**Державний університет «Житомирська політехніка»*

ПОРІВНЯЛЬНИЙ АНАЛІЗ JAVASCRIPT-РАНТАЙМІВ У МІКРОСЕРВІСНІЙ АРХІТЕКТУРІ

Порівняння JavaScript-рантаймів у контексті мікросервісної архітектури доцільно розглядати з позиції їхнього впливу на життєвий цикл сервісів, стабільність розподіленої системи, інтеграцію з інфраструктурою та експлуатаційні характеристики. У мікросервісній архітектурі середовище виконання прикладного коду виступає не лише технічним інструментом, а повноцінним елементом архітектури, який визначає швидкість запуску сервісів, ефективність обробки мережових запитів, споживання ресурсів контейнерів та можливості інтеграції зі засобами моніторингу, логування і трасування [1].

Найбільш поширеним і фактично стандартним середовищем виконання JavaScript для серверних мікросервісних систем залишається Node.js. Його основною перевагою у контексті розподілених backend-систем є висока зрілість платформи, стабільність API та наявність розвинутої екосистеми бібліотек і фреймворків, орієнтованих саме на побудову серверних застосунків. Для мікросервісної архітектури принципово важливою є передбачувана поведінка рантайму під навантаженням, а також сумісність із типовими інструментами контейнеризації, оркестрації, централізованого логування та розподіленого трасування, що у випадку Node.js забезпечується багаторічною практикою використання у промислових середовищах [2]. Асинхронна подієво-орієнтована модель виконання Node.js добре узгоджується з характером мережових мікросервісів, де значна частина часу витрачається на очікування відповідей від інших сервісів або зовнішніх ресурсів.

Разом з тим у контексті сучасних вимог до швидкості старту сервісів та ефективності використання ресурсів дедалі більшої уваги набувають альтернативні JavaScript-рантайми. Одним із таких середовищ є Deno, який орієнтований на усунення низки архітектурних обмежень, притаманних класичному підходу до виконання JavaScript на сервері. Для мікросервісної архітектури важливою особливістю Deno є вбудована модель безпеки, що передбачає явне надання дозволів на доступ до файлової системи, мережі та змінних середовища. Такий підхід потенційно дозволяє підвищити ізольованість окремих сервісів і зменшити ризики неконтрольованого доступу до ресурсів у розподілених середовищах [3]. Водночас у практичному застосуванні

для мікросервісних систем суттєвим обмеженням Depo залишається менша сумісність з існуючою серверною екосистемою та обмежена кількість бібліотек.

Окремий інтерес у контексті мікросервісної архітектури становить рантайм Bun, який позиціонується як високопродуктивне середовище виконання JavaScript і TypeScript із мінімальними накладними витратами. Для мікросервісних систем, що розгортаються у контейнеризованих середовищах і характеризуються частими перезапусками сервісів, важливою характеристикою є швидкість холодного старту та загальна швидкодія рантайму [4]. Саме у цих аспектах Bun демонструє відчутні переваги порівняно з класичним підходом, що може бути актуальним для допоміжних або високонавантажених сервісів. Однак у межах складних розподілених систем менша зрілість платформи та обмежений досвід експлуатації Bun у великих production-середовищах створюють додаткові ризики, пов'язані з довгостроковою стабільністю та підтримкою інфраструктурних інструментів.

У мікросервісній архітектурі вибір JavaScript-рантайму не може ґрунтуватися виключно на показниках продуктивності або швидкості запуску застосунків. Значно більшого значення набувають стабільність платформи, передбачуваність її поведінки у довготривалій експлуатації, наявність інструментів для централізованого логування, збору метрик і розподіленого трасування, а також сумісність із типовими процесами автоматизованого тестування та безперервного розгортання [5]. Саме ці характеристики визначають, наскільки безболісно конкретний рантайм може бути інтегрований у вже існуючу мікросервісну інфраструктуру.

Узагальнюючи результати порівняння, можна стверджувати, що Node.js на сьогодні залишається найбільш практичним і безпечним вибором для побудови промислових мікросервісних backend-систем завдяки своїй зрілості, екосистемі та широкій підтримці інфраструктурних інструментів.

Список використаної літератури:

1. Newman S. Building Microservices. 2nd ed. Sebastopol: O'Reilly Media, 2021. 352 с..
2. NGINX Inc. Microservices Reference Architecture: NGINX Whitepaper [Електронний ресурс]. 2021. Режим доступу: <https://www.nginx.com>
3. IBM Corporation. Microservices Guide 2023: Principles, Patterns, and Deployment Models [Електронний ресурс]. 2023. Режим доступу: <https://www.ibm.com/cloud/architecture>
4. Microsoft Azure Architecture Center. Microservices Architecture Style – Updated Best Practices 2022 [Електронний ресурс]. 2022. Режим доступу: <https://learn.microsoft.com/azure/architecture>
5. Dragoni N., Giallorenzo S., Lafuente A. L., et al. Microservices: Migration and Architectural Perspectives – 2020 Update. ACM Digital Library, 2020. DOI: 10.1145/3380768.3380775

УДК 004

*Татаренко Н. С, магістрант**Петросян Р. В., ст. викладач**Державний університет «Житомирська політехніка»*

АНАЛІЗ ВИКОРИСТАННЯ PROXMOX VE У СЕРЕДОВИЩІ HOMELAB НА СПОЖИВЧОМУ ОБЛАДНАННІ

Сучасні тенденції розвитку інформаційних технологій демонструють зростання популярності домашніх лабораторій (Homelab) як середовища для навчання, експериментів та самостійного хостингу сервісів [1]. У цьому контексті особливого значення набувають рішення для віртуалізації, які дозволяють ефективно використовувати обмежені апаратні ресурси. Одним із таких рішень є Proxmox Virtual Environment (Proxmox VE) – гіпервізор з відкритим кодом, який поєднує можливості віртуалізації та контейнеризації [2].

Homelab визначається як приватне ІТ-середовище, що створюється користувачем для розгортання серверів, мережевих сервісів та експериментів без ризиків для виробничих систем [3]. Згідно з сучасними дослідженнями, популярність домашніх лабораторій зростає завдяки розвитку DIY-культури, підвищенню попиту на самостійно розміщені сервіси та прагненню до цифрової автономії [4].

Однією з ключових причин поширення Proxmox VE є його відкритість та відсутність ліцензійних витрат, що вигідно відрізняє його від комерційних рішень, таких як VMware [1]. Платформа базується на Debian Linux та використовує KVM для віртуальних машин і LXC для контейнерів, що дозволяє досягати високої ефективності використання ресурсів [2].

Для оцінки придатності Proxmox VE до використання в умовах Homelab було розглянуто конфігурацію на базі споживчого обладнання: Dell OptiPlex 3080 SFF (Intel Core i5, 16 ГБ RAM, 256 ГБ SSD для системи та 512 ГБ SSD для зберігання даних). Аналіз показує, що навіть така базова конфігурація забезпечує достатню продуктивність для запуску кількох віртуальних машин або контейнерів одночасно. Наприклад, 16 ГБ оперативної пам'яті дозволяють ефективно розгортати:

- 2–3 повноцінні віртуальні машини, наприклад, сервери Linux або Windows;
- декілька LXC-контейнерів для легких сервісів: Docker, веб-сервери, бази даних тощо;
- інфраструктурні сервіси: DNS, VPN, NAS.

Важливою перевагою Proxmox VE є можливість гнучкого розподілу ресурсів, що дозволяє оптимізувати навантаження навіть на обмеженому обладнанні. Контейнеризація значно зменшує накладні витрати у порівнянні з традиційними віртуальними машинами, що особливо актуально для домашніх умов [1].

Згідно з офіційними вимогами Proxmox VE, платформа може ефективно працювати навіть на звичайному апаратному забезпеченні без необхідності використання серверних компонентів [5]. Це підтверджує доцільність використання таких систем, як Dell OptiPlex, у якості домашніх серверів.

У результаті проведеного аналізу можна зробити висновок, що Proxmox VE є ефективним та доцільним рішенням для використання на споживчому апаратному забезпеченні в умовах Homelab. Його переваги – відкритість, гнучкість, низькі системні вимоги та підтримка контейнеризації роблять його оптимальним вибором для базових і середніх сценаріїв використання.

Таким чином, навіть відносно недорогі системи, такі як Dell OptiPlex 3080 SFF, здатні забезпечити функціональність, близьку до корпоративних середовищ, що сприяє розвитку технічних навичок та підвищенню рівня цифрової автономії користувачів.

Список використаної літератури:

1. Lee B. Top Home Lab Trends in 2024. Virtualizationhowto. 01.03.2024. URL: <https://www.virtualizationhowto.com/2024/03/top-home-lab-trends-in-2024/> (дата звернення: 19.11.2025).
2. Proxmox Server Solutions GmbH. Introduction – Proxmox VE Wiki. URL: <https://pve.proxmox.com/wiki/Introduction> (дата звернення: 19.11.2025).
3. Stormagic. What Is a Homelab and Why Is It Important?. Stormagic. 22.05.2025. URL: <https://stormagic.com/company/blog/what-is-homelab/> (дата звернення: 19.11.2025).
4. Dhapte A. Homelab Market. Market Research Future. 01.10.2025. URL: <https://www.marketresearchfuture.com/reports/homelab-market-21555> (дата звернення: 19.11.2025).
5. Proxmox Server Solutions GmbH. Proxmox Virtual Environment Requirements. URL: <https://www.proxmox.com/en/products/proxmox-virtual-environment/requirements> (дата звернення: 19.11.2025).

УДК 621.3.049.77:004.85

*Васьківська Д.С., здобувач,
Доровська С.О., здобувач,
Глазок О.М., доцент*

Державний університет «Київський авіаційний інститут»

ЗАСТОСУВАННЯ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ У ПРОЄКТУВАННІ ІНТЕГРАЛЬНИХ СХЕМ

Зростання складності проектування інтегральних схем та швидкий розвиток машинного навчання зумовили пошук нових методів оптимізації автоматизації проектування електронних схем. Оскільки електронні схеми, при їх розгляді на рівні транзисторів, вентилів, з'єднань регістрів тощо, природним чином моделюються як графи, графові нейронні мережі (ГНМ) демонструють значний потенціал у вирішенні завдань автоматизації проектування, забезпеченні апаратної надійності та безпеки інтегральних електронних схем. Метою роботи є наукове обґрунтування доцільності впровадження ГНМ в інженерію інтегральних схем та визначення параметрів адаптації інструменту GNN4CIRCUITS для автоматизації перетворення схем у графові структури.

Для розв'язання поставлених задач авторами запропоновано використання відкритого інструментарію GNN4CIRCUITS як бази для побудови систем предиктивного аналізу. Наукова новизна полягає у визначенні оптимальних архітектур (GCN, GIN, PNA) для специфічних завдань класифікації вузлів у топологіях високої складності. ГНМ автоматично вивчають специфічні для конкретних завдань ознаки (ембединги) безпосередньо з графів схем. Базовий процес ГНМ полягає в агрегації ознак сусідніх вузлів, що у моделі графових згорткових мереж GCN описується наступною формулою:

$$Z^{(l)} = \sigma \left(\hat{D}^{-\frac{1}{2}} \hat{A} \hat{D}^{-\frac{1}{2}} Z^{(l-1)} W^{(l)} \right)$$

де $Z^{(l)}$ – матриця ембедингів вузлів на l -му рівні, $\hat{A}$ – матриця суміжності з доданими петлями (self-loops), $\hat{D}$ – відповідна їй матриця степенів, $W^{(l)}$ – матриця ваг, що навчається, а σ – нелінійна функція активації.

ГНМ можуть бути застосовані для оцінки затримок та прогнозування перевантаження маршрутизації. Вони дозволяють аналізувати топологію схеми для прогнозування її поведінки ще до завершення етапу фізичного дизайну.

Також використання ГНМ є доцільним для предиктивного аналізу деградації затримок, що відбувається через знос пристроїв, оскільки це дозволяє уникнути ресурсомісткого статичного часового аналізу (STA).

В той же час графові моделі сприяють локалізації дефектів та оцінці стійкості до збоїв [1].

В умовах глобалізації ланцюгів постачання та відсутності еталонної моделі, застосування ГНМ є перспективним методом аналізу апаратної безпеки та виявлення апаратних троянів [1]. Ці мережі також ефективні для аналізу вразливостей методів логічного блокування [2]. У роботі [3] запропоновано застосування ГНМ для аналізу апаратних структур з метою виявлення можливого порушення авторських прав на використані у них схемотехнічні рішення.

У межах даної роботи запропоновано використовувати відкритий інструмент GNN4CIRCUITS як технологічну основу для автоматизації перетворення схем (форматів Verilog або Bench) у графи. Авторами визначено, що підтримка моделей GCN, GIN та PNA дозволяє адаптувати цей інструмент для специфічних задач авіаційної електроніки та легко інтегрувати його в існуючі процеси проєктування.

Висновки

Проаналізовано та підтверджено високу ефективність ГНМ у моделюванні та дослідженні топологій інтегральних схем завдяки їх здатності працювати зі складними графовими структурами. Запропоновано методику інтеграції інструменту GNN4CIRCUITS у цикли проєктування EDA, що дозволяє автоматизувати підготовку даних для навчання моделей GCN та GIN. Визначено ключові технічні проблеми, зокрема масштабованість для схем з мільйонами елементів. Запропоновано шляхи їх подолання через апаратне прискорення мереж та оптимізацію матричних обчислень.

Список використаних джерел:

1. Graph Neural Networks for Integrated Circuit Design, Reliability, and Security: Survey and Tool / Z. El Sayed, Z. Wang, H. Selmani et al. *ACM Computing Surveys*. 2025. Vol. 58, no. 4. Art. 102.
2. Kipf T. N., Welling M. Semi-supervised classification with graph convolutional networks. *Proceedings of the 5th International Conference on Learning Representations (ICLR 2017)*. Toulon, France, 2017. DOI: 10.48550/arXiv.1609.02907.
3. GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection / L. Alrahis, H. Saleh, B. Mohammad et al. *Proceedings of the 58th ACM/IEEE Design Automation Conference (DAC)*. San Francisco, CA, USA, 2021. P. 1–6.

УДК 004.056

*Целуєв В.О., здобувач,
Савицький Р.С., аспірант, ст. викладач
Державний університет «Житомирська політехніка»*

МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ У ГЕЙМЕРСЬКИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Стрімкий розвиток ігрових соціальних мереж супроводжується накопиченням значних обсягів чутливих персональних даних користувачів, таких як ігрова статистика, платіжна інформація, геолокаційні дані, записи голосового та текстового чату. За даними звітів з кібербезпеки, ігрова індустрія входить до трійки найбільш атакованих секторів, що свідчить про критичну необхідність комплексного підходу до захисту персональних даних на таких платформах.

Аналіз існуючих ігрових платформ, таких як Steam, Discord, Battle.net, виявив типові вразливості, а саме зберігання паролів у незашифрованому вигляді, відсутність обмежень на кількість спроб входу, недостатній контроль доступу до API-ендпоінтів. На основі проведеного аналізу загроз за методологією STRIDE розроблено багаторівневу модель захисту персональних даних користувачів соціальної мережі для геймерів [1].

Перший рівень захисту реалізує шифрування даних у стані спокою за алгоритмом AES-256 та транспортне шифрування TLS 1.3 для всіх з'єднань між клієнтом і сервером. Паролі користувачів зберігаються виключно у вигляді хешів, отриманих алгоритмом bcrypt із коефіцієнтом складності 12, що унеможливує їх відновлення навіть у разі витоку бази даних [2].

Другий рівень забезпечує багатофакторну автентифікацію, яка реалізована як підтримка TOTP-кодів через застосунки Google Authenticator та Authy, апаратних ключів стандарту FIDO2/WebAuthn, а також адаптивна автентифікація з аналізом поведінкових патернів користувача. Система автоматично блокує обліковий запис після п'яти невдалих спроб входу та надсилає сповіщення власнику [3].

Третій рівень включає контроль доступу на основі ролей (RBAC) та атрибутів (ABAC) при зверненні мікросервісів до бази даних. Реалізація принцип мінімальних привілеїв надає перевагу в контролі. Кожен сервіс має доступ лише до тих таблиць і полів, які необхідні для виконання його функцій. Персональні дані псевдонімізуються перед передачею до аналітичних підсистем відповідно до вимог GDPR.

Для виявлення підозрілої активності впроваджено систему моніторингу на базі ELK Stack (Elasticsearch, Logstash, Kibana) з набором правил кореляції подій. Журнали аудиту всіх операцій із персональними даними зберігаються у незмінному сховищі протягом 90 днів. Час реакції системи на виявлену аномалію не перевищує 3 секунди, після чого автоматично ініціюється процедура блокування підозрілої сесії.

Тестування на проникнення варто проводити за методологією OWASP Testing Guide v4.2, щоб підтвердити відсутність критичних вразливостей класів SQL Injection, XSS та IDOR у реалізованій системі. Навантажувальне тестування показує стабільну роботу модуля автентифікації при одночасній обробці 5 000 запитів на секунду без деградації часу відповіді.

Окремої уваги заслуговує організація безпечного зберігання медіаконтенту користувачів, таких як аватари, знімки екрану та ігрові кліпи. Усі завантажені файли проходять перевірку сигнатур для виявлення замаскованих виконуваних файлів, зберігаються в ізольованому об'єктному сховищі S3-сумісного типу та доступні виключно через підписані тимчасові URL-посилання з терміном дії 15 хвилин, що унеможливорює несанкціонований прямий доступ до медіафайлів.

Запропонована багаторівнева модель захисту відповідає вимогам Загального регламенту захисту даних ЄС та Закону України «Про захист персональних даних» [4, 5]. Практична цінність роботи полягає у можливості адаптації розробленої архітектури для широкого класу соціальних платформ із великою кількістю користувачів. Подальші дослідження спрямовані на впровадження технологій виявлення аномалій на основі машинного навчання для проактивного захисту облікових записів від компрометації.

Список використаних джерел:

1. OWASP Top Ten 2023. Open Web Application Security Project. – URL: <https://owasp.org/Top10>.
2. Stallings W. Cryptography and Network Security. – Pearson, 2022. – 816 p.
3. Howard M., LeBlanc D. Writing Secure Code. – Microsoft Press, 2003. – 800 p.
4. Regulation (EU) 2016/679 (General Data Protection Regulation). – Official Journal of the EU, 2016.
5. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>.

УДК 004.738.5

*Целуєв В.О., здобувач,
Савицький Р.С., аспірант, ст. викладач
Державний університет «Житомирська політехніка»*

REAL-TIME КОМУНІКАЦІЯ У ІГРОВІЙ ПЛАТФОРМІ ЗАСОБАМИ WEBSOCKET

Сучасні ігрові соціальні мережі ставлять принципово нові вимоги до комунікаційної інфраструктури, а саме миттєва доставка повідомлень, сповіщення про ігрові події в реальному часі, одночасна підтримка десятків тисяч активних з'єднань. Традиційна модель HTTP-запитів за схемою «запит-відповідь» принципово не здатна задовольнити ці вимоги через надмірні накладні витрати на встановлення з'єднання та неможливість серверної ініціації передачі даних [1].

Порівняльний аналіз технологій real-time комунікації, таких як HTTP Long Polling, Server-Sent Events та WebSocket, засвідчив беззаперечну перевагу протоколу WebSocket (RFC 6455) для сценаріїв ігрової платформи [2]. WebSocket встановлює постійне повнодуплексне з'єднання між клієнтом і сервером поверх єдиного TCP-з'єднання, що забезпечує двосторонню передачу даних з мінімальними накладними витратами на рівні 2–10 байт на фрейм порівняно з кількома сотнями байт HTTP-заголовків [3].

Серверна частина запропонованого модуля реалізована на платформі Node.js з використанням бібліотеки Socket.IO версії 4.x, яка надбудовує над нативним WebSocket додатковий рівень абстракції. Існує автоматичний fallback до HTTP Long Polling для клієнтів без підтримки WebSocket, кімнати для групової адресації повідомлень та вбудований механізм повторного підключення з експоненційним відступом [4, 5].

Для горизонтального масштабування серверного кластера застосовується Redis Pub/Sub як розподілена шина повідомлень між вузлами. Кожен вузол Node.js підписується на канали Redis, що відповідають активним кімнатам чату, та ретранслює повідомлення підключеним до нього клієнтам. Така архітектура забезпечує прозору маршрутизацію повідомлень між користувачами, підключеними до різних вузлів кластера.

Розроблений модуль реалізує повний спектр комунікаційних сценаріїв ігрової платформи, зокрема особисті повідомлення між гравцями з підтвердженням доставки та прочитання, групові чати ігрових спільнот із підтримкою до 10 000 учасників, push-сповіщення

про ігрові, трансляція оновлень стрічки активності та індикація онлайн-статусу друзів у реальному часі.

Безпека з'єднань забезпечується обов'язковою JWT-автентифікацією при встановленні WebSocket-з'єднання, зокрема токен передається у параметрі запиту на апгрейд, перевіряється на сервері до прийняття з'єднання, а термін його дії обмежений 15 хвилинами з автоматичним оновленням через механізм refresh-токенів. Усі повідомлення передаються виключно через захищене з'єднання WebSocket Secure поверх TLS 1.3.

Вимірювання ключових метрик продуктивності проводилось за допомогою інструменту Artillery із симуляцією реалістичних сценаріїв навантаження. При 10 000 одночасних з'єднань на один вузол середня затримка доставки повідомлення становила 18 мс, 99-й перцентиль – 47 мс. Після горизонтального масштабування до трьох вузлів система стабільно обслуговує 30 000 активних підключень із пропускнуою здатністю до 85 000 повідомлень на секунду.

Реалізований модуль real-time комунікації демонструє ефективність протоколу WebSocket як основи для побудови комунікаційної інфраструктури геймерських платформ. Запропонована архітектура є масштабованою та може бути розширена для підтримки більших навантажень шляхом додавання нових вузлів до кластера без зміни програмного коду. Перспективним напрямом подальших досліджень є інтеграція протоколу WebRTC для організації голосового та відеозв'язку між гравцями безпосередньо в межах платформи.

Список використаних джерел:

1. Fette I., Melnikov A. The WebSocket Protocol. RFC 6455. – IETF, 2011. – URL: <https://www.rfc-editor.org/rfc/rfc6455>.
2. Grigorik I. High Performance Browser Networking. – O'Reilly Media, 2013. – 396 p.
3. Casciaro M., Mammino L. Node.js Design Patterns. – Packt Publishing, 2020. – 660 p.
4. Socket.IO Documentation. – URL: <https://socket.io/docs/v4/>.
5. Lubbers P., Albers B., Salim F. Pro HTML5 Programming. – Apress, 2011. – 308 p.

УДК 004.7

*Черниш М., здобувач,
Коротун О.В., к.пед.н., доцент
Державний університет «Житомирська політехніка»*

ОПИС МЕТОДІВ АДАПТИВНОГО КЕРУВАННЯ ПОВЕДІНКОЮ ШІ-АГЕНТІВ У ФАЙТИНГАХ

Сучасна індустрія відеоігор у жанрі файтинг стикається з проблемою створення інтелектуальних агентів (ворогів), які були б не лише складними для подолання, а й цікавими для гравця з точки зору стратегічної взаємодії. Опишемо методи адаптивного керування, що забезпечують еволюцію ШІ-агентів у реальному часі для підтримки динамічної складності.

Фундаментальною проблемою класичного ШІ у файтингах є статичність алгоритмів: після вивчення патернів поведінки ворога гравець швидко втрачає інтерес. Використання нейронних мереж, оптимізованих алгоритмом рою часток (Particle Swarm Optimization Neural Network, PSO-NN), пропонує розв'язання цієї проблеми через механізм безперервного навчання та стратегічної еволюції агента [1].

На відміну від класичних методів, алгоритм PSO дозволяє ефективно шукати оптимальні параметри поведінки в багатовимірному просторі ігрових станів, використовуючи механізм безперервного навчання. Система базується на гібридній архітектурі, де спеціальні шари пам'яті та механізми уваги фокусуються на найбільш значущих минулих діях опонента. Ключовою перевагою PSO-NN є здатність до динамічного коригування стратегії: ШІ ініціює перенавчання лише тоді, коли помічає суттєві зміни в тактиці гравця (понад 30%). Це створює ефект «живого» суперника, який адаптується до рівня майстерності людини, підтримуючи стан потоку та високу залученість гравця.

Альтернативним методом є імітаційне моделювання майбутніх станів на основі пошуку по дереву Монте-Карло (MCTS). Модифікація Puppet-Master MCTS використовує єдину структуру дерева для одночасного контролю обох персонажів, що дозволяє ШІ глибше прогнозувати контрзаходи опонента та діяти без попереднього навчання. Такий підхід забезпечує високу тактичну точність, оскільки агент розраховує тисячі можливих сценаріїв розвитку бою в межах кожного кадру, обираючи найбільш вигідну послідовність дій [2].

Ключовою новацією є впровадження «персон» – конкретних стилів бою (RushDown для ближнього бою, Zoning – для дистанційного), де система оцінює дії через призму обраного характеру. Агент у ролі RushDown отримує перевагу за скорочення дистанції та активний тиск,

тоді як Zoning-агент фокусується на утриманні суперника на безпечній відстані. Рулеткова селекція на етапі симуляції дозволяє III дотримуватися стилю бою, зберігаючи тактичну варіативність та «людянність» поведінки. Порівняння підходів наведено у таблиці 1.

Таблиця 1 – Порівняльна характеристика алгоритмів PSO-NN та PM-MCTS

Критерій порівняння	Еволюційний підхід (PSO-NN)	Пошук у дереві (PM-MCTS)
Основний механізм	Оптимізація ваг нейромережі роєм часток	Прогнозне моделювання станів (Look-ahead)
Потреба у навчанні	Висока (потребує ітерацій для еволюції)	Відсутня (працює в реальному часі)
Обчислювальні витрати	Низькі під час бою (швидкий інференс)	Високі (симуляція тисяч варіантів шокадру)
Тип адаптації	Глобальна (зміна стратегії під гравця)	Локальна (вибір найкращого удару зараз)
Вплив на геймплей	Динамічна складність	Реалізація впізнаваних стилів (персон)

На основі отриманих даних встановлено, що перехід від жорстко детермінованих скриптів до самовизначальних систем на основі PSO-NN дозволяє досягти високого рівня залученості гравця завдяки еволюції стратегій. Водночас використання PM-MCTS з рулетковою селекцією успішно інтегрує в поведінку агентів тактичні персони, урізноманітнюючи геймплей. Перспективним напрямком подальших досліджень є розробка гібридних архітектур, де PSO-NN відповідає за стратегічне планування, а MCTS – за тактичні рішення та дотримання стилістики персонажа для когнітивної конкуренції з людиною.

Список використаних джерел:

1. Imtiaz U., Mujtaba H. Adaptive AI for competitive gaming: particle-swarm-optimized neural network for skill, engagement, and strategic evolution. PeerJ Computer Science. 2025. Т. 11. С. е3347. URL: <https://doi.org/10.7717/peerj-cs.3347> (дата звернення: 02.03.2026).
2. Monte-Carlo Tree Search Implementation of Fighting Game AIs Having Personas / R. Ishii та ін. 2018 IEEE Conference on Computational Intelligence and Games (CIG), м. Maastricht, 14–17 серп. 2018 р. 2018. URL: <https://doi.org/10.1109/cig.2018.8490367> (дата звернення: 09.03.2026).

УДК 004.7

*Залозний О.А., здобувач,
Савіцький Р.С., аспірант, ст. викладач
Державний університет «Житомирська політехніка»*

ОРГАНІЗАЦІЯ ЗБЕРІГАННЯ ПОВІДОМЛЕНЬ, СПОВІЩЕНЬ ТА ДІЙ КОРИСТУВАЧІВ У ВЕБПЛАТФОРМІ АНІМЕ Й МАНГІ

Вебплатформи з активною взаємодією користувачів потребують ефективного зберігання різних типів комунікації та подій системи. Використання єдиної структури для повідомлень і системних сповіщень призводить до ускладнення обробки даних, зниження продуктивності та складності масштабування. Відсутність механізму фіксації дій користувачів ускладнює аналіз поведінки та контроль змін у системі. Додатково виникає проблема узгодженості даних при великій кількості одночасних запитів, що характерно для вебплатформ із високою активністю користувачів.

У вебзастосунках підсистеми комунікації реалізуються з урахуванням розділення типів взаємодії. Повідомлення між користувачами та системні сповіщення розглядаються як різні за призначенням сутності, що мають окремі структури зберігання та обробки. Повідомлення забезпечують двосторонню комунікацію та потребують збереження історії діалогів, тоді як сповіщення формуються системою та відображають події, пов'язані з активністю користувачів або змінами в системі.

У сучасних підходах до розробки вебзастосунків використовується розділення даних за функціональним призначенням та застосування ORM-інструментів для роботи з реляційними базами даних [1–3]. Також застосовується збереження історії дій користувачів у вигляді журналів подій, що дозволяє виконувати аналіз активності та забезпечувати контроль змін у системі.

Потрібно визначити підхід до організації зберігання повідомлень, сповіщень та історії дій користувачів у вебплатформі аніме й манги. Необхідно розмежувати типи комунікації, визначити структуру таблиць бази даних та забезпечити фіксацію активності користувачів із урахуванням можливості масштабування системи.

Повідомлення між користувачами мають двосторонній характер і використовуються для передачі текстової інформації. Вони містять ідентифікатори відправника та отримувача, текст повідомлення, часову мітку та статус прочитання. Зберігання повідомлень реалізується в

окремій таблиці, що забезпечує ведення історії переписки та ефективну обробку діалогів.

Системні сповіщення призначені для інформування користувачів про події платформи. Вони формуються автоматично та мають односторонній характер. Сповіщення містять тип події, ідентифікатор користувача, посилання на пов'язаний об'єкт та статус прочитання. Використання окремої таблиці дозволяє оптимізувати обробку подій та спростити реалізацію відповідної функціональності.

Розділення повідомлень і сповіщень на різні сутності дозволяє уникнути змішування різнорідних даних, зменшити складність запитів та забезпечити гнучкість архітектури системи.

Для фіксації активності користувачів використовується таблиця історії дій, яка містить тип дії, ідентифікатор користувача, пов'язаний об'єкт та часову мітку. Збереження історії дій дозволяє виконувати аналіз поведінки користувачів та забезпечувати контроль змін у системі.

При реалізації історії дій доцільно враховувати обсяг даних, що накопичуються. Для цього може застосовуватися архівація або обмеження глибини збереження історії. Також можливе використання окремих механізмів обробки подій, що дозволить зменшити навантаження на основну базу даних.

Реалізація здійснюється із використанням фреймворку Next.js, який забезпечує інтеграцію клієнтської та серверної частин застосунку [1]. Для взаємодії з базою даних використовується Prisma ORM, що забезпечує типобезпечні запити [2]. Зберігання даних реалізовано у PostgreSQL, що підтримує складні зв'язки між сутностями [3].

Розмежування повідомлень, сповіщень та історії дій користувачів забезпечує структуроване зберігання даних, спрощує обробку запитів та підвищує ефективність роботи вебплатформи.

Список використаних джерел:

1. Next.js Documentation. URL: <https://nextjs.org/docs> (дата звернення: 02.03.2026)
2. Prisma ORM Documentation. URL: <https://www.prisma.io/docs> (дата звернення: 02.03.2026)
3. PostgreSQL Documentation. URL: <https://www.postgresql.org/docs> (дата звернення: 02.03.2026)

УДК 519.8: 004.9

*Безкоровайний В. В., д. т. н, професор,
Сирятський В. В., здобувач
Харківська гуманітарно-педагогічна академія*

МОДЕЛЮВАННЯ ПРОЦЕСУ БАГАТОКРИТЕРІАЛЬНОГО ОЦІНЮВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОЇ ОСВІТИ

Розвиток інформаційно-комунікаційних технологій і впровадження технологій дистанційного навчання в закладах освіти потребує відповідних змін у складі програмного забезпечення (ПЗ) [1]. Для оцінювання якості ПЗ використовується множина різномірних показників: функціональність, надійність, зручність використання і супроводу, портативність, вартість ліцензії тощо.

Розглядається задача вибору найкращого комплексу програмних засобів у такій постановці. Задані: множина завдань для забезпечення технології навчання $i = \overline{1, I}$; множина програмних засобів для реалізації завдань $j = \overline{1, J}$; якість кожного з засобів оцінюється за множиною часткових критеріїв $k_l, l = \overline{1, L}$. Необхідно обрати комплекс ПЗ, найбільш ефективних для реалізації всієї множини завдань навчального процесу.

В створюваній моделі використаємо такі позначення: $r = [r_{ij}]$ – булева матриця ($r_{ij} = 1$, якщо засіб j здатен реалізувати завдання i , $r_{ij} = 0$ – в іншому випадку); $x(r) = [x_j(r)]$ – булевий вектор ($x_j(r) = 1$, якщо засіб j включається до комплексу, $x_j(r) = 0$ – в іншому випадку).

Для вибору найкращого комплексу з ефективних ПЗ скористаємось його оцінкою на основі теорії корисності. У рамках цієї теорії можна визначити узагальнену скалярну оцінку якості кожного з альтернативних комплексів ПЗ з множини допустимих $X \in$ за всією множиною показників $P(x)$, значення якої визначають їх упорядкування за цінністю [2–3]. При цьому, для всіх комплексів $\forall x, y \in X$ виконуються умови:

$$P[x(r)] = P[y(r)] \leftrightarrow x(r) \boxtimes y(r), \quad (1)$$

$$P[x(r)] > P[y(r)] \leftrightarrow x(r) \boxtimes y(r), \quad (2)$$

$$P[x(r)] \geq P[y(r)] \leftrightarrow x(r) \succcurlyeq y(r). \quad (3)$$

З урахуванням цього математичну модель задачі вибору найкращого комплексу ПЗ пропонується подати у такій формі:

$$x^0 = \arg \max_x \sum_{l=1}^L \lambda_l \xi_l[x(r)] \rightarrow \max_{x(r) \in X}, \quad (4)$$

$$\forall i = \overline{1, I} : \sum_{j=1}^J r_{ij} \geq 1, \quad (5)$$

$$\xi_l[x(r)] \equiv \xi_l(x) = \{[k_l(x) - k_l^-(x)] / [k_l^+(x) - k_l^-(x)]\}^{\alpha_l}, \quad (6)$$

де λ_l – ваговий коефіцієнт локального критерію, $\lambda_l \geq 0$, $\sum_{l=1}^L \lambda_l = 1$; $\xi_l[x(r)]$, $k_l^-(x)$, $k_l^+(x)$ – значення функції корисності локального критерію для комплексу x , його найгірше та найкраще значення; α_l – параметр, який визначає вид залежності $\xi_l(x)$ (лінійна, випукла вгору чи донизу).

Обмеження (5) гарантує покриття всієї множини завдань і допускає використання декількох засобів для розв’язання однієї задачі.

Запропонована математична модель (4) – (6) дозволяє здійснювати скалярне оцінювання $P(x)$, упорядкування (1) – (3) і вибір найкращого комплексу ПЗ з множини допустимих $x(r) \in X$ за множиною функціональних і витратних показників їх якості.

Список використаних джерел:

1. Твердохліб І. Організаційно-педагогічне та програмно-технічне забезпечення дистанційного навчання в умовах воєнного стану. Український педагогічний журнал. 2022. №2. С 116–124.
2. Beskorovainyi V. V., Petryshyn L. B., Shevchenko O. Yu. Specific subset effective option in technology design decisions. Applied Aspects of Information Technology. 2020. Vol. 3. No.1. P. 443–455. URL: <https://aait.op.edu.ua/?fetch=articles&with=info&id=40>. (дата звернення: 19.03.2026).
3. Beskorovainyi V. Combined method of ranking options in project decision support systems. Innovative Technologies and Scientific Solutions for Industries. 2020. No 4 (14). P. 13–20. URL: <http://journals.uran.ua/itssi/article/view/ITSSI.2020.14.013> (дата звернення: 19.03.2026).

УДК 004.9:159.9

О. І. Вербіцький, здобувач

Національний університет «Київський авіаційний інститут»

КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ "ПСИХОЛОГ ОНЛАЙН"

В умовах воєнного стану в Україні проблема психологічного здоров'я населення набула критичного значення. Дослідження українських вчених фіксують суттєво підвищений рівень депресії, тривожності, безсоння та ПТСР серед населення країни [1], що обумовлює зростаючу потребу у доступних інструментах психологічної підтримки. На жаль, більшість людей не звертаються до фахівців через фінансові причини, суспільну стигматизацію психологічної допомоги, або через відсутність доступних сервісів у своєму регіоні. Саме тому розробка комплексної інформаційної системи психологічної підтримки є актуальною та практично значущою задачею. Цифрові платформи психологічної допомоги здатні суттєво розширити доступ населення до послуг психологічної підтримки для, знижуючи бар'єри стигматизації та географічної віддаленості [2].

Проведений аналіз виявив кілька основних платформ психологічної допомоги в Україні, кожна з яких має суттєві обмеження у функціональності. Жоден із розглянутих сервісів не має вбудованого AI-чатботу для миттєвої цілодобової підтримки, не поєднує модуль самодіагностики з валідованими методиками та автоматичною інтерпретацією результатів, не має відеобібліотеки з персоналізованими рекомендаціями на основі тестів, не відстежує динаміку психологічного стану користувача у часі, не має автоматичного скерування до фахівця у кризових ситуаціях, не інтегрує результати тестів із підбором спеціаліста та відеоматеріалів в єдиному процесі, а також не поєднує одночасно повну анонімність, безкоштовний доступ, мобільний додаток та відеоконсультації з фахівцем в єдиній системі.

На основі виявлених недоліків запропоновано інформаційну систему що реалізується у вигляді вебсайту та мобільного додатку для Android і iOS і містить чотири ключові модулі.

AI-чатбот психологічної підтримки забезпечує цілодобову первинну психологічну підтримку без очікування на живого спеціаліста, аналізує емоційний стан користувача на основі його повідомлень, пропонує персоналізовані техніки саморегуляції такі як дихальні вправи та медитації, а у разі виявлення критичного стану автоматично скерує користувача до живого фахівця.

Ефективність AI-чатботів для зниження симптомів депресії та тривожності підтверджена систематичним оглядом та мета-аналізом рандомізованих контрольованих досліджень [3]. Впровадження AI-чатбота є головною відмінністю запропонованої системи від усіх існуючих українських платформ.

Онлайн-консультації з психологом реалізовані через власну вбудовану платформу відеозв'язку без необхідності переходу у зовнішні месенджери.

Система забезпечує зручний підбір спеціаліста за напрямком, мовою та зручним часом, автоматичні нагадування про заплановані сесії, можливість анонімних консультацій для захисту персональних даних, а також передачу результатів діагностики психологу перед сесією.

Модуль тестів та самодіагностики включає валідовані психологічні методики зокрема тест Бека на депресію та шкалу тривожності Гамільтона. Система автоматично інтерпретує результати та надає персоналізовані рекомендації. Користувач може відстежувати динаміку свого психологічного стану у часі через графіки та аналітику в особистому кабінеті, а також вести структурований щоденник настрою між сесіями.

Відеобібліотека є унікальним компонентом, якого не має жоден із проаналізованих конкурентів. Вона містить структуровану базу навчальних відео з психології та самопомоги за тематичними категоріями – тривожність, стрес, стосунки та горювання.

Список використаних джерел:

1. Kurapov A., Balashevych O., Borodko Y., Vovk Y., Borozenets A., Danyliuk I. Psychological wellbeing of Ukrainian civilians: a data report on the impact of traumatic events on mental health. // *Frontiers in Psychology*. 2025. Vol. 16. Article 1553555. DOI: 10.3389/fpsyg.2025.1553555.
2. Frankova I., Sijbrandij M. Preventing common mental health problems in war-affected populations: the role of digital interventions. // *Frontiers in Digital Health*. 2025. Vol. 7. Article 1586030. DOI: 10.3389/fdgh.2025.1586030.
3. Zhang Y. et al. Efficacy of generative AI chatbots in improving mental health: a systematic review and meta-analysis of randomized controlled trials. // *Journal of Medical Internet Research*. 2025. DOI: 10.2196/78238.

УДК 004.7

*Кузнєцов Д.О, магістрант,
Євланов М.В, д.т.н, професор
«Харківський національний університет радіоелектроніки»*

УПРАВЛІННЯ БІЗНЕС-ВИМОГАМИ ЯК КЛЮЧОВИЙ ФАКТОР УСПІШНОСТІ ПРОЕКТІВ: МЕТОДИЧНИЙ АСПЕКТ

У сучасному середовищі управління проектами роль бізнес-аналітика набуває дедалі більшої стратегічної ваги. Бізнес-аналіз розглядається як критична управлінська компетенція на рівні проектів, програм і портфелів, оскільки фахівці цього напрямку забезпечують якість вимог, залучають стейкхолдерів та сприяють досягненню успішних результатів. Особливістю ролі бізнес-аналітика є її наскрізний характер у межах проектного життєвого циклу: він включається в роботу ще до офіційного старту проекту, формуючи бізнес-кейс і проводячи аналіз потреб організації вже на етапі ініціації. ЦентRALЬНОЮ функцією протягом усього циклу залишається робота з вимогами - їх збір, узгодження із стейкхолдерами, фіксація та своєчасна передача відповідальним сторонам. Проекти нерідко стикаються з труднощами не через брак технічної експертизи, а саме через неналежне управління вимогами - неповноту, неузгодженість або несвоєчасну ескалацію проблем. Таким чином, бізнес-аналітик супроводжує проект від ініціації до передачі в підтримку, виступаючи гарантом узгодженості між бізнес-потребами та кінцевим рішенням, що і визначає актуальність дослідження управління бізнес-вимогами як ключового фактору успішності проектів.

Практика управління проектами підтверджує дію принципу Парето: близько 20% недостатньо опрацьованих або некоректно сформульованих бізнес-вимог стають причиною 80% проектних проблем - від технічних багів і регресій до критичних змін у скоупі, зривів дедлайнів і конфліктів між стейкхолдерами. Саме вимоги є тим фундаментом, на якому будується вся архітектура рішення, тому прогалини на цьому етапі мають мультиплікативний ефект: вони проявляються не одразу, а накопичуються і вибухають на пізніх фазах проекту - під час тестування, інтеграцій або масштабування. Серед типових проблем, що виникають унаслідок неякісних вимог, виділяють: розмитість або суперечливість формулювань, відсутність критеріїв прийнятності, неврахування сценаріїв інтеграції із суміжними системами, ігнорування нефункціональних вимог до продуктивності та безпеки, а також недостатнє залучення ключових стейкхолдерів на етапі

збору. Кожна з цих прогалин у подальшому трансформується у дорогі зміни, технічний борг або повторне проектування процесів.

Для мінімізації цих ризиків сучасний бізнес-аналітик застосовує комплекс взаємопов'язаних методів і практик управління вимогами впродовж усього проектного циклу. На операційному рівні це передусім регулярні грумінги беклогу - сесії уточнення і пріоритизації вимог разом із командою та замовником, які дозволяють виявляти протиріччя до початку розробки. Ретроспективи забезпечують зворотний зв'язок і дають змогу коригувати підходи до збору вимог між ітераціями. Канбан-дошки слугують інструментом візуалізації статусу вимог і прозорого відстеження їх реалізації, а також дозволяють своєчасно ідентифікувати блокери та ескалювати їх відповідальним особам. Паралельно, ще до передачі вимог у розробку, бізнес-аналітик бере участь у підготовці тест-кейсів - статичному тестуванні специфікацій, що є одним із найефективніших способів виявити неповноту або некоректність вимог на ранньому етапі. У критичних ситуаціях - при виявленні конфлікту вимог, зміні скоупу або ризику зриву термінів - застосовується структурована ескалація: чітке документування проблеми, визначення її впливу та передача на відповідний рівень прийняття рішень із запропонованими варіантами вирішення.

Таким чином, управління бізнес-вимогами є не допоміжною, а системоутворювальною функцією в проектному менеджменті. Якість вимог безпосередньо визначає якість кінцевого продукту, стабільність процесів і здатність організації до масштабування та інтеграції нових рішень. Бізнес-аналітик, який методично збирає, верифікує, пріоритизує та супроводжує вимоги через увесь життєвий цикл проекту, стає ключовою ланкою між бізнесом і командою реалізації. Саме тому дослідження управління бізнес-вимогами як ключового фактору успішності проектів є актуальним і практично значущим завданням для сучасного проектного менеджменту.

Список використаних джерел:

1. International Institute of Business Analysis. *A Guide to the Business Analysis Body of Knowledge (BABOK® Guide)*. Version 3.0. Toronto: IIBA, 2015. 514 p.
2. Project Management Institute. *Business Analysis for Practitioners: A Practice Guide*. Newtown Square, PA: PMI, 2015. 178 p. (Дата звернення: 25.03.2026)

UDC 004.9

***Pushkar Anton, Postgraduate Student,
Yahup Kateryna, D.Sc., Professor,
Kopp Andrii, Ph.D., Associate Professor
National Technical University «Kharkiv Polytechnic Institute»***

TOWARDS ML-DRIVEN ARCHITECTURAL SOLUTION FOR PREVENTING MALICIOUS SQL TRANSACTIONS

SQL injections are the most common vulnerabilities in information systems. They arise from improper handling of input data and errors in the construction of SQL transactions. According to [1], this category of attacks consistently ranks among the most prevalent, accounting for approximately 18.01% of all vulnerabilities. The consequences of SQL injections extend beyond individual services and affect the system architecture as a whole. The integrity of processes is compromised, risks of vulnerability propagation arise, and threats of non-compliance with security standards such as GDPR or ISO/IEC 27001 increase [2]. Existing approaches are often based on static rules and do not account for complex attack patterns. The goal of this study is to develop an architectural approach to prevent malicious SQL transactions based on machine learning methods.

The proposed concept involves integrating an intelligent SQL transaction monitoring tool into the overall architecture of the information system. The tool functions as an intermediary component between the application layer and the database. It analyzes all SQL queries before they are executed. Its main function is to detect potentially harmful transactions and block them.

Architecturally, the proposed system consists of a data collection module, a processing module, and a decision-making module (Fig. 1). This system receives SQL transactions along with their execution context as input. This is followed by preprocessing, which includes SQL code normalization, feature extraction, and conversion into a vector-based format suitable for machine learning. Features may include query structure, the presence of suspicious patterns, string length, and the frequency of key operators.

A key component of the proposed architectural approach (Fig. 1) is a set of machine learning algorithms that classify SQL transactions. The following machine learning algorithms are considered: Single-Layer Perceptron (SLP), Logistic Regression, k-Nearest Neighbors (k-NN), Support Vector Machine (SVM), Naive Bayes, and Decision Trees. Each algorithm should be trained on historical data containing both legitimate and malicious SQL transactions. The result of the analysis is planned as a probabilistic assessment of whether a transaction is malicious.

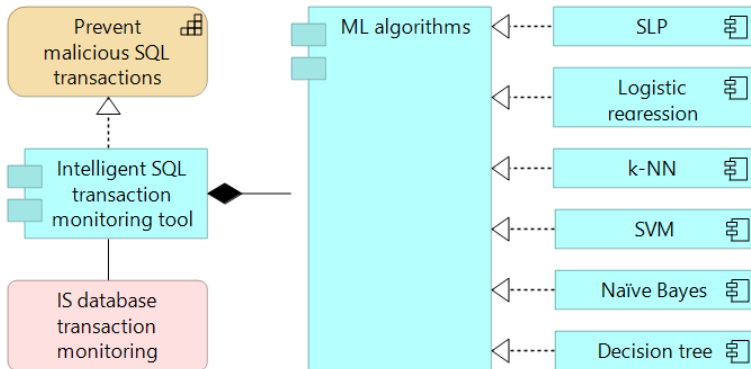


Fig. 1. ML-driven tool for preventing malicious SQL transactions

The formalization of this approach involves an SQL transaction as a feature vector and applying a classification function that maps this vector to a binary decision: to commit or rollback a transaction. To improve accuracy, an ensemble approach can be used, in which the results of multiple algorithms are aggregated. The final decision is made based on a threshold value.

Integrating this tool into the information system ensures continuous monitoring of SQL transactions. This makes possible to detect attacks at an early stage and reduce the risk of vulnerabilities spreading across system components. The proposed architecture (Fig. 1) allows for scalability and adaptation to the new types of attacks through model retraining.

References:

1. Mustapha A. A., Udeh A. S., Ashi T. A., Sobowale O. S. Comprehensive review of machine learning models for SQL injection detection in e-commerce // World Journal of Advanced Research and Reviews. 2024. Vol. 23, No. 1. DOI: <https://doi.org/10.30574/wjarr.2024.23.1.2004>
2. Imtiaz M. A., Ahmed M. Z., Khalid F. et al. Data exploration with SQL: A machine learning based end-to-end prediction and data security framework for the detection of attack in emerging cloud computing databases and integrated paradigms: analysis on taxonomy, challenges, and opportunities // Sustainable Engineering and Smart Technologies Journal. 2025. URL: <https://www.sesjournal.com/index.php/1/article/download/155/149>.

УДК330.4:004.8

Осауленко І. А., д.т.н., доцент

*Черкаський національний університет імені Богдана
Хмельницького*

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ АНАЛІТИЧНИХ ПРОЄКТІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Безпрецедентні виклики, з якими зіткнулась Україна внаслідок повномасштабної агресії, серед іншого значно ускладнили процеси прийняття рішень як у державному, так і в корпоративному секторі. Безпосередні безпекові ризики, перебої з енергопостачанням, порушення логістичних маршрутів, міграція населення та інші пов'язані чинники зумовлюють стабільно високий рівень невизначеності більшості соціально-економічних параметрів і впливають на різні аспекти поведінки людей. За таких умов для аналітиків важливо постійно відслідковувати актуальні дані та мати належний інструментарій для моделювання різних сценаріїв, побудови коротко і середньострокових прогнозів.

Основний фокус аналітичних проєктів у сфері бізнесу безумовно зосереджений на питаннях дослідження попиту на продукцію або послуги і виявлення наявних на відповідному ринку тенденцій. Одним із базових завдань є групування клієнтів за характерними ознаками, що реалізується за допомогою кластерного аналізу. Отримані результати дозволяють за допомогою інструментів штучного інтелекту розробляти рекламу, адресовану конкретній цільовій аудиторії, а при детальнішому аналізі створювати персоналізовані пропозиції навіть для кожного клієнта. Великі та середні компанії почали активно впроваджувати цифрових онлайн-консультантів з елементами штучного інтелекту. Водночас дуже важливо постійно відслідковувати динаміку, щоб не випустити з поля зору прояви аномальної поведінки споживачів, які можуть призвести до зменшення клієнтської бази в найближчому майбутньому [1]. Очевидно, виявлення таких відхилень може бути покладене на відповідним чином налаштованого ШІ-асистента.

Інший пов'язаний напрям стосується підвищення рівня впізнаваності бренду. Основним об'єктом аналізу при цьому виступає вебсайт виробника або надавача послуг. Підхід, відомий як SEO-аналітика, передбачає виявлення недоліків у внутрішній організації сайтів і визначення необхідних кроків для покращення видимості та підвищення рейтингів відповідних ресурсів у пошукових системах. Проєкт може передбачати створення і використання ШІ-інструментів для вирішення комплексу завдань, таких як збирання даних за допомогою API і їхнє оброблення, аналіз розміщеного на сайті тексту і

ключових слів, аналіз наявних посилань і формування рекомендацій [2]. Загалом відповідні інструменти можуть використовуватись у значно ширшому контексті аналізу різних інформаційних ресурсів із застосуванням методів штучного інтелекту, що в перспективі стане важливим чинником вироблення і прийняття стратегічних рішень у різних сферах.

Попередній рік фактично ознаменувався початком активного впровадження ШІ-інструментів в державне управління. Серед перспективних напрямів відзначають експертизу вітчизняних нормативно-правових актів, переклад європейського законодавства, прогнозування суспільних проблем. Прикладом аналітичного проекту загальнонаціонального масштабу може бути дослідження ринку праці. Мають бути охоплені поточні дані державної статистики і служби зайнятості, галузеві прогнози, спеціалізовані інтернет-ресурси, врахована очікувана кількість випускників закладів вищої і професійної освіти. У найближчому майбутньому очікується поява регламентів щодо автоматизованого прийняття урядових рішень [3].

Серед визначених державою пріоритетів також впровадження ШІ-технологій в медицину для аналізу даних про стан здоров'я і персоналізації рекомендацій, інтеграція з біотехнологіями [4].

Список використаних джерел:

1. Солодков Н. Є., Гришко Н. Є. Інтеграція штучного інтелекту та бізнес-аналітики для підтримки прийняття управлінських рішень підприємствами в умовах обмеженості ресурсів. Економічний простір. 2025. №198. С. 115–122.
2. Горбань Г. В., Кандиба І. О. Раленко В. С., Стоєв Є. Д. Використання штучного інтелекту в системі seo-аналітики вебсайтів. Таврійський науковий вісник. Серія: Технічні науки. 2024. Вип. 1. С. 36–46.
3. Фурашев В. М., Корж І. Ф. Штучний інтелект та адміністративна (контрольна) діяльність публічної влади: європейський погляд. Інформатика і право, 2025. №1(52). С. 51–61.
4. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025 – 2027 роках: Розпорядження Кабінету Міністрів України від 31.12.2024 р. № 1351-р. із змінами, внесеними згідно з розпорядженням КМ № 704-р від 14.07.2025. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-p#Text> (дата звернення: 24.03.2026).

УДК 004.7

**Васянович О.А., здобувач,
Морозов А.В., к.т.н., доцент**
Державний університет «Житомирська політехніка»

АРХІТЕКТУРА РЕКОМЕНДАЦІЙНИХ СИСТЕМ В УМОВАХ ВІДСУТНОСТІ СТАТИСТИКИ ВЗАЄМОДІЙ

Базовою проблемою інформаційних платформ, орієнтованих на розміщення нового користувацького контенту, є неможливість його початкового ранжування. Традиційні алгоритми рекомендацій, побудовані на методах колаборативної фільтрації, вимагають накопиченої історії взаємодій користувачів з об'єктом (кількість переглядів, прослуховувань, додавань до обраного). Щойно завантажений медіафайл не має такої статистики, тому алгоритм не здатний рекомендувати його цільовій аудиторії. Цей стан системи визначається як проблема «холодного старту» [1].

Для забезпечення просування нових публікацій під час розробки інформаційної системи організації прослуховування аудіоконтенту (проект «IndieStream») реалізовано контентно-орієнтовану архітектуру рекомендацій (content-based filtering) [2]. Алгоритм базується на аналізі внутрішніх метаданих самого об'єкта, що дозволяє формувати видачу незалежно від поведінки користувачів.

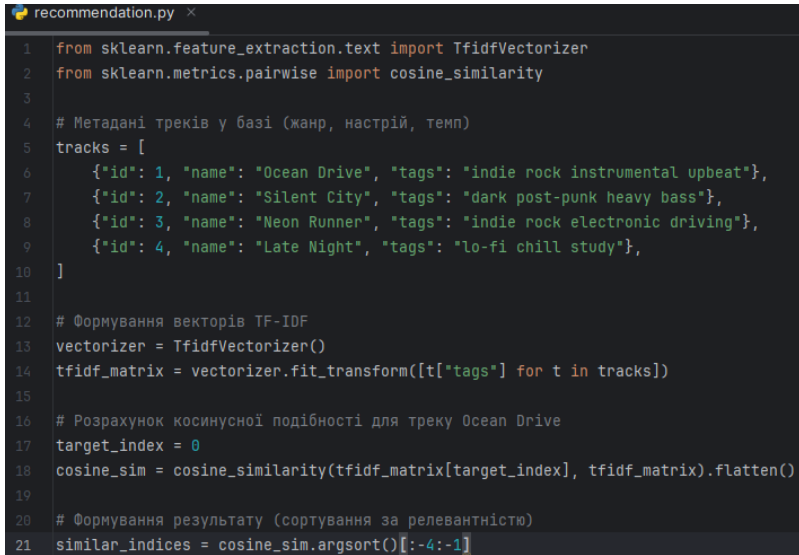
Під час завантаження аудіотреку в базу даних система фіксує його текстові характеристики: жанр, настрій, темп та інструментальні теги. Для обчислення релевантності між поточним треком та іншими записами ці характеристики перетворюються на багатовимірні числові вектори за допомогою алгоритму TF-IDF (Term Frequency-Inverse Document Frequency) [3].

Пошук подібних композицій здійснюється через розрахунок косинусної подібності між вектором цільового треку A та векторами інших записів B . Математична модель розрахунку має вигляд:

$$\text{sim}(A, B) = \cos(\theta) = \frac{A \cdot B}{\|A\| \|B\|} = \frac{\sum_{i=1}^n A_i B_i}{\sqrt{\sum_{i=1}^n A_i^2} \sqrt{\sum_{i=1}^n B_i^2}}$$

Значення функції наближається до одиниці за умови високого збігу векторних характеристик композицій.

На програмному рівні цю архітектуру імплементовано мовою Python з використанням математичної бібліотеки scikit-learn. При запиті до сторінки конкретного треку бекенд динамічно обчислює матрицю подібності для тегів і формує JSON-відповідь із вибіркою композицій, що мають найвищий коефіцієнт збігу.



```

1 from sklearn.feature_extraction.text import TfidfVectorizer
2 from sklearn.metrics.pairwise import cosine_similarity
3
4 # Метадані треків у базі (жанр, настрій, темп)
5 tracks = [
6     {"id": 1, "name": "Ocean Drive", "tags": "indie rock instrumental upbeat"},
7     {"id": 2, "name": "Silent City", "tags": "dark post-punk heavy bass"},
8     {"id": 3, "name": "Neon Runner", "tags": "indie rock electronic driving"},
9     {"id": 4, "name": "Late Night", "tags": "lo-fi chill study"},
10 ]
11
12 # Формування векторів TF-IDF
13 vectorizer = TfidfVectorizer()
14 tfidf_matrix = vectorizer.fit_transform([t["tags"] for t in tracks])
15
16 # Розрахунок косинусної подібності для треку Ocean Drive
17 target_index = 0
18 cosine_sim = cosine_similarity(tfidf_matrix[target_index], tfidf_matrix).flatten()
19
20 # Формування результату (сортування за релевантністю)
21 similar_indices = cosine_sim.argsort()[::-1]

```

Рис. 1. Реалізація косинусної подібності на стороні бекенду.

Впровадження контентно-орієнтованого алгоритму з розрахунком векторної подібності вирішує проблему «холодного старту». Архітектура забезпечує авторам отримання органічного трафіку відразу після публікації матеріалу в інформаційній системі, спираючись виключно на початкові характеристики контенту.

Список використаних джерел:

1. Isinkaye F. O., Folocunso Y. O., Ojokoh B. A. Recommendation systems: Principles, methods and evaluation. Egyptian Informatics Journal. 2015. Vol. 16, P. 261-273. URL: <https://doi.org/10.1016/j.eij.2015.06.005> (дата звернення: 23.03.2026).
2. Pengshi Alvin. Content-Based Recommender for E-Commerce Web Store. Towards Data Science. 2020. URL: <https://towardsdatascience.com/a-content-based-recommender-for-e-commerce-web-store-7554b5b73eac> (дата звернення: 23.03.2026).
3. Офіційна документація бібліотеки scikit-learn. URL: <https://scikit-learn.org/> (дата звернення: 23.03.2026).

UDC 004.65:655.3

Tetyana Neroda, professor,
Institute of Printing Art and Media Technologies in Lviv Polytechnic

DETERMINING PRIORITY FACTORS FOR PRINTING ORDER EXECUTION THROUGH BIG DATA PREDICTIVE ANALYTICS

The traditional printing industry is historically based on mass production principles, where economic viability is achieved through high-volume runs and extended pre-press cycles. Major printing enterprises focus on process stability and systematic capacity utilization to minimize unit costs through economies of scale. However, the modern market demands personalization and rapid turnaround, which has driven the development of on-demand printing networks [1].

Unlike traditional enterprises, the print-on-demand segment operates under conditions of high uncertainty regarding order volumes and specifications, which arrive in a continuous stream. Such production organization shifts the focus from the mechanical reproduction of identical copies to the management of agile workflows. Every operation in digital printing generates a significant volume of digital footprints: from input file parameters and user metadata to equipment logs and real-time energy consumption. The accumulation of these disparate data arrays forms a specific Big Data environment that, within rapid-response printing, encompasses the entire order lifecycle: from the moment of online cost estimation to the delivery of the finished print run. [2]. Static price lists fail to allow for an agile response to critical print queue overloads or, conversely, to equipment downtime during low-productivity hours. Therefore, there is a pressing need to rethink dynamic pricing mechanisms as a tool for automated demand regulation through cost. Such mechanisms must be based on the analysis of Big Data regarding current network load and the prioritization of lead times.

The collection and structuring of data arrays to determine order execution priority begins with Customer Relationship Management systems. These systems maintain a comprehensive communication history and record the primary input flow of requests, customer parameters, and the history of their interaction with the rapid-response printing network (Fig.1). It is precisely this data that enables the identification of consumer behavior patterns and seasonal demand fluctuations. The next level involves the integration of technical metrics from Raster Image Processors, which provide precise data on the resource intensity of layouts, alongside inventory management systems that reflect the real-time availability of consumables.

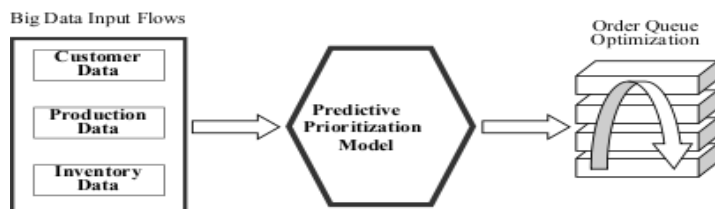


Figure 1. Generation of order execution priority based on multivariate data analysis

The comprehensive results derived from the analysis of these extensive Big Data arrays facilitate the construction of sophisticated predictive models for optimal distribution and scheduling of production queues, meticulously accounting for a complex set of deterministic factors. In this specific context, determination of order execution priority is fundamentally based on continuous, real-time synchronization of required lead times with current production line utilization and the immediate availability of necessary substrates and consumables. Should the data analysis indicate a critical deficit in available machine time or processing capacity, the system is designed to automatically identify and isolate orders possessing the highest importance coefficients. This automated intervention is crucial for maintaining the overall stability of technological cycle and preventing systemic bottlenecks.

Consequently, the proposed methodology ensures a strategic balance between the market demand for specific product types and the technical capability of the retail and production network to fulfill these orders within strictly regulated timeframes. The practical application of such predictive models, built upon accumulated historical and real-time data, significantly minimizes the operational risks of equipment overloads. Furthermore, it enables the network to respond with high flexibility to shifting market conditions through the sophisticated tools of dynamic pricing and value-based regulation. Future research trajectories are planned to focus on the engineering and design of a comprehensive analytical framework. This framework will be aimed at quantitatively evaluating and weighting the specific impact of each identified factor on the integrated operational efficiency of rapid-response printing networks.

List of sources used:

1. The Future of Digital Printing to 2032 : Market Report / Smithers. Akron : Smithers Information Ltd., 2022. 214 p.
2. Neroda T. Big data categorization in operational digital printing processes. Academic and University Science: Results and Prospect, Vol. 18, 2025. P. 207–209

УДК 004.032.26

Кисіль К.О., здобувач*Державний університет «Київський авіаційний інститут»*

ІМПУЛЬСНІ НЕЙРОННІ МЕРЕЖІ З ГІБРИДНИМ КОДУВАННЯМ ДЛЯ ОБРОБКИ ПОТОКОВИХ ДАНИХ У РЕАЛЬНОМУ ЧАСІ

Імпульсні нейронні мережі (Spiking Neural Networks, SNN) є перспективним підходом до обробки поточкових даних, оскільки дозволяють представляти інформацію у вигляді часових послідовностей імпульсів. На відміну від класичних нейронних мереж, де використовується статичне числове представлення, у SNN інформація кодується моментами виникнення спайків, що дає змогу враховувати часову структуру сигналу та його динаміку.

Сучасні методи кодування в SNN мають певні обмеження [1, 2]. Частотне (rate) кодування добре відображає середню інтенсивність сигналу, однак ігнорує швидкі зміни. Часове кодування є чутливим до точного моменту виникнення імпульсів, але менш стійким до шуму. Тобто кожен із підходів відображає лише окремі характеристики сигналу, що може призводити до втрати частини інформації [1].

У спайкових нейронах інформація формується шляхом накопичення впливу імпульсів, що надходять у різні моменти часу. Часова залежність внеску імпульсу описана функцією

$$\alpha(t) = \frac{t}{\tau} e^{1-\frac{t}{\tau}},$$

що показує залежність ваги імпульсу від моменту його виникнення. Це дозволяє враховувати різні часові характеристики сигналу та створює передумови для комбінування підходів до кодування.

Тому доцільно використовувати гібридне кодування, яке поєднує change-based (Delta–Sigma) та rate-кодування. У підході Delta–Sigma імпульс генерується при перевищенні сигналом адаптивного порогу:

$$s(t) = \begin{cases} 1, & x(t) > r(t) \\ 0, & \text{інакше} \end{cases}$$

$$r(t+1) = r(t) + s(t) - \Delta,$$

де $r(t)$ – адаптивний рівень сигналу. Такий механізм виділяє швидкі зміни сигналу.

У свою чергу rate-кодування описує амплітуду сигналу через ймовірність генерації імпульсу:

$$p(t) = \frac{1}{1 + e^{-x(t)}}$$

$$b(t) \sim \text{Bernoulli}(p(t)),$$

де імпульси виникають стохастично, а їх середня частота відображає рівень сигналу. Це забезпечує збереження інформації про повільні зміни та загальну інтенсивність сигналу [2].

Комбіноване представлення сигналу можна подати як:

$$S = \{t_i, f, ISI_i\},$$

де t_i – моменти імпульсів, f – частотні характеристики, ISI_i – інтервали між імпульсами. Такий підхід дозволяє інтегрувати часову та частотну інформацію в єдиному представленні.

Інтервали між імпульсами визначаються як:

$$ISI_i = t_i - t_{i-1}$$

і відіграють важливу роль у аналізі динаміки сигналу. Для їх урахування вагові коефіцієнти задають залежно від часу:

$$W_i = \beta e^{t_i} \text{ або } W_i = \frac{\beta}{e^{t_i}},$$

що дозволяє регулювати чутливість нейрона до ранніх або пізніх імпульсів. Формування вихідного імпульсу нейрона описується виразом:

$$t_{out} = \frac{V_{th}\tau + \sum t_i v_i}{w\tau + \sum v_i},$$

що дозволяє інтегрувати внесок різних імпульсів у часі.

Гібридне кодування забезпечує більш інформативне представлення сигналу, оскільки поєднує переваги різних підходів: Delta-Sigma підкреслює швидкі зміни, тоді як gate-кодування відображає середню інтенсивність. Це дозволяє підвищити стійкість до шуму та покращити роздільну здатність класів.

Таким чином, гібридні імпульсні нейронні мережі забезпечують ефективну обробку поточкових даних у реальному часі, оскільки дозволяють одночасно враховувати як швидкі, так і повільні компоненти сигналу при збереженні низької обчислювальної складності.

Список використаних джерел:

1. Spiking neural networks for efficient temporal data processing. *Electronics*. 2023. Vol. 12, No 19. URL: <https://www.mdpi.com/2079-9292/12/19/3992>
2. Maass W. Spiking neural networks: Learning, applications and analysis. *Neural Networks*. 1997. Vol. 10, No 9. P. 1659–1671. URL: https://www.researchgate.net/publication/266144130_Spiking_Neural_Networks_Learning_Applications_and_Analysis

УДК 004:658.5

*Красношанка М.М., здобувач
Одарченко Р.С., д.т.н., професор
Державний університет «Київський авіаційний інститут»*

ФОРМУВАННЯ ВИМОГ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДБОРУ НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ ЗАКЛАДІВ ОСВІТИ

Внаслідок військових дій, відтоку інтелектуального потенціалу за кордон, недостатнього фінансування, ринок праці в науково-педагогічній сфері в Україні спостерігається серйозна нестача кадрів. За час війни з України виїхали або змінили професію близько 20% науковців. Війна торкнулася всіх галузей і наука не виключення, зміни відчутні перш за все кадрові [1]. В цих умовах, заклади вищої освіти вимушені шукати нові підходи до підбору фахового персоналу, зміцнюючи свій науковий та освітній потенціал.

Водночас українська освітня система прагне стати повноправним членом Європейського освітнього простору. А тому, необхідним є використання кращих практик, які застосовуються у кращих світових вишах [2, 3]. Як показав аналіз цих та інших світових практик, підбір персоналу не є тривіальною, а багатокритеріальною задачею, що вимагає аналізу великих об'ємів даних. Так, відбір зазвичай здійснюється за чотирма ключовими блоками, які відповідають міжнародним стандартам академічного рекрутингу:

- науковий потенціал (кількість публікацій у Scopus / Web of Science; якість журналів (Q1–Q2); h-index; рівень цитування; наукова новизна досліджень;
- міжнародна активність (оцінюється участь у вітчизняних та міжнародних дослідницьких проєктах; Horizon Europe; Erasmus+; NATO Science programs тощо);
- викладацький потенціал (здатність викладати сучасні дисципліни; використання інноваційних методів навчання; досвід розроблення освітніх програм; участь у міжнародних освітніх ініціативах);
- інноваційна та прикладна діяльність (участь у R&D проєктах; співпраця з індустрією; патенти; технологічні розробки).

Таким чином, як показав даний аналіз, підбір фахового персоналу вимагатиме залучення значних людських ресурсів. А тому, необхідною є автоматизація даного процесу. Тому метою даної роботи є формування вимог до інформаційної системи підбору науково-педагогічних працівників закладів вищої освіти (ЗВО).

Дана інформаційна система має забезпечувати виконання наступних взаємопов'язаних задач: формування запиту від структурних підрозділів ЗВО; валідація запитів зі сторони керівної ланки; автоматизований аналіз ключових блоків, які включені в світові практики підбору персоналу; формування списку кандидатів; оцінка рейтингу кандидатів; додаткові функції (на вимогу користувача).

Отже, з огляду на складність окресленої задачі підбору науково-педагогічного персоналу та необхідність аналізу значних обсягів різномірних даних, інформаційна система повинна відповідати ряду технічних вимог, що забезпечують її ефективність, масштабованість, надійність та інтеграцію з зовнішніми інформаційними ресурсами.

Інформаційна система повинна бути побудована за багаторівневою модульною архітектурою, що забезпечує розділення функцій представлення, бізнес-логіки та обробки даних. Така архітектура включатиме:

- рівень користувацького інтерфейсу (presentation layer);
- рівень прикладної логіки (application layer);
- рівень інтеграції з зовнішніми джерелами даних (integration layer);
- рівень зберігання та управління даними (data layer).

Подібна архітектура дозволить забезпечення масштабованості системи, спрощення та модернізації. При цьому, вона також дозволить забезпечити можливість інтеграції з іншими інформаційними системами ЗВО. Дані вимоги створюють підґрунтя для формування вже специфічних вимог, які будуть використані при розробці системи. Крім того, окремим напрямком досліджень буде розробка нової моделі, яка дозволить оптимальним чином оцінити кандидатів на посади науково-педагогічних працівників ЗВО.

Список використаної літератури:

1. У Міносвіті розповіли, скільки науковців покинуло Україну за час війни. *Новини України - останні новини України сьогодні*. URL: <https://www.unian.ua/society/vidtik-naukovciv-skilki-naukovciv-vijihalo-z-ukrajini-za-chas-viyni-13079622.html> (дата звернення: 20.03.2026).
2. Faculty Appointments. URL: <https://policies.mit.edu/policies-procedures/20-faculty-and-other-academic-appointments/21-faculty-appointments> (date of access: 20.03.2026).
3. The appointment process. *ETH Zurich*. URL: <https://ethz.ch/en/the-eth-zurich/working-teaching-and-research/faculty/faculty-affairs/professorenberufungen/ablauf-berufungsverfahren.html> (date of access: 20.03.2026).

Секція 4
ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ,
ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА

УДК 519.21

Мельник А.О., аспірантка

Київський національний університет імені Тараса Шевченка

СТАТИСТИЧНЕ ОЦІНЮВАННЯ ТА ПОБУДОВА
ДОВІРЧИХ ІНТЕРВАЛІВ ДЛЯ ІМПУЛЬСНОЇ ПЕРЕХІДНОЇ
ФУНКЦІЇ

Проблема оцінювання стохастичних лінійних систем є предметом активних досліджень в останні роки. Сфера застосування таких моделей є дуже широкою і охоплює обробку сигналів, автоматичне керування та економетрику. У даній роботі розглядається неперервна лінійна система з одним входом та одним виходом (SISO), що повністю описується своєю дійснозначною імпульсною перехідною функцією $H(\tau)$, визначеною на обмеженому інтервалі $[0, \Lambda]$.

Зв'язок між вхідним сигналом $X(t)$ та вихідним сигналом $Y(t)$ у будь-який момент часу t описується інтегралом згортки:

$$Y(t) = \int_0^{\Lambda} H(\tau)X(t - \tau)d\tau$$

Вхідний сигнал системи моделюється як центрований стаціонарний гауссівський стохастичний процес. Для його математичного представлення використовується зрізаний тригонометричний ряд Фур'є. Вхідний процес задається наступним чином:

$$X_N(u) = \sqrt{\frac{2}{\Lambda}} \sum_{k=1}^N \left(\xi_k \cos\left(\frac{2k\pi u}{\Lambda}\right) + \eta_k \sin\left(\frac{2k\pi u}{\Lambda}\right) \right)$$

де N – фіксоване ціле число, що позначає рівень зрізання (складність моделі), а ξ_k та η_k – послідовності некорельованих гауссівських випадкових величин.

Як оцінка невідомої функції $H(\tau)$ на основі одного спостереження використовується інтегральна взаємна корелограма. Оцінка $\hat{H}_{N,T,\Lambda}(\tau)$ визначається як усереднення за часом добутку вихідного сигналу та зсунутої в часі версії вхідного сигналу:

$$\hat{H}_{N,T,\Lambda}(\tau) = \frac{1}{T} \int_0^T Y_N(t)X_N(t - \tau)dt$$

Збудована оцінка залежить від двох ключових параметрів: довжини інтервалу усереднення T та рівня зрізання для вхідного сигналу N .

Встановлено, що центрований процес похибки оцінювання $\hat{Z}_{N,T,\Lambda}(\tau) = \hat{H}_{N,T,\Lambda}(\tau) - E\hat{H}_{N,T,\Lambda}(\tau)$ належить до класу квадратично-гауссівських процесів. Для цього випадку виведено явні верхні межі для зміщення та дисперсії оцінки. Показано, що дисперсія зменшується зі швидкістю $O(1/T^2)$, що гарантує швидке покращення точності зі збільшенням часу усереднення T .

Завдяки властивостям простору квадратично-гауссівських величин, було отримано явну неасимптотичну оцінку ймовірності великих відхилень для похибки у просторі неперервних функцій $C([0, \Lambda])$. Ця експоненційна межа залежить від параметрів експерименту N та T , а також від бажаної точності ε .

Отримана нерівність дозволила розробити статистичний критерій узгодженості для перевірки гіпотез щодо форми імпульсної перехідної функції. Крім того, на основі цього критерію побудовано рівномірні довірчі інтервали, які забезпечують кількісну оцінку невизначеності для всієї досліджуваної функції. З імовірністю принаймні $1 - \alpha$, довірчий інтервал набуває вигляду:

$$\hat{H}_{N,T,\Lambda}(\tau) - \varepsilon_\alpha < H(\tau) < \hat{H}_{N,T,\Lambda}(\tau) + \varepsilon_\alpha$$

Для підтвердження теоретичних результатів проведено імітаційне моделювання. Зокрема, вирішено обернену задачу планування експерименту: визначено мінімальний час усереднення T , необхідний для досягнення бажаної точності та надійності при оцінюванні затухаючої синусоїди. Отримані результати демонструють нелінійний компроміс між тривалістю експерименту та точністю оцінювання.

Список використаних джерел:

1. Kozachenko Yu., Rozora I. On Statistical Properties of the Estimator of Impulse Response Function. *Stochastic Processes, Statistical Methods, and Engineering Mathematics*. Springer, Cham, 2023. P. 563–585.
2. Rozora I., Melnyk A. Statistical estimation and hypothesis testing on impulse response function. *Austrian Journal of Statistics*. 2025. Vol. 54, № 1. P. 200–213.

*Пятін І.С., к.т.н., доцент,
Хмельницький політехнічний фаховий коледж
Бойко Ю.М., д.т.н., професор,
Хмельницький національний університет*

RL МОБІЛЬНІ ТЕЛЕКОМУНІКАЦІЇ З LDPC КОДУВАННЯМ

Сучасні бездротові системи зв'язку працюють в умовах завмирань, завад, швидких змін стану каналу та зростаючих вимог до швидкості передавання і якості обслуговування. Використання адаптивної модуляції і кодування дає змогу динамічно змінювати вид модуляції та кодову швидкість відповідно до поточного стану каналу, забезпечуючи компроміс між спектральною ефективністю, часткою помилкових блоків і затримкою. Reinforcement Learning (рис. 1) здійснюється через багаторазову взаємодію із середовищем і є інтелектуальною надбудовою для вибору режиму передавання. Замість жорсткої таблиці порогів для певного відношення сигнал/шум присутній агент, який після кожного фрейму або інтервалу передавання спостерігає стан каналу, вибирає режим передавання і отримує “винагорода”.



Рис. 1. а – Схема взаємодії агента RL з середовищем; б – схема системи зв'язку, що використовує навчання з підкріпленням (RL)

Агентом є блок керування адаптацією на боці передавача. Саме він вирішує, який режим роботи вибрати для наступного фрейму. Середовище включає канал, демодулятор, LDPC-декодер, інформація про якість якого передається через CQI, HARQ. Стан – це вектор ознак: оцінене SNR; CQI; попередній режим роботи; останній ACK/NACK; кількість ітерацій декодування (затримка). Дія – це вибір сигнально-кової конструкції (тип модуляції, кодова швидкість).

Винагорода повинна змушувати агента знаходити компроміс між пропускну здатністю, BER і затримкою.

Для систем з Reinforcement Learning (RL) для адаптації лінії зв'язку критичні затримка обчислення і застарівання CQI, бо якщо агент працює повільно, канал швидко змінюється. Для FPGA-платформи AXU2CGB, тракт передавання та приймання реалізується у програмованій логіці, а RL-агент – на процесорній системі.

Адаптивну систему зв'язку з RL представляємо як задачу “стан → вибір режиму роботи → винагорода → оновлення правил”. Передача індексу режиму роботи до приймача відбувається каналом управління.

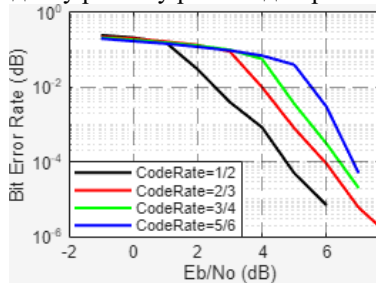


Рис. 2. – Залежність BER від E_b/N_0 для різних CodeRate

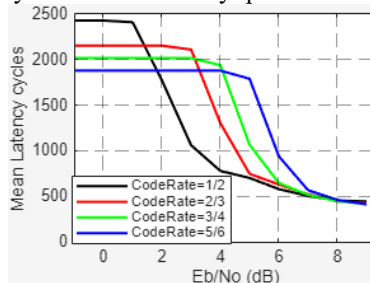


Рис. 3. – Залежність середньої затримки від E_b/N_0 для різних CodeRate

LDPC-декодер працює у режимі з early termination: при малому E_b/N_0 декодер працює з максимальною кількістю ітерацій, а при зростанні E_b/N_0 зупиняється раніше, тому середня затримка падає. Виходячи з отриманих залежностей, одна ітерація триває 284 системні такти, а базова складова алгоритму декодування триває 157 тактів.

За діапазонами E_b/N_0 (рис. 2-3) можна зробити такий висновок: при малих E_b/N_0 декодер працює в режимі насичення і використовує максимальні 8 ітерацій. У діапазоні 2–4 дБ маємо перехідний режим: середня затримка швидко зменшується, а розкид між фреймами найбільший. Для 6–7 дБ декодер завершує декодування за 1–2 ітерації, затримка зменшується більш ніж у 5 разів.

Використання Reinforcement Learning корисно в області $E_b/N_0 \approx 3 \dots 6$ дБ, де спостерігається розкид затримки та кількості ітерацій між фреймами, що дозволяє використовувати орієнтоване на фреймах адаптивне керування параметрами декодування. При низькому BER Reinforcement Learning можна використовувати для адаптивного зменшення обчислювальної складності декодування.

Список використаних джерел:

1. Xie, C., El-Hajjar, M., Ng, S.X.: Machine learning assisted adaptive LDPC coded system design and analysis. IET Commun.18, 1–10 (2024). <https://doi.org/10.1049/cmu.2.12707>

*Залевський В.Й, с.н.с. НЦ
Сидорчук О.Л. к.т.н., доцент, ст. викладач
Волянський Є.А., здобувач*

Житомирський військовий інститут імені С.П. Корольова

ЗМЕНШЕННЯ РАДІОЛОКАЦІЙНОЇ ПОМІТНОСТІ АНТЕННИХ СИСТЕМ

Досвід сучасних бойових дій свідчить про зростання значущості радіоелектронної розвідки (РЕР), радіоелектронної боротьби (РЕБ) та протиповітряної оборони (ППО). Застосування засобів РЕР і РЕБ забезпечує своєчасне виявлення та протидію системам радіолокаційної розвідки повітряного базування (літаків, вертольотів і безпілотних літальних апаратів). Разом з тим технічні засоби РЕР, РЕБ та ППО є основними цілями, що виявляються засобами повітряної радіолокаційної розвідки противника та можуть бути уражені в першу чергу. Тому в умовах застосування противником авіації з бортовими радіолокаційними системами (БРЛС) необхідним є зменшення радіолокаційної помітності наземних сил і засобів, що налаштовані на розвідку в діапазоні частот повітряних БРЛС.

Значний внесок у радіолокаційну помітність зразків озброєння та військової техніки (ОВТ) здійснюють їх антенні системи. Найбільш проблемним завданням є зменшення електромагнітного поля, перевищеного дзеркальними антенами з рупорним опромінювачем, який знаходиться у фокусі антенної системи та істотно впливає на її загальну ефективну поверхню розсіювання (ЕПР). Саме зменшення ЕПР призводить до збільшення дальності виявлення цілей, зменшення їх радіолокаційної помітності, а отже й до підвищення розвідзахисності та живучості.

У доповіді пропонуються спроби впровадження нових, захищених патентами на винахід, конструктивних рішень, які дозволять зменшити радіолокаційну помітність таких антенних систем.

Для вирішення поставленого завдання пропонується два варіанти, запатентованих автором, опромінювачів дзеркальних антен ОВТ.

Перший варіант це малогабаритна рупорна антена колової поляризації з конусоподібним поглиначем вищих гармонік (патент на винахід № 96661 від 13.07.2011). На відміну від прототипів запропонована конструкція має діелектричний конус з поглинаючими канавками, прикріплений до поглинаючої пластини. Експеримент показав, що завдяки введенню додаткового хвилеводного навантаження, у вигляді конуса з поглинаючими канавками,

зменшується рівень відбитої хвилі, що призводить до зменшення ЕПР антени.

Нова, антена має фазуючу трапецієподібну діелектричну пластину, яка, окрім утворення колової поляризації, поліпшує узгодження хвилеводу з довгими неоднорідними гантелеподібними щілинами. Така антена працює в широкій смузі частот (більше 35%), має добре узгодження двох неоднорідних гантелеподібних щілин з відрізком квадратного хвилеводу і малу ЕПР.

Експериментальні дослідження запропонованої антени у діапазоні 8-12 ГГц довели, що її ЕПР було зменшено на 12 дБ, коефіцієнт стоячої хвилі за навантаженням становив 1,25–1,3, а втрати 0,5–0,7 дБ.

Другий варіант – це рупорна антена зі зменшеною ЕПР від кромek (патент № 97037 від 26.12.2011). Проведено експериментальні дослідження запропонованої конструкції антени у діапазоні 8–12,5 ГГц. Вимірювання показали, що, у порівнянні з прототипом, ЕПР нової конструкції в області головної пелюстки діаграми розсіювання було знижено з 20 дБ до 12 дБ.

Результати експерименту нових конструкцій довели, що найбільш ефективними щодо зниження радіолокаційної помітності антен є способи, пов'язані зі зменшенням коефіцієнта стоячої хвилі у колі навантаження та зниженням рівня бічних пелюсток діаграм їх зворотного розсіювання. Отже доцільно замінити штатні опромінювачі дзеркальних антен на нові, описані вище. Це дозволить зменшити ЕПР зразка ОБТ в цілому, а отже підвищити його живучість.

Список використаних джерел:

1. Сидорчук О. Л. Проблематика методів оцінювання антен зі зменшеною ефективною поверхнею розсіювання засобів радіоелектронної розвідки та радіоелектронної боротьби // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. Житомир : ЖВІ, 2022. Вип. 22. С. 14–29. <https://doi.org/10.46972/2076-1546.2022.22.02.10>.

2. Сидорчук О. Л. Аналіз методів і способів зменшення ефективної поверхні розсіювання антенних систем // Вісник ЖДТУ. Технічні науки. Житомир, 2012. № 2 (61). С. 94–106.

3. Сидорчук О. Л., Залевський В. Й. Дослідження дифракції електромагнітної хвилі на кромках пірамідальної рупорної антени як однієї з причин розсіювання // Вісник НТУУ «КПІ». Серія «Радіотехніка. Радіоапаратобудування». 2022. № 89. С. 11–20. <https://doi.org/10.20535/RADAP.2022.89.11-20>.

Бобронніков А.С., аспірант

*Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»*

СТВОРЕННЯ МОДИФІКОВАНИХ МЕТОДІВ ОЦІНКИ СТАНУ КОМФОРТУ ЛЮДИНИ В ЖИТЛОВОМУ ПРИМІЩЕННІ З ВИКОРИСТАННЯМ МОДЕЛІ PMV

Пропонується використання підходу PMV (Predicted Mean Vote) та PPD (Predicted Percentage of Dissatisfied) для світлового комфорту, тобто зорового відчуття та навантаження на зорову систему методами оцінки теплового комфорту.

Підхід, описаний у ISO 7730 можна застосувати до світлового комфорту знайшовши певні відповідники між факторами, що впливають на термічні та зорові відчуття.

Вводимо поняття PLV (Predicted Light Vote) (прогнозоване середнє відчуття яскравості освітлення) та PPD для світла (Predicted Percentage Dissatisfied for Light) (прогнозований відсоток незадоволених яскравості освітлення).

PLV прийматиме значення від -3 до +3, що означають наступне:

Оцінка	Стан	Оцінка	Стан	Оцінка	Стан
+3	Сліпуче яскраво	0	Нейтрально	-1	Трохи темно
+2	Дуже яскраво			-2	Темно
+1	Трохи яскраво			-3	Дуже темно (не видно)

Введено наступні основні фактори комфортності освітлення:

- Освітленість (lux) – головний параметр, умовно аналог температури повітря. Комфортна робота за комп'ютером 300–500 Лк, точні роботи 750–1000 Лк;
- Яскравість у полі зору – контрасти між об'єктами в полі зору (екраном, столом, стінами);
- Блискучість / засліплення (UGR), умовно аналог протягів у тепловому комфорті;
- Колірна температура (СТ). 2700K – тепле, 4000K – нейтральне, 6500K – холодне. Невідповідність колірної температури та часу доби може призвести до дискомфорту;

- Також можна вказати людські фактори такі як вік (старшим людям потрібно більше світла) і, звісно, тип роботи, що виконується.

Як і PMV в тепловому комфорті, PLV приймає значення від -3 до +3. Запропоновано формулу:

$$PLV = S_E + S_C + S_{UGR} + S_{CT} + S_H,$$

де кожен доданок – це “внесок дискомфорту” від окремого фактора освітлення. Задачею забезпечення комфорту є отримання суми доданків якомога ближчою до 0. Аналог формули Фангера для PPD:

$$PPD_L = 100 - 95 \cdot e^{-0.03353PLV^4 - 0.2179PLV^2}$$

Приклад розрахунку PLV та PPD:

Вік = 25 (вік не впливає на зір);

Робота = офісна робота за ПК (немає особливих умов роботи);

E = 750 Лк (забагато для офісної роботи за ПК);

$\frac{L_{max}}{L_{min}} = 12$ (велика контрастність);

UGR = 22 (є засліплення);

CCT = 6500K (холодне, а на вулиці тепле освітлення);

Коефіцієнти важливості (наведені для прикладу, будуть коригуватися) візьмемо як 0.5 для кожної складової.

Отримуємо:

$$\begin{aligned} PLV &= S_E + S_C + S_{UGR} + S_{CT} + S_H = \\ &= a \cdot \ln\left(\frac{E}{E_{opt}}\right) + b \cdot \left(\frac{L_{max}}{L_{min}} - R_{opt}\right) + c \cdot (UGR - UGR_{opt}) + d \\ &\quad \cdot \frac{CT - CT_{opt}}{1000} + e_1(Age) + e_2(Task) = \\ &= 0.5 * 0.405 + 0.5 * 2 - 0.5 * 3 + 0.5 * 1.5 + 0.5 * 0 + 0.5 * 0 = 0,452 \end{aligned}$$

PLV = 0,452 (робоче місце створює дискомфорт), тоді PPD на рівні 13%. Теоретичні розрахунки показали, що модель PMV-PPD може бути застосована для інших параметрів середовища, що впливають на комфорт людини, а результат розрахунків, що є числом у певному діапазоні, є зручним інструментом для оцінки комфортності середовища та прогнозування відсотка невдоволених.

Список використаних джерел:

1. ISO 7730:2005 Ergonomics of the thermal environment – Analytical determination and interpretation of thermal comfort using calculation of the PMV and PPD indices and local thermal comfort criteria. Режим доступу: <https://www.iso.org/standard/39155.html>

ЗАВАДОСТІЙКИЙ МОДЕМ ПЕРЕДАВАННЯ КОМАНД КЕРУВАННЯ РУХОМИМ ОБ'ЄКТОМ

Більшість аналогових засобів радіозв'язку використовують амплітудну або частотну модуляцію радіосигналу при обмеженій смузі частот. Такі радіосигнали мають достатньо високу спектральну щільність, що дає змогу виявити і заглушити їх засобами радіоелектронної боротьби. Одним з методів підвищення прихованості та завадостійкості засобів радіозв'язку є розширення спектру радіосигналу на робочій частоті передавача [1]. При запровадженні цього методу в існуючих аналогових засобах зв'язку ширина спектру сигналу не повинна перевищувати 25 кГц. Тому запровадження методів розширення спектру радіосигналу фактично вимагає розробки нового засобу зв'язку. Отже актуальним завданням залишається розробка методу підвищення завадостійкості, який може бути реалізований у вигляді низькочастотного модему-приставки до існуючих вузькосмугових засобів зв'язку.

У роботі розглядається розробка низькочастотного модему для реалізації бездротової радіолінії передавання команд керування на базі існуючих аналогових радіоліній. Пропонується використання структурованого сигналу з лінійною частотною модуляцією (ЛЧМ), ширина спектру якого не перевищує ширину смуги каналу зв'язку. Застосування запропонованого методу не підвищує прихованості передавання, але забезпечує підвищення завадостійкості каналу зв'язку шляхом збільшення відношення сигнал/шум на виході оптимальної системи обробки корисного сигналу. Дальність дії радіолінії керування визначається дальністю дії обраного для реалізації засобу радіозв'язку.

У якості рухомого об'єкта розглядається носій з камерою, для управління яким достатньо подати п'ять команд. Кожна команда передбачає зміну часової позиції імпульсу ЛЧМ на певну величину, відповідно до номера команди [2]. Принцип роботи завадостійкого засобу передавання команд керування можливо описати наступним чином. Передавальна частина завадостійкого модему містить модулятор з фазо-імпульсною модуляцією (ФІМ) та генератор ЛЧМ сигналу з ЦАП, що реалізуються на одному мікроконтролері ESP32. З виходу ЦАП сформований ЛЧМ сигнал подається на вхід модулятора засобу зв'язку, що обраний для реалізації радіоканалу. Перенесення сформованого сигналу на несучу частоту каналу, що обраний для роботи, здійснюється у передавачі засобу зв'язку. Приймач засобу

зв'язку налаштовується на частоту обраного для роботи каналу. З виходу приймального пристрою засобу зв'язку демодульований низькочастотний ЛЧМ сигнал буде надходити до АЦП демодулятора модему, який забезпечує формування цифрових відліків прийнятого сигналу. Цифрові відліки подаються на вхід корелятора ЛЧМ сигналу, який є ідеальним накопичувачем енергії корисного сигналу. Відношення сигнал/шум на виході корелятора суттєво перевищує це відношення на його вході. Цифрові відліки з виходу корелятора подаються на вхід демодулятора ФІМ. Визначення часової відстані між відгуками у демодулятор ФІМ дозволить визначити номер команди, що була передана по радіоканалу. АЦП, корелятор ЛЧМ сигналу та демодулятор ФІМ також реалізовані на мікроконтролері ESP32.

У роботі описуються результати практичної перевірки працездатності запропонованого низькочастотного модему-приставки передавання команд керування рухомим об'єктом з використанням аналогових радіостанцій з амплітудною та частотною модуляцією несучого коливання та смугою пропускання приймача 25 кГц.

Запропонований низькочастотний модем дозволить провести модернізацію великої кількості вже існуючих аналогових радіостанцій з метою створення засобу передавання дискретних команд керування з підвищеною завадостійкістю. На відміну від відомих методів розширення спектру сигналу на радіочастоті, запропонований метод підвищення завадостійкості не вимагає розширення спектру сигналу, а отже і смуги пропускання існуючих засобів радіозв'язку. Розробка модему у вигляді окремого блоку з цифровим формуванням і обробкою сигналів дозволить запровадити запропонований завадостійкий метод передавання команд керування рухомим об'єктом на базі існуючих засобів зв'язку без їх суттєвої доробки.

Список використаних джерел:

1. Андреев О.В., Ципоренко В.В., Ципоренко В.Г., Андреева Є.О., Дубина О. Ф., Пулеко І.В. Електромагнітна сумісність широкосмугових та вузькосмугових короткохвильових засобів радіозв'язку, *Sciences of Europe*. 2025. Vol 1, № 158. P.78–86. URL: <https://www.europe-science.com/wp-content/uploads/2025/02/Sciences-of-Europe-No-158-2025.pdf>

2. Vakaliuk T., Andreiev O., Nikitchuk T., Osadchyi V., Dubyna O. Using the ESP32 Microcontroller for Physical Simulation of the Operation of a Broadband Radio Communication Modem. *Радіоелектроніка, інформатика, управління*. 2023. Вип. 3 (63). С. 206-214.

*Єгоян В.Б., здобувач,
Бурмістров С.В., к.т.н., викладач,
Бондаренко В.В., викладач
Державний університет «Черкаський національний
університет імені Богдана Хмельницького»*

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ІОТ- СИГНАЛІЗАЦІЇ: ІНТЕГРАЦІЯ СУЧАСНИХ РАДІОТЕХНІЧНИХ ТА КОМУНІКАЦІЙНИХ РІШЕНЬ

Метою проєкту є розробка розширеної системи охоронної сигналізації на базі мікроконтролерів із багаторівневою архітектурою, призначеної для контролю доступу до ряду кімнат, об'єднаних єдиним контуром приміщення.

Апаратна частина системи розроблена за дворівневою ієрархічною топологією, яка чітко розподіляє завдання між керуючим та периферійним рівнями.

Керуючий рівень призначений для централізованої обробки інформації, прийняття рішень та взаємодії із зовнішніми мережами. Він виступає в ролі центрального аналізатора та комунікаційного ядра, який представлений потужним двоядерним мікроконтролером ESP32. Для забезпечення комунікацію із зовнішнім світом та передачу даних до хмарних сервісів реалізовано через дротовий мережевий інтерфейс Ethernet за допомогою модуля W5500.

Периферійний рівень призначений для безпосереднього збору даних з об'єкта та контролю фізичного середовища. Він представлений розподіленою мережею сенсорних вузлів на базі енергоефективних плат ESP32-C3 SuperMini [1]. Інтеграція інфрачервоних датчиків SR602 та герконових датчиків МС-38 на цьому рівні забезпечує точну детекцію руху в приміщеннях та надійну фіксацію порушення периметра.

Для зв'язку між датчиками та центральним шлюзом використано спеціалізований радіопротокол ESP-NOW замість підключення до Wi-Fi [0]. Передача кадрів відбувається на рівні MAC-адрес, що виключає затримки на встановлення з'єднання з маршрутизатором та забезпечує швидку доставку повідомлення. Застосування цього протоколу з вбудованим шифруванням ускладнює перехоплення даних, що робить систему стійкішою до спроб несанкціонованого доступу (див. рис. 1).



Рис. 1 – Принцип передачі даних за протоколом ESP-NOW

Взаємодія системи з кінцевим користувачем має комплексний характер і розділена на оперативну та аналітичну частини. Оперативний моніторинг, керування режимами охорони та доставка миттєвих Push-сповіщень реалізовані на базі хмарної екосистеми Blynk [0]. Водночас для надійного збереження та структурування історії подій систему інтегровано з хмарною NoSQL базою даних Amazon DynamoDB. Усі тривожні сповіщення, зміни статусів системи та системні логи автоматично архівуються до цієї БД. Для зручного доступу до зібраних даних розроблено Telegram-бот, за допомогою якого користувач може зчитувати історію записів, переглядати хронологію спрацювань датчиків та здійснювати аудит системних логів без необхідності використання основного інтерфейсу керування.

Створений прототип IoT-сигналізації доводить технічну та економічну ефективність запропонованих рішень. Система використовує акумулятори 18650 та режими сну, що забезпечує високу автономність і надійність роботи системи. Проєкт демонструє поєднання відкритих IoT-технологій, надійних комунікацій та хмарних сервісів, що дозволяє розробити гнучку систему безпеки, яка не поступається комерційним аналогам у швидкодії, але є значно доступнішою.

Список використаних джерел:

1. ESP32-C3 SuperMini Datasheet / Espressif Systems. 2026. URL: <https://dl.artronshop.co.th/ESP32-C3%20SuperMini%20datasheet.pdf> (дата звернення: 20.03.2026).
2. ESP-NOW User Guide / Espressif Systems. 2026. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/network/esp_now.html (дата звернення: 20.03.2026).
3. Blynk Documentation / Blynk IoT Platform. 2026. URL: <https://docs.blynk.io/> (дата звернення: 20.03.2026).

*Жабський С.О., здобувач,
Снитюк С.О., здобувач,
Христинець Н.А., к.т.н., доцент
Луцький національний технічний університет*

АНАЛІЗ ПРОДУКТИВНОСТІ ТА РЕСУРСІВ ПАМ'ЯТІ У ПРОЕКТУВАННІ ІНФОРМАЦІЙНИХ СИСТЕМ НА ARDUINO UNO

У процесі дослідження можливостей використання Arduino Uno у складі інформаційних систем було проведено аналіз апаратних характеристик плати та їх впливу на продуктивність системи під час роботи з периферійними пристроями. Апаратною основою плати є мікроконтролер ATmega328P, який працює з тактовою частотою 16 МГц, має 32 КБ Flash-пам'яті, 2 КБ SRAM та 1 КБ EEPROM [1]. Дослідження показують, що під час використання стандартних бібліотек середовища розробки приблизно 20–30 % Flash-пам'яті та до 40 % оперативної пам'яті можуть бути зайняті системними функціями ще до реалізації прикладної логіки інформаційної системи [2]. Це обмежує складність алгоритмів обробки даних та кількість одночасно підключених програмних модулів.

Окреме дослідження було проведено щодо кількості доступних інтерфейсів введення-виведення. Плата Arduino UNO має 14 цифрових входів/виходів, з яких 6 підтримують широтно-імпульсну модуляцію PWM, а також 6 аналогових входів з розрядністю 10 біт, що дозволяє вимірювати аналоговий сигнал з точністю до 1024 рівнів [3]. Дослідження швидкості обміну даними показало, що ефективність роботи периферійних пристроїв значною мірою залежить від використаного комунікаційного протоколу [4]. Для послідовного інтерфейсу UART стандартна швидкість передачі становить 9600–115200 біт/с, що дозволяє передавати приблизно 1–11 КБ даних за секунду. Для високошвидкісного обміну застосовується інтерфейс SPI, який у мікроконтролері ATmega328P може працювати зі швидкістю до 8 Мбіт/с, що приблизно у 20–80 разів швидше, ніж типова швидкість I2C.

Числовий аналіз енергетичних характеристик показав, що стандартне споживання плати Arduino UNO становить приблизно 45–50 мА при напрузі 5 В, тобто близько 0,25 Вт потужності. Підключення додаткових периферійних модулів, таких як датчики, дисплеї або бездротові передавачі, може збільшити загальне споживання системи до 150–300 мА, що у 3–6 разів більше від базового значення [5]. У

випадку використання бездротових модулів зв'язку або сервоприводів споживання може перевищувати 500 мА, що потребує застосування зовнішніх джерел живлення або стабілізаторів.

Окремі експериментальні вимірювання продуктивності [6] показали, що при одночасному опитуванні 5–7 датчиків з інтервалом 100 мс навантаження на процесор становить приблизно 60–70 % обчислювального ресурсу, що залишає обмежений запас для виконання додаткових алгоритмів обробки даних або мережових операцій. При збільшенні кількості сенсорів до 10–12 затримки обробки можуть зростати до 200–300 мс, що є критичним для систем реального часу.

Отримані числові результати свідчать, що використання Arduino UNO є ефективним для інформаційних систем малого та середнього рівня складності, де кількість сенсорів не перевищує 8–10 пристроїв, а обсяг оброблюваних даних є помірним. Для розширення функціональних можливостей системи доцільно використовувати шинні інтерфейси, у якій Arduino виконує функції збору даних, а подальша обробка здійснюється на більш продуктивних платформах.

Список використаних джерел:

1. Fingerprint Based Attendance System Using ATMEGA328P. International Research Journal of Modernization in Engineering Technology and Science. 2022. URL: <https://doi.org/10.56726/irjmets32915> (date of access: 05.03.2026).
2. Поліщук М., Гринюк С., Янчук Д. Тесла-світч 4-х батарей на основі системної плати Arduino Uno. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2019. № 37. С. 97–105.
3. Aldea Rivas M., Perez Tijero H. M2OS for Arduino Uno. ACM SIGAda Ada Letters. 2022. Vol. 41, no. 1. P. 78–82. URL: <https://doi.org/10.1145/3570315.3570322>(date of access: 05.03.2026).
4. Radar Using Arduino UNO / S. Thele et al. International Journal of Research Publication and Reviews. 2024. Vol. 5, no. 4. P. 7606–7610. URL: <https://doi.org/10.55248/gengpi.5.0424.10113> (date of access: 05.03.2026).
5. Котунова Д. Г. Бездротові пристрої системи «Smart Home»: bachelor's thesis. 2020. 57 с. URL: <https://ela.kpi.ua/handle/123456789/34545> (дата звернення: 05.03.2026).
6. Anwar Y. S., Durahman N. Smart restroom berbasis arduino uno. Jurnal Informatika dan Teknik Elektro Terapan. 2023. Vol. 11, no. 3, p. 11–16.

Соболенко С.О., к.т.н., доцент,

Дубина О.Ф., к.т.н., доцент,

Заєць Ю.О., здобувач

Житомирський військовий інститут імені С. П. Корольова

Пивовар О.П., ад'юнкт

Національний університет оборони України

ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ КАНАЛІВ ЗВ'ЯЗКУ В ПІДРОЗДІЛАХ SHORAD

Досвід ведення бойових дій в ході широкомасштабного вторгнення РФ показав важливість засобів захисту об'єктів від ударів противника з повітря (БПЛА, ракети, КАБи і т.д.).

Short Range Air Defense (SHORAD) – це комплекс протиповітряної оборони, призначений для захисту сухопутних військ та об'єктів від повітряних загроз на малих висотах і дальностях. Вони забезпечують безпосереднє прикриття об'єктів, часто будучи мобільними.

Існуючі канали передачі даних в підрозділах SHORAD будуються на сучасних мережевих технологіях із використанням технології захисту інформації (*міжмережеві екрани (Firewall), системи виявлення втручань (Intrusion Detection System), засоби створення віртуальних приватних мереж (Virtual Private Network)*). Цей процес, як правило передбачає додатково виконання значної кількості операцій, в тому числі шифрування, що збільшує сумарний час передачі інформації $\tau_{\Sigma ni}(t)$. Окрім сталої складової цього часу $\tau_{\Sigma ni}$, що враховує розповсюдження сигналу по каналам зв'язку, існує змінна складова, яка не піддається точному прогнозуванню, вона враховує пропуски і затримки в роботі цифрової мережі (Jitter) $\tau_{Jet}(t)$ (1):

$$\tau_{\Sigma ni}(t) = \tau_{\Sigma ni} + \tau_{Jet}(t). \quad (1)$$

Час передачі інформації є критично важливим для підрозділів, які виконують завдання щодо виявлення та знищення цілі у реальному часі. Повітряна ціль рухається із швидкістю від сотні до тисяч км/г і чим більше час на передавання інформації, тим більше похибка точності наведення. Методами зменшення часу передачі інформації мають бути, в першу чергу, організаційні заходи, які забезпечать таку побудову мережі, що істотно не збільшуватиме час проходження команд управління.

Класичний підхід до формування захищених мереж зв'язку, прагнення впорядкувати та централізувати інформаційні потоки, зашифрувати, забезпечити тощо призводять до зниження ефективності роботи підрозділів типу SHORAD. Це призводить до певного ряду проблем, пов'язаних із критичною залежністю від якості каналів зв'язку на всьому далеко не близькому шляху до серверів VPN і в зворотному напрямку, якості роботи сервісів VPN тощо.

Тому, засоби кожного тактичного підрозділу ППО з АСУ повинні входити в склад своєї локальної мережі, яка навіть у випадку виходу із ладу глобальної мережі, повинна залишитись функціональною. Система зв'язку повинна бути децентралізованою, само відновлюваною з багатоланковою ретрансляцією з резервуванням фізичних каналів.

Таким вимогам відповідає технологія Mobile Ad hoc Network (MANET). Вона складається з мобільних пристроїв, які самостійно встановлюють з'єднання між собою, передаючи дані один через одного (багато-стрибковий режим), що робить її стійкою та динамічною. Тому поєднання всіх засобів в підрозділі пропонується на основі розгортання автономної високошвидкісної радіомережі шляхом використання комунікаційних засобів Silvus [1], MPU5 [2, 3] або їх аналогів. Практичне випробування таких систем показало їх ефективність в умовах впливу РЕБ та спроможність забезпечити передавання даних в межах підрозділу без затримок інформації, які істотно впливають на точність наведення.

Список використаних джерел:

1. Silvus Technologies : офіційний сайт. URL: <https://www.silvustechologies.com> (дата звернення: 12.03.2026).
2. Сайт оборонних технологій та мережевих рішень (Persistent Systems, LLC): Persistent Systems : офіційний сайт. URL: <https://persistentsystems.com/> (дата звернення: 12.03.2026).
3. Радіо MPU5: протестовано Rakkasan. Army.mil : веб-сайт. URL: https://www.army.mil/article/222056/mpu5_radio_rakkasan_tested (дата звернення 15.03.2026).

*Горбачов І.О., PhD аспірант
Литвинюк О.М., PhD аспірант*

*Гнатюк В.О., к.т.н., доцент, завідувач кафедри
Державний університет «Київський авіаційний інститут»*

МЕТОД ПРОГНОЗУВАННЯ ЗАВАНТАЖЕННЯ ТА РОЗПОДІЛУ РЕСУРСІВ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Сучасні телекомунікаційні системи характеризуються високою динамічністю трафіку, нерівномірним розподілом навантаження та необхідністю оперативного масштабування ресурсів для забезпечення QoS/QoE. Зростання кількості користувачів, інтенсивне використання мультимедійних сервісів, інтеграція IoT-пристроїв та поява сервісів із жорсткими вимогами до затримки призводять до постійних коливань навантаження на мережеву інфраструктуру.

Аналіз існуючих досліджень [1-4] підкреслює необхідність вирішення наукової задачі щодо прогнозування завантаження та розподілу ресурсів в телекомунікаційних системах.

Метою роботи є розроблення методу прогнозування завантаження та розподілу ресурсів у телекомунікаційних системах на основі нейронних мереж, який забезпечує підвищену точність передбачення майбутнього навантаження, динамічну адаптивність до змін трафіку та можливість ефективного й оптимального управління мережевими ресурсами в умовах інтенсивно змінюваного середовища.

Архітектура запропонованої моделі прогнозування. Попередня обробка даних. Для підвищення точності прогнозування використовується багатоступенева підготовка даних: нормалізація часових рядів методом Min–Max або StandardScaler; виявлення та фільтрація аномалій (раптом виникаючі піки, пропуски даних); формування ковзного вікна фіксованої довжини (Sliding Window) для подачі даних до моделі; збагачення датасета екзогенними ознаками: час доби, день тижня, тип сервісу, події мережі (handover, зміна соти тощо). Такі ознаки дозволяють моделі навчитися складним сезонним і поведінковим залежностям.

Модель нейронної мережі. Запропонована архітектура складається з таких компонентів: компонент ознак (Feature Extraction Layer) із використанням 1D-CNN для виділення локальних часових патернів. Основний прогнозний компонент – двошарова LSTM або GRU модель з 32–128 нейронами, здатна моделювати довготривалі залежності.

Dropout-шари для зменшення перенавчання. Dense-шар для формування кінцевого прогнозу.

Гібрид CNN–LSTM дає змогу одночасно обробляти короткострокові коливання (CNN) і глобальні тренди (LSTM). На практиці така архітектура демонструє кращу стабільність прогнозів у пікові періоди.

Процедура навчання моделі. Навчання здійснюється методом оптимізації Adam із функцією втрат MSE. Гіперпараметри (довжина вікна, кількість нейронів, dropout, швидкість навчання) підбираються шляхом k-fold cross-validation.

Інтеграція прогнозовної моделі з механізмом управління ресурсами. Запропонована система складається з трьох взаємодіючих модулів: Модуль моніторингу, який збирає телеметричні метрики (CPU, throughput, RRC-конекції, затримки, Packet Loss, PRB utilization). Модуль прогнозування, де розгорнуто згадану нейронну модель. Модуль управління ресурсами, що виконує дії на основі прогнозу: масштабування інстансів vNF/NF, регулювання ресурсів MEC-вузлів, балансування трафіку між вузлами, забезпечення гарантій QoS для критичних сервісів.

Взаємодія між модулями реалізується через API SDN-контролера та оркестратор NFV, що дозволяє динамічно змінювати конфігурації мережевих компонентів у режимі near-real-time.

Запропонований підхід дозволяє враховувати короткострокові та довгострокові залежності в мережевому трафіку, забезпечуючи високу точність прогнозування та адаптивне управління ресурсами в умовах динамічної зміни навантаження.

Список використаних джерел:

1. Donatti, A., *et al.* (2024). Survey on machine learning-enabled network slicing: Covering the entire life cycle. *IEEE Transactions on Network and Service Management*, 21(1), 994–1011.
2. Uzel, Z. (2023). *Comparative analysis of LSTM, ARIMA, and Facebook's Prophet for traffic forecasting: Advancements, challenges, and limitations* (Bachelor's thesis). Delft University of Technology.
3. Ye, W., Zheng, Y., Bai, H., *et al.* (2025). A neural network for traffic flow prediction with parallel processing of expanded convolutional and radial networks. *Scientific Reports*, 15, Article 38243. <https://doi.org/10.1038/s41598-025-22073-4>
4. Zangooei, M., Saha, N., Golkarifard, M., & Boutaba, R. (2023). Reinforcement learning for radio resource management in RAN slicing: A survey. *IEEE Communications Magazine*, 61(2), 118–124. <https://doi.org/10.1109/MCOM.004.2200532>

*Каращук Н. М., к.т.н., доцент, ст. викладач
кафедри телекомунікацій та радіотехніки*

Андрє Т. В., здобувач, гр. 333/1

Житомирський військовий інститут імені С. П. Корольова

УМОВА ВИБОРУ ЧАСТОТИ ПОВТОРЕННЯ ЗОНДУВАЛЬНИХ СИГНАЛІВ ДЛЯ УСУНЕННЯ СПІЛЬНИХ НЕОДНОЗНАЧНОСТЕЙ ВИЗНАЧЕННЯ КУТОВИХ КООРДИНАТ ТА ДАЛЬНОСТІ РСА

Використання методу синтезування апертури антени в бортових радіолокаційних станціях (РСА) має певні особливості. Вони полягають у тому, що виникає неоднозначність у визначенні кутових координат цілей та визначенні дальності до цілі.

Підходи по усуненню неоднозначностей, а саме: використання спрямованих властивостей елементів антенної решітки; застосування широкосмугових зондувальних сигналів; перехід до нееквідистантних решіток недостатньо ефективні або мають труднощі практичної реалізації.

Пропонується метод усунення спільної неоднозначності – збільшення частоти повторення зондувальних сигналів до величини, при якій невизначеність зникає.

При врахуванні спрямованих властивостей реальної бортової антени для однозначного визначення кутових координат цілі, частота повторення зондувальних сигналів повинна бути не більше спектра доплерівських частот. Тоді може виникнути неоднозначність визначення координат цілі з дальності.

Умову однозначності визначення координат цілі з дальності можна замінити на наступну:

$$T_n \geq \frac{2\Delta R}{c}, \quad (1)$$

де c – швидкість світла, ΔR – різниця ходу променів в межах ширини діаграми спрямованості (ДС) реальної бортової антени у вертикальній площині за похилою дальністю, яку можна записати

$$\Delta R = \frac{H}{\cos(\alpha + \beta)} - \frac{H}{\cos \alpha}, \quad (2)$$

де H – висота польоту носія, α – кут нахилу антени відносно надіру, β – ширина ДС реальної бортової антени в вертикальній площині.

Тоді умова (1) може бути представлена у вигляді

$$T_n \geq \frac{2H \left[\frac{1}{\cos(\alpha + \beta)} - \frac{1}{\cos \alpha} \right]}{c}. \quad (3)$$

Тоді умова однозначності визначення РСА координат цілі з дальності буде

$$F_n \leq \frac{c}{2H \left[\frac{1}{\cos(\alpha + \beta)} - \frac{1}{\cos \alpha} \right]}. \quad (4)$$

Спільна умова однозначності визначення кутових координат та координат цілі з дальності, згідно з (4) та врахування того, що частота повторення зондувальних сигналів повинна бути не більше спектра доплерівських частот становить

$$\frac{2v}{L_e} \leq F_n \leq \frac{c}{2H \left[\frac{1}{\cos(\alpha + \beta)} - \frac{1}{\cos \alpha} \right]}, \quad (5)$$

де v – швидкість руху носія, L_e – розмір розкриття реальної бортової антени.

При виникненні протиріччя в (5) можна змінювати параметри діаграми спрямованості реальної бортової антени.

Отже, пропонується умова вибору частоти повторення зондувальних сигналів для усунення спільних неоднозначностей визначення кутових координат цілей та визначення дальності до цілі РСА. А саме – збільшення частоти повторення зондувальних сигналів до величини при якій невизначеність зникає.

Величина частоти повторення зондувальних сигналів для усунення спільних неоднозначностей вибирається за умовою (5).

У випадку виникнення протиріч можна знаходити компроміс шляхом зміни ширини ДС реальної антени у вертикальній площині за умовою (5).

Перспективи подальших досліджень полягають у чисельних методах дослідження умови (5).

Результати можуть бути застосовані при проектуванні РСА.

Список використаних джерел:

1. Манойлов В.П., Омельчук В.В., Опанюк В.В. Дистанційне зондування Землі із космосу: науково-технічні основи формування й обробки видової інформації мельчук. Житомир: ЖДТУ. 2008. 384 с.

Кондратюк В.А., здобувач, гр. ТР-23-1
Макієвський О.А., здобувач, гр. PhD-172-24-1

Ципоренко В.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

СИСТЕМА ДОБОВОГО КОНТРОЛЮ ЧАДНОГО ГАЗУ З ВИКОРИСТАННЯМ ТРАНСИВЕРА NRF24L01 ТА ESP8266

У сучасних умовах експлуатації житлових, навчальних і виробничих приміщень проблема контролю якості повітря набуває особливої актуальності. Одним із найбільш небезпечних забруднювачів повітря є чадний газ (CO), який утворюється внаслідок неповного згоряння палива та становить серйозну загрозу для здоров'я і життя людини. Особливістю чадного газу є відсутність запаху та кольору, що унеможливає його своєчасне виявлення без застосування спеціальних технічних засобів. У зв'язку з цим виникає необхідність створення автоматизованих систем безперервного моніторингу концентрації CO з можливістю оперативного реагування на небезпечні ситуації.

Метою даної роботи є розробка системи добового контролю концентрації чадного газу в приміщенні з використанням технологій Інтернету речей, яка забезпечує безперервний збір даних, їх бездротову передачу, відображення на web-сторінці та автоматичне керування системою вентиляції при перевищенні допустимих рівнів CO. Для досягнення поставленої мети було виконано аналіз існуючих газових сенсорів, бездротових засобів передачі даних та мікроконтролерних платформ, а також обґрунтовано вибір елементної бази системи.

Об'єктом дослідження є процеси автоматизованого моніторингу концентрації чадного газу в повітрі приміщень. Предметом дослідження є апаратні та програмні засоби побудови бездротових IoT-систем контролю газового середовища.

У якості чутливого елемента в системі використано напівпровідниковий газовий датчик MQ-7, принцип роботи якого базується на зміні електричного опору чутливого шару діоксиду олова залежно від концентрації чадного газу. Для коректної роботи датчика реалізовано двофазний термоцикл, що забезпечує стабільність вимірювань і підвищену чутливість до CO. Аналоговий сигнал з датчика зчитується мікроконтролером Arduino Nano, де виконується його оцифрування, первинна обробка та усереднення результатів вимірювань.

Передача даних між вимірювальним та приймальним вузлами здійснюється за допомогою бездротового трансивера nRF24L01, який працює у діапазоні 2,4 ГГц та забезпечує надійний зв'язок на відстані до 30 метрів у межах приміщення. Застосування даного модуля дозволило реалізувати стабільну передачу даних із мінімальним енергоспоживанням та апаратною підтримкою контролю доставки пакетів. Центральним керуючим елементом системи є мікроконтролер ESP8266, який виконує функції приймання даних, їх аналізу, збереження та відображення. На базі ESP8266 реалізовано вбудований web-сервер, що забезпечує доступ користувача до поточних і архівних даних через стандартний веб-браузер. Web-інтерфейс відображає числові значення концентрації чадного газу та графік її зміни протягом доби, що дозволяє аналізувати динаміку стану повітря.

Особливу увагу в роботі приділено розробці алгоритму автоматичного керування вентиляційною системою. У разі перевищення встановленого порогового значення концентрації CO мікроконтролер ESP8266 формує керуючий сигнал на релейний модуль, який забезпечує автоматичне ввімкнення вентиляції. Після зниження концентрації чадного газу до безпечного рівня вентиляція автоматично вимикається. Для підвищення стабільності роботи системи реалізовано механізм гістерезису, що запобігає частим перемиканням виконавчих елементів.

Для перевірки працездатності системи проведено моделювання її роботи, яке підтвердило коректність алгоритмів вимірювання, передачі та обробки даних. Отримані результати свідчать про здатність системи забезпечувати безперервний добовий контроль концентрації чадного газу та своєчасне реагування на аварійні ситуації.

Розроблена система є функціональною, масштабованою та придатною для практичного застосування в житлових і навчальних приміщеннях. Подальший розвиток проєкту може передбачати використання хмарних сервісів для зберігання даних, інтеграцію мобільного застосунку та розширення кількості контрольованих параметрів навколишнього середовища.

Список використаних джерел:

1. Datasheet MQ-7 Gas Sensor. Технічний опис та характеристики датчика чадного газу MQ-7.
2. ESP8266 Technical Reference Manual. – Espressif Systems, 2021.
3. Al-Fuqaha A. et al. Internet of Things: A Survey. IEEE Communications Surveys & Tutorials, 2019.

Підкаменний О.М., здобувач, гр. ІВ-22-1

Ципоренко В.В., к.т.н., доцент

Державний університет «Житомирська політехніка»

РОЗРОБЛЕННЯ СИСТЕМИ МОНІТОРИНГУ ПРИСУТНОСТІ ТА ПЕРЕМІЩЕННЯ В ПРИМІЩЕННІ НА БАЗІ ІОТ ТЕХНОЛОГІЙ

У сучасних умовах актуальним є створення доступних та ефективних систем безпеки для приміщень. Традиційні рішення, такі як відеоспостереження або інфрачервоні датчики, мають обмеження у вартості, складності встановлення та точності виявлення нерухомих об'єктів. Альтернативою є використання радарних сенсорів у поєднанні з технологіями Інтернету речей (IoT).

Метою роботи є розробка системи моніторингу присутності та переміщення людини в приміщенні на базі радарного сенсора 24 ГГц, мікроконтролера ESP32-C3 та веб-інтерфейсу.

Об'єктом дослідження є процес виявлення присутності людини у приміщенні та передача даних у реальному часі. Предметом дослідження є методи побудови систем моніторингу з використанням радарних сенсорів та IoT-технологій.

Система складається з радарного сенсора Hi-Link LD2450, мікроконтролера ESP32-C3 та веб-інтерфейсу. Сенсор здійснює виявлення руху та присутності людини, включаючи нерухомі об'єкти. Мікроконтролер обробляє отримані дані та передає їх на сервер через Wi-Fi у форматі JSON. Веб-інтерфейс забезпечує відображення інформації у вигляді інтерактивної карти приміщення.

Принцип роботи системи полягає у безперервному моніторингу простору. У разі виявлення присутності людини дані передаються на сервер і відображаються у веб-додатку в режимі реального часу. Для передачі даних використовуються протоколи HTTP або MQTT.

Особливістю системи є використання мапінгу приміщення з поділом на зони, що дозволяє локалізувати активність та відстежувати переміщення людини між зонами. Це підвищує інформативність системи порівняно з традиційними сигналізаціями.

Програмна реалізація включає розробку прошивки для ESP32-C3 у середовищі Arduino IDE та створення веб-інтерфейсу з використанням HTML, CSS та JavaScript.



Рис. 1 – Прототип відстеження через веб-інтерфейс

У ході тестування встановлено, що система стабільно виявляє присутність людини, включаючи випадки нерухомого перебування. Затримка передачі даних становить близько 1–2 секунд, що є прийнятним для систем реального часу.

Отримані результати підтверджують ефективність використання радарних сенсорів у системах моніторингу та контролю доступу. Розроблена система може застосовуватися у житлових та офісних приміщеннях як доступне рішення для підвищення рівня безпеки.

Список використаних джерел:

1. Espressif Systems. ESP32-C3 Technical Reference Manual. [Електронний ресурс]. – 2025. – Режим доступу: 2025.https://documentation.espressif.com/esp32-c3_technical_reference_manual_en.pdf
2. Hi-Link. LD2450 Radar Sensor Documentation. [Електронний ресурс]. – 2023. – Режим доступу: https://www.tinytronics.nl/product_files/006000_HLK-LD2450-Instruction-Manual.pdf
3. Espressif Systems. ESP-IDF Programming Guide [Електронний ресурс]. – 2024. – Режим доступу: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32c3/>
4. Arduino. WiFi Library Documentation [Електронний ресурс]. – 2023. – Режим доступу: <https://www.arduino.cc/en/Reference/WiFi>

Пономаренко І.С., здобувач, гр. ТР-23-1

Ципоренко В.Г., к.т.н., доцент

Державний університет «Житомирська політехніка»

РОЗРОБКА ОММЕТРА НА ОСНОВІ ARDUINO UNO

У сучасних технічних системах точність та оперативність вимірювань електричних величин є визначальними факторами для забезпечення надійності обладнання та автоматизації процесів. Омметри, як прилади для визначення електричного опору, широко застосовуються у лабораторній практиці, сервісному обслуговуванні та виробничих технологіях. З урахуванням розвитку мікроконтролерних платформ, виникає потреба у створенні компактних, програмовано керованих вимірювальних пристроїв, що поєднують доступність, точність та можливість модернізації.

У даній роботі розглянуто розробку цифрового омметра на основі мікроконтролера Arduino Uno з діапазоном вимірювання від 1 до 10 кОм та максимальною допустимою похибкою 3%. Актуальність роботи зумовлена поширенням мікроконтролерних систем у навчальних лабораторіях та практичних інженерних застосуваннях, де потрібні прості та надійні засоби вимірювання. Запропонований прилад відзначається мінімальною апаратною складністю, що робить його зручним у реалізації та подальшому використанні.

У процесі роботи проведено огляд конструктивних та функціональних особливостей аналогових і цифрових омметрів, подано їх класифікацію за технічними характеристиками та сферами застосування. Окремо підкреслено переваги цифрових омметрів, зокрема можливість програмної фільтрації сигналів, підвищеної точності вимірювань та інтеграції з іншими системами.

Запропонована структурна схема омметра включає мікроконтролер Arduino Uno, еталонні резистори, вимірювальний вхід та модуль індикації на базі LCD-дисплея. Такий підхід забезпечує стабільність показів та спрощує калібрування пристрою. Функціональна схема розкриває логіку обробки даних від моменту зчитування аналогового сигналу до формування результату для відображення. Використання фіксованих резисторів замість потенціометрів мінімізує вплив зовнішніх факторів на результат вимірювання та підвищує повторюваність експериментів.

Програмна реалізація омметра створена на основі бібліотеки LiquidCrystal. Алгоритм роботи передбачає періодичне зчитування

даних з аналогового входу, обчислення опору та виведення результату у форматі чотирьох символів. Додатковий вивід даних у серійний монітор забезпечує зручність налагодження та оцінювання точності вимірювань. Це робить прилад придатним як для лабораторних робіт, так і для використання у віддалених або мобільних вимірювальних системах.

Моделювання пристрою проведено у віртуальному середовищі Tinkercad, що дозволило підтвердити правильність вибраних параметрів, стабільність обчислень та відповідність результатів технічному завданню. Отримані результати свідчать про те, що розроблений омметр забезпечує точність, достатню для навчальних і базових інженерних задач, а його конструкція може бути легко масштабована або доповнена новими модулями.

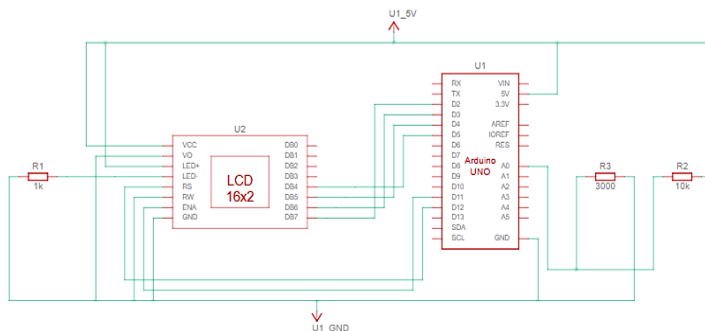


Рис. 1 – Електрична принципова схема омметра

Узагальнюючи результати дослідження, слід зазначити, що запропонований омметр є ефективним прикладом використання мікроконтролерних платформ для побудови простих вимірювальних приладів. Його гнучка структура дозволяє розширювати функціонал, змінювати діапазон вимірювань та інтегрувати пристрій у складніші системи автоматизації, що робить розробку перспективною у контексті подальших інженерних досліджень.

Список використаних джерел:

1. Electronics Hub. [Електронний ресурс]. Режим доступу: <https://www.electronicshub.org/>
2. ElectroSchematics. [Електронний ресурс]. Режим доступу: <https://www.electroschematics.com/>
3. Circuit Digest. [Електронний ресурс]. Режим доступу: <https://circuitdigest.com/>

Сорокін Д.А., аспірант

Зилевіч М.О., PhD, ст. викладач

*Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»*

ФАКТОРИ ТЕХНОГЕННОГО ТА ГЕОМЕТРИЧНОГО ВПЛИВУ НА ТОЧНІСТЬ ЛОКАЛІЗАЦІЇ ОБ'ЄКТІВ У МЕРЕЖАХ LORA

Технологія LoRa, що базується на методі модуляції CSS, на сьогодні є фундаментом для побудови низькоспоживаючих мереж великого радіусу дії (LPWAN). Попри високу чутливість приймачів, ефективність систем наземного позиціонування на її основі суттєво лімітується специфікою розповсюдження радіосигналу в реальних умовах. Наявність щільної забудови в урбанізованих районах та значне загасання енергії сигналу на відкритій місцевості створюють комплексні перешкоди. Аналіз природи похибок, що виникають у таких умовах, є критично важливим для розробки стійких алгоритмів локалізації.

Фундаментальною проблемою при використанні показника потужності сигналу (RSSI) для дистанційного вимірювання є нелінійність його деградації в неідеальних середовищах. Втрати потужності (Path Loss) суттєво відхиляються від теоретичних значень для вільного простору. У зв'язку з цим, для підвищення адекватності математичного опису каналу зв'язку доцільно застосовувати моделі затінення, які враховують специфіку середовища. Експериментальні дані підтверджують, що параметри потребують динамічної адаптації під конкретний ландшафт, оскільки фіксовані коефіцієнти призводять до значних похибок позиціонування.

Специфіка логарифмічної залежності між RSSI та відстанню обумовлює високу вразливість системи на великих дистанціях [1, 3]. На периферії зони покриття навіть незначні амплітудні флуктуації, спричинені шумами, призводять до непропорційно великих відхилень при розрахунку фізичних координат. Ситуація ускладнюється зниженням співвідношення сигнал/шум (SNR), що робить результати локалізації нестабільними та важкопередбачуваними [3, 4].

Окрім фізичних параметрів сигналу, вагомим чинником є просторова архітектура мережі. Ефективність алгоритмів трилатерації безпосередньо залежить від геометричного фактора – взаємного розташування шлюзів та об'єкта пошуку [2]. Неоптимальна конфігурація базових станцій спричиняє розширення області невизначеності (площі ймовірного знаходження вузла). Для мінімізації

негативних наслідків геометричної розбіжності необхідно впроваджувати методи стохастичної апроксимації, такі як метод найменших квадратів, що дозволяють уточнити координати в умовах зашумлених даних.

Для забезпечення прийнятної точності RSSI-позиціонування необхідно відмовитися від спрощених моделей поширення хвиль на користь адаптивних логарифмічних моделей, що враховують специфіку конкретного середовища. Математична нестабільність оцінки координат на великих відстанях потребує розробки додаткових механізмів фільтрації шумів та врахування поточного рівня SNR. Точність систем локалізації LoRa є похідною від топології розміщення інфраструктури, що вимагає ретельного планування мережі для уникнення зон критичних геометричних похибок.

Список використаних джерел:

1. Alireza S. Evaluation and Improvement of the RSSI-based Localization Algorithm: Received Signal Strength Indication (RSSI). Digitala Vetenskapliga Arkivet, 2015. 109 p.
2. D'Arienzo M. An Experimental Comparison of Basic Device Localization Systems in Wireless Sensor Networks. Network. 2025. Vol. 5, № 2. P. 11. DOI: 10.3390/network5020011
3. Bouras C., Gkamas A., Kokkinos A., Papachristos N. Real-Time Geolocation Approach through LoRa on Internet of Things. 2021 International Conference on Information Networking (ICOIN). 13-16 January 2021. DOI: 10.1109/ICOIN50884.2021.9333860
4. Xu T., Ma D., Fang W., Huang Y. Experimental Study on the Propagation Characteristics of LoRa Signals in Maize Fields. Electronics. 2025. Vol. 14. P. 2156. DOI: 10.3390/electronics14112156

*Горшенін О.Є., к.т.н., доцент
Державний університет «Житомирська політехніка»*

АНАЛІЗ ХАРАКТЕРИСТИК МЕТОДУ НАВІГАЦІЇ БПЛА ЗА ПОЛЕМ РАДІОВИПРОМІНЮВАНЬ ВІД НИЗЬКООРБІТАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ КОСМІЧНИХ АПАРАТІВ: ДОСЯГНЕННЯ ТА НЕДОЛКИ

В поточних умовах радіонавігація БПЛА традиційними методами за сигналами глобальних супутникових навігаційних систем стає вкрай ненадійною з-за впливу радіоелектронних завад за методами «спуфінгу» [1]. Сучасний напрямок розвитку радіонавігації БПЛА базується на загальній концепції «сигналів можливості» (Signals of Opportunity, SoOP), коли існуючі комунікаційні або радіотрансляційні системи в той чи інший спосіб використовуються як орієнтири для навігації [2]. Такій підхід дозволяє покращити завадостійкість навігаційного обладнання за рахунок нетрадиційного використання джерел радіовипромінювань у тому числі радіовипромінювань космічних апаратів [3].

Метою доповіді є обґрунтування основних засад реалізації та опис реальних можливостей стійкого до «спуфінгу» методу визначення поточного просторового положення БПЛА на основі SoOP за кутами надходження сигналів (Angle of Arrival, AoA). За початковою гіпотезою саме такий метод з урахуванням величезної кількості низькоорбітальних телекомунікаційних КА (на кшталт Starlink, OneWeb, Iridium тощо) мав забезпечити величезну стійкість до спуфінгових завад, бо є нечутливим до синхронізації та хибних затримок сигналів.

Сучасна концепція SoOP розглядає такі методи радіонавігації, коли існуючі комунікаційні або радіотрансляційні системи в той чи інший спосіб використовуються як орієнтири для навігації. Більшість робіт розглядає використання методів SoOP на основі частотно-часового аналізу сигналів джерел наземних та супутникових радіовипромінювань у різних діапазонах. В науковій літературі розглядалися системи, які використовують інтерферометричні пеленги від наземних базових станцій GSM та методом тріангуляції визначають поточне положення БПЛА.

Методи оцінювання за SoOP, що засновані на аналізі часу приходу сигналів від джерел з точно відомими координатами: TOA (time of arrival), TDOA (time difference of arrival), дають найвищу точність позиціонування. Але роботі систем SoOP навігації, які використовують

методи часових та доплеровських вимірювань (TOA/TDOA), значно перешкоджають системи радіоелектронної протидії (РЕП), які використовують метод так званого «спуфінгу». В умовах таких перешкод для навігації за SoOP може виявитися доцільним використання способу оцінювання місцеположення за АОА. Цей спосіб вимірювання має нижчі точності, але не потребує точної синхронізації шкали часу, а так, не піддається «спуфінгу».

У випадку використання за опорні джерела сигналів радіоканалів «борт-земля» КА низькоорбітальних (LEO) систем різного призначення виникає значна проблема – ідентифікація сигналів щодо конкретного КА щоб пов'язати напрямок приходу сигналу з координатами цього КА. Останнім часом задача ідентифікації постійно ускладнюється стрімким зростанням кількості КА в угрупованні, що працюють на тих самих діапазонах частот з складним і часто непрозорим алгоритмом періодичного перепризначення несучих частот конкретному КА. Для подолання проблеми ідентифікації пропонується використати множини сигналів від КА як прогнозованого (детермінованого) поля потужності випромінювань в певному діапазоні з використанням його як у методах навігації за фізичними полями: навігація за рельєфом поверхні під повітряним об'єктом навігації (Terrain Contour Matchin, TERCOM) або за зображенням поверхні під об'єктом (Digital Scene Matching Area Correlator, DSMAC).

Проведені дослідження та розрахунки показали, що реалізація такого підходу сучасними засобами можлива, але досягнути задовільної для практичних потреб не вдається саме з-за геометричних умов проведення вимірювань.

Список використаних джерел:

1. *Spravil, J., Hemminghaus, C., von Rechenberg, M., Padilla, E., & Bauer, J.* (2023). Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. *Journal of Marine Science and Engineering*, 11(5), 928C. URL: <https://doi.org/10.3390/jmse11050928>
2. *Wilfred E. Noel.* Signals of Opportunity Navigation Using Wi-Fi Signal. Thesis. USAF Department of the air force. Air university. Air force institute of technology. Wright-Patterson Air Force Base, Ohio, 2011. URL: <https://apps.dtic.mil/sti/tr/pdf/ADA540162.pdf>.
3. *Yixuan Zhu.* Opportunistic Positioning with Starlink. / *Zhu Yixuan* // [Electronic resource]. – Access mode : https://www.researchgate.net/publication/387955381_Oportunistic_Positioning_with_Starlink, DOI:10.13140/RG.2.2.35301.10724

*Клочко К.А., к.т.н., доцент
Журавель Р.В., здобувач
Завгородній Д.А., здобувач
Куропятник Б.В., здобувач
Ломоносов М.С., здобувач*

Дніпровський державний технічний університет

ІНТЕГРОВАНА ІoT-СИСТЕМА МОНІТОРИНГУ ТА КЕРУВАННЯ ІНФРАСТРУКТУРОЮ НАСЕЛЕНИХ ПУНКТІВ

Сучасні концепції розвитку міст (Smart City) передбачають інтеграцію інформаційно-комунікаційних технологій моніторингу та керування інфраструктурою населеного пункту, таких як Інтернет речей (ІoT), з метою підвищення безпеки, енергоефективності та комфорту життя населення. Розглянуто ІoT-систему «розумного освітлення», систему забезпечення безпеки дорожнього руху, систему моніторингу та прибуття громадського транспорту.

Запропоновану інтегровану систему реалізовано на базі Raspberry Pi 4 Model B та Raspberry Pi 5, які виконують функції периферійного вузла збору, локальної обробки та передавання даних. Raspberry Pi 4B застосовано для задач зчитування показів сенсорів, передавання телеметрії, роботи з MQTT, Node-RED та веб-інтерфейсом. Raspberry Pi 5 – у задачах з підвищеною обчислювальною продуктивністю, як обробка відеопотоку з камер та аналіз ситуації, детекції транспортних засобів та прогнозуванні його прибуття в реальному часі.

Для реалізації ІoT-системи «розумного освітлення» до Raspberry Pi можуть бути підключені: датчики освітленості (LDR з ADC-модулем ADS1115 або BH1750 по I2C); датчики руху типу PIR HC-SR501; релейні модулі або MOSFET-драйвери для керування світильниками. Програмна частина цієї підсистеми реалізована засобами Python із використанням бібліотек I2C, а також smbus2 для роботи з I2C-пристроями. Для диспетчеризації й візуалізації стану освітлення застосовано Node-RED, який забезпечує швидке створення логіки керування, панелей моніторингу та сценаріїв автоматизації.

Для побудови системи забезпечення безпечного руху транспорту в місті базовими апаратними засобами є: Raspberry Pi Camera Module; ультразвукові датчики, індуктивні сенсори або ІЧ-датчики для фіксації присутності об'єктів; світлофори/сигнальні модулі, виконавчі реле, інформаційні табло; модулі звукового або світлового сповіщення.

На програмному рівні така підсистема може використовувати OpenCV для аналізу відеозображень, виділення об'єктів, підрахунку кількості транспорту, фіксації порушень або виявлення небезпечних ситуацій. Для інтеграції з мережею та серверною частиною використано Mosquitto, а для збереження подій базу даних SQLite.

Для реалізації системи моніторингу громадського транспорту до Raspberry Pi підключено: GPS-модулі типу u-blox NEO-6M; модулі Wi-Fi для передавання координат транспортних засобів.

Отримані координати зчитуються через UART або USB та надсилаються на сервер через MQTT або HTTP. На стороні сервера дані накопичуються і відображаються на картографічному веб-інтерфейсі. Таким чином формується підсистема диспетчерського контролю місцеположення транспортних засобів у реальному часі.

Для системи визначення та прогнозування прибуття громадського транспорту на зупинку використовуються ті самі GPS-модулі, сенсори моніторингу транспорту на контрольних точках; кнопки запиту інформації на зупинках; світлодіодні, LCD або e-paper дисплеї для виведення часу прибуття. Алгоритм роботи передбачає збір поточних координат транспорту, розрахунок швидкості руху, визначення відстані до зупинки та оцінювання орієнтовного часу прибуття.

Запропонована інтегрована IoT-система дозволяє об'єднати різні аспекти міської інфраструктури як автоматизація освітлення вулиць, моніторинг транспортних потоків та «розумних зупинок» в єдину інформаційну платформу для реалізації компонентів Smart City. Використання Raspberry Pi та сучасних IoT-технологій забезпечує гнучкість, доступність та ефективність впровадження таких рішень. Подальші дослідження можуть бути спрямовані на використання методів машинного навчання для підвищення точності прогнозування транспортних потоків.

Список використаних джерел:

1. Ключко К.А., Пупков С.С. Розподілена система керування трафіком в «розумному» місті. Комп'ютерні технології: інновації, проблеми, рішення: матеріали VIII Всеукраїнської науково-технічної конференції (Житомир, 02-03 грудня 2025 р.). Житомир: Житомирська політехніка, 2025. С.309-310.
2. Bradski G., Kaehler A. Learning OpenCV: Computer Vision with the OpenCV Library. – Sebastopol: O'Reilly Media, 2008. – 555 p.
3. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // IEEE Internet of Things Journal. – 2014. – Vol. 1, No. 1. – P. 22–32.

Віктор Гнатюк^{1,2}, Левон Петросян¹

¹Державний університет «Київський
авіаційний інститут»

²Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації

МЕТРИКИ ОПЕРАЦІЙНОЇ РЕЗИЛЬЄНТНОСТІ ДЛЯ ОЦІНЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ NETWORK DIGITAL TWIN

Телекомунікаційні мережі є критичною інфраструктурою, стійкість якої визначає функціонування суспільства. За даними Світового банку (RDNA4), збитки телекомунікаційного сектору України становлять 2,24 млрд доларів [1]. Технологія Network Digital Twin (NDT) – віртуальне представлення мережевої інфраструктури, синхронізоване з визначеною частотою [2], – дозволяє моделювати поведінку мережі та оптимізувати рішення. Проте ефективне застосування NDT потребує формалізованих кількісних метрик резильєнтності.

Існуючі системи NMS/OSS фіксують поточний стан мережі, але не оцінюють структурну резильєнтність – здатність мережі протистояти збоєм та відновлюватися [3]. Сучасні дослідження пропонують часову декомпозицію резильєнтності (absorption–adaptation–recovery) [4], просторове моделювання покриття [5], CVaR-метрики хвостового ризику [6] та ймовірнісні графові моделі [7]. Водночас бракує уніфікованого набору метрик на рівні мережевої топології в контексті NDT.

Мета роботи – формалізація набору метрик операційної резильєнтності для інтеграції в архітектуру NDT та демонстрація їх працездатності.

На основі синтезу джерел [1]–[7] виділено шість метрик:

Доступність (Availability): $A = T_{up}/T_{total}$ – частка часу функціонування; $A \geq 0,99$ для магістральних вузлів [1].

Зв’язність (Connectivity): $C = P_{connected}/P_{total}$ – частка пар вузлів із наскрізним з’єднанням при частковій деградації [7].

Відмовостійкість (Fault Tolerance): $FT = 1 - |V_{critical}|/|V|$ – частка некритичних вузлів; $V_{critical}$ – точки артикуляції графа [6].

Час відновлення (Time-to-Recover): $TTR = (1/n) \sum (t_{restore\_i} - t_{detect\_i})$ – середній час усунення інциденту [1], [4].

Надлишковість (Redundancy): $R = (E - V + 1)/E$ – нормалізована цикломатична надлишковість зв’язного графа [7].

Енергетична автономність (Energy Autonomy): $EA = N_{\text{autonomous}}/N_{\text{total}}$
– частка базових станцій із резервним живленням ≥ 72 год [1], [3].

Працездатність метрик продемонстровано на гіпотетичній мережі із 7 вузлів та 7 ребер. Базові значення: $C_0=1,000$; $R_0=0,143$; $EA_0=0,286$; $FT_0=0,571$. Після руйнування хаба V6: $C'=0,667$; $R'=0,000$; $EA'=0,167$. Мінімальне відновлення (інтервенція A: +1 ребро) повертає C до 1,000, але R та EA не змінюються. BBV-модернізація (інтервенція B: +2 ребра та автономне живлення) дає $C_B=1,000$; $R_B=0,167$; $EA_B=0,500$. За вагами $w_C=0,50$; $w_R=0,20$; $w_{EA}=0,30$ пріоритетний бал B (0,300) перевищує бал A (0,167) на 80%, що підтверджує перевагу системного підходу.

Висновки. Запропоновано набір із шести формалізованих метрик операційної резильєнтності (A, C, FT, TTR, R, EA), адаптованих для NDT. Числовий приклад підтверджує обчислювальну працездатність та здатність метрик кількісно диференціювати варіанти відновлення. Перспективи – пілотна валідація на реальному сегменті мережі та калібрування порогових значень.

Список використаних джерел:

1. Ukraine Fourth Rapid Damage and Needs Assessment (RDNA4). Washington : World Bank, 2025.
2. Network Digital Twin Use Case Classification. Ver. 2.0. IOWN Global Forum, 2024. 84 p.
3. Ayers S., Birk T. Resilient Telecommunications Infrastructure. Washington : World Bank, 2024. 44 p.
4. Reifert R.-J., Roth S., Ahmad A. A., Sezgin A. Comeback Kid: Resilience for Mixed-Critical Wireless Network Resource Management // IEEE Trans. Veh. Technol. 2023. Vol. 72, no. 12. P. 16177–16194.
5. Liang Z., Li Y.-F. Holistic Resilience and Reliability Measures for Cellular Telecommunication Networks // Reliab. Eng. Syst. Saf. 2023. Vol. 237. Art. 109335.
6. Xue Z., Liang Z. Service Risk Evaluation of Telecommunication Core Network: A Perspective of Routing Resilience // Reliab. Eng. Syst. Saf. 2025. Vol. 255. Art. 110629.
7. Kuikka V., Rantanen H. Resilience of Multi-Layer Communication Networks // Sensors. 2023. Vol. 23, no. 1. Art. 86.

*Клочко К.А., к.т.н., доцент
Коваленко Д.В., здобувач
Вантух М.В., здобувач
Черняков М.Є., здобувач
Лан В.В., здобувач*

Дніпровський державний технічний університет

ІоТ-СИСТЕМА МОНІТОРИНГУ ІНФРАСТРУКТУРИ ТА ЕКОЛОГІЧНОГО СТАНУ НАСЕЛЕНИХ ПУНКТІВ

Сучасні міста потребують ефективних рішень для управління екологічним станом, поводження з відходами та організації моніторингу дорожнього руху і паркування транспортних засобів. Використання технологій Інтернету речей (IoT) дозволяє створювати розподілені системи збору та обробки даних у реальному часі, що є основою концепції «розумного» міста (Smart City).

В запропонованій інтегрованій системі розглянуто наступні ключові підсистеми:

1) IoT-система моніторингу екологічного стану міського середовища, яка призначена для контролю параметрів якості повітря. Вона реалізується на базі Raspberry Pi 4B або Raspberry Pi 5 із підключенням наступних сенсорів: датчики газів (MQ-135, MQ-7); датчики твердих частинок (PM2.5/PM10, SDS011); датчики температури та вологості (DHT22, BME280).

2) IoT-система моніторингу заповнення контейнерів твердих побутових відходів, яка забезпечує контроль рівня заповнення контейнерів для оптимізації маршрутів збору та вивезення відходів. Основними апаратними компонентами є: ультразвукові датчики (HC-SR04) для вимірювання рівня заповнення; модулі зв'язку (Wi-Fi або GSM) для передавання даних; Raspberry Pi як вузол збору, обробки інформації та сповіщення про необхідність вивезення сміття, що зменшує витрати на логістику та покращує санітарний стан міста.

3) IoT-система моніторингу, ідентифікації та керування міським паркуванням, яка призначена для виявлення учасників дорожнього руху, визначення зайнятості паркомісць та інформування користувачів. Для цього використовуються: датчики зайнятості (магнітні, індуктивні або ІЧ-сенсори); камери; Raspberry Pi для обробки сигналів; індикатори або веб-інтерфейси для відображення інформації. Дані про вільні місця передаються в систему, що дозволяє водіям швидко знаходити доступні паркомісця та зменшує затори.

Програмна реалізація виконана мовою Python із використанням бібліотек для роботи з GPIO, I2C та UART, а також Node-RED для інтеграції та візуалізації даних.

Для міської інфраструктури запропоновані системи дозволяють:

1) у сфері екологічного моніторингу здійснювати постійний контроль якості повітря та оперативно реагувати на перевищення показників, які відстежуються, від допустимих норм забруднення з застосуванням звукового та/чи світлового супроводу для привертання уваги оператора.

2) у сфері поводження з відходами забезпечує оптимізацію маршрутів вивезення сміття, що знижує експлуатаційні витрати та підвищує ефективність роботи комунальних служб.

3) у сфері моніторингу, ідентифікації та паркування сприяє контролю порушень правил дорожнього руху, зменшенню затримок, економії часу водіїв та підвищенню пропускної здатності міських доріг.

Запропонована інтегрована IoT-система дозволяє об'єднати різні аспекти моніторингу міста в єдину інформаційну платформу. Із переваг системи слід відмітити використання відкритих апаратних і програмних рішень, можливість роботи в режимі реального часу

Використання Raspberry Pi та сучасних сенсорних технологій забезпечує гнучкість, доступність і ефективність реалізації таких рішень. У роботі розглянуто підхід до побудови інтегрованої IoT-системи моніторингу міського середовища, що об'єднує підсистеми контролю якості повітря, заповнення контейнерів твердих побутових відходів та керування міським трафіком і паркуванням. Запропоновано архітектуру системи на базі Raspberry Pi, сенсорних модулів та мережевих технологій передачі даних.

Список використаних джерел:

1. Ключко К.А., Пупков С.С. Розподілена система керування трафіком в «розумному» місті. Комп'ютерні технології: інновації, проблеми, рішення: матеріали VIII Всеукраїнської науково-технічної конференції (Житомир, 02-03 грудня 2025 р.). Житомир: Житомирська політехніка, 2025. С.309-310.

2 Bradski G., Kaehler A. Learning OpenCV: Computer Vision with the OpenCV Library. – Sebastopol: O'Reilly Media, 2008. – 555 p.

3. Данилюк А., Муляревич О. Методи та засоби керування дорожнім рухом. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024, 1(25). С.89-102.

4. Raspberry Pi Foundation. Documentation. – URL: <https://www.raspberrypi.com> (дата звернення 25.03.2026)

*Бугайов М. В., к.т.н., ст. досл., ЗННДВ НДУ
Житомирський військовий інститут імені С. П. Корольова*

ДВОКАНАЛЬНИЙ МЕТОД АМПЛІТУДНОГО ПЕЛЕНГУВАННЯ З КОМПЕНСАЦІЄЮ РІВНЯ ШУМУ

У зв'язку з розвитком систем радіомоніторингу (РМ) із використанням безпілотних літальних апаратів (БпЛА) виникла необхідність у розробленні простих і дешевих засобів пеленгування джерел радіовипромінювання (ДРВ). Для розміщеного на борту малорозмірного БпЛА засобу РМ метод пеленгування повинен бути стійким до впливу багатопроменевого поширення, простим у реалізації та мати високу швидкість пошуку ДРВ за напрямком. Даним вимогам задовольняє амплітудний метод пеленгування, перевагою якого є не такі жорсткі вимоги до синхронізації та фазової ідентичності каналів порівняно з більш точними фазовим та кореляційним методами.

Серед існуючих методів амплітудного пеленгування при реалізації антенної системи для розміщення на БпЛА доцільно використати сумарно-різницевий метод. Широке поширення даного методу зумовлене такими його перевагами як низька обчислювальна складність та висока швидкість розрахунку напрямку на ДРВ [1-2]. Сумарно-різницевий метод пеленгування при відносно високих значеннях (більше 20 дБ) відношення сигнал-шум (ВСШ) забезпечує практично незміщені оцінки напрямку на ДРВ. Проте при пеленгуванні слабких сигналів оцінки напрямку на ДРВ будуть зміщеними, особливо при значних відхиленнях від рівносигнального напрямку [3]. Для уникнення зміщення необхідно повертати антенну систему для приймання радіосигналу за рівносигнальним напрямком, що потребує додаткових часових затрат на пеленгування ДРВ, а також постійної зміни орієнтації антенної системи або БпЛА під час польоту. У роботі запропоновано двоканальний метод амплітудного пеленгування з компенсацією рівня шуму, що дозволяє суттєво зменшити зміщення оцінки азимуту при низьких значеннях ВСШ і не повертати при цьому антенну систему.

Оцінку напрямку на ДРВ у двох сусідніх каналах антенної системи для невідомого рівня шуму можна записати у такому вигляді:

$$\hat{\theta} = \frac{\Delta\theta^2 N_{ant}}{4\pi \ln 2} \ln \sqrt{\frac{P_2(\theta) - \hat{\sigma}_{\xi 2}^2}{P_1(\theta) - \hat{\sigma}_{\xi 1}^2}} + \frac{\pi}{N_{ant}}, \quad (1)$$

де $\Delta\theta$ – ширина діаграми спрямованості логоперіодичної антени;

N_{ant} – кількість антен;

$P_1(\theta), P_2(\theta)$ – потужності прийнятих сигналів у двох каналах;

$\hat{\sigma}_{\xi_1}^2, \hat{\sigma}_{\xi_2}^2$ – оцінки дисперсії шуму в каналах.

Із виразу (1) видно, що на точність оцінки азимуту впливають помилки оцінок потужності сигнальної суміші в каналах, дисперсії шуму та помилки апроксимації ДС антени, зокрема випадковим відхиленням форми ДС антен від розрахункової, що впливає на значення її ширини $\Delta\theta$, і безпосередньо використовується для оцінювання азимуту. Такі відхилення можуть виникати через деформацію антени та проліт БПЛА біля металевих об'єктів.

Для оцінювання пеленгу на ДРВ за допомогою виразу (1) сигнал повинен бути виявлений у двох сусідніх каналах. Якщо сигнал перевищить поріг лише в одному каналі, то тоді можна вважати, що напрямок на ДРВ знаходиться в межах ширини ДС антени.

Компенсація дисперсії шуму забезпечує суттєве зменшення (практично повну компенсацію) зміщення оцінки азимуту та незначне зростання її середньоквадратичного відхилення (СКВ). Останнє зумовлено тим, що дисперсія різниці двох випадкових величин (в нашому випадку оцінок потужності сигнальної суміші та шуму) дорівнює сумі їх дисперсій. Неповна компенсація рівня шуму, що пов'язана з помилками його оцінювання через обмежений об'єм вибірки, призводить до зростання значень як зміщення оцінки азимуту так і її СКВ. Для рівносигнального напрямку якість компенсації рівня шуму несуттєво впливає як на СКВ оцінки кута так і на її зміщення. Проте при збільшенні відхилення від рівносигнального напрямку вплив якості компенсації рівня шуму на помилки оцінювання напрямку на ДРВ зростає.

Список використаних джерел:

1. Shi Y., Zhou Y. Direction Finding Rectenna Array Based on Amplitude Comparison Method // *International Applied Computational Electromagnetics Society Symposium*, Hangzhou, China, 2023, pp. 1-3, doi: 10.23919/ACES-China60289.2023.10249816.
2. Orduyilmaz A. et al. Passive direction finding using amplitude and phase comparison techniques // *22nd Signal Processing and Communications Applications Conference (SIU)*, Trabzon, Turkey, 2014, pp. 935-938, doi: 10.1109/SIU.2014.6830384.
3. Yan E. et al. Improving Accuracy of an Amplitude Comparison-Based Direction-Finding System by Neural Network Optimization // *IEEE Access*, 2020, vol. 8, pp. 169688-169700, doi: 10.1109/ACCESS.2020.3024031.

Секція 5 ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 378.147:004

*Шуліка О. С., аспірант
Полтавський національний педагогічний університет
імені В. Г. Короленка*

ЦИФРОВІ ОСВІТНІ СЕРВІСИ ЯК ЗАСІБ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ

Сучасний етап розвитку інформаційного суспільства характеризується інтенсивним впровадженням цифрових технологій у всі сфери людської діяльності, що зумовлює якісні трансформації в освітній галузі. Глобалізаційні процеси, стрімкий розвиток інформаційно-комунікаційних технологій, а також виклики, пов'язані з необхідністю організації дистанційного та змішаного навчання, актуалізують проблему підготовки конкурентоспроможного вчителя нового типу. Особливої ваги це набуває у контексті підготовки майбутніх учителів інформатики, які не мають володіти сучасними цифровими інструментами, а й бути здатними ефективно інтегрувати їх у освітній процес.

Цифрова трансформація освіти передбачає зміну традиційних підходів до навчання, орієнтацію на компетентнісну модель освіти, розвиток цифрової грамотності та формування здатності до безперервного професійного саморозвитку. У цьому контексті цифрові освітні сервіси виступають важливим інструментом модернізації змісту, форм і методів навчання, забезпечуючи інтерактивність, мобільність і доступність освітнього процесу.

Нові вимоги до підготовки майбутніх учителів інформатики зумовлюють необхідність формування у них не лише ґрунтовних теоретичних знань, а й практичних навичок використання цифрових технологій у педагогічній діяльності. Це актуалізує потребу в науковому осмисленні можливостей цифрових освітніх сервісів як засобу формування професійної компетентності майбутніх педагогів.

Психолого-педагогічні засади теорії інформатизації сучасної освіти знайшли ґрунтовне відображення у наукових дослідженнях вітчизняних учених, зокрема В. Бикова, Р. Гуревича, М. Жалдака, М. Кадемії, О. Лілік, Н. Морзе, Л. Шевченко та інших.

Цифрові освітні сервіси доцільно розглядати як сукупність програмних засобів, платформ і технологій, що функціонують на основі

інформаційно-комунікаційних технологій і спрямовані на підтримку, організацію та оптимізацію освітнього процесу. Їх використання відкриває широкі можливості для реалізації інноваційних педагогічних підходів, зокрема змішаного та дистанційного навчання, адаптивного навчання, а також персоналізації освітніх траєкторій здобувачів освіти.

У сучасній педагогічній практиці цифрові освітні сервіси виконують не лише допоміжну, але й системоутворюючу функцію. Вони забезпечують інтеграцію різних компонентів освітнього процесу – змісту навчання, засобів подання інформації, комунікації та оцінювання результатів – у єдине цифрове середовище.

У професійній підготовці майбутніх учителів інформатики цифрові освітні сервіси виконують багатофункціональну роль. Зокрема, системи управління навчанням (LMS), представлені такими платформами, як Moodle, Google Classroom, Canvas забезпечують структуровану організацію навчального контенту, контроль і оцінювання результатів навчання, а також моніторинг освітньої діяльності студентів. Хмарні технології (Google Drive, Microsoft OneDrive, а також пакет Google Workspace) сприяють реалізації колективної взаємодії, забезпечують доступ до навчальних матеріалів у будь-який час і з будь-якого пристрою, що особливо важливо в умовах дистанційного навчання. Інтерактивні освітні платформи дозволяють підвищити рівень залученості студентів до освітнього процесу за рахунок використання елементів гейміфікації, інтерактивних завдань і миттєвого зворотного зв'язку. Вони представлені такими сервісами, як Kahoot!, Quizizz, Mentimeter, Nearpod [1. с. 18-19].

Особливого значення набуває використання цифрових сервісів для формування професійних компетентностей майбутніх учителів інформатики. Насамперед йдеться про розвиток інформаційно-цифрової компетентності, яка передбачає здатність ефективно використовувати сучасні інформаційні технології у професійній діяльності. Крім того, цифрові освітні сервіси сприяють формуванню методичної компетентності, оскільки майбутні педагоги набувають досвіду проєктування та реалізації навчального процесу з використанням цифрових інструментів. Серед сервісів для програмування та моделювання, які є особливо важливими у підготовці майбутніх учителів інформатики, варто виділити Replit, GitHub, CodePen та Scratch.

Важливим є також розвиток комунікативної компетентності, що реалізується через організацію онлайн-взаємодії, участь у вебінарах, форумах та інших формах цифрової комунікації. До комунікаційних платформ, що забезпечують синхронну та асинхронну взаємодію, належать Zoom, Microsoft Teams, Google Meet.

Водночас ефективність використання цифрових освітніх сервісів значною мірою залежить від дотримання певних дидактичних умов. До них належать: методично обґрунтований добір цифрових інструментів відповідно до цілей і змісту навчання; інтеграція цифрових технологій у навчальні дисципліни; забезпечення належного рівня цифрової грамотності як студентів, так і викладачів; створення сприятливого інформаційно-освітнього середовища; а також формування критичного мислення та інформаційної культури здобувачів освіти. Недотримання цих умов може призвести до формального використання цифрових технологій без досягнення очікуваних педагогічних результатів [2, с. 123-125].

Варто також зазначити, що цифрові освітні сервіси виступають не лише засобом навчання, але й об'єктом професійного опанування для майбутніх учителів інформатики. У процесі їх використання студенти не лише здобувають знання, але й формують практичні навички роботи з цифровими інструментами, що є необхідною складовою їхньої майбутньої професійної діяльності. Це, у свою чергу, сприяє підвищенню їх конкурентоспроможності на ринку праці та готовності до роботи в умовах цифрової школи.

Таким чином, застосування цифрових освітніх сервісів у професійній підготовці майбутніх учителів інформатики є важливим чинником підвищення якості освіти та її відповідності сучасним викликам. Воно забезпечує модернізацію освітнього процесу, сприяє формуванню ключових професійних компетентностей і створює умови для реалізації інноваційних педагогічних підходів. Перспективи подальших досліджень полягають у розробленні ефективних методичних моделей інтеграції цифрових сервісів у систему підготовки майбутніх педагогів, а також проведенні емпіричних досліджень, спрямованих на оцінювання їх педагогічної ефективності.

Список використаних джерел:

1. Гуревич Р., Кобиця В., Кобиця А., Кізім С., Куцак Л., Опушко Н. Використання цифрових сервісів та інструментів у професійній підготовці майбутніх учителів. *Modern Information Technologies and Innovation Methodologies of Education in Professional Training Methodology Theory Experience Problems*. 2022. С. 5-22. DOI: <https://doi.org/10.31652/2412-1142-2022-64-5-22>

2. Лілік О., Бивалькевич Л. Використання цифрових освітніх платформ у професійній підготовці майбутніх учителів. *Вісник*. 2025. №33 (189). С. 121-126.

DOI:

<https://visnyk.chnpu.edu.ua/index.php/visnyk/article/view/919/967>

УДК 37.091.3:004

Куцан А.В., здобувач

Житомирський державний університет імені Івана Франка

СТВОРЕННЯ ТА ВПРОВАДЖЕННЯ ІНТЕРАКТИВНОГО ОСВІТНЬОГО КОНТЕНТУ

Сучасна освітня парадигма перебуває у стані докорінної трансформації. Традиційна класно-урочна система, що десятиліттями базувалася на статичних паперових носіях, поступово поступається місцем динамічному, високотехнологічному цифровому середовищу. Ключовим інструментом вчителя в цих умовах стає електронний освітній контент (ЕОК). Це не просто оцифрована копія підручника, а складна, багаторівнева дидактична система, що інтегрує мультимедійність, гіпертекстовість та глибоку персоналізацію навчання. Актуальність цієї теми зумовлена не лише викликами дистанційної освіти, а й стратегічними вимогами Нової української школи (НУШ), де формування наскрізної цифрової компетентності є фундаментом успішної особистості.

Теоретичний фундамент ЕОК базується на глибокому розумінні його видової різноманітності та функціонального призначення. Ми класифікуємо сучасний контент на кілька ключових сегментів: від інформаційних лонгвідів у Canva до складних алгоритмічних симуляторів та віртуальних лабораторій. Особливе місце в сучасній школі посідає гейміфікований контент. Використання таких платформ, як Kahoot, Quizizz чи Wordwall, дозволяє перетворити рутинне заучування технічних термінів чи правил безпеки в інтернеті на захопливий змагальний процес. Якісний ЕОК не просто транслює знання – він створює простір для взаємодії, де учень отримує миттєвий зворотний зв'язок, аналізує свої помилки та самостійно коригує освітню траєкторію в режимі реального часу.

Процес створення авторського контенту для уроків інформатики має свою унікальну методичну специфіку. Вчитель у цій системі одночасно виступає і як педагог-методист, і як архітектор цифрового досвіду (Instructional Designer). Головною особливістю розробки матеріалів з інформатики є необхідність візуалізації складних абстракцій. Такі поняття, як логічні оператори, цикли в програмуванні або структура мережових пакетів, стають зрозумілими для школяра лише тоді, коли вони представлені у вигляді динамічної моделі, створеної, наприклад, у Genially. Важливим принципом тут є мікронавчання (micro-learning) – розподіл об'ємного матеріалу на короткі, логічно завершені відеоблоки або інтерактивні картки.

Скринкасти, записані в OBS Studio, тривалістю до 5 хвилин, дозволяють учневі фокусуватися на конкретній операції, що мінімізує когнітивне перевантаження та підтримує стійку увагу протягом усього заняття.

Технологічний аспект створення ЕОК вимагає від педагога володіння широким стеком інструментів. Для структурування теоретичного блоку доцільно використовувати інтерактивні плакати та презентації нового покоління, де кожен елемент є клікабельним і містить додаткові рівні інформації. Для практичної частини ідеальним рішенням є інтеграція хмарних середовищ виконання коду (наприклад, Trinket або Replit) безпосередньо в тіло навчального ресурсу. Це реалізує засадничий принцип ІТ-освіти – «learning by doing» (навчання через дію), коли теорія миттєво перевіряється практикою без перемикання між зайвими вікнами браузера.

Методика використання ЕОК на уроках вимагає радикального перегляду традиційної ролі вчителя. Найбільш ефективною моделлю сьогодні визнано змішане навчання (Blended Learning), зокрема формат «перевернутого класу». У цій моделі учні самостійно опановують теоретичну базу за допомогою заздалегідь підготовленого вчителем електронного контенту, а дорогий час у класі використовується виключно для живого обговорення проблемних питань, командної проєктної діяльності та розв'язання складних кейсів.

Підсумовуючи, можна стверджувати, що створення та професійне використання електронного освітнього контенту – це не просто данина моді, а вимога часу. Впровадження таких підходів на уроках інформатики дозволяє змінити фокус освіти: з пасивного накопичення фактів на активне освоєння інструментів перетворення світу.

Список використаних джерел:

1. Коваленко В.В., Шишкіна М.П., Модель відкритого освітнього середовища з елементами штучного інтелекту для професійного розвитку педагогічних кадрів. Наукові записки. Серія: Педагогічні науки (219). 2025, стор. 43- 49.
2. Кривонос О. М., Кулик С. П., Кривонос М. П. Теоретичні основи візуалізації навчального контенту. Актуальні питання у сучасній науці. 2024. № 12(30). С. 911-922.
3. Сидоренко В., Геревенко А., Головка Д., Чертов В., Коссова-Сіліна Г. Застосування цифрових технологій і штучного інтелекту при розробленні навчально-методичного забезпечення підготовки майбутніх кваліфікованих робітників в умовах профільної освіти: освітньо-професійна програма для короткотермінових курсів підвищення кваліфікації / Вікторія Сидоренко, Андрій Геревенко. Біла Церква: БІНПО ДЗВО «УМО» НАПН України, 2025. 65 с.

УДК 004.77

*Казаков Н.С., здобувач,
Ніжегородцев В.О., к.пед.н, доцент
Державний податковий університет*

АНАЛІЗ СУЧАСНИХ ПРОТОТИПІВ ІНТЕРФЕЙСІВ КОМЕРЦІЙНИХ ВЕБСЕРЕДОВИЩ ОСВІТНІХ ПОСЛУГ

Сучасний ринок комерційної онлайн-освіти вже давно перейшов від простого депонування відеолекцій до реалізації складних екосистем. Прототипування інтерфейсів у цій ніші сьогодні базувалося не лише на естетиці, а й на принципах Learning Experience Design - проєктуванні досвіду навчання.

Аналіз сучасних прототипів дозволив нам виділити обов'язкові модулі комерційного освітнього середовища та зосередитися виявленні закономірностей у побудові інтерфейсів, які максимізують утримання користувача та ефективність засвоєння матеріалу.

Сучасні платформи для створення онлайн курсів є повноцінними LMS-системами керування навчанням, оскільки дають змогу розробляти та розміщувати курси в онлайн просторі, проводити заняття та контролювати успішність кожного [3].

Використання у таких системах інтелектуальних підказок та візуального зворотного зв'язку дозволяє знизити когнітивне навантаження. Концепція сучасних прототипів вебсередовищ освітніх послуг поступово відходять від статичних сіток на користь динамічних інтерфейсів та виступає як персоналізований центр управління, де інтерфейс адаптується під прогрес користувача навчання.

Сучасна онлайн-освіта зіштовхується з викликами, такими як насичення ринку, необхідність забезпечення авторських прав та конфіденційності даних, а також потреба в адаптації до швидких технологічних змін. Технології, які інтегруються в навчальний процес, вимагають значних інвестицій, що є важливим аспектом для підтримки конкуренто-спроможності платформ [2, с.803].

Технологічним проривом в дизайні прототипів стають технології використання ШІ для зміни структури інтерфейсу, додаткові підказки або альтернативний шлях навігації, тач-інтерфейси та офлайн-режим, контрастність, підтримка скрінрідерів, керування з клавіатури, тощо. Замість текстових описів використовуються інтерактивні «спробуй сам» блоки, вбудовані безпосередньо в UI картки курсу. Для спеціалізованих комерційних послуг (медицина, інженерія) інтерфейси передбачають перехід у 3D-простір безпосередньо з браузерного вікна за допомогою WebXR.

У дистанційній освітній системі використовуються мультимедійні педагогічні ресурси, які повинні індивідуалізуватися відповідно до потреб та здібностей кожного [1].

Сучасні інтерфейси проєктуються так, щоб подрібнювати контент на блоки по 5-10 хвилин, а впровадження рівнів доступу, віртуальних нагород та лідербордів безпосередньо в інтерфейс дашборду підвищує ряд когнітивних особливостей сприйняття інформації слухачем.

Аналіз візуальної ідентичності та брендингу розкривається у використанні стриманих кольорових палітр (синій, білий, зелений) для академічних курсів або яскравих, креативних градієнтів для творчих шкіл; часто використовують ілюстрації та анімації для підтримки позитивного настрою при виконанні складних завдань.

Аналіз сучасних прототипів комерційних освітніх вебсередовищ свідчить про зміщення акценту з суто інформативної функції на емоційно-когнітивну взаємодію. На етапі створення прототипів сьогодні домінують інструменти, що дозволяють створювати високоточні моделі та висококонтрастні режими та можливість масштабування без втрати функціональності.

Підсумовуючи вищесказане, проведений аналіз прототипів вказав на те, що майбутнє освітніх інтерфейсів лежатиме у площині гіперперсоналізації, тобто освітнє середовище поступово стає інтелектуальним помічником у навчанні користувачів.

Ефективність таких інтерфейсів трендових комерційних платформ здатна мінімізувати шлях користувача до цільової дії (від початку уроку) та підтримки стану «поток» навчання до завершальної перевірки знань симуляції практичних навичок в інтеграції з використанням VR/AR компонентів.

Список використаних джерел:

1. Вишнівський В.В., Гніденко М.П., Гайдур Г.І., Ільїн О.О. Організація дистанційного навчання. Створення електронних навчальних курсів та електронних тестів. - Навчальний посібник. Київ: ДУТ, 2014. – 140 с.

2. Журба О. М., Перегуда Ю. А. Конкуренція на ринку онлайн-освіти: сучасні тенденції та перспективи розвитку. *Наукові перспективи* № 1(55). СЕРІЯ «Економіка» No 1(55) 2025. С. 798-810.

3. Платформа для створення онлайн курсів: критерії вибору. URL: <https://talken.cloud/blog/platform-for-creating-online-courses/>.

УДК 37.013.4:004.738

*Матвієнко Л.Г., к.пед.н., доцент
Полтавський державний аграрний університет*

МУЛЬТИМОДАЛЬНІ ЦИФРОВІ ПЛАТФОРМИ У ВИКЛАДАННІ ІНОЗЕМНИХ МОВ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Мультимодальні цифрові платформи набувають дедалі більшого значення у системі викладання іноземних мов у закладах вищої освіти, оскільки забезпечують інтеграцію різних способів подання інформації та створюють сприятливі умови для активної взаємодії здобувачів вищої освіти з навчальним матеріалом. У сучасному освітньому дискурсі мультимодальність розглядається як поєднання кількох комунікативних модальностей – текстової, аудіальної, візуальної та інтерактивної, що використовуються для репрезентації та опрацювання навчального контенту [2]. Такий підхід дозволяє підвищити ефективність засвоєння іншомовного матеріалу, оскільки залучає різні канали сприйняття інформації та активізує когнітивні процеси здобувачів освіти.

Використання мультимодальних цифрових платформ у процесі навчання іноземних мов сприяє створенню інтерактивного освітнього середовища, у межах якого поєднуються різні типи навчальних ресурсів: текстові матеріали, відеолекції, аудіозаписи, інтерактивні вправи, графічні елементи та мультимедійні презентації. Така інтеграція дозволяє реалізувати комплексний підхід до формування іншомовної комунікативної компетентності, що охоплює розвиток навичок аудіювання, читання, письма та усного мовлення [1]. Водночас мультимедійні елементи забезпечують візуалізацію мовних явищ і сприяють глибшому розумінню змісту навчального матеріалу.

Використання мультимодальних цифрових платформ у процесі викладання іноземних мов активно впроваджується у практику освітньої діяльності Полтавського державного аграрного університету. Університет реалізує сучасний підхід до організації освітнього процесу, який передбачає інтеграцію інформаційно-комунікаційних технологій та цифрових ресурсів у підготовку здобувачів вищої освіти різних спеціальностей. Розвиток цифрового освітнього середовища сприяє підвищенню ефективності навчання, забезпечує доступ до навчальних матеріалів у дистанційному форматі та створює умови для інтерактивної взаємодії між викладачем і здобувачами освіти.

У підготовці здобувачів вищої освіти з іноземної мови важливу роль відіграє система дистанційного навчання Moodle, яка функціонує в

університеті як складова цифрового освітнього середовища. На базі цієї платформи створюються електронні навчальні курси, що містять теоретичні матеріали, мультимедійні презентації, відеолекції, інтерактивні вправи та тестові завдання. Система забезпечує постійний доступ до навчального контенту, що дозволяє здобувачам освіти працювати з матеріалами у зручний час і повторювати їх у процесі самостійної роботи. Функціональні можливості Moodle дозволяють організовувати онлайн-обговорення, виконувати письмові завдання, проходити тестування та отримувати зворотний зв'язок від викладача. У Полтавському державному аграрному університеті ця платформа використовується протягом кількох років як основне середовище дистанційного та змішаного навчання.

Під час викладання дисциплін з іноземної мови цифрове навчальне середовище доповнюється використанням інтерактивних платформ для створення дидактичних вправ і навчальних матеріалів. Зокрема, застосовується платформа LearningApps, що дозволяє розробляти інтерактивні завдання різних типів: вправи на встановлення відповідності, класифікацію понять, заповнення пропусків, інтерактивні вікторини та кросворди. Такі ресурси використовуються для закріплення лексичного та граматичного матеріалу, розвитку навичок читання і розуміння текстів, а також для формування мовної компетентності здобувачів освіти. Мультимедійний формат завдань, який поєднує текстові, графічні та аудіальні елементи, забезпечує реалізацію принципу мультимодальності та підвищує рівень зацікавленості здобувачів у навчальному процесі.

Важливим інструментом формування лексичної компетентності у процесі вивчення іноземної мови є використання платформи Quizlet. За допомогою цифрових карток здобувачі вищої освіти можуть опановувати нову лексику, термінологію та фразеологічні одиниці. Поєднання текстових елементів із зображеннями та аудіосупроводом забезпечує багатоканальне сприйняття інформації, що сприяє більш ефективному запам'ятовуванню лексичного матеріалу. Інтерактивні режими навчання, які пропонує платформа, дозволяють організовувати різні типи тренувальних завдань і тестування.

З метою активізації навчальної діяльності та здійснення поточного контролю знань здобувачів освіти у процесі викладання іноземних мов використовуються також елементи гейміфікації, зокрема платформа Kahoot!. Вона дозволяє проводити інтерактивні онлайн-вікторини, тестування та опитування, що сприяє підвищенню мотивації здобувачів освіти та створює динамічне освітнє середовище. Використання таких інструментів під час занять дозволяє ефективно перевіряти рівень

засвоєння лексико-граматичного матеріалу, а також стимулює активну участь здобувачів у навчальному процесі.

Окрему роль у розвитку навичок усного мовлення відіграє платформа Flip, яка використовується для створення відеовідповідей на запропоновані теми та організації онлайн-дискусій. Такий формат роботи дозволяє здобувачам вищої освіти практикувати усне мовлення, розвивати комунікативні навички та формувати впевненість у використанні іноземної мови у професійній і міжкультурній комунікації.

Важливим інструментом для організації роботи з автентичними відеоматеріалами є Edpuzzle, який дозволяє створювати інтерактивні відеоуроки з вбудованими запитаннями, коментарями та завданнями на розуміння змісту. Його функціонал забезпечує можливість інтеграції відео з різних джерел (YouTube, Vimeo та інших відкритих платформ), а також редагування навчального контенту шляхом додавання пауз, голосових пояснень викладача, текстових підказок і контрольних запитань у ключових фрагментах відео. Це дає змогу трансформувати пасивне сприйняття відеоматеріалу в активний навчальний процес, у межах якого здобувачі вищої освіти постійно взаємодіють із контентом, аналізують інформацію та здійснюють самоконтроль розуміння.

У забезпеченні комунікації та організації навчального процесу важливу відіграє Microsoft Teams, який поєднує функції відеоконференцій, чату, спільної роботи з файлами та організації занять у режимі реального часу. Його використання створює цілісне цифрове середовище для синхронного та асинхронного навчання іноземної мови, що дозволяє забезпечити безперервність освітнього процесу незалежно від місця перебування здобувачів вищої освіти.

Завдяки інтеграції різних інструментів у межах однієї платформи Microsoft Teams забезпечує ефективну організацію навчального курсу: викладач може створювати окремі канали для різних видів діяльності (лексичної, граматичної, комунікативної практики), розмішувати навчальні матеріали, завдання, інструкції та додаткові ресурси. Це сприяє структурованості навчального контенту та полегшує орієнтацію здобувачів у навчальному середовищі. Перевагою платформи є можливість проведення інтерактивних онлайн-занять у форматі відеоконференцій, під час яких реалізуються різні форми мовленнєвої діяльності: говоріння, аудіювання, дискусії, рольові ігри та презентації. Такий формат сприяє розвитку комунікативної компетентності, формуванню навичок спонтанного мовлення та подоланню мовного бар'єра.

Для розвитку навичок академічного письма та підвищення мовної грамотності здобувачів освіти ефективно застосовується Grammarly, що

дозволяє здійснювати автоматизовану перевірку граматики, стилістики та орфографії англomовних текстів. Використання цього інструмента сприяє формуванню вміння дотримуватися норм академічного письма, підвищує точність мовного оформлення висловлювань, а також допомагає виявляти типові лексико-граматичні помилки, що виникають у процесі іншомовної продукції. Завдяки функціям пояснення виправлень здобувачі вищої освіти не лише отримують готові корекції, але й опановують правила їх застосування, що має важливе дидактичне значення для формування автономності навчання та розвитку мовної саморефлексії.

Інструмент DeepL використовується як допоміжний засіб для перекладу та аналізу іншомовних текстів, що є особливо актуальним у контексті формування перекладацької та лінгвістичної компетентності. Його перевагою є висока якість машинного перекладу, здатність відтворювати контекстуальні значення лексичних одиниць і забезпечувати більш природне синтаксичне оформлення тексту порівняно з традиційними системами автоматичного перекладу. У навчальному процесі DeepL доцільно використовувати не як заміну перекладацької діяльності, а як інструмент для порівняльного аналізу перекладацьких рішень, виявлення семантичних зсувів та обговорення можливих варіантів перекладу.

Таким чином, мультимодальні цифрові платформи формують нове освітнє середовище, у межах якого поєднуються різні способи репрезентації навчальної інформації та інтерактивні форми навчальної діяльності. Їх використання у процесі викладання іноземних мов у закладах вищої освіти сприяє підвищенню ефективності освітнього процесу, розвитку іншомовної комунікативної компетентності та формуванню цифрової грамотності здобувачів вищої освіти. Інтеграція таких платформ у навчальний процес відповідає сучасним тенденціям цифровізації освіти та створює умови для впровадження інноваційних педагогічних практик у сфері мовної підготовки.

Список використаних джерел:

1. Биков В. Ю. Цифрова трансформація суспільства і розвиток комп'ютерно орієнтованих систем освіти. *Інформаційні технології і засоби навчання*. 2019. Т. 70. № 2. С. 15–36.
2. Jiang L., Hafner C. Digital multimodal composing in L2 classrooms: A research agenda. *Language Teaching*, №58. № 2024. P. 528 – 546. DOI:10.1017/S0261444824000107

УДК 004.056:37.018

*Будзінська О. О., науковий співробітник НДУ
Житомирський військовий інститут імені С. П. Корольова*

ПРИНЦИПИ СЕМАНТИЧНОГО АНАЛІЗУ ДАНИХ У ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ ТА ЙОГО ВПЛИВ НА СИСТЕМУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Повномасштабна агресія російської федерації проти України спричинила суттєві трансформації у всіх сферах суспільного життя, зокрема у сфері освіти та науково-технічної діяльності. У цих умовах особливого значення набуває використання інформаційно-комунікаційних технологій, які забезпечують безперервність освітнього процесу, доступ до наукових ресурсів, ефективне управління знаннями та сприяють формуванню цифрового освітнього середовища, у якому значні обсяги інформації циркулюють у вигляді електронних ресурсів, наукових баз даних, цифрових бібліотек та освітніх платформ. Ці сервіси дають змогу підтримувати навчальну і дослідницьку діяльність навіть за умов обмеженого доступу до матеріальної інфраструктури та підвищених безпекових ризиків. За таких умов важливого значення набуває ефективна організація інформаційних ресурсів, їх змістове структурування та забезпечення належного рівня захисту відповідно до чинного законодавства [2; 4].

Важливим елементом сучасного освітнього середовища є інформаційно-аналітичне забезпечення, яке передбачає систематичний збір, оброблення, аналіз і поширення інформації для підтримки навчальної, наукової та управлінської діяльності. Створення єдиного науково-інформаційного простору сприяє ефективному обміну даними між закладами освіти, науковими установами, міжнародними дослідницькими мережами та розширює можливості інтеграції української освіти у світовий науково-освітній простір.

У контексті стрімкого зростання обсягів інформації особливої актуальності набуває застосування методів семантичного аналізу. Семантичний аналіз дозволяє досліджувати змістові зв'язки між поняттями, виявляти структуру знань у текстових масивах, аналізувати наукові публікації та визначати релевантність інформаційних джерел. Інтеграція інструментів автоматизованого семантичного аналізу у цифрові освітні середовища сприяє оптимізації пошуку інформації, структуризації навчального контенту, розвитку критичного мислення та формуванню навичок роботи з великими обсягами даних [5; 6].

Водночас важливою є класифікація інформації за характеристиками її правового режиму. Відповідно до законодавства України інформація

поділяється на відкриту та інформацію з обмеженим доступом, до якої належать конфіденційна, службова та таємна інформація [1]. Зростання обсягів електронних освітніх ресурсів, дистанційних платформ навчання та хмарних сервісів зумовлює необхідність підвищення рівня кібербезпеки, захисту персональних даних учасників освітнього процесу та забезпечення цілісності інформаційних ресурсів. У цьому контексті важливого значення набувають технології криптографічного захисту даних, системи резервного зберігання інформації, багаторівнева автентифікація користувачів, а також використання захищених інформаційно-комунікаційних мереж. [3; 4].

Поєднання семантичної класифікації інформації з її правовим розподілом дозволяє створювати ефективні системи управління інформаційними ресурсами, які враховують як змістові характеристики даних, так і вимоги їх правового захисту. Такі підходи сприяють упорядкуванню інформаційних потоків, підвищенню якості освітніх ресурсів та забезпеченню належного рівня інформаційної безпеки. Уміння безпечно працювати з інформаційними ресурсами, розпізнавати дезінформацію та захищати власні дані є необхідною складовою сучасних цифрових компетентностей [4; 7].

Отже, інтеграція інформаційно-комунікаційних технологій, методів семантичного аналізу та сучасних засобів захисту інформації створює передумови для формування ефективного цифрового освітнього середовища. Їх використання сприяє підвищенню якості освіти, розвитку наукових досліджень і формуванню інформаційно-аналітичних компетентностей здобувачів освіти. Подальший розвиток таких підходів має бути спрямований на створення інтегрованих науково-освітніх інформаційних систем, які поєднуюватимуть цифрові ресурси, аналітичні інструменти та технології захисту інформації для забезпечення стійкого розвитку освіти й науки. [1; 4].

Список використаних джерел:

1. Закон України «Про інформацію». – Київ, 1992 (зі змінами).
2. Закон України «Про освіту». – Київ, 2017.
3. Закон України «Про захист персональних даних». – Київ, 2010.
4. Закон України «Про основні засади забезпечення кібербезпеки України». – Київ, 2017.
5. Биков В.Ю. Цифрова трансформація освіти і науки: проблеми та перспективи розвитку. – Київ: Інститут цифровізації освіти НАПН України, 2020.
6. Морзе Н.В., Буйницька О.П. Інформаційно-комунікаційні технології в освіті. – Київ: Університет «Україна», 2019.
7. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems

УДК 378.147:004.738.5:811.111

*Дягилева О.С., к.пед.н., доцент,
Юрженко А.Ю., к.пед.н., доцент,
Свирида В.С., викладач
Херсонська державна морська академія
Кононова О.С., викладач
Морський фаховий коледж Херсонської державної морської
академії*

ВИКОРИСТАННЯ ПЛАТФОРМИ DISCOURSE У МОРСЬКІЙ ОСВІТІ ТА ПІДГОТОВЦІ

Наразі морська освіта та підготовка в Україні зазнає значних змін, зокрема через нові вимоги морської індустрії. Різні фактори, такі, як використання Штучного Інтелекту, декарбонізація тощо, змушують викладачів морської англійської мови шукати нові інструменти викладання, зокрема інформаційно-комп'ютерні технології. До таких технологій відносимо платформу Discourse [1].

Платформа налічує більш ніж 22 000 спільноти, використовуючи які можна спілкуватися у реальному часі і розвивати комунікативну компетентність. Discourse надає можливість безкоштовно використовувати блоки та інші інструменти для створення своєї спільноти (наприклад, спільнота під назвою «Заняття з морської англійської мови для майбутніх суднових механіків»).

Розвиток комунікативної компетентності для майбутніх морських фахівців – важливий інструмент не тільки під час роботи на судні, але і для пошуку цієї роботи (під час інтерв'ю в круїнгових компаніях). Discourse адаптується під потреби користувачів і забезпечує простором, де здобувачі вищої освіти можуть дискутувати, обговорювати різні ідеї, зберігати інформацію (кейси, документи, глосарій термінів) [2].

Для створення спільноти Discourse викладач натискає кнопку «Get started» на платформі, дає назву спільноті, початок адреси (веб-посилання), обирає свій логін та Discourse ID (на цьому етапі можна переглянути своє ім'я, фото та пошту, які будуть відображатися іншим користувачам спільноти). Викладач може також обрати примусову мову інтерфейсу, видимість спільноти (приватна чи публічна), тип реєстрації до спільноти.

Поза звичайним спілкуванням на платформі, є можливість писати приватні повідомлення (розділ «Мої повідомлення»). Для зручності даний розділ поділено на наступне: вхідні, останні, надіслані, новий, непрочитані, архів, нове повідомлення.

Спільноти Discourse містять елементи гейміфікації (ігрові елементи, які сприяють залученості здобувачів вищої освіти до комунікації). До таких елементів відносимо розділ «Нагороди» (наприклад, значки «Перша відповідь електронною поштою», «Новий користувач місяця») [3]. Приклад спільноти у Discourse можна побачити на рисунку 1 нижче.

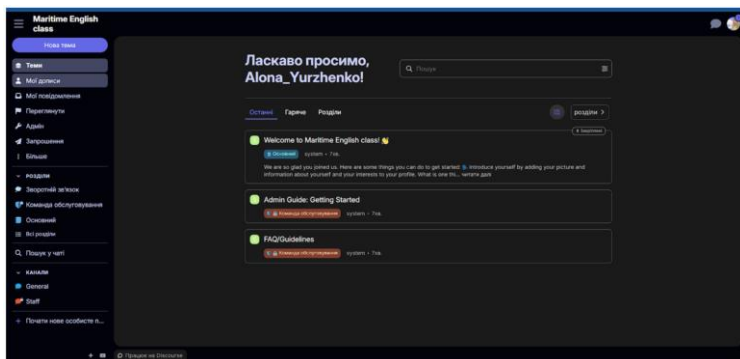


Рис.1. Приклад головної сторінки спільноти Maritime English class у Discourse

Таким чином, використання платформи Discourse у процесі навчання морської англійської мови створює ефективне цифрове середовище для розвитку комунікативної компетентності майбутніх морських фахівців.

Завдяки можливостям онлайн-спілкування, обміну навчальними матеріалами та використанню елементів гейміфікації платформа сприяє активній участі здобувачів освіти у навчальному процесі, підвищує їхню мотивацію та забезпечує додаткові можливості для практики професійного спілкування англійською мовою.

Список використаних джерел:

1. Discourse. URL: <https://www.discourse.org/> (дата звернення: 11.03.2026).
2. Diahyleva O., Kononova O., Yurzenko A. Maritime English Instruction for Future Ship Engineers: A Pedagogical Study Using ChatGPT and Digital Learning Platforms. International Journal of Multilingualism and Languages for Specific Purposes. 2025. Vol. 7, No. 2. P. 20–32.
3. Diahyleva O., Kononova O., Yurzenko A. Integrating Gamification in Maritime English Teaching: Enhancing Communicative Competence of Future Seafarers. Головний редактор. P. 308.

УДК 004.8:378.018.43

*Слісаренко Р.В., аспірант,
Дейнеко Ж.В., к.т.н., доцент
Харківський національний університет радіоелектроніки*

МОДЕЛЬ ПРЕДСТАВЛЕННЯ ТА ІНТЕРПРЕТАЦІЇ РЕЗУЛЬТАТІВ ТЕМАТИЧНОГО АНАЛІЗУ ДЛЯ ВІРТУАЛЬНОГО АСИСТЕНТА ДИСТАНЦІЙНОГО НАВЧАННЯ

Сучасне цифрове освітнє середовище акумулює значні обсяги текстових даних: форумні обговорення, відповіді здобувачів освіти, коментарі викладачів, описи курсів та матеріали зворотного зв'язку. Тематичне моделювання дає змогу виявляти латентну семантичну структуру таких корпусів, ідентифікувати домінантні змістові напрями та аналізувати динаміку навчальної комунікації [1], [2]. Прикладна цінність результатів визначається способом їх представлення, що забезпечує подальшу інтерпретацію та підтримку педагогічних рішень.

Для дистанційного навчання це особливо важливо, оскільки значна частина педагогічно релевантних сигналів існує саме у текстовій формі. Дослідження у сфері штучного інтелекту в освіті засвідчують, що тематичне моделювання дозволяє формувати інтерпретовані репрезентації освітнього домену [3], а застосування чат-ботів зі штучним інтелектом підтверджує важливість релевантних і контекстно адаптованих відповідей [4]. Метою роботи є формалізація моделі форматів представлення результатів тематичного аналізу у віртуальному асистенті дистанційного навчання.

Формалізацію моделі доцільно подати у вигляді кортежу:

$$F = \langle R, U, S, \Phi, \Psi \rangle$$

де R - множина результатів тематичного аналізу, U - множина ролей користувачів, S - множина сценаріїв застосування, Φ - множина форматів представлення, Ψ - множина правил інтерпретації.

У цій постановці вибір формату представлення визначається відображенням:

$$\varphi: \langle r, u, s \rangle \rightarrow \phi, \phi \in \Phi$$

де r - результат тематичного аналізу, u - роль користувача, s - сценарій застосування.

Процедура інтерпретації задається відображенням:

$$\psi: \langle r, \phi, u, s \rangle \rightarrow e, e \in E$$

де e - інтерпретаційний результат у формі текстового узагальнення, аналітичного сигналу, рекомендації або візуального подання.



Рис.1. Схема інтерпретації результатів тематичного аналізу

Запропонована модель охоплює описовий, динамічний, порівняльний, наративний та сигнально-аналітичний формати представлення, які забезпечують подання тематичної структури корпусу, відображення її змін у часі, зіставлення тематичних профілів, інтерпретацію результатів і виявлення змістових ризиків дистанційного навчання [2], [4].

Інтерпретація результатів визначається структурою тематичної моделі, роллю користувача та сценарієм застосування. Для викладача значущими є сигнали про складні теми й типові труднощі, для адміністративного рівня - агреговані індикатори стану освітнього середовища, для дослідницького сценарію - когерентність, відтворюваність і динаміка тематичної структури [3], для здобувача освіти - спрощений наративний формат [4].

Практична значущість моделі полягає у використанні тематичного аналізу як інструмента формування змістового зворотного зв'язку, виявлення ризикових тематичних зон і підтримки стійкості дистанційного навчання. Отже, модель забезпечує перехід від статистичного тематичного представлення до інтерпретованого результату [2], [4].

Список використаних джерел:

1. Blei D. M., Ng A. Y., Jordan M. I. Latent Dirichlet Allocation // Journal of Machine Learning Research. 2003. Vol. 3. P. 993-1022.
2. Hosseiny M., Marani M., Baumer E. P. S. A Review of Stability in Topic Modeling: Metrics for Assessing and Techniques for Improving Stability // ACM Computing Surveys. 2024. Vol. 56, No. 5. Art. 108.
3. Філь Н. Ю., Слісаренко Р. В., Дейнеко Ж. В., Морозова Л. Ю. Тенденції розвитку досліджень у сфері штучного інтелекту в освіті: тематичне моделювання за допомогою латентного розподілу Діріхле // Вісник Харківського національного автомобільно-дорожнього університету. 2025. № 108. С. 17–24.
4. Слісаренко Р. В. Чат-бот зі штучним інтелектом як засіб дистанційного навчання: вплив на процес та результати / Р. В. Слісаренко // Поліграфічні, мультимедійні та web-технології : тези доп. IX Міжнар. наук.-техн. конф., 14-18 травня 2024 р. – Т. 1. – Харків: ТОВ «Друкарня Мадрид», 2024. – С. 332-333

УДК 004.65:002.1:37

Титарчук С. В., аспірант

Український державний університет імені Михайла Драгоманова

Малежик П.М., д.пед.н., професор

*Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»*

МЕТОД ОПТИМІЗАЦІЇ ДОСТУПУ ДО АРХІВНИХ ДОКУМЕНТІВ У СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З УРАХУВАННЯМ ПОТРЕБ ОСВІТНЬОГО ПРОЦЕСУ

Електронний документообіг (ЕДО) є ключовою складовою цифрової трансформації суспільства. Він охоплює всі етапи роботи з документами: створення, обробку, передачу та архівування, що сприяє підвищенню ефективності управління інформаційними ресурсами [4].

Особливе значення в цьому контексті мають електронні архіви, які забезпечують довготривале збереження документів та швидкий доступ до них. Оперативний доступ до інформації є критично важливим в умовах зростання обсягів даних [2].

Освітній процес потребує оперативного та релевантного доступу до різноманітних документів: навчальних матеріалів, наукових публікацій і адміністративних даних. У великих архівах їх пошук часто ускладнений, що підтверджується дослідженнями цифровізації документообігу [1].

Основною проблемою є відсутність єдиних підходів до організації доступу: структура даних різноманітна, метадані не уніфіковані, пошукові механізми працюють неефективно, а системи не враховують специфічні потреби користувачів освітнього середовища [3].

Метою даної роботи є розробка методу оптимізації доступу до архівних документів із урахуванням особливостей освітнього процесу.

Запропонований метод ґрунтується на комплексному підході, який поєднує стандартизацію метаданих, семантичний аналіз та персоналізацію доступу.

1. Стандартизація метаданих. Для кожного документа формується уніфікований опис, який включає назву, автора, дату, тип документа, ключові слова та освітню категорію. Це забезпечує єдину структуру даних і підвищує точність пошуку.

2. Класифікація документів. Документи групуються за освітніми потребами: навчальні матеріали, наукові роботи, методичні документи та адміністративні дані. Така класифікація спрощує навігацію архівом та підвищує ефективність пошуку.

3. **Семантична індексація.** Використання методів семантичного аналізу дозволяє автоматично виділяти ключові терміни, встановлювати зв'язки між ними та формувати тематичні кластери. Це забезпечує реалізацію інтелектуального пошуку.

4. **Персоналізація доступу.** Враховуються ролі користувачів (студент, викладач, науковець, адміністратор). Для кожної категорії визначаються рівні доступу та пріоритети пошукових запитів, що підвищує зручність використання системи.

5. **Інтелектуальний пошук.** Пошукова система аналізує не лише ключові слова, а й зміст документа, використовуючи фільтри та рекомендаційні механізми. Система пропонує релевантні документи на основі попередніх запитів користувача.

Запропонований метод дозволяє скоротити час пошуку та підвищити релевантність результатів, що сприяє ефективнішому використанню архівних ресурсів.

Наукова новизна полягає в інтеграції трьох підходів: структурного, семантичного та користувацького, із фокусом на специфіку освітнього процесу.

Практичне значення методу полягає у можливості його застосування у закладах освіти для покращення доступу до навчальних та наукових ресурсів, що підвищує якість освітнього процесу.

Отже, оптимізація доступу до архівних документів є актуальним завданням сучасної електронної освіти. Подальші дослідження мають бути спрямовані на розвиток інтелектуальних технологій пошуку.

Список використаних джерел:

1. Костякова А. Діджиталізація документообігу. *Економіка та суспільство*. 2021. № 26. DOI: <https://doi.org/10.32782/2524-0072/2021-26-72>

2. Кравець Р., Бойко П., Марковець О. Електронний архів як засіб швидкого доступу до управлінської інформації. *Бібліотекознавство. Документознавство. Інформологія*. 2023. № 4. С. 14-21. DOI: <https://doi.org/10.32461/2409-9805.4.2023.293967>

3. Перчук О., Вовченко Р., Артюх О. Особливості впровадження цифровізації документообігу в державних установах (на прикладі бібліотек та архівів). *Економіка та суспільство*. 2023. № 53. DOI: <https://doi.org/10.32782/2524-0072/2023-53-70>

4. Плаксієнко В., Черненко К. Електронний (безпаперовий) документообіг. Електронний цифровий підпис. *Економіка. Управління. Інновації*. 2019. № 1(24). DOI: [https://doi.org/10.35433/ISSN2410-3748-2019-1\(24\)-7](https://doi.org/10.35433/ISSN2410-3748-2019-1(24)-7)

УДК 37.091.33:004

*Ушаткіна С.О., викладач
Криворізький національний університет*

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ФОРМУВАННЯ НАВЧАЛЬНОЇ МОТИВАЦІЇ ЗДОБУВАЧІВ ОСВІТИ

У сучасних умовах цифровізації освіти проблема підвищення мотивації здобувачів освіти набуває особливої актуальності, оскільки традиційні методи навчання не завжди забезпечують достатній рівень залученості та активності. Попри активне впровадження інформаційно-комунікаційних технологій (ІКТ), їх використання часто має фрагментарний характер і не завжди спрямоване на формування внутрішньої мотивації [1]. Це зумовлює необхідність переосмислення ролі ІКТ не лише як технічного засобу, а як педагогічного інструменту цілеспрямованого мотиваційного впливу.

Сучасні підходи до використання ІКТ у навчанні свідчать, що їх мотиваційний потенціал реалізується за трьома основними напрямками: забезпечення когнітивної активності, підтримка автономності та розвиток рефлексії результатів навчання. Цифрові освітні середовища створюють умови для активної взаємодії з навчальним матеріалом, змінюючи характер пізнавальної діяльності з репродуктивної на продуктивну [2]. Це проявляється у виконанні інтерактивних завдань, роботі з цифровими ресурсами та моделюванні практичних ситуацій, що стимулює інтелектуальну активність і підвищує інтерес до навчання.

Важливим аспектом є забезпечення автономності навчання, що досягається завдяки можливості вибору темпу, послідовності та форм виконання завдань. ІКТ дозволяють реалізувати адаптивний підхід, за якого здобувач освіти стає активним суб'єктом навчальної діяльності, а не пасивним споживачем інформації. Це сприяє формуванню внутрішньої мотивації, оскільки навчання набуває особистісного значення та враховує індивідуальні потреби [4].

Окреме значення має забезпечення оперативного зворотного зв'язку та візуалізація результатів навчання. Цифрові інструменти дозволяють відстежувати прогрес у вигляді зрозумілих показників, що створює умови для самоконтролю та рефлексії. У цьому випадку мотивація формується не через зовнішнє стимулювання, а через усвідомлення власних досягнень і динаміки розвитку [5].

Узагальнення педагогічної практики свідчить, що найбільш ефективним є комплексне використання ІКТ, яке поєднує інтерактивність, адаптивність і наочність результатів. Такий підхід

підвищує рівень залученості здобувачів освіти та сприяє переходу до активної, самостійної навчальної діяльності, орієнтованої на пошук, аналіз і застосування знань. У результаті формується стійка мотивація, що базується на інтересі до навчання та розумінні його практичної значущості.

Водночас ефективність використання ІКТ залежить від їх педагогічно обґрунтованої інтеграції у навчальний процес. Застосування цифрових технологій без чіткої дидактичної мети не забезпечує належного мотиваційного ефекту [3]. Отже, визначальним чинником є не сама наявність ІКТ, а методика їх використання, спрямована на активізацію пізнавальної діяльності та розвиток внутрішньої мотивації.

Таким чином, наукова новизна дослідження полягає у розгляді ІКТ як інструменту цілеспрямованого впливу на мотиваційну сферу здобувачів освіти через поєднання когнітивної активності, автономності та рефлексії результатів навчання, що розширює підходи до їх використання в сучасній освіті. Практичне значення полягає у можливості застосування запропонованого підходу під час розроблення навчальних курсів та організації освітнього процесу в умовах цифрового середовища. Перспективи подальших досліджень пов'язані з експериментальною перевіркою ефективності запропонованих підходів у різних освітніх контекстах. Окремої уваги потребує вивчення впливу конкретних цифрових інструментів на формування довготривалої внутрішньої мотивації здобувачів освіти. Це дозволить уточнити методичні засади використання ІКТ у навчальному процесі та підвищити його результативність.

Список використаних джерел:

1. Биков В. Ю. Інформаційно-комунікаційні технології в освіті: стан і перспективи розвитку. *Інформаційні технології і засоби навчання*. 2012. № 1. С. 5–18.
2. Морзе Н. В. *Основи інформаційно-комунікаційних технологій в освіті*. Київ: Видавнича група BVH, 2010. 352 с.
3. Спірін О. М. Цифрові технології в освіті: теоретико-методологічні засади. *Педагогіка і психологія*. 2018. № 3. С. 15–22.
4. Deci E. L., Ryan R. M. *Intrinsic Motivation and Self-Determination in Human Behavior*. New York: Springer, 1985. 371 p.
5. Mayer R. E. *Multimedia Learning*. 2nd ed. Cambridge: Cambridge University Press, 2009. 304 p.

УДК 519.1:004.94

*Філіпчук М.П., к.ф.-м.н., доцент,
Мельничук Н.І., здобувач,
Філіпчук О.І., к.ф.-м.н., доцент*

Чернівецький національний університет імені Юрія Федьковича

ПОБУДОВА ТА ВІЗУАЛІЗАЦІЯ ДЕЯКИХ РІЗНОВИДІВ ГРАФІВ

Вимушене онлайн-навчання, з яким систематично стикається Україна, починаючи з 2020 року, і деградує рівень математичних знань випускників ЗЗСО [1] вимагають зміни традиційних засобів викладання та навчання, зокрема, і у вищій школі. Як показує практичний досвід, все більш ефективним напрямком тут стає інтерактивна комп'ютерна візуалізація інформації, що підвищує розуміння та якість засвоєння матеріалу.

Одним із найбільш важливих і практично ціннісних розділів сучасної математики є теорія графів. Велика кількість структур у математиці та інформатиці можуть бути подані графами. Графи, як структурні моделі, також доволі широко використовуються в багатьох інших галузях науки та техніки.

У сучасній теорії графів класифіковано чимало різновидів графів [2]. Більшість із них утворюють параметричні сімейства графів зі змінною кількістю вершин, а отже, і ребер. Безпосередня ручна побудова таких графів у випадку великої кількості вершин стає доволі нетривіальною та часозатратною задачею.

Враховуючи вищевикладене, авторами було розроблено Web-додаток для швидкої побудови деяких різновидів графів, зокрема, параметризованих. Вивід зображення графа, за бажанням користувача, може бути здійснено як за допомогою технології растрової графіки HTML 5 Canvas API, так і за допомогою технології масштабованої векторної графіки SVG.

З непараметризованих графів у додатку підтримується побудова графів Петерсена, Хівуда, Франкліна, Дюрера, Мебіуса-Кантора, Дезарга та Науру, а з параметризованих – циклів, зірок, коліс, повних і повних дводольних графів, драбин, призм, зірчатих многокутників, вітряків, гіперкубів і корон.

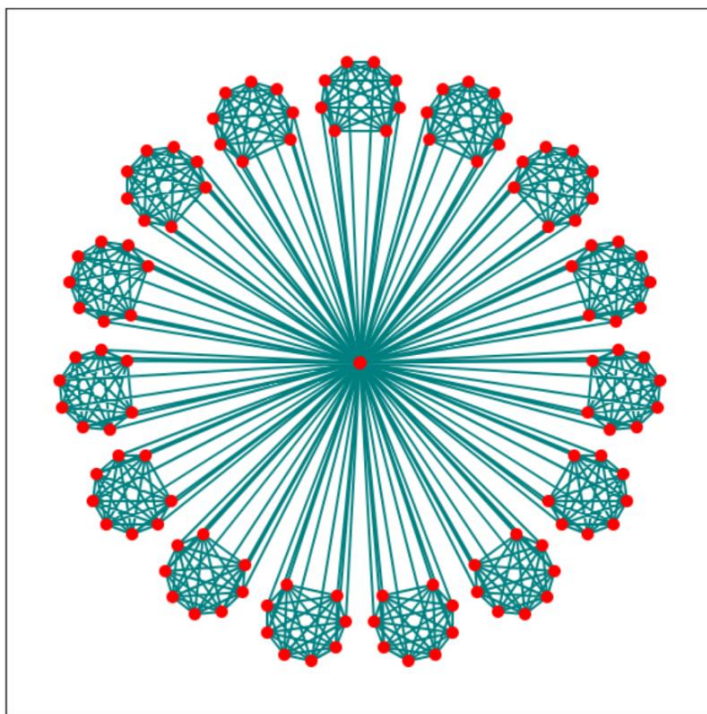
Створений Web-додаток доступний за адресою

<http://pmit.pp.ua/graph-builder/>

На рис. 1 наведено фрагмент інтерфейсу додатка для налаштування параметрів графа, а на рис. 2 продемонстровано приклад побудови параметризованого графа – графа-вітряка $W(9,15)$.

Кількість вершин (n):	1	Колір вершин:	<input type="color" value="#FF0000"/>
Кількість вершин (m):	1	Колір ребер:	<input type="color" value="#008080"/>
Розмір вершин:	5	Колір канви:	<input type="color" value="#FFFFFF"/>
Товщина ребер:	2	Розмір графа:	+ -

Рис.1. Налаштування параметрів графа



Граф-вітряк $W_{9,15}$

Рис.2. Приклад побудови графа

Список використаних джерел:

1. Лазуркевич С. Майже половина українських школярів не знають базової математики. ZAXID.NET. URL: <https://tinyurl.com/zaxid1630293> (дата звернення: 21.03.2026).
2. Diestel R. Graph Theory : 5th edition. Springer, 2017. 447 p.

УДК 004.9

*Ястребова А.В., здобувач,
Вакалюк Т.А. д.пед.н., професор
Державний університет «Житомирська політехніка»*

НЕОБХІДНІСТЬ РОЗРОБКИ ВЕБСИСТЕМИ З ОПТИМІЗАЦІЇ УПРАВЛІННЯ НАУКОВОЮ РОБОТОЮ ЗДОБУВАЧІВ СТУПЕНЯ ДОКТОР ФІЛОСОФІЇ

Модернізація вищої освіти в Україні вимагає глибокого та всебічного впровадження інформаційно-комунікаційних технологій як в академічні, так і в адміністративні процеси університетів. Навчання в аспірантурі є важливим, багаторічним етапом наукової підготовки, який потребує ретельного та безперервного відстеження надзвичайно різноманітних видів діяльності здобувачів. Сучасні кризові реалії, зокрема воєнний стан в Україні, не змогли повністю зупинити освітній процес, а навпаки, значною мірою зумовили інтенсивний пошук нових форм, методів та засобів організації навчання і наукової діяльності [3]. Оскільки підготовка здобувачів сьогодні відбувається у гібридних умовах, які вимагають комбінування офлайн- та онлайн-взаємодію зі здобувачами, виникає об'єктивна необхідність застосовувати технологічні рішення для забезпечення наукової роботи.

Згідно з чинним Порядком підготовки здобувачів вищої освіти, аспіранти зобов'язані неухильно виконувати індивідуальний план наукової роботи та щонайменше двічі на рік офіційно звітувати про хід його виконання на засіданнях кафедри [1]. Однак у реальних умовах виконання цієї вимоги створює надмірне навантаження як на здобувачів, так і на їхніх наукових керівників. Дистанційна взаємодія додатково ускладнює ситуацію: загострюються проблеми обмеженого доступу до ресурсів, відсутності належного особистого спілкування, виникають значні труднощі в організації робочого часу та комунікації [2]. Сукупність цих несприятливих обставин також ускладнює наукову комунікацію, тому інтеграція надійної електронної системи моніторингу є важливою вимогою для забезпечення безперервності підготовки здобувачів.

Для вирішення вище перелічених проблем пропонується розробка спеціалізованої вебсистеми з використанням сучасної клієнт-серверної архітектури. Вона дозволить повністю автоматизувати документообіг та оптимізувати управління науковою роботою. Серверну частину застосунку доцільно реалізувати на базі прогресивного фреймворку NestJS у поєднанні з надійною системою управління реляційними базами даних PostgreSQL. Такий архітектурний вибір забезпечить

безпечну обробку великих масивів інформації, високу масштабованість та стабільну роботу платформи під час великих навантажень. Тим часом, клієнтська частина системи має розроблятися з використанням бібліотеки React та з урахуванням передових принципів UX/UI дизайну. Орієнтація на користувачів із різним цифровим досвідом вимагає розробки прозорого інтерфейсу, що не лише полегшить сприйняття функціоналу, а й зробить регулярне звітування оперативним та зручним.

Надійна технічна база дозволяє реалізувати головну функціональну мету системи – повну цифровізацію індивідуального плану наукової роботи аспіранта. Система дозволить перевести паперову звітність у формат інтерактивного середовища. Такі обов’язкові завдання, як підготовка дисертації, друк наукових праць і участь у конференціях, існують у вигляді незалежних електронних процесів. Це надасть змогу максимально гнучко адмініструвати наукову діяльність, плануючи навантаження по семестрах та встановлюючи конкретні дати завершення.

Ключовим елементом такої платформи буде підсистема електронного документообігу та комунікації. Через персональний кабінет здобувач отримає змогу зручно завантажувати звітні матеріали. При цьому алгоритми системи забезпечать версіонування файлів, тобто під час завантаження оновленого варіанта рукопису програма не перезаписує попередній документ, а зберігає повну історію внесених змін. Для наукових керівників буде передбачено окремий інтерфейс, який автоматично збирає надіслані аспірантами роботи та надає засоби для їх перевірки прямо в системі. Наявність внутрішнього модуля для коментування і внесення правок виключає потребу у використанні зовнішніх месенджерів. Таке єдине комунікаційне середовище не лише структурує взаємодію, а й забезпечить фіксацію в базі даних факту офіційного погодження матеріалів.

Список використаних джерел:

1. Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах): Постанова Кабінету Міністрів України від 23.03.2016 № 261 (зі змінами). URL: <https://zakon.rada.gov.ua/laws/show/261-2016-%D0%BF#Text> (дата звернення: 10.03.2026).
2. Мандич Т. М. Підготовка докторів філософії у закладах вищої освіти м. Херсона в умовах воєнного стану. Педагогічні науки. 2025. Вип. 111. С. 69–75.
3. Рібцун Ю. В. Підготовка докторів філософії у галузі спеціальної освіти: сучасні виклики та перспективи. 2024. С. 132–145.

УДК 004.04

*Хомочкін А.П., вчитель хімії,
Мигун А.О., вчитель фізики,
Красношлик О.Ю., вчитель інформатики
ПЗО «КМДШ»*

ДОСЛІДЖЕННЯ ВПЛИВУ КОЛИВАНЬ МАГНІТНОГО ПОЛЯ, ЩО ВИНИКАЮТЬ ПІД ЧАС НАВЧАЛЬНОГО ПРОЦЕСУ В МОМЕНТ ПЕРЕБУВАННЯ УЧНІВ ШКОЛИ В УКРИТТІ

Ідея проведення аналізу впливу коливань магнітного поля, що виникає в укритті під час повітряної тривоги продовж навчального процесу, пов'язана з великою концентрацією цифрових пристроїв (ноутбуків, планшетів та телефонів) в обмеженому просторі. Більшість цих пристроїв створює суттєве навантаження на біоритми живих організмів, зокрема нервову, серцево-судинну, ендокринну систему. Загалом кожна людина постійно піддається дії магнітного поля, що зазвичай коливається в межах норми. Проте перебування протягом тривалого часу в середовищі дії магнітного поля, що перевищує допустимі показники, все ж можна відчутти. Саме під час повітряних тривог коли необхідно надати вільний доступ учням до мобільного телефону та проводити навчання не завжди просторих кабінетах, виникають симптоми, імовірно впливу магнітного поля, що створюють різноманітні пристрої.

Магнітні датчики слугують фундаментальними компонентами в широкому спектрі застосувань, від промислових та автомобільних систем до побутової електроніки та медичних пристроїв.[1]

Збільшення значення магнітної індукції зафіксовано саме під час перебування дітей в укритті, відбувається неконтрольована зміна магнітного поля, яка фіксували датчиками Холла. Аналоговий датчик Холла перетворює індукцію магнітного поля в напругу, знак і величина якої будуть залежати від полярності і сили поля і для оцифрування сигналу використовували пристрій мультиметр OWON 33+ в інтеграції з ноутбуком. Опрацювання сигналу здійснювалось програмовим забезпеченням OWON(iMeter). Цифровий датчик використовувався для визначення наявності чи відсутності магнітного поля.

Наявність шуму суттєво впливає на точність вимірювань. Імпульсні джерела живлення та системи електромереж генерують численні сигнали перешкод. Ці сигнали можуть спричинити суттєві відхилення у тестованих даних у певних частотних точках. Впровадження відповідних заходів фільтрації, ізоляції та вимірювань з живленням від

батарейок сприяє зменшенню системного шуму та мінімізації похибок вимірювань.[2]

Згідно наказу МОЗ №81 Про затвердження мінімальних вимог до охорони здоров'я та безпеки працівників, які піддаються впливу електромагнітних полів, слід зазначити, що протягом хоч і не тривалих, але системних підвищень значень індукції магнітного поля спостерігались зміни в поведінці, як учнів так і вчителів. Хоча норми магнітного поля залежать від частоти та тривалості впливу не слід зневажливо ставитись до безпеки свого здоров'я, особливо коли вплив непомітний.

В стресовий момент фактично неможливо контролювати чи зменшити вплив цифрових пристроїв, проте варто замислюватись, якими діями можна обмежити чи хоча б «розсіяти» дію магнітних полів.

Сучасні телефони здебільшого оснащені датчиками Холла і з їх допомогою та необхідного програмного забезпечення можна в деяких ситуаціях спостерігати і здійснювати контроль за зміною значень імпульсів магнітного поля.

Висновок. Аналізуючи розрахункові дані отримані в ході проведених дослідження було зроблено висновки, що хаотичність використання великої кількості гаджетів у вузькому просторі шкільного сховища одночасно може негативно впливати на самопочуття всіх оточуючих.

Непомітне для ока електромагнітне випромінювання при значному і тривалому впливі хоч і може мати негативні симптоми та їх прояви, його можна відслідковувати тим же пристроєм, що його створює.

Є підстави вважати, що магнітне поле, яке виникає в результаті роботи пристроїв РЕБ та ін. також діють на зміну ІМП. Виходячи з цього можна стверджувати, що ці пристрої, які працюють неподалік укриттів значної мірою впливають на розумову та фізичну діяльність учнів, що в свою чергу потребує детального дослідження.

Список використаних джерел:

1. Díaz-Michelena, M. (2009). Small magnetic sensors for space applications. *Sensors*, 9(4), 2271-2288.
2. Roy, A., Sampathkumar, P., & Kumar, P. A. (2020). Development of a very sensitivity magnetic field sensor based on planar Hall effect. *Measurement*, 156, 107590.

УДК 004.62:004.8:378.091.26

*Зварич О.Л., студент,
Вовк Р.Б., к.т.н., доцент*

Івано-Франківський національний технічний університет нафти і газу

МЕТОДОЛОГІЧНІ ЗАСАДИ ВПРОВАДЖЕННЯ АДАПТИВНИХ СИСТЕМ НАВЧАННЯ У ВИЩІЙ ОСВІТІ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Трансформація сучасної парадигми вищої освіти зумовлює необхідність переходу від уніфікованих освітніх моделей до персоналізованих стратегій навчання. Пріоритетним напрямом модернізації навчального процесу є імплементація адаптивних платформ на базі штучного інтелекту, що забезпечують динамічну корекцію змісту та темпу опанування дисциплін відповідно до когнітивних особливостей суб'єктів навчання. У контексті технічної освіти застосування зазначених технологій сприяє підвищенню якості фахової підготовки, глибшій детермінації зв'язків між теоретичним базисом та практичною інженерною діяльністю.

Фундаментом функціонування адаптивних систем виступає синергія методів інтелектуального аналізу освітніх даних (Educational Data Mining) та байєсівських мереж знань. Концептуальна архітектура таких рішень базується на моделі інтелектуальних систем навчання, що інтегрує три взаємозалежні компоненти:

- доменну модель (експертна база предметної галузі);
- модель студента (динамічний профіль компетенцій);
- педагогічну модель (алгоритм адаптивного керування).

Безперервна верифікація профілю студента на основі аналізу логів взаємодії дозволяє системі в режимі реального часу ідентифікувати лакуни у знаннях та генерувати релевантний мікроконтент. Застосування методів глибокого навчання підвищує достовірність класифікації навчальних стилів, що є критично важливим для візуалізації складних процесів у технічних дисциплінах [1].

Важливим аспектом функціонування інтелектуальних систем є впровадження механізмів предиктивної аналітики. Використання алгоритмів машинного навчання, зокрема методу випадкових лісів та рекурентних нейронних мереж, уможливорює прогнозування академічної успішності та ймовірності завершення курсу. Аналіз «цифрового сліду» (часова експозиція завдань, інтенсивність звернення до репозиторіїв, результативність проміжного контролю) дозволяє здійснювати ранню діагностику студентів «групи ризику» та впроваджувати превентивні корекційні заходи. Окрему наукову

цінність становлять технології обробки природної мови, які автоматизують аналіз відкритих відповідей та забезпечують інтелектуальну детермінацію зворотного зв'язку, мінімізуючи когнітивне навантаження на викладацький склад [2].

Технологічна стійкість освітніх платформ забезпечується використанням мікросервісної архітектури, де кожна функціональна одиниця функціонує як автономний сервіс. Такий підхід гарантує високу масштабованість системи в умовах пікових навантажень. Питання інтероперабельності вирішується через впровадження галузевих стандартів LTI (Learning Tools Interoperability) та xAPI (Experience API). Останній дозволяє агрегувати дані про навчальну активність із зовнішніх джерел: спеціалізованих симуляторів, віртуальних лабораторій та VR-тренажерів, що формує цілісний об'єктивний профіль професійної придатності майбутнього фахівця [3].

Розробка та експлуатація адаптивних систем має ґрунтуватися на принципах пояснювального ШІ та суворого дотримання протоколів захисту персональних даних. Перспективним є використання децентралізованих технологій (блокчейн) для верифікації цифрових сертифікатів компетенцій у розподілених освітніх екосистемах.

Підсумовуючи, впровадження адаптивних платформ на основі ШІ у технічних ЗВО є складним науково-технічним завданням, що потребує інтеграції педагогічної теорії, когнітивістики та сучасних методів Data Science. Використання предиктивних моделей та персоналізованих сценаріїв дозволяє не лише оптимізувати освітній процес, а й забезпечити підготовку конкурентоспроможних фахівців, адаптованих до вимог Індустрії 5.0.

Список використаних джерел:

1. Hariyanto H., Kristianingsih F. X. D., Maharani R. Artificial intelligence in adaptive education: a systematic review of techniques for personalized learning. Discover Education. 2025. URL: <https://link.springer.com/article/10.1007/s44217-025-00908-6> (дата звернення: 20.03.2026).
2. Educational Stakeholders' Evaluation of an Artificial Intelligence-Enabled Adaptive Learning System Using Bayesian Networks. 2019. Vol. 9, No. 2. URL: <https://surl.li/xsrvbb> (дата звернення: 20.03.2026).
3. Eryılmaz M., Adabashi A. Development of an Intelligent Tutoring System Using Bayesian Networks and Fuzzy Logic for a Higher Student Academic Performance. Applied Sciences. 2020. Vol. 10, No. 19. URL: <https://surl.li/dsgnve> (дата звернення: 20.03.2026).

УДК 004.946:37

*Косовський С.Б., здобувач,
Кобилін І.О., к.т.н., ст. викладач
Харківський національний університет радіоелектроніки*

ВПРОВАДЖЕННЯ VR-ТЕХНОЛОГІЙ В ОСВІТНІЙ ПРОЦЕС: МОЖЛИВОСТІ ТА ВИКЛИКИ

Сьогодні освітня сфера зазнає суттєвих трансформацій під впливом цифрових технологій, серед яких особливе місце займає віртуальна реальність (VR). Використання VR відкриває нові можливості для інтерактивного навчання, дозволяючи студентам занурюватися у змодельовані середовища та отримувати практичний досвід без фізичних обмежень. Попри значний потенціал, впровадження VR у навчальний процес супроводжується низкою проблем, які потребують детального аналізу.

Віртуальна реальність – це технологія, що створює штучне середовище, у якому користувач може взаємодіяти з об'єктами за допомогою спеціальних пристроїв, таких як VR-гарнітури та контролери. У контексті освіти VR застосовується для моделювання складних процесів, вивчення історичних подій, проведення лабораторних робіт та розвитку професійних навичок. Це особливо актуально для медицини, інженерії та природничих наук, де практичний досвід є критично важливим.

У минулому освітній процес базувався переважно на традиційних методах викладання: лекціях, підручниках та обмежених лабораторних експериментах. З появою комп'ютерних технологій навчання стало більш інтерактивним, однак рівень залученості студентів залишався недостатнім. Сучасні VR-рішення дозволяють подолати ці обмеження, забезпечуючи ефект повного занурення та підвищуючи мотивацію до навчання. Наприклад, студенти можуть досліджувати внутрішню будову людського тіла або відвідувати історичні місця без необхідності фізичної присутності.

Попри переваги, впровадження VR має низку суттєвих викликів. По-перше, це висока вартість обладнання та його обслуговування, що обмежує доступність технології для багатьох навчальних закладів. По-друге, існує проблема технічної підготовки викладачів, які повинні не лише володіти предметною областю, але й вміти ефективно використовувати новітні технології. По-третє, тривале використання VR може викликати фізичний дискомфорт, зокрема втому очей та запаморочення.

Ще одним важливим аспектом є педагогічна доцільність використання VR. Не всі навчальні завдання потребують повного занурення, і в деяких випадках традиційні методи можуть бути більш ефективними. Тому необхідно ретельно оцінювати доцільність застосування VR у кожному конкретному випадку, щоб уникнути перевантаження навчального процесу технологіями.

Таблиця 1

Порівняння ефективності традиційного та VR-навчання за даними досліджень[1–3]

Показник	Традиційне навчання	VR-навчання
Частка правильних відповідей(%)	68%	82%
Рівень залученості(шкала 1–5)	3.1	4.2
Час виконання завдання(хв)	45	32

Отже, впровадження VR-технологій в освітній процес має значний потенціал для підвищення якості навчання та розвитку практичних навичок. Наведені дані демонструють, що використання VR сприяє підвищенню рівня засвоєння знань, залученості студентів та ефективності навчання загалом. Водночас існує низка технічних, економічних та методичних проблем, які стримують широке використання цієї технології. Ефективна інтеграція VR потребує комплексного підходу, що включає зниження вартості обладнання, підготовку викладачів та розробку чітких педагогічних методик.

Список використаних джерел:

1. Freina L., Ott M. A literature review on immersive virtual reality in education. *eLearning & Software for Education*. 2015. Vol. 1. p. 133–141.
2. Radianti J., Majchrzak T., Fromm J., Wohlgenannt I. A systematic review of immersive virtual reality applications for higher education. *Education and Information Technologies*. 2020. Vol. 25. p. 1–38.
3. Jensen L., Konradsen F. A review of the use of virtual reality head-mounted displays in education. *Education and Information Technologies*. 2018. Vol. 23. p. 1515–1529.

УДК 004.7

*Кривонос О.М., к.пед.н., доцент
Житомирський державний університет імені Івана Франка*

ПЕРСОНАЛІЗАЦІЯ НАВЧАННЯ ПРОГРАМУВАННЯ НА ОСНОВІ АДАПТИВНИХ ЦИФРОВИХ СЕРЕДОВИЩ

Актуальність теми персоналізації навчання програмування на основі адаптивних цифрових середовищ зумовлена необхідністю врахування індивідуальних освітніх потреб учнів у процесі опанування складних понять програмування та розвитку алгоритмічного мислення. У сучасній школі спостерігається значна неоднорідність рівня підготовки здобувачів освіти, що потребує впровадження інструментів, здатних забезпечити диференційований підхід до навчання. Використання адаптивних цифрових середовищ, зокрема платформи CodinGame, яка поєднує елементи гейміфікації, інтерактивного навчання та автоматизованого оцінювання, дозволяє створити персоналізовану траєкторію навчання, підвищити мотивацію учнів і забезпечити практичну спрямованість освітнього процесу. Це обумовлює необхідність наукового обґрунтування методики використання таких середовищ у навчанні програмування.

Платформа CodinGame реалізує персоналізоване навчання через постійний аналіз взаємодії користувача із завданнями, що відповідає принципам learning analytics. Система фіксує успішність виконання вправ, кількість спроб, час розв'язання та використані підходи, що дозволяє формувати індивідуальний профіль учня. На основі цих даних платформа опосередковано визначає рівень підготовки та адаптує подальший навчальний контент, пропонуючи завдання відповідної складності.

Адаптивність у CodinGame реалізується через поступове ускладнення задач і варіативність сценаріїв їх виконання. Учень має можливість обирати різні напрями (ігрові завдання, алгоритмічні задачі, змагання), що дозволяє враховувати індивідуальний темп навчання та стиль мислення. Якщо користувач демонструє високий рівень успішності, система пропонує складніші виклики; у разі труднощів — доступніші завдання або підказки, що підтримує оптимальний рівень когнітивного навантаження.

Важливим елементом персоналізації є гейміфікація, яка виступає механізмом адаптації мотиваційної складової навчання. У CodinGame навчальний процес побудований у формі ігрових сценаріїв, де кожне завдання має сюжет, систему балів та рейтингів. Це дозволяє враховувати індивідуальні освітні потреби учнів, зокрема потребу в

змагальності, досягненнях або поступовому саморозвитку, що підвищує залученість до навчання програмування.

Крім того, платформа забезпечує персоналізований зворотний зв'язок через автоматизоване тестування коду та миттєву перевірку результатів. Учень отримує інформацію про помилки, ефективність алгоритму та можливі шляхи покращення, що сприяє самостійному коригуванню навчальної діяльності. Таким чином, CodinGame поєднує елементи адаптивного контенту, індивідуальної траєкторії навчання та інтерактивного середовища, забезпечуючи ефективну реалізацію персоналізованого підходу у навчанні програмування.

Використання платформи CodinGame у контексті персоналізованого навчання програмування супроводжується низкою методичних ризиків. Насамперед, адаптивність середовища має переважно алгоритмічний характер і не забезпечує глибокої педагогічної діагностики навчальної діяльності учнів, зокрема не враховує причини помилок чи індивідуальні когнітивні особливості. Крім того, домінування гейміфікаційних елементів може зумовлювати зміщення акценту з осмисленого засвоєння навчального матеріалу на досягнення ігрових результатів, що формує поверхневий підхід до навчання. Також варто враховувати часткову невідповідність змісту платформи вимогам шкільних програм, що ускладнює її інтеграцію в освітній процес без додаткової методичної адаптації з боку вчителя.

Окрему групу ризиків становлять організаційно-педагогічні аспекти. Зокрема, автоматизований зворотний зв'язок у CodinGame має обмежений характер і здебільшого фіксує технічні помилки без глибокого пояснення, що потребує активного педагогічного супроводу. Для учнів із низьким рівнем підготовки можливий високий поріг входу, що негативно впливає на мотивацію. Крім того, індивідуалізація навчання в цифровому середовищі може знижувати рівень соціальної взаємодії, зокрема командної роботи та обговорення рішень. Ефективність використання платформи також залежить від технічних умов і цифрової компетентності вчителя, що в сукупності визначає необхідність комплексного методичного забезпечення її застосування.

Список використаних джерел:

1. Андросчук М. В., Кривонос О. М., Кулик С. П. Доцільність використання платформ Codewars та Codingame під час програмування в школі. *Наука і техніка сьогодні*. 2024. № 39. С. 409–419.
2. Медведева М., Жмурко О., Криворучко І., Ковтанюк М. Використання ігрових онлайн-сервісів у процесі вивчення мов програмування. *Актуальні питання гуманітарних наук*. 2021. Т. 2, № 36. С. 248–255.

УДК 004.41:004.8:378.091.3

Олексієнко А.О., здобувач,

Вовк Р.Б., к.т.н., доцент

Івано-Франківський національний технічний університет нафти і газу

МЕТОДОЛОГІЯ ПІДГОТОВКИ ІНЖЕНЕРІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ІМПЛЕМЕНТАЦІЇ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Сучасна парадигма професійної підготовки інженерів програмного забезпечення перебуває у стані фундаментальної трансформації, детермінованої масовою дифузією великих мовних моделей (Large Language Models, LLM). Інтеграція інтелектуальних агентів, таких як GitHub Copilot та Claude, у дидактичний процес створює прецедент нівелювання чіткої межі між автономним інтелектуальним пошуком суб'єкта навчання та автоматизованою генерацією програмних рішень. Ключовою проблемою даного переходу постає феномен «когнітивного розвантаження», що полягає у делегуванні складних логічних операцій алгоритмічним системам. Це призводить до ерозії етапу побудови внутрішніх ментальних моделей коду та формування ілюзії компетентності: при високій операційній швидкості здобувач втрачає здатність до самостійної дедукції та верифікації рішень у нетривіальних сценаріях [1].

Аналіз когнітивної взаємодії людини з системами штучного інтелекту свідчить про якісну зміну характеру інтелектуальної праці інженера. Традиційний акцент на синтаксичній коректності та алгоритмічній грамотності зміщується у площину «архітектурного нагляду» [2]. Рольова модель студента еволюціонує від лінійної імплементації коду до експертної валідації та рецензування. Зазначена трансформація вимагає не лише опанування методів промпт-інжинірингу, а й розвитку здатності до критичного аудиту згенерованого контенту на предмет безпеки та логічних аберацій («галюцинацій»). Мінімізація «продуктивних труднощів» (productive failure) у процесі написання коду з нуля загрожує зниженням когнітивної пластичності та аналітичної глибини фахівця.

Реалізація оновленої освітньої моделі в умовах домінування генеративного ШІ потребує системної реконфігурації структури підготовки. На зміну ізольованим технічним навичкам приходить комплексна цифрова грамотність, що базується на синергії з інтелектуальними системами. У межах науково-технічного дискурсу виокремлюються такі стратегічні компетенції:

- **Метакогнітивний архітектурний аналіз** - здатність до концептуальної декомпозиції складних систем за умови делегування рутинних операцій ШІ при збереженні контролю над цілісністю системних зв'язків.

- **Технічний аудит та етико-правова валідація** - верифікація згенерованих артефактів на відповідність стандартам безпеки (зокрема CWE) та аналіз ліцензійної чистоти отриманого коду [3].

- **Адаптивне забезпечення якості** - перехід від детермінованого написання тест-кейсів до проектування стратегій автоматизованого тестування для виявлення граничних умов та вразливостей.

- **Гібридна технічна комунікація** - формалізація вимог у специфікації, що є релевантними як для людського сприйняття, так і для обробки інтелектуальними агентами.

Запропонований структурний підхід дозволяє конвертувати інструменти ШІ з фактора когнітивної деградації у засіб інтелектуального масштабування, що корелює із запитом індустрії на підготовку адаптивних фахівців [4].

Перспективи подальших досліджень полягають у розробці адаптивних навчальних планів, що інтегрують етичні та безпекові виклики використання LLM. Виховання професійної відповідальності за автоматизований результат має бути імплементовано як базисну компетенцію нарівні з фундаментальними знаннями структур даних та алгоритмів. Пріоритет теоретичного базису над швидкістю імплементації є необхідною умовою підготовки інженерів, здатних до генерації інновацій у пост-алгоритмічну епоху.

Список використаних джерел:

1. Lau S., Guo P. J. The Impact of AI on Computer Science Education: A Study of Cognitive Offloading [Електронний ресурс]. Stanford University. 2024. URL: <https://hci.stanford.edu/publications/2024/ai-educognitive-offloading.pdf> (дата звернення: 22.03.2026).

2. White J., Fu Q., Hays S. Prompt Engineering for Software Engineering Education [Електронний ресурс]. IEEE Software. 2023. URL: <https://arxiv.org/abs/2302.11382> (дата звернення: 22.03.2026).

3. Pearce H., Ahmad B., Tan B. Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions [Електронний ресурс]. 2023. URL: <https://arxiv.org/abs/2108.09293> (дата звернення: 22.03.2026).

4. Designing Transparent Rubrics for AI-Based Evaluation: A Practical Guide [Електронний ресурс]. The Case HQ. 2026. URL: <https://thecasehq.com/designing-transparent-rubrics-for-ai-basedevaluation/> (дата звернення: 22.03.2026).

УДК 004.8:37.018.43

*Сікора Я.Б., д.пед.н., професор
Житомирський державний університет імені Івана Франка*

КОНЦЕПЦІЯ «HUMAN-IN-THE-LOOP» У ЦИФРОВІЙ ОСВІТІ

Цифрова трансформація освіти базується на інтеграції штучного інтелекту (ШІ), нейронних мереж та аналізу великих даних. Впровадження автоматизованого оцінювання, адаптивних систем та глибинної аналітики освітнього процесу створює передумови для підвищення якості навчання. Водночас повна автономність алгоритмів породжує виклики, пов'язані з етичністю, точністю та прозорістю прийняття рішень. Тому особливого значення набуває концепція Human-in-the-loop (HITL), яка передбачає поєднанні автоматизованих алгоритмів і людського контролю, що забезпечує більш обґрунтоване прийняття рішень [1].

Ефективність такого підходу підтверджується актуальними науковими дослідженнями. Зокрема, у роботі [2] наводиться порівняльний аналіз освітніх систем США, Індії та Китаю з використанням моделі HITL. У педагогічній практиці ця концепція передбачає, що викладач не лише використовує цифрові інструменти, а й бере участь у перевірці, інтерпретації та корекції результатів, отриманих за допомогою ШІ [3].

Розглянемо основні напрями використання технологій ШІ в практиці вищої освіти.

ШІ в навчальній аналітиці передбачає вимірювання, збір, аналіз і представлення даних про здобувачів та освітнє середовище для розуміння та вдосконалення процесу навчання. На відміну від традиційної аналітики, ШІ здатний аналізувати весь обсяг даних у режимі реального часу, навчаючись на них і виявляючи проблеми студентів ще в процесі їх виникнення. Основні цілі ШІ-аналітики передбачають прогнозування поведінки та успішності студентів на основі їхнього «цифрового сліду» та особистісних характеристик; проектування адаптивного контенту; дослідження взаємодії у системах «викладач – здобувач» або «середовище навчання – здобувач»; вивчення психології навчання та мотиваційного компонента для надання рекомендацій щодо підвищення успішності.

Використання ШІ у персоналізації навчання спрямоване на управління освітнім процесом та матеріалами, які адаптуються під конкретного здобувача освіти. Технології ШІ дозволяють відстежувати індивідуальний прогрес кожного студента та автоматично коригувати

освітнє середовище, враховуючи його досвід, вподобання та швидкість сприйняття інформації. У свою чергу, адаптивні платформи навчання використовують дані про успішність студентів для формування персоналізованих траєкторій навчання, проте потребують контролю з боку людини для уникнення некоректних рекомендацій.

Штучний інтелект в оцінюванні компетентностей здобувачів. Завдяки алгоритмам обробки природної мови ШІ дозволяє автоматизувати аналіз та оцінювання великих обсягів робіт: тестів, навчальних завдань, диктантів та есе. Крім того, ШІ активно використовується в системах автоматичного прокторингу для онлайн-навчання. Такі системи здатні самостійно контролювати поведінку здобувача під час дистанційного іспиту: відстежувати відведення погляду від монітора, спроби змінити вкладку браузера, появу сторонніх осіб або голосів у кадрі.

Впровадження ШІ показало свою ефективність у розвитку м'яких навичок (soft skills) здобувачів, формуванні проєктних команд та діагностиці комунікативних навичок в полікультурному середовищі. Також ці технології сприяють забезпеченню інклюзивності навчання та допомагають ефективніше впроваджувати елементи гейміфікації.

Водночас реалізація цієї концепції супроводжується певними труднощами, зокрема необхідністю підвищення цифрової компетентності викладачів і додатковим навантаженням, пов'язаним із аналізом результатів роботи ШІ-систем.

Отже, концепція HITL є важливим напрямом розвитку цифрової освіти, оскільки дозволяє поєднати переваги штучного інтелекту з критичним мисленням і професійним досвідом викладача. Її впровадження сприяє підвищенню якості освітнього процесу та забезпечує більш відповідальне використання цифрових технологій.

Список використаних джерел:

1. Memarian B., Doleck T. Human-in-the-loop in artificial intelligence in education: A review and entity-relationship (ER) analysis. *Computers in Human Behavior: Artificial Humans*. 2024. Vol. 2, Iss.1. 100053. DOI: <https://doi.org/10.1016/j.chbah.2024.100053>.
2. Bhutoria A. Personalized Education and Artificial Intelligence in the United States, China, and India: A Systematic Review Using a Human-in-The-Loop Model. *Computers and Education: Artificial Intelligence*. 2022. Vol. 3. 100068. DOI: <https://doi.org/10.1016/j.caeai.2022.100068>.
3. Ninaus M., Sailer M. Closing the loop – The human role in AI for education. *Frontiers in Psychology*. 2022. Vol. 13. DOI: <https://doi.org/10.3389/fpsyg.2022.956798>.

УДК 378 147:004.92

*Карман О.С., аспірант,
Малежик П.М., к.ф.-м.н., д.пед.н., професор
Український державний університет імені Михайла Драгоманова*

VR-ТЕХНОЛОГІЇ ЯК ЧАСТИНА КОМП'ЮТЕРНОЇ 3D-ГРАФІКИ ТА ЇХ ЗАСТОСУВАННЯ В НАВЧАННІ

Вступ: У сучасному інформаційному суспільстві цифрові технології активно впроваджуються у різні сфери діяльності, зокрема в освіту. Одним із перспективних напрямів розвитку комп'ютерної 3D-графіки є технології віртуальної реальності (VR). Вони дозволяють створювати інтерактивні тривимірні середовища, у яких користувач може взаємодіяти з об'єктами та отримувати новий досвід навчання. Використання VR-технологій відкриває нові можливості для підвищення ефективності освітнього процесу, наочності навчальних матеріалів та розвитку практичних навичок у студентів[1].

Постановка задачі: Сучасна освіта потребує нових методів подання інформації, які б сприяли кращому засвоєнню матеріалу, розвитку просторового мислення та підвищенню зацікавленості студентів. Традиційні методи навчання не завжди дозволяють повною мірою продемонструвати складні процеси та об'єкти, особливо у технічних і природничих дисциплінах. У зв'язку з цим актуальним є дослідження можливостей використання VR-технологій як складової комп'ютерної 3D-графіки в освітньому середовищі.

Мета дослідження: Дослідити роль VR-технологій як частини комп'ютерної 3D-графіки та проаналізувати можливості їх застосування у навчальному процесі.

Ключові слова: віртуальна реальність, VR-технології, комп'ютерна 3D-графіка, освітні технології, інтерактивне навчання, віртуальні лабораторії.

Основна частина: VR-технології (Virtual Reality) — це технології створення штучного інтерактивного середовища, яке імітує реальний або вигаданий світ за допомогою комп'ютерної 3D-графіки. Основою VR є тривимірне моделювання, рендеринг, анімація та взаємодія користувача з цифровими об'єктами у режимі реального часу[2].

Завдяки використанню спеціального обладнання, такого як VR-окуляри, контролери руху та сенсори, користувач може зануритися у віртуальний простір і взаємодіяти з елементами середовища. Це створює ефект присутності, який значно підвищує рівень сприйняття інформації.

У сфері освіти VR-технології використовуються для створення інтерактивних навчальних матеріалів, віртуальних лабораторій, симуляцій та тренажерів. Наприклад, у медицині VR дозволяє моделювати хірургічні операції, у фізиці — візуалізувати складні фізичні процеси, а в архітектурі — досліджувати тривимірні моделі будівель.

Перевагами використання VR у навчанні є підвищення наочності навчального матеріалу, розвиток просторового мислення, безпечне виконання експериментів та можливість багаторазового повторення практичних завдань. Крім того, VR сприяє підвищенню мотивації студентів та залученню їх до активної участі у навчальному процесі.

Разом із тим впровадження VR-технологій потребує відповідного технічного забезпечення, спеціалізованого програмного забезпечення та підготовки викладачів до використання таких інструментів у навчальному процесі[3].

Висновки: VR-технології є важливим напрямом розвитку комп'ютерної 3D-графіки та мають значний потенціал для використання у сфері освіти. Вони забезпечують новий рівень наочності та інтерактивності навчального процесу, сприяють формуванню практичних навичок і підвищують ефективність засвоєння навчального матеріалу. Подальший розвиток VR-технологій відкриває перспективи створення інноваційних освітніх середовищ та методів навчання.

Список використаних джерел:

1. Кривонос Мирослава Петрівна, Мінгальова Юлія Ігорівна. ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ (VR) І ДОДАТКОВОЇ (AR) РЕАЛЬНОСТЕЙ У СУЧАСНІЙ ОСВІТІ. Modern Approaches to Problem Solving in Science and Technology. 2023. URL: https://eprints.zu.edu.ua/38329/1/Modern-Approaches-to-Problem-Solving-in-Science-and-Technology_Nov_15_17_Warsaw_Poland-306-311.pdf
2. Учасники проєктів Вікімедіа. Віртуальна реальність – Вікіпедія. URL: https://uk.wikipedia.org/wiki/Віртуальна_реальність
3. Дереза, О., Болтянський, Б., & Дереза, С. (2023). ВИКОРИСТАННЯ VR-ТЕХНОЛОГІЙ В НАУКОВИХ ДОСЛІДЖЕННЯХ. Науковий вісник Таврійського державного агротехнологічного університету, 12(2). <https://doi.org/10.31388/sbtsatu.v12i2.331>

УДК 004.9

Чінкує Паола, здобувач

*Інститут поліграфії та медійних технологій НУ «Львівська
політехніка»*

ІНТЕЛЕКТУАЛЬНА VR/AR-ПЛАТФОРМА З АДАПТИВНИМ НАВЧАННЯМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний розвиток інформаційних технологій сприяє впровадженню інноваційних підходів до організації навчального процесу. Перспективним напрямом є інтеграція технологій віртуальної (VR) та доповненої (AR) реальності зі штучним інтелектом (AI), що дозволяє створювати інтерактивні та персоналізовані освітні середовища.

VR/AR-технології забезпечують високий рівень наочності та залученості користувачів завдяки моделюванню складних об'єктів і процесів. У поєднанні з AI це дає змогу адаптувати навчальний контент відповідно до індивідуального рівня знань та поведінки користувача.

У роботі запропоновано архітектуру інтелектуальної VR/AR-платформи з адаптивним навчанням. Система включає VR/AR-середовище, модуль збору даних, модуль AI-аналітики, адаптивний модуль та базу даних.

VR/AR-середовище забезпечує взаємодію користувача з навчальним контентом у вигляді інтерактивних сцен. Модуль збору даних фіксує параметри взаємодії, зокрема дії користувача, час виконання завдань та кількість помилок.

Отримані дані обробляються модулем AI-аналітики, який здійснює оцінку рівня знань користувача та визначає складність навчальних завдань. На основі цього формується індивідуальний профіль.

Адаптивний модуль змінює параметри навчання, підбираючи завдання, надаючи підказки та коригуючи сценарії взаємодії. Це забезпечує персоналізацію навчального процесу та підвищує його ефективність.

База даних зберігає профілі користувачів, історію навчання та навчальний контент. Наявність зворотного зв'язку між модулями дозволяє системі динамічно адаптуватися до змін у поведінці користувача.

Перевагами запропонованого підходу є підвищення ефективності навчання, автоматизація оцінювання знань та можливість індивідуалізації освітнього процесу. Використання VR/AR також дозволяє моделювати складні або недоступні у реальності ситуації.

Таким чином, поєднання VR/AR та AI є перспективним напрямом розвитку освітніх технологій і може бути ефективно застосоване у різних сферах підготовки фахівців.

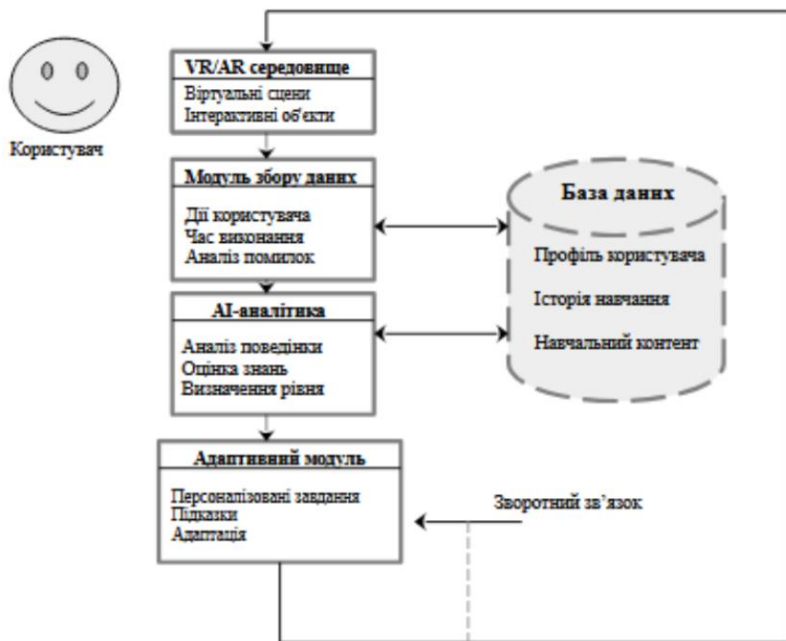


Рис.1. Архітектура інтелектуальної VR/AR-платформи з адаптивним навчанням на основі AI

Список використаних джерел:

1. Radianti J. [та ін.] Immersive virtual reality in higher education // Computers & Education. – 2020. – Vol. 147. – Art. 103778.
2. Billinghurst M., Clark A., Lee G. A survey of augmented reality // Foundations and Trends in Human–Computer Interaction. – 2015. – Vol. 8, № 2–3. – P. 73–272.

УДК 004.8:37.018.43:351.862

Смолт О.О., к.т.н., професор

Львівський державний університет безпеки життєдіяльності

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ СТРАТЕГІЧНОГО УПРАВЛІННЯ ОСВІТОЮ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Сучасна освіта у сфері цивільного захисту потребує багаторівневої архітектури, що координує підготовку між університетами, спеціалізованими інститутами, регіональними центрами та польовими тренувальними комплексами. Ця ієрархічна система (від стратегічного формування політики на національному рівні до оперативного забезпечення навчального процесу регіонально та тактичного набуття навичок локально) повинна реагувати на непередбачувані змінні, такі як новітні гібридні загрози, кліматично зумовлені катастрофи та технологічні зрушення. Традиційні підходи до управління, що спираються на статичне планування та ручний контроль, виявляються недостатніми в таких мінливих умовах.

Системи підготовки фахівців цивільного захисту за своєю природою є багаторівневими. На найвищому рівні міністерства формують стандарти компетентностей і визначають фінансування, на проміжному рівні технічні університети та академії відповідають за розробку навчальних програм, на операційному рівні працюють симуляційні центри та програми підвищення кваліфікації. Така структура подібна до світових моделей підготовки у сфері безпеки, але адаптована до цивільних і гібридних цивільно-військових контекстів.

Невизначеність пронизує всі рівні. Ландшафт загроз швидко змінюється: природні катастрофи, кібератаки або геополітична напруга, роблять статичні навчальні програми застарілими. Ресурсні обмеження коливаються через бюджетні цикли та термінові перерозподіли, а групи слухачів відрізняються за знаннями та темпами навчання. Освітні дані самі по собі є «шумними»: показники завершення курсів, збереження навичок і результати тренувань залежать від неврахованих змінних (мотивація, стрес тощо). Класична теорія прийняття рішень визначає, що такі середовища поєднують невизначеність (невідомі ймовірності), складність (взаємопов'язані змінні) та двозначність (суперечливі інтерпретації даних). Емпіричні дослідження підготовки до реагування на надзвичайні ситуації підтверджують ці проблеми.

Однак, новітні застосування AI (Artificial intelligence) на етапах пом'якшення наслідків, готовності, реагування та відновлення демонструють скорочення часу прийняття рішень на 35-40 % за умови

інтеграції прогнозної аналітики в тренувальні процеси. Втім, існуючі програми з цивільного захисту здебільшого не мають уніфікованих цифрових платформ для стратегічного коригування в режимі реального часу, що створює критичну прогалину, яку можуть заповнити AI-орієнтовані системи підтримки прийняття рішень (AI-СППР).

Нижче подаю пропонувану структурно-логічну схему AI-орієнтованої системи підтримки прийняття рішень для управління багаторівневою підготовкою фахівців цивільного захисту



Рис.1. Архітектура AI-СППР для управління багаторівневою підготовкою фахівців цивільного захисту (зображення, згенероване ШІ (Gemini) у відповідь на авторський промпт; авторські права на промпт належать автору статті.)

AI-СППР повинні використовувати машинне навчання для прогнозу та прескриптивної аналітики, здійснення стратегічного планування, прогнозування набору та оптимізації ресурсів із помітними покращеннями ефективності та довіри стейкхолдерів. Що в свою чергу потребує цифрової готовності освітніх інституцій усіх рівнів: від модернізації інфраструктури освітніх закладів до програм підвищення AI-компетентності викладачів.

Список використаних джерел:

1. Domfeh, E. A., et al. Human-AI Use Patterns for Decision-Making in Disaster Scenarios: A Systematic Review. arXiv:2509.12034, 2025. Режим доступу: <https://arxiv.org/pdf/2509.12034.pdf>
2. Rak T., Smotr O. AI-based trend modeling for managing educational resources in training civil protection specialists. // Sustainable Development Solutions: Regional Aspects : монографія / Lithuania Business College. – Klaipėda, 2025. – С. 80–91.

УДК 378.147:811.111:004:669

Довгаль І.А., ст. викладач

ТОВ «Технічний університет «Метінвест політехніка»

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ОПАНУВАННЯ ПРОФЕСІЙНОЇ АНГЛІЙСЬКОЇ МОВИ МАЙБУТНІМИ ІНЖЕНЕРАМИ-МЕТАЛУРГАМИ

Використання інформаційно-комунікаційних технологій (ІКТ) у навчанні англійської мови для майбутніх металургів — це не просто «цифровізація», а спосіб зробити складні технічні процеси наочними та зрозумілими. Для здобувачів освіти цієї спеціальності важливо не лише знати граматику, а й вільно оперувати термінологією в контексті реального виробництва.

Розглянемо основні напрями використання інформаційно-комунікаційних технологій, які допоможуть майбутнім фахівцям у сфері металургії опанувати професійну англійську. Металургія — це галузь, де багато процесів приховані всередині печей або відбуваються на мікрорівні. Тому актуальним буде використання 3D-моделювання та анімації. Замість статичних картинок у підручнику, здобувачі освіти можуть переглядати англomовні ролики про роботу доменної печі або конвертера. Це допомагає пов'язати візуальний образ із терміном (наприклад, blast furnace, molten metal, slag). Використання програм-тренажерів, де інтерфейс налаштований англійською мовою, допомагає здобувачам освіти віртуально «керувати» плавкою, вивчаючи команди та назви обладнання в дії.

Застосування онлайн-ресурсів типу Cambridge Dictionary або вузькоспеціалізованих технічних глосаріїв дає можливість створити професійні корпуси текстів та словники. Перегляд технічних оглядів від компаній тренує сприйняття технічної англійської на слух з різними акцентами. Доречним є створення наборів карток у Quizlet з металургійною термінологією (наприклад, назви сплавів: stainless steel, cast iron, carbon steel). На базі Moodle або Google Classroom викладач може створювати інтерактивні завдання: від аналізу технічних паспортів (Material Safety Data Sheets) до перекладу інструкцій з техніки безпеки. Інформаційно-комунікаційні технології дають можливість здобувачам освіти долучитися до міжнародних професійних форумів, онлайн-вебінарів та конференцій, де вони можуть почути, як обговорюють екологічні стандарти (Green Steel) або автоматизацію виробництва. VR-тури на заводи сприяють зняттю мовного бар'єру в умовах "реального" цеху. Chat GPT / AI-інструменти дозволяють редагувати технічні звіти та підготовку до презентацій англійською.

Інтерактивні схеми активізують швидке запам'ятовування назв частин обладнання. Для металурга англійська мова — це інструмент роботи з міжнародними стандартами (ISO, ASTM) та сучасною документацією до імпортного обладнання. Використання інформаційно-комунікаційних технологій в освіті сьогодні — це не просто заміна паперового зошита на планшет. Це потужний інструмент для розвитку «soft» та «hard skills», які критично важливі в сучасному цифровому світі.

За допомогою інформаційно-комунікаційних технологій здобувачі освіти спеціальності Металургія можуть розвивати когнітивні, цифрові, технічні, комунікаційні навички та самоменеджмент.

ІКТ вчать здобувачів освіти перевіряти дані через різні джерела, це розвиває вміння аналізувати показники датчиків у реальному часі. Використовуючи програми для розрахунку шихти або моделювання лиття майбутні інженери та металурги вчаться передбачати дефекти металу ще до того, як він буде залитий у форму. Знання програмування та алгоритмів активізує розуміння логіки роботи контролерів (PLC), які керують автоматичними лініями прокатки. Побудова графіків залежності міцності сталі від вмісту вуглецю в Excel або спеціалізованих BI-системах розвиває аналітичне мислення та вміння виявляти закономірності в технологічних процесах, що є базою для сучасного інженера. Інформаційно-комунікаційні технології допомагають займатися самоосвітою та стежити за новими методами прямого відновлення заліза на спеціалізованих порталах.

Впровадження інформаційно-комунікаційних технологій у процес навчання майбутніх фахівців-металургів дозволяє зробити головний перехід: від теоретичного вивчення мови та технологій до практичного моделювання професійної діяльності.

Список використаних джерел

1. Биков В. Ю. Цифрова трансформація суспільства і розвиток комп'ютерно-технологічної платформи освіти і науки. Інформаційні технології і засоби навчання. 2019. Т. 70, № 2. С. 1–13.
2. Коноваленко Т. В. Використання ІКТ у навчанні професійно орієнтованої англійської мови студентів технічних спеціальностей. Наукові записки [Національного університету "Острозька академія"]. Серія: Філологічна. 2015. Вип. 51. С. 317–319.
3. Ніколаєва С. Ю. Сучасні технології навчання іноземних мов у закладах вищої освіти. Вісник КНЛУ. Серія: Педагогіка та психологія. 2018. Вип. 28. С. 5–15.

УДК 373.5.091.3:004.896

*Шевчук П.Г., к.пед.н., ст. викладач
Житомирський державний університет імені Івана Франка
Гиндич І.Є., вчитель інформатики
Миропільський ліцей Житомирської області*

МІЖНАРОДНА STEM-ПРОГРАМА FIRST LEGO LEAGUE ТА НАВЧАННЯ ІНФОРМАТИКИ У ЗЗСО

Сучасна парадигма шкільної інформатики передбачає окрім виключно теоретичного вивчення алгоритмів дослідження їх практичного застосування у реальному світі. Інтеграція робототехніки у навчання інформатики відповідає концепції Нової української школи та оновленим модельним програмам для 5-9 класів [1, 2, 3, 4], які виділяють час на вивчення робототехніки та створення алгоритмів. Це забезпечує практичне спрямування та експоненційно підвищує мотивацію учнів. Використання освітньої робототехніки на уроках дозволяє наочно ілюструвати програмний код. Учні миттєво бачать результати своєї роботи, що створює оптимальні умови для емпіричного тестування гіпотез, розуміння причинно-наслідкових зв'язків та зневадження помилок. Це і є передумовами для можливої інтеграції міжнародної STEM-програми FIRST LEGO League [5, 6] зі шкільним курсом інформатики закладів загальної середньої освіти. **То ж мета даного дослідження:** теоретично обґрунтувати та методично розкрити можливості інтеграції міжнародних дослідницько-орієнтованих програм (на прикладі FIRST LEGO League) у курс інформатики закладів загальної середньої освіти для формування STEM-компетентностей та розвитку алгоритмічного мислення учнів в умовах реалізації реформи «Нова українська школа».

Завдання дослідження:

- проаналізувати нормативно-правове забезпечення та модельні навчальні програми інформатичної галузі в контексті впровадження інноваційного обладнання;
- дослідити архітектуру та освітній потенціал програми FIRST LEGO League як інструменту проектного навчання;
- оцінити дидактичні можливості сучасного апаратного та програмного забезпечення (LEGO SPIKE Prime, мова Python) для навчання алгоритмізації. Розкрити потенціал міжпредметних зв'язків через аналіз тематики сезонів (кейс сезону «UNEARTHED»);
- визначити вплив програми на когнітивний розвиток та формування «м'яких навичок» (Soft Skills) школярів.

Архітектуру програми FIRST LEGO League можна використовувати і як основу для проєктного навчання. Комплексна екосистема: FLL — це масштабна дослідницько-орієнтована програма, розрахована на тривалий період підготовки протягом навчального року [5].

Дивізіон FLL Challenge створений для дітей віком від 9 до 16 років, що ідеально збігається з аудиторією учнів базової середньої школи (5-9 класи) [5].

Програма базується на трьох рівноцінних напрямках, які комплексно розвивають учня: Гра роботів (інженерія та програмування), Інноваційний проєкт (науково-дослідна робота над актуальною проблемою) та Основні цінності (взаємоповага і командна робота) [5, 6]. «Гра роботів» фокусується на технічній складовій — алгоритмізації та автономному програмуванні кіберфізичних систем, що є фундаментом практичного курсу інформатики. «Інноваційний проєкт» розширює ці знання через науково-дослідницьку роботу, де учні використовують IT-інструменти для пошуку інформації та цифрового моделювання рішень реальних проблем, наприклад, в археологічному сезоні UNEARTHED. «Основні цінності» інтегрують ці процеси через командну співпрацю та етичне ставлення до технологій, формуючи навички колаборації, необхідні для успішної реалізації групових IT-проєктів.

Щороку команди отримують нову Задачу Сезону, присвячену актуальній науковій проблемі (екологія, логістика, космос), яку обирають реальні вчені та інженери. А це є основою глибоких міжпредметних зв'язків навчання інформатики з іншими дисциплінами. Сезон 2025-2026 років під назвою «UNEARTHED» присвячений археології [7, 8]. Щоб виконати завдання, учні мають об'єднати інформатику з історією та фізикою. Учні досліджують, як сучасні інструменти (лідари, 3D-моделювання, бази даних) допомагають у пошуку скарбів, дешифруванні стародавніх символів та збереженні крихких артефактів. Це формує розуміння того, що STEM-навички потрібні в будь-якій сфері.

Базовим обладнанням для шкільних команд є кіберфізичні набори LEGO Education (зокрема лінійки SPIKE Prime та Mindstorms EV3) [9]. Вони містять програмовані мікроконтролери, високоточні сервомотори та набір інтелектуальних сенсорів (гіроскопи, датчики кольору, відстані). Програмування автономного робота дозволяє учням на практиці досліджувати концепції введення та виведення даних, а також критичну важливість систем зворотного зв'язку в управлінні динамічними об'єктами.

Програмне середовище дозволяє учням 5-6 класів починати зі створення вкладених алгоритмічних структур через візуальні блоки

(подібні до Scratch), а у старших класах легко переходити до професійного текстового програмування (наприклад, мовою Python) [10].

Додатковим мотиватором є фестивальний рух за підтримки профільних організацій (наприклад, ГО «Міжнародна Організація «Інноваційні освітні технології» [5, 10]). Ці організації здійснюють методичний супровід та локалізацію матеріалів. Участь команд у масштабних наукових подіях, таких як Всеукраїнський чемпіонат FIRST LEGO League та STEM-фестиваль «Robotica», дарує дітям відчуття приналежності до світової спільноти інноваторів та є потужним стимулом до навчання.

Висновки

Інтеграція міжнародних програм (FIRST LEGO League) у шкільний курс інформатики повністю відповідає вимогам Державного стандарту базової середньої освіти та концепції НУШ, забезпечуючи перехід до діяльнісного та компетентнісного навчання.

Структура FLL дозволяє системно реалізувати проєктне навчання, де програмування автономних роботів є засобом розв'язання актуальних наукових проблем реального світу.

Використання сучасних рішень (LEGO SPIKE Prime) забезпечує наступність навчання: від візуального програмування у 5-6 класах до вивчення індустріальних мов (Python) у 7-9 класах.

Міжпредметний потенціал сезонів (зокрема археологічного сезону «UNEARTHED») сприяє формуванню цілісної картини світу, поєднуючи ІТ з природничими та гуманітарними науками.

Програма є потужним інструментом розвитку Soft Skills (командна співпраця, критичне мислення, медіаграмотність), що підвищує конкурентоспроможність майбутніх випускників.

Список використаних джерел:

1. Морзе Н. В., Барна О. В. Модельна навчальна програма «Інформатика. 5-6 класи» для закладів загальної середньої освіти [Електронний ресурс] / Н. В. Морзе, О. В. Барна // Міністерство освіти і науки України. – 2021. – Режим доступу: <https://mon.gov.ua/storage/app/media/zagalna%20serednya/Navchalni.prohramy/2021/14.07/Model.navch.prohr.5-9.klas.NUSH-poetap.z.2022/Inform.osv.haluz.5-6-kl/Inform.5-6-kl.Morze.Barna.14.07.pdf> (дата звернення: 12.03.2026).

2. Ривкінд Й. Я., Лисенко Т. І., Чернікова Л. А., Шакотько В. В. Модельна навчальна програма «Інформатика. 7-9 класи» для закладів загальної середньої освіти [Електронний ресурс] // Міністерство освіти і науки України. – 2023. – Режим доступу: <https://it->

teacher.pp.ua/модельна-навчальна-програма-інформ-7-9/ (дата звернення: 15.03.2026).

3. Громко Г. Ю., Шевчук П. Г., Ковбаса В. М. Модельна навчальна програма «Інформатика. 7–9 класи» для закладів загальної середньої освіти [Електронний ресурс] / Г. Ю. Громко, П. Г. Шевчук, В. М. Ковбаса // Міністерство освіти і науки України. – 2023. – Режим доступу: <https://mon.gov.ua/.../Informatyka.7-9.kl.Hromko.ta.in.21.12.2023.pdf> (дата звернення: 10.04.2026).

4. Сокол І. М., Ченцов О. М. Модельна навчальна програма «Робототехніка. 7-9 класи (міжгалузевий інтегрований курс)» [Електронний ресурс] / І. М. Сокол, О. М. Ченцов // Teach-inf.com.ua. – 2024. – Режим доступу: https://teach-inf.com.ua/load/kabinet_informatiki/navchalni_programi/modelna_navchalna_programa_robototekhnika_7_9_klasi_mizhgaluzevij_integrovaniy_kurs_avtori_sokol_i_m_chencov_o_m/39-1-0-4339 (дата звернення: 15.03.2026).

5. Офіційний сайт FIRST LEGO League в Україні [Електронний ресурс] / ГО «Міжнародна Організація «Інноваційні освітні технології». – Режим доступу: <http://firstlegoleague.org.ua/> (дата звернення: 12.03.2026).

5. Навички, що отримують діти. Вплив FIRST LEGO League [Електронний ресурс] // FIRST LEGO League Україна. – Режим доступу: <http://firstlegoleague.org.ua/navychky-shcho-otrymuyut-dity/> (дата звернення: 12.03.2026).

6. Challenge. FIRST LEGO League [Електронний ресурс] // FIRST LEGO League Україна. – Режим доступу: <http://firstlegoleague.org.ua/challenge-en/> (дата звернення: 25.03.2026).

7. Game & Season Info: UNEARTHED [Electronic resource] // FIRST Inspires. – 2025. – Mode of access: <https://www.firstinspires.org/programs/fl/game-and-season> (date of access: 25.03.2026).

8. SPIKE™ Prime Teacher Resources [Електронний ресурс] / LEGO Education. – Режим доступу: <https://education.lego.com/en-us/teacher-resources/lego-education-spike-prime/> (дата звернення: 25.03.2026).

9. Welcome to SPIKE™ Prime [Електронний ресурс] / LEGO Education. – Режим доступу: <https://spike.legoeducation.com/prime/lobby/> (дата звернення: 25.03.2026).

УДК 004.9: 519.81

*Безкоровайний В. В., д.т.н, професор,
Кисельова О. Б., к.пед.н., доцент,
Шербак І. В., д.пед.н., доцент
Харківська гуманітарно-педагогічна академія*

АДАПТАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ ПРИ ВПРОВАДЖЕННІ ТЕХНОЛОГІЙ ІНДИВІДУАЛІЗАЦІЇ НАВЧАННЯ

Динамічний характер технологічного суспільства, суспільні запити, сучасні інформаційно-комунікаційні технології створюють умови для індивідуалізації процедур набуття освіти [1]. Їх впровадження супроводжується суттєвим зростанням кількості користувачів, що потребує відповідної адаптації комп'ютерних мереж навчальних закладів.

Типовим прикладом є технологія BYOD (Bring Your Own Device), впровадження якої призводить до суттєвого зростання трафіку і перевантаження обладнання існуючих мереж [2].

Адаптація комп'ютерних мереж у найбільш складному випадку приводить до необхідності їхнього перепроєктування (реінжинірингу) з можливістю використання обладнання існуючих мереж [3]. Це передбачає ітераційне розв'язання множини комбінаторних задач їх структурної, топологічної, параметричної та технологічної оптимізації.

Об'єктом дослідження є тривірневі централізовані комп'ютерні мережі, що поєднують користувачів з головними серверами через вузли (маршрутизатори, локальні сервери). Для існуючої мережі вважаються

задані: множина елементів $I = \{i\}$, $i = \overline{1, n}$; існуючий варіант топологічної структури з множини допустимих $s' \in S^*$. Множина S^* задається місцями можливого розташування елементів і можливими зв'язками між елементами; наведеними витратами на створення чи модернізацію вузлів і зв'язків між елементами. З урахуванням достатньої надійності сучасного обладнання необхідно визначити найкращий варіант адаптації мережі $s^0 \in S^*$ за показниками наведених

витрат $k_1(s) \rightarrow \min_{s \in S^*}$ та її оперативності (часу отримання відповідей на

запити) $k_2(s) \equiv \tau(s) \rightarrow \min_{s \in S^*}$. Варіант адаптації мережі задається кількістю і типами вузлів у ній, місцями їх розміщення, схемою та типами зв'язків між елементами, вузлами і центром.

Адитивна згортка локальних критеріїв дозволяє звести багатокритеріальну задачу до традиційної задачі оптимізації мережі зі скалярним критерієм загальної корисності [3]:

$$P(s) = \sum_{i=1}^2 \eta_i \xi_i(s) \quad \xi_i(s) = \xi_i(k_i(s)) = \left[\frac{k_i(s) - k_i^-(s)}{k_i^+(s) - k_i^-(s)} \right]^{\delta_i}, \quad i = \overline{1, 2}, \quad (1)$$

де η_i – ваговий коефіцієнт критерію $k_i(s)$, $\eta_i \geq 0$, $\sum_{i=1}^2 \eta_i = 1$; $\xi_i(s) = \xi[k_i(s)]$, $k_i^-(s)$, $k_i^+(s)$, – функція корисності, найгірше та найкраще значення критерію; $k_i(s)$; δ_i – параметр, який визначає вид залежності $\xi_i(s)$.

Для розв’язання задачі пропонується використовувати модифікацію методу спрямованого перебору з додаванням процедури обчислення значення загальної корисності $P(s)$ (1) [4]. Для оцінки оперативності кінцевих варіантів побудови мережі пропонується використати імітаційне моделювання.

Напрямок подальших досліджень може бути врахування в моделі задачі адаптації мереж навчальних закладів неповної визначеності вхідних даних, зокрема, стохастичного характеру потоків запитів користувачів, функціональних та вартісних характеристик їх обладнання.

Список використаних джерел:

1. Семеновська Л., Важеніна І., Фазан В. Індивідуалізація навчання як актуалітет розвитку інформаційно-технологічного суспільства. Педагогічні науки, (2023). №82. С. 30–34.
2. Скибун О. Ж., Гайдур Г. І., Гахов С. О. Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації. 2024. №1(57). С. 50–56.
3. Безкоровайний В. В., Кисельова О. Б., Щербак І.В. Оптимізація комп’ютерних мереж навчальних закладів у процесі переходу до технології BYOD. Інформаційні системи та інноваційні технології управління проектами і програмами. Збірник праць. Харків: ХНУРЕ, 2025. С. 86–88.
4. Beskorovainyi V., Russkin V. Directed search of variants in technologies for reengineering of corporate computer networks. Intelligent information systems for decision support in project and program management. European University Press, Riga: ISMA, 2021. P. 15-24.

УДК 004.9:[37.091.33:005.591.6]

Сокорчук І.П., ст. викладач

Харківський національний університет радіоелектроніки

БУДОВА АВТОМАТИЗОВАНОГО РОБОЧОГО МІСЦЯ ВИКЛАДАЧА ДЛЯ ОСВІТНЬОГО ПРОЦЕСУ В ДИСТАНЦІЙНІЙ ФОРМІ

Розвиток інформаційно-комунікаційних технологій і поширення дистанційного навчання зумовлюють необхідність автоматизації діяльності викладача. Значний обсяг адміністративних і технічних завдань, пов'язаних із підготовкою матеріалів, перевіркою робіт та веденням документації, потребує застосування інтегрованих програмних рішень.

Автоматизоване робоче місце (АРМ) викладача доцільно будувати за модульним принципом, що забезпечує гнучкість і масштабованість. До основних функціональних модулів належать: система управління навчанням (LMS), модуль автоматизації перевірки завдань, аналітичний модуль, засоби комунікації та управління проектами. Така структура забезпечує комплексну підтримку освітнього процесу.

Ключовим елементом АРМ є LMS, яка забезпечує організацію курсів, контроль виконання завдань і взаємодію учасників. Використання систем із відкритим програмним кодом дозволяє адаптувати їх до специфічних вимог навчального процесу та інтегрувати з іншими сервісами через API. Інтеграція з хмарними платформами та сервісами відеоконференцій розширює функціональні можливості, забезпечуючи спільну роботу та проведення занять у реальному часі.

Для організації командної роботи над програмними проектами доцільно застосовувати системи контролю версій. Вони забезпечують централізоване зберігання коду, відстеження змін і підтримку колективної розробки. Інструменти автоматизації, такі як системи безперервної інтеграції, дозволяють виконувати тестування, статичний аналіз коду та формування звітів, що підвищує об'єктивність оцінювання.

Важливу роль відіграють засоби операційної системи Linux та утиліти командного рядка. Використання скриптів оболонки дає змогу автоматизувати перевірку завдань, обробку текстових даних і управління файлами. Зокрема, утиліти порівняння, обробки тексту та пошуку дозволяють ефективно аналізувати результати виконання завдань. Інструменти статичного аналізу коду забезпечують виявлення помилок і порушень стандартів програмування. Практичне

впровадження таких засобів дозволяє скоротити час перевірки робіт приблизно на 50%.

Перспективним напрямом є інтеграція технологій штучного інтелекту. Методи аналізу освітніх даних дають змогу виявляти закономірності навчальної діяльності, прогнозувати успішність студентів і формувати рекомендації щодо оптимізації навчального процесу. Алгоритми машинного навчання можуть застосовуватися для аналізу активності в LMS, визначення складних тем і адаптації навчального контенту. Окремим напрямом є автоматизація перевірки завдань, включаючи аналіз текстових відповідей і програмного коду. Використання чат-ботів забезпечує оперативну підтримку студентів у межах типових запитів.

Таким чином, інтеграція LMS, систем контролю версій, інструментів Linux та технологій штучного інтелекту формує єдине цифрове середовище організації освітнього процесу. Використання такого підходу сприяє зниженню навантаження на викладача, підвищенню якості оцінювання та ефективності взаємодії зі студентами.

Впровадження автоматизованого робочого місця викладача на основі модульної архітектури забезпечує ефективну інтеграцію інструментів управління навчанням, автоматизації перевірки та аналітики освітніх даних.

Список використаних джерел:

1. GitHub – офіційна сторінка сервісу [Електронний ресурс]. – Режим доступу: <https://github.com/>
2. GNU Bash, Awk, sed, tar, gzip, grep, wget – офіційна сторінка. [Електронний ресурс]. – Режим доступу: <https://www.gnu.org/software/>
3. ShellCheck – офіційна сторінка інструмента. [Електронний ресурс]. – Режим доступу: <https://www.shellcheck.net/>
4. Rsync – офіційна сторінка. [Електронний ресурс]. – Режим доступу: <https://rsync.samba.org/>
5. Moodle Documentation [Електронний ресурс] – Режим доступу: <https://docs.moodle.org>
6. Сокорчук І. П. Автоматизація повсякденних завдань викладачів за допомогою засобів штучного інтелекту: покращення робочого процесу та ефективності / І. П. Сокорчук // Поліграфічні, мультимедійні та web-технології : тези доп. IX Міжнар. наук.-техн. конф., 14-18 травня 2024 р. – Т. 1. – Харків: ТОВ «Друкарня Мадрид», 2024. – С. 330-331.

УДК 004.588

Михайлюк О.В., здобувач

Національний університет «Київський авіаційний інститут»

МЕТОДИ ЗБОРУ ТА ОБРОБКИ ДАНИХ ПРО СТАН СЕРВІСІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS

У роботі досліджено методи збору та обробки даних про стан системних сервісів у операційній системі *Windows*. Розглянуто сучасні підходи до моніторингу, включаючи використання *WMI* та *PowerShell*, а також принципи аналізу даних у системах забезпечення надійності. Обґрунтовано необхідність комплексного підходу до моніторингу.

Ключові слова: моніторинг, *Windows*, сервіси, *WMI*, *PowerShell*, обробка даних, *SRE*, *observability*

У сучасних інформаційних системах стабільність роботи програмного забезпечення значною мірою залежить від коректного функціонування системних сервісів. В операційній системі *Microsoft Windows* сервіси забезпечують виконання ключових фонових процесів, що впливають на продуктивність, безпеку та надійність системи.

Згідно з дослідженнями у сфері *Site Reliability Engineering (SRE)*, ефективний моніторинг дозволяє зменшити час простою систем і підвищити їх надійність [1]. Концепція *observability* передбачає аналіз системи на основі метрик, логів і трасувань [2].

Таким чином, проблема ефективного збору та обробки даних про стан сервісів є актуальною.

Метою роботи є аналіз та систематизація методів збору й обробки даних про стан сервісів у середовищі *Windows* з урахуванням сучасних підходів [1].

Завдання дослідження

1. Дослідити особливості функціонування сервісів у *Windows*.
2. Проаналізувати методи збору інформації про їх стан [3].
3. Розглянути підходи до обробки та аналізу даних [4].
4. Визначити ефективність сучасних підходів до моніторингу [2].
5. Сформулювати вимоги до систем моніторингу [5].

Об'єкт дослідження: процеси функціонування системних сервісів у операційній системі *Microsoft Windows*.

Предмет дослідження: методи збору та обробки даних про стан сервісів та підходи до їх аналізу [4].

Системні сервіси в *Microsoft Windows* є важливими компонентами, які забезпечують виконання фонових процесів і підтримку функціонування прикладного програмного забезпечення.

Моніторинг сервісів передбачає збір, аналіз і інтерпретацію даних про їх стан. Сучасні підходи базуються на концепції *observability*, яка включає метрики, логи та трасування [2].

Основними методами збору інформації є: використання вбудованих засобів Windows; застосування технологій *Windows Management Instrumentation* та *PowerShell*; аналіз системних журналів подій.

Згідно з документацією *Microsoft*, використання *WMI* та *PowerShell* забезпечує ефективний доступ до системної інформації та дозволяє автоматизувати процес моніторингу [3].

Після збору даних виконується їх обробка. Вона включає фільтрацію, агрегацію та аналіз тенденцій, що дозволяє виявляти аномалії [4].

Сучасні дослідження показують, що системи моніторингу повинні підтримувати прогнозування збоїв та автоматичне реагування [5].

Таким чином, ефективний моніторинг сервісів повинен базуватися на комплексному підході.

Висновки: У результаті дослідження встановлено, що ефективний моніторинг сервісів у середовищі *Windows* потребує комплексного підходу, який включає сучасні методи збору та обробки даних.

Використання *WMI* та *PowerShell* дозволяє отримувати детальну інформацію про стан системи, а впровадження підходів *observability* підвищує ефективність аналізу [2].

Список використаних джерел:

1. Beyer B., Jones C., Petoff J., Murphy N. Site Reliability Engineering: How Google Runs Production Systems. – Sebastopol: O'Reilly Media, 2016. – 552 p. – URL: <https://sre.google/sre-book/table-of-contents/>
2. Mukhi N. From Monitoring to Observability. – Zenodo, 2024. – URL: <https://zenodo.org/records/17410892>
3. Microsoft Docs. Windows Management Instrumentation (WMI) and PowerShell Documentation. – URL: <https://learn.microsoft.com>
4. Cleland-Huang J. et al. Monitoring in Software Engineering // Information and Software Technology. – 2016. – Vol. 80. – P. 1–20. – URL: <https://doi.org/10.1016/j.infsof.2016.07.002>
5. Sosnowski J., Król M. Dependability Evaluation Based on System Monitoring // InTech. – 2010. – URL: <https://www.intechopen.com>

Секція 6
ЦИФРОВА ОБРОБКА СИГНАЛІВ ТА
ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА
ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ
СИСТЕМАХ

УДК 004.932

*Андрікевич С.А., аспірант,
Щербатюк А.В., аспірант,
Тужанський С.Є., к.т.н., доцент
Вінницький національний технічний університет*

МЕТОД ПОКРАЩЕННЯ ЗОБРАЖЕНЬ ОЧНОГО ДНА НА
ОСНОВІ ФАЗОВОГО ПІДХОДУ

Якість візуалізації структур медичних зображень є ключовою для точного аналізу та діагностики. У роботі запропоновано метод покращення зображень очного дна на основі модифікації фазового спектру з використанням високочастотної фільтрації та комбінування фазової й амплітудної інформації.

У роботі використано цифрові зображення очного дна, отримані за допомогою фундус-камери з відкритої бази HRF [1]. Зображення мають роздільну здатність 3504×2336 пікселів, формат .jpg і глибину кольору 24 біти. Обробку виконано окремо для кожного каналу в колірному просторі RGB з подальшим об'єднанням отриманих результатів.

Запропонований метод включає обчислення двовимірного перетворення Фур'є для кожного каналу зображення з подальшим розділенням спектру на амплітудну та фазову складові. Для підсилення структурних елементів застосовано високочастотний гаусів фільтр до фазового спектру, що дозволяє виділити дрібні деталі [2]. Додатково використано нормалізацію та логарифмічне масштабування амплітудного спектру для стабілізації динамічного діапазону.

Формування результуючого зображення здійснюється як зважена комбінація фазової та амплітудної складових із вихідним зображенням, що дозволяє досягти балансу між підсиленням деталей і збереженням його наочності. Результати обробки зображення очного дна 12_dr.jpg разом із гістограмами інтенсивностей наведено на рисунку 1.

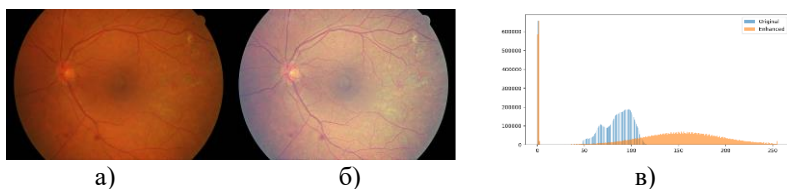


Рис.1. Приклад обробки зображення очного дна 12_dr.jpg [2]:
а) оригінал; б) фазовий метод; в) гістограми інтенсивностей

Для покращення контрастності додатково застосовано адаптивне розтягнення інтенсивностей у межах заданих процентилів. З метою уникнення спотворень поза межами робочої зони використано маскування області очного дна. Аналіз гістограм показує розширення динамічного діапазону та більш рівномірний розподіл інтенсивностей після обробки, що свідчить про підвищення контрастності зображення.

Оцінювання ефективності обробки виконано за допомогою індексу структурної подібності (SSIM) та показника підсилення контрасту (EME) на вибірці з 40 тестових зображень бази HRF [1]. Результати за SSIM свідчать про збереження структурних характеристик між початковими та обробленими зображеннями, тоді як підвищення значень EME вказує на ефективне покращення локального контрасту.

Результати дослідження показали, що значення SSIM (≈ 0.56 – 0.80 , медіана ~ 0.67) є співставними з вейвлет-методами (0.65 – 0.83 для bior2.2), що свідчить про збереження структурної подібності зображень, водночас показник EME оброблених зображень досягає ≈ 3.0 – 3.4 , що свідчить про вищу ефективність підсилення контрасту порівняно з вейвлет-перетвореннями (2.5 – 3.5). Це дозволяє вважати фазовий метод більш стабільним та універсальним для задач попередньої обробки зображень очного дна.

Список використаних джерел:

1. Visualization Tools for High Resolution Fundus Dataset / Dataset Ninja. URL: <https://datasetninja.com/high-resolution-fundus>
2. Long, J., Meng, C., Ding, Y., & Xi, J. (2023). Suppressing the Zero-Frequency Components in Single Quantitative Phase Imaging by Filtering the Low-Frequency Intrinsic Mode Function Components. *Photonics*, 10(7), 790. URL: <https://doi.org/10.3390/photonics10070790>

УДК 621.37

Бугайов М. В., к.т.н., ст. досл., ЗННДВ НДУ

Поздняков В. В., ад'юнкт

Житомирський військовий інститут імені С. П. Корольова

МЕТОД ПРОСТОРОВО-СПЕКТРАЛЬНОГО ОБРОБЛЕННЯ ГРУПОВИХ АКУСТИЧНИХ СИГНАЛІВ ГВИНТОМОТОРНИХ ЛІТАЛЬНИХ АПАРАТІВ

В умовах сучасних збройних конфліктів спостерігається стрімке зростання масштабів застосування ударних гвинтомоторних літальних апаратів (ГЛА). Їх пріоритетними цілями є об'єкти критичної інфраструктури та енергетичного сектору. Вони здатні здійснювати політ на надмалих висотах поза зоною прямої видимості радіолокаційних станцій. Виникає потреба у розвитку пасивних акустичних систем виявлення ГЛА. Перехід до групових польотів ГЛА зумовлює складну акустичну обстановку. Це зумовлює критичну необхідність пошуку та створення нових просторово-спектральних методів оброблення групових сигналів, здатних виділяти окремі джерела в багатокомпонентному звуковому сигналі.

Вихідними даними для роботи запропонованого методу просторового оброблення є результати спектрального аналізу групового сигналу, а саме кількість ГЛА, що одночасно перебувають у зоні дії акустичного детектора та набори їхніх індивідуальних спектральних сигнатур. Зокрема, для кожного ідентифікованого об'єкта вже виділено масиви значень його фундаментальної частоти та відповідних вищих гармонік. Отримання цих даних забезпечується розділенням алгоритмами шляхом адаптивного порогового оброблення та спектрального усереднення [1]. Сутність алгоритму полягає у просторово-спектральній фільтрації сигналів на рівні мікрофонних пар. Для збереження фазової інформації вихідні акустичні сигнали перетворюються у частотно-часову область за допомогою віконного перетворення Фур'є, формуючи масиви комплексних спектральних відліків $Z(t, f) = A(t)e^{j2\pi f t + \varphi}$. Процес виділення окремого ГЛА реалізується шляхом фільтрації цих масивів динамічним спектральним фільтром $H(t, f)$, що синтезований на основі апріорно визначених кінематичних параметрів. Цей фільтр функціонує як багатосмуговий адаптивний гребінчастий фільтр. Його принциповою особливістю є жорстке присвоєння нульових вагових коефіцієнтів усім частотним відлікам, які не належать спектральній сигнатурі обраного ГЛА в момент часу аналізу. Натомість одиничні значення фільтра динамічно супроводжують виділені фундаментальну частоту та гармоніки,

адаптуючись до їхнього пропорційного доплерівського зсуву. Операція поелементного множення комплексного взаємного спектра мікрофонної пари на коефіцієнти фільтра залишає лише відфільтрований спектр $Y_{12}(t, f)$:

$$Y_{12}(f, t) = H(f, t) \cdot (Z_1(f, t) \cdot Z_2^*(f, t)),$$

де $Z_1(t, f)$ та $Z_2(t, f)$ комплексні спектри першого та другого мікрофонів відповідно, а $*$ – знак спряження.

Завершальним етапом алгоритму є просторова локалізація ГЛА на основі отриманих фазових зсувів. Для визначення міжканальних часових затримок $\Delta\tau$ застосовується модифікований метод узагальненої взаємокореляції з фазовим перетворенням (GCC-PHAT) [2], що виконується безпосередньо в частотній області:

$$R_{12}(\tau) = F^{-1} \left\{ \frac{Y_{12}(f, t)}{|Y_{12}(f, t)|} \right\},$$

де F^{-1} – оператор зворотного перетворення Фур'є, а $|Y_{12}(t, f)|$ – модуль відфільтрованого спектра. Завдяки роботі попереднього каскаду алгоритм оперує виключно цільовими фазовими відліками, а нормалізація їхніх амплітуд додатково мінімізує похибки, викликані перевідбиттями в середовищі. Виконання зворотного перетворення Фур'є над відфільтрованим взаємним спектром дозволяє виділити єдиний глобальний кореляційний максимум, що відповідає істинній затримці поширення сигналу між мікрофонною парою.

Наявність сукупності таких часових затримок, отриманих від різних просторово рознесених пар мікрофонної решітки, формує систему геометричних рівнянь. Її розв'язання дозволяє однозначно обчислити просторовий кут (азимут θ) напрямку на ГЛА. Послідовне виконання описаної процедури у кожному часовому вікні забезпечує формування неперервних просторових траєкторій польоту для кожного окремого літального апарата в умовах групового польоту.

Список використаних джерел

1. Поздняков В. В. Застосування алгоритму CFAR для виявлення гармонічних складових акустичних сигналів засобів повітряного нападу // Збірник наукових праць ЖВІ. 2025. Вип. 28 (I). С. 51-64.
2. Lim J., Joo J., Kim S. C. Performance Enhancement of Drone Acoustic Source Localization Through Distributed Microphone Arrays. Sensors. 2025. Vol. 25, No. 6. P. 1928.

УДК 621.317

*Горобець О.С., аспірант,
Подчашиїнський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

МЕТОДИ ВИЗНАЧЕННЯ ЯКОСТІ ПОВЕРХНІ ОБЛИЦЮВАЛЬНИХ ВИРОБІВ З ПРИРОДНОГО КАМЕНЮ

Якість поверхні облицювальних виробів із природного каменю впливає як на декоративні властивості, так і на фізико-механічні характеристики матеріалу, зокрема його міцність, зносостійкість і стійкість до зовнішніх впливів. Тому контроль якості поверхні таких виробів є досить актуальним практичним завданням. На даний час використовують широкий спектр методів, які умовно можна поділити на традиційні методи неруйнівного контролю (оптична, цифрова та конфокальна мікроскопія; вимірювання блиску і білизни; контактна профілометрія; капілярний контроль) та методи цифрової обробки зображень. Проаналізуємо їх переваги та недоліки.

Оптичні методи дозволяють досліджувати мікроструктуру поверхні, виявляти тріщини, пори та неоднорідності матеріалу. Сучасні цифрові мікроскопи забезпечують отримання високоякісних зображень для подальшого аналізу, але ці результати суттєво залежать від умов освітлення та якості оптичної системи. Використання конфокальних мікроскопів дозволяє отримати тривимірне зображення поверхні зразка з високою роздільною здатністю та точністю. Їх переваги – безконтактність та наочність, недоліки – висока вартість, складність обробки результатів і обмеження щодо великих поверхонь [1]. Декоративні властивості облицювального каменю можна оцінити за допомогою блискомірів, оскільки встановлено, що шорсткість поверхні суттєво впливає на показники блиску. Перевагами є швидкість і простота вимірювання, а недоліками – чутливість до забруднень, залежність від умов освітлення та обмежена інформативність щодо мікрodefektів [2]. Контактна профілометрія є одним із найбільш поширених методів оцінювання мікроегеометрії поверхні. Вона базується на переміщенні алмазного щупа по поверхні з реєстрацією відхилень профілю, що дозволяє визначати параметри шорсткості. Цей метод застосовується для оцінки якості полірованих поверхонь каменю, де шорсткість є ключовим показником якості. Перевагами даного методу є висока точність вимірювання параметрів шорсткості, стандартизованість, простота інтерпретації результатів. Недоліками є

неможливість аналізу крихких матеріалів та обмеження щодо складної геометрії поверхні. Виявлення дефектів поверхні каменю із застосуванням методу капілярного контролю є досить ефективним і високочутливим до дрібних поверхневих дефектів. Метод дозволяє виявляти дефекти складної форми незалежно від геометрії поверхні та типу матеріалу, не потребує складного обладнання та має невисоку вартість. Капілярний контроль може застосовуватися для різних видів природного каменю. Проте достовірність отриманих результатів суттєво залежить від якості підготовки поверхні, а сам процес є досить трудомістким і потребує точного дотримання технології [2].

Методи цифрової обробки зображень (ЦОЗ), до яких належать класична обробка зображень, методи машинного та глибокого навчання, дають змогу автоматизувати контроль якості поверхні, підвищити його швидкість і об'єктивність. Цифрові зображення поверхні каменю містять значну кількість вимірювальної інформації, включаючи колірні та геометричні характеристики, однак їх аналіз потребує спеціалізованих методів обробки [3]. Класичні методи ЦОЗ найбільш ефективні для попередньої обробки та первинного аналізу зображень, однак вони мають низьку адаптивність до складних текстур і залежать від параметрів обробки. Методи машинного навчання більш гнучкі та точні, проте суттєво залежать від якості ознак, що використовуються для навчання. Найефективнішими є згорткові нейронні мережі, які автоматично виділяють ознаки та забезпечують високу точність і стійкість до шуму, але потребують значних обчислювальних ресурсів і великих обсягів даних.

В цілому, жоден метод не є універсальним, що зумовлює доцільність комплексного підходу з використанням декількох методів.

Список використаних джерел:

1. Leach R. Optical Measurement of Surface Topography. URL: <https://doi.org/10.1007/978-3-642-12012-1> (дата звернення: 20.03.2026).
2. Шамрай В. І. Управління декоративними показниками природного каменю на основі фактурної обробки: монографія. Житомир: «Житомирська політехніка», 2021. 134 с.
3. Подчашинський Ю. О. Кирилович В. А., Лугових О. О. Застосування автоматизованих та інформаційних систем з цифровими зображеннями при відкритій розробці родовищ природного каменю. URL: [https://doi.org/10.26642/ten-2022-2\(90\)-161-169](https://doi.org/10.26642/ten-2022-2(90)-161-169) (дата звернення: 20.03.2026).

УДК 681.518.22

*Григоренко І.В., д.т.н., доцент,
Лашков А.Г., аспірант*

*Національний технічний університет «Харківський політехнічний
інституту»*

УДОСКОНАЛЕНА КОМП'ЮТЕРИЗОВАНА ВИМІРЮВАЛЬНА СИСТЕМА ДЛЯ КОНТРОЛЮ ВИГОТОВЛЕННЯ МАКАРОННИХ ВИРОБІВ

Виготовлення макаронних виробів здійснюється у більшості країн світу [1] і тому проблема підтримки високої якості даного продукту є актуальним завданням як для виробництва та і для наукових досліджень. У роботі [2] запропоновано інформаційно-вимірювальну систему, яка побудована на сучасній високоточній елементній базі, що дає можливість забезпечувати необхідний рівень точності і вірогідності отриманих результатів. Однак на деяких підприємствах є недоцільним прокладати дротовий інтерфейс через високий рівень електромагнітних перешкод. Виникає необхідність використання радіоканалів для передачі інформації до ЕОМ. Структурна схема такої удосконаленої комп'ютеризованої системи представлена на рис. 1. Вона складається із системи збору інформації і системи прийняття та обробки інформації. У якості сенсорів температури використано DS18B20-3М-TUBE-IP67 (ПВП 1, ПВП 6, ПВП 7, ПВП 10). Для контролю вологості тіста використано вологомір FIZEPR-SW1 00.11 (ПВП 2). Для контролю тиску використано сенсор тиску APZ3420s (ПВП 3). На етапі «Формування сирих виробів» тиск вимірюється сенсором APZ 3420s (ПВП 4), а швидкість пресування виробів оптичним сенсором SPLC-SEN-HY-38P6-L5AR-1000 (ПВП 5). Для вимірювання відносної вологості повітря використано сенсор SHT31 (ПВП 8), а для контролю швидкості повітря MPXV7002 (ПВП 9). На етапі «Стабілізація вологості макаронних виробів» вологість вимірюється завдяки *Hydronix (Hydro-Mix XT)* (ПВП 11) [2]. У якості мікроконтролера обрано *ATmega16*. Результат вимірювань передається до ЕОМ через послідовний інтерфейс RS485. Пульти керування надає можливість програмувати контролер на виконання алгоритмічних функцій. У якості передавача і приймача використано радіомодуль NRF24L01, призначений для передачі даних на відстань до 50 м. Приймач здійснює приймання даних та передачу їх для подальшої обробки на мікроконтролер приймача, який через інтерфейс зв'язується з ЕОМ.

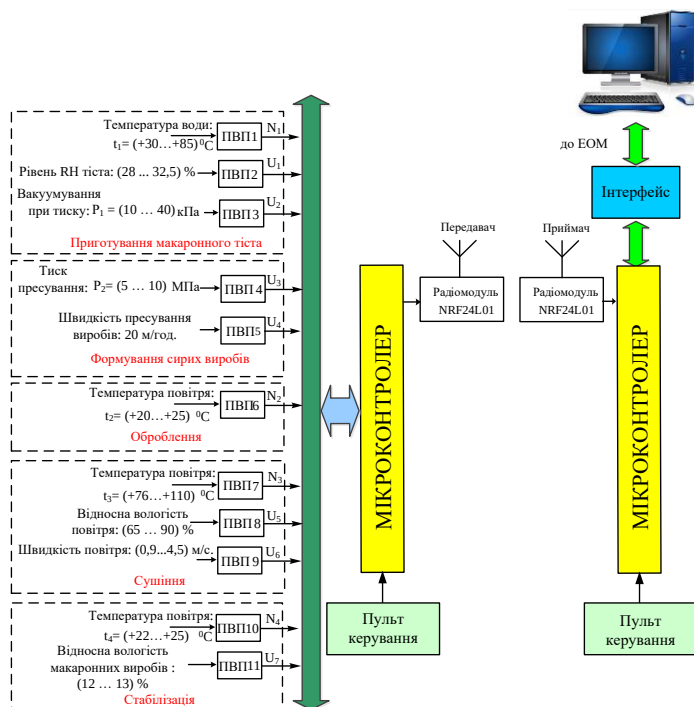


Рис. 1 Структурна схема комп'ютеризованої системи

Удосконалена комп'ютеризована система може бути використана на підприємствах на підприємствах харчової промисловості.

Список використаних джерел:

1. Roshini J., Pandey A. K., Vashishth R. History and Origin of Pasta. In: Sharma S., Sharma R., Gupta A., Bobade H. (eds) Advances in Pasta Technology. 2025. doi: 10.1007/978-3-031-84497-3_1.
2. Григоренко І. В., Лашков А. Г. Інформаційно-вимірювальна система для заводів з виготовлення макаронних виробів. Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях. – Харків: НТУ «ХПІ». 2025. № 4 (26). С. 24–29. doi:10.20998/2413-4295.2025.04.04.

УДК 681.518.22

*Григоренко І.В., д.т.н., доцент,
Лиска С.В., аспірант,
Григоренко С.М., к.т.н., доцент,
Національний технічний університет «Харківський політехнічний
інститут»*

КОМП'ЮТЕРИЗОВАНА СИСТЕМА КОНТРОЛЮ ВИРОБНИЦТВА ТВЕРДОГО СИРУ

Проблеми контролю виробництва твердого сиру для забезпечення високої якості продукції цікавлять вчених багатьох країн, оскільки твердий сир є у кулінарних традиціях багатьох світових культур [1, 2]. Для здійснення контролю технологічного процесу (ТП) виготовлення твердого сиру доцільно використовувати інформаційно-вимірювальні системи [3], завдяки яким стає можливим проводити вимірювання параметрів ТП, проводити накопичення статистичної інформації та її аналіз з метою підтримки встановленої у стандартах якості продукції. Метою роботи є розробка комп'ютеризованої вимірювальної системи, що дає змогу контролювати технологію виробництва твердого сиру на основних етапах та обробляти вимірювальну інформацію.

Структурна схема розробленої комп'ютеризованої системи представлено на рис. 1.

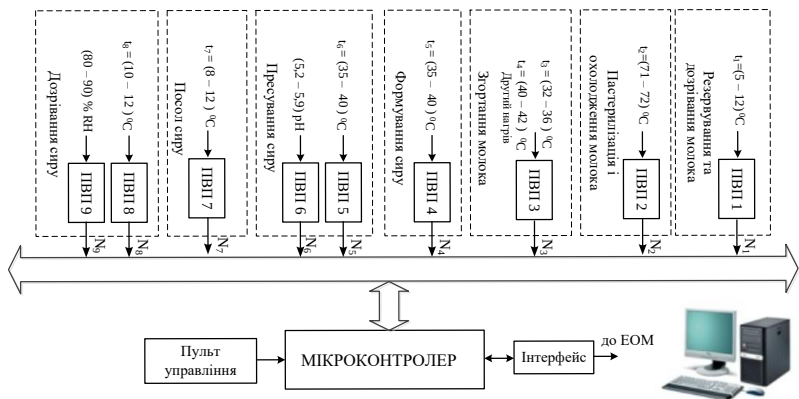


Рис. 1 Структурна схема комп'ютеризованої системи

У розробленій системі у якості первинних вимірювальних

перетворювачів (ПВП) температури використано сенсор температури 1-3ФТ (ПВП 1 – ПВП 5, ПВП 7), який вимірює температуру на етапі «Резервування та дозрівання молока». Контроль рівня рН на етапі «Пресування сиру» здійснюється за допомогою сенсора Memosens CPS96D (ПВП 6). Контроль температури у приміщенні на етапі «Дозріванні сиру» здійснюється за допомогою п'яти сенсорів температури DS18B20 (ПВП 8). Вологість повітря у приміщенні на етапі «Дозріванні сиру» контролюється сенсором вологості та температури SHT21 (ПВП 9). У якості мікроконтролера використано ATmega16, програмування якого здійснено на мові програмування Сі. Пульст управління здійснює початкове налаштування мікроконтролеру, та забезпечення його скидання. У якості інтерфейсу для передачі даних до ЕОМ обрано промисловий послідовний інтерфейс RS485 на мікросхемі ADM485.

Комп'ютеризована система контролю має три режими: установка / корекція дати й часу; вимірювання температури як на ділянках технологічного процесу так і у приміщенні цеху, рівня рН сиру, рівня вологості повітря у складському приміщенні; передача інформації про поточні значення параметрів ТП до ЕОМ.

Точність вимірювань технологічних параметрів по кожному з каналів не перевищують 1,5 %.

Розроблена комп'ютеризована система може бути використана на підприємствах молочної промисловості для покращення контролю за стабільністю основних параметрів ТП, з метою забезпечення високої якості твердого сиру.

Список використаних джерел:

1. Pappa, EC, E Kondyli, A-M Vlachou, and E Malamou. 2025. «Characteristics of a Hard Cheese Manufactured Using High Heat-Treated Sheep or Mixed Sheep-Goat Milk». *Journal of the Hellenic Veterinary Medical Society* 76 (2):9363-74. <https://doi.org/10.12681/jhvms.39401>.
2. Jurado M, Vicente CJ. Penicillium commune affects textural properties and water distribution of hard and extra-hard cheeses. *Journal of Dairy Research*. 2020;87(1):117–122. doi:10.1017/S0022029919000906.
3. Григоренко І.В., Григоренко С.М., Лиска С.В., Хроль Д.В. Метрологічні дослідження вимірювальної системи для молочної промисловості. *Метрологія та прилади*. Харків: Харківський Національний університет радіоелектроніки, 2025. № 2 С.54–59. doi: 10.20998/2522-9052.2025.2.07.

УДК 681.518

І.В. Зімчук, к.т.н., доц., доцент

Т.М. Шапар, ст. викладач

Житомирський військовий інститут імені С.П. Корольова

АЛГОРИТМ КОМПЛЕКСОВАНОЇ ФІЛЬТРАЦІЇ ВИМІРЮВАНЬ В СУПУТНИКОВИХ СИСТЕМАХ НАВІГАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Широке застосування безпілотних літальних апаратів (БпЛА) різних класів у військовій і в цивільній сферах вимагає розробки та виробництва високоточних бортових навігаційних систем малої вартості, ваги та габаритів. Важливою характеристикою, яка визначає спроможність та якість виконання польотного завдання БпЛА, є точність його позиціонування.

Задача визначення інформації про кутову орієнтацію та координати місцеперебування БпЛА автоматичному і в напівавтоматичному режимах польоту розв'язується пілотажно-навігаційним комплексом (ПНК) БпЛА, основу якого складають інерціальна та супутникова навігаційні системи (ІНС та СНС). Обидві системи працюють одночасно і, як правило, комплексуються [1]. Автономність та висока інформативність ІНС висувають її в клас універсальних систем як із визначення траєкторних рухів БпЛА (координат та швидкості польоту), так і з визначення кутових координат (кутів крену, тангажа та курсу) та інших параметрів, наприклад, прискорень, кутових швидкостей тощо. Однак визначення координат БпЛА лише на основі вимірювань ІНС буде призводити до накопичення похибок, тому є необхідність визначення координат додатково за допомогою СНС [1]. Необхідність досягнення високої точності навігаційних вимірювань передбачає застосування СНС як основних навігаційних систем літальних апаратів. СНС залишається основним джерелом навігаційної інформації для багатьох малих БпЛА.

Основними навігаційними параметрами, які вимірюються СНС є дальність до супутника та радіальна швидкість [2]. Головною вимогою, яка висувається до СНС, є висока точність вимірювання навігаційних параметрів і, як наслідок, висока точність визначення координат місцезнаходження БпЛА. Підвищення точності позиціонування досягається застосуванням різних алгоритмів обробки прийнятих навігаційних даних. Одним з рішень, що дозволяє підвищити достовірність, зменшити обсяг навігаційної інформації, переданої користувачеві, є фільтрація помилкових та надлишкових даних

отриманих від GPS модуля, що входить до складу ПНК БпЛА. Для фільтрації вимірювань в СНС використовуються різні модифікації фільтра Калмана [1]. Такі алгоритми є досить універсальними щодо практичного застосування, однак характеризуються високою складністю. Кожна наступна модифікація фільтра вимагає значно більших обчислювальних потужностей. Крім того, інженери часто стикаються з проблемою їх практичної реалізації через абстрактну форму опису, яка не відображає усіх деталей процесу.

Альтернативним підходом до розв'язання задачі фільтрації навігаційних даних є застосування алгоритмів комплексованої фільтрації. В таких алгоритмах позитивний ефект досягається завдяки врахуванню в моделі вимірювань не тільки дальностей, але і результатів доплерівських вимірювань, які використовуються для визначення не лише швидкості, а й дальності. При цьому забезпечується слабка чутливість навігаційних алгоритмів до динаміки споживача і знижуються вимоги до продуктивності навігаційного обчислювача.

Саме тому в роботі викладено синтез алгоритму фільтрації вимірювань дальності, в якому реалізується сумісна обробка результатів вимірювань як дальності, так і швидкості. Викладений підхід ґрунтується на поліноміальній моделі вхідних даних та поданні згладжувальних фільтрів як динамічних систем, які описуються дискретними передаточними функціями. Теоретичною основою визначення передаточних функцій є третя форма умов інваріантності помилки фільтра відносно моделі вхідного впливу. Працездатність та ефективність синтезованого алгоритму досліджено шляхом комп'ютерного моделювання. Показано, що застосування синтезованого фільтра дозволяє зменшити динамічну помилку оцінювання дальності в умовах зміни математичної моделі вхідних даних без погіршення якості фільтрації помилок вимірювань.

Список використаних джерел:

1. Харченко В.П., Чепіженко В.І., Тунік А.А., Павлова С.В. Авіоніка безпілотних літальних апаратів. Київ: ТОВ "Абрис-принт", 2012. 464с.
2. Захарін Ф.М., Синеглазов В.М., Філяшкін М.К. Алгоритмічне забезпечення інерціально-супутникових систем навігації: монографія. Київ: Вид-во Нац. Авіа. Ун-ту «НАУ-друку», 2011. 320 с.

УДК 681.128+681.518.2

*Іващев Д. В., аспірант,
Герасимов В. В., к.т.н., доцент
Дніпровський національний університет імені Олеся Гончара
Король А. В., магістрант,
Мукачівський державний університет*

ВИЯВЛЕННЯ ТА ІНТЕРПОЛЯЦІЯ ПРОПУСКІВ У ТЕЛЕМЕТРИЧНИХ ДАНИХ МОНІТОРИНГУ ПАЛИВА ТРАНСПОРТНИХ ЗАСОБІВ

В умовах експлуатації транспортних засобів, зокрема маневрових тепловозів, у промислових зонах, складських терміналах та металевих ангарах телеметричний потік даних піддається значному впливу електромагнітних перешкод. Це спричиняє систематичну втрату корисного сигналу [1]. Апаратні навігаційні термінали та ємнісні датчики рівня палива мають заданий базовий крок дискретизації. Для об'єктів, що аналізуються, цей крок становить рівно 1 хвилину. Втрата зв'язку або збої датчиків призводять до появи інформаційних пропусків та нефізичних стрибків сигналів. Це порушує хронологічну рівномірність часового ряду. Відсутність рівномірності робить неможливим коректне застосування диференціальних та інтегральних методів розрахунку динаміки витрати палива.

Алгоритм обробки телеметричних даних. Для відновлення цілісності часових рядів розроблено алгоритм попередньої багатоступеневої обробки. На першому етапі застосовується фізичне порогове фільтрування за двома критеріями. Першим кроком визначається мінімальний об'єм палива в баці. Усі точки, що падають нижче цього мінімального об'єму, примусово видаляються з часового ряду [2]. Другим кроком алгоритм детектує точки, що перевищують максимальний об'єм палива. Вони також видаляються, як порожні значення для подальшої обробки.

Відновлення втрачених значень здійснюється методами лінійної інтерполяції з жорстким часовим обмеженням. Встановлений тайм-аут дорівнює 10 тактам вимірювання. Динаміка витрати палива під маневровим навантаженням має нелінійний та стохастичний характер. Введений часовий критерій перешкоджає наскрізній інтерполяції при довготривалих розривах телеметрії. Це не дозволяє алгоритму згладжувати неконтрольовані зміни об'єму пального [2].

Експериментальна валідація методу. Для перевірки методу проаналізовано масив історичних даних 6 транспортних засобів

загальним обсягом 4898881 щохвилинних вимірювань. Алгоритм відфільтрував 97 494 точки апаратних збоїв нижньої межі. Також зафіксовано 53 макророзривів зв'язку, тривалість яких перевищила встановлений алгоритмом поріг. Максимальна задокументована відсутність телеметрії склала 220 діб. Спроба наскрізної математичної інтерполяції такого масиву призвела б до розмиття даних [3].

Для обґрунтування точності лінійної інтерполяції мікропропусків тривалістю до 10 хвилин проведено обчислювальний експеримент. На еталонних ділянках безперервної роботи дизель-генераторної установки програмно виконувалося штучне вилучення 10-хвилинних фрагментів даних. Після цього алгоритм відновлював втрачені точки. Сумарно реалізовано 6000 ітерацій незалежного тестування по 1000 для кожного транспорту. Відновлені результати зіставлялися з фактичними прихованими показаннями датчиків рівня палива.

Результати експерименту підтвердили працездатність розробленого підходу. Середня абсолютна відсоткова похибка відновлення рівня палива склала від 0,029 % до 0,112 %. Максимальне зафіксоване відхилення серед усіх 6000 тестових вибірок дорівнювало 0,24 %. Це зберігає безперервність телеметричного сигналу для подальшого застосування фільтрів та автокореляційного аналізу. Запропонована методика примусово розриває часовий ряд у точках макророзривів. Вона фіксує різницю палива під час сліпої зони як окремий ізольований сегмент розрахунку. Впровадження такого підходу дозволяє суттєво підвищити надійність автоматизованих систем контролю палива. Окрім цього, це відкриває нові можливості для створення більш точних алгоритмів предиктивної аналітики технічного стану тепловозів.

Список використаних джерел:

1. Navixy. Fuel level sensors: resistive, capacitive, ultrasonic methods. URL: <https://www.navixy.com/docs/expert-center/vehicle-telematics-technology/fuel-management/> (дата звернення: 18.03.2026).
2. Іващев Д. В., Герасимов В. В. Виділення подій заправки та обробка даних рівня палива маневрових локомотивів // Measuring and Computing Devices in Technological Processes. 2025. № 4 (84). DOI: 10.31891/2219-9365-2025-84-37.
3. Wialon. Automated fuel management solution. URL: <https://wialon.com/en/case-studies/fuel-dispensing-management-system> (дата звернення 19.03.2026).

УДК 621:317

*Ищенко О.С., аспірант,
Подчаїшинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ПОРІВНЯЛЬНИЙ АНАЛІЗ ДАТЧИКІВ ВИМІРЮВАННЯ РІВНЯ РІДИНИ В КОМП'ЮТЕРИЗОВАНИХ ІНФОРМАЦІЙНО- ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Промислові системи контролю рівня історично використовують різноманітні фізичні принципи – ємнісні, гідростатичні, радарні тощо [1]. Останні дослідження і розробки фокусуються на підвищенні точності та надійності цих методів, а також на кращій інтеграції датчиків у цифрові мережі.

Принцип дії ємнісного датчика – два електрода (щупи) формують конденсатор, ємність якого змінюється зі зміною рівня рідини (діелектрика між електродами). Переваги – відсутність рухомих частин; довговічність конструкції; придатність для різних рідин і навіть сипучих матеріалів; відносно невисока вартість та широкий діапазон робочих температур. Недоліки – потребує контакту з рідиною (занурення щупів); чутливий до налипання продукту на електродах; залежить від діелектричної проникності рідини і її змін; вимагає калібрування (на «порожній» і «повний» рівень), складність експлуатації при значних змінах температури чи вологості [2].

Принцип дії гідростатичного датчика – п'єзорезистивний або ємнісний датчик вимірює гідростатичний тиск стовпа рідини від дна ємності; за відомої густини тиск перераховується в висоту рівня. Переваги – простота і надійність; низька ціна датчиків; універсальність для більшості рідин; низьке енергоспоживання, можливість вимірювання у герметичних резервуарах без проникнення зверху. Недоліки – контакт із середовищем вимагає матеріалів, стійких до корозії; похибка при зміні густини рідини (потрібне внесення поправок або вимірювання густини); необхідність періодичної повірки [2].

Принцип дії ультразвукового датчика – ультразвуковий перетворювач (п'єзоелектричний) випромінює короткий звуковий імпульс високої частоти і приймає його відлуння від поверхні рідини. Час між посылкою та прийомом імпульсу пропорційний відстані до поверхні. Переваги – безконтактний метод: датчик не занурений у рідину, що ідеально для агресивних, гарячих, токсичних рідин; немає рухомих частин: мінімальне обслуговування, довгий строк служби [2];

відносно невисока вартість порівняно з радарним; універсальність: підходить для більшості рідин, а також може застосовуватися для сипких матеріалів. Недоліки – перешкоди для звуку: піна на поверхні, густий пар або сильна турбулентність можуть поглинати чи розсіювати ультразвук, спотворюючи вимір; обмежена дальність: типово до ~30 м для стандартних датчиків; на малих відстанях наявна «мертва зона»; вимагає вільного простору: установка повинна забезпечити «поле зору» без перешкод – конструкції всередині резервуара (труби, мішалки тощо) можуть давати хибні відбиття, що потребує налаштування фільтрів ехо [2].

Принцип дії радарного датчика – випромінює електромагнітний мікрохвильовий сигнал і приймає відбите від поверхні ехо. Час прольоту сигналу пропорційний відстані до рівня. Застосовуються як безконтактні (антена над рідиною), так і контактні радари (направлені хвилеводи). Переваги – не залежить від властивостей рідини: на відміну від ультразвуку, відбивання радіохвиль визначається діелектричною проникністю, тому метод не чутливий до змін густини чи в'язкості продукту; працює в екстремальних умовах: датчики витримують високі температури і тиски, можуть вимірювати рівень крізь пару, вакуум, інертний газ. Висока точність і дальність: сучасні радари забезпечують стабільну роботу на десятки метрів, доступний вільний вибір діапазону вимірювання. Недоліки – висока вартість: радарні рівнеміри значно дорожчі за ультразвукові; чутливість до діелектричної проникності: для дуже низьких ϵ_r (менше ~1.5, наприклад, зріджені гази, легкі вуглеводні) сигнал може частково проходити крізь межу «повітря – рідина» і відбиватися від дна, що ускладнює вимір; необхідність налаштування: потребує більш складної електроніки та конфігурації (задані «мертві зони» зверху і знизу бака, калібрування під геометрію ємності) [2].

Список використаних джерел:

1. Best Chemical Liquid Level Sensors: Ensuring Safety and Efficiency in Industrial Applications / LiquidLevelSensor. – 2023 [Electronic resource]. – Access mode : LiquidLevelSensor.co.uk.
2. Подчашинський, Ю. О., & Іщенко, О. С. (2025). Використання ультразвукових датчиків для вимірювання рівня та густини рідини в комп'ютеризованих інформаційно-вимірювальних системах. Технічна інженерія, (1(95), 389–394. [https://doi.org/10.26642/ten-2025-1\(95\)-389-394](https://doi.org/10.26642/ten-2025-1(95)-389-394).

УДК 621:317

*Левицький А.В., аспірант,
Подчащинський Ю.О., д.т.н., професор,
Єфіменко Н.А., д.е.н., к.т.н., професор,
Чепюк Л.О., к.т.н., доцент*

Державний університет «Житомирська політехніка»

СТАТИСТИЧНІ МЕТОДИ АНАЛІЗУ ЗОБРАЖЕНЬ З ІНФОРМАЦІЄЮ ПРО ГЕОМЕТРИЧНІ ПАРАМЕТРИ ТА ПАРАМЕТРИ РУХУ ОБ'ЄКТІВ

Раніше статистичний аналіз базувалися на аналізі взаємного розташування відтінків сірого кольору зображення та частоти їх появи, що описувались двовимірною функцією щільності ймовірності. Для ефективної класифікації та розпізнавання текстур за допомогою функції щільності ймовірності було визначено чотири характерних ознаки: кореляція; контрастність; кутовий момент і ентропія [1-3].

Кореляційний аналіз зображень – метод матриць взаємозв'язку, які описують частоту пар різних градацій сірого кольору, що присутні в зображенні, і визначаються шляхом кореляційного аналізу пікселів зображення, водночас якщо піксель відповідає вибраній градації, то він враховується як одиничне значення, якщо ні, то як нульове. У разі кольорових зображень даний підхід застосовується до аналізу кожного з трьох базових кольорів. Відповідно до методу формування матриць взаємозв'язку, вони оптимально підходять до розв'язання задач класифікації текстур.

Активно застосовується аналіз в спектральній області на основі двовимірного дискретного перетворення Фур'є. При цьому використовують різні ортогональні бази: дискретні експоненціальні, косинусні функції, перетворення Уолша-Адамара, Хаара та інші. Для дослідження текстур застосовують метод гістограм розподілу отриманих спектральних коефіцієнтів. Перевагою такого підходу є те, що гістограми спектральних коефіцієнтів, отримані в результаті інтегральних перетворень є більш стійкими та надійнішими, ніж гістограми розподілу окремих пікселів або їх сукупностей. Метод демонструє низьку чутливість до цифрового шуму зображень, що є одночасно і недоліком в разі застосування методу до розв'язання задачі розпізнавання незначних за розміром об'єктів на текстурованому фоні.

Характерною особливістю спектральних методів є те, що вони згладжують різкі межі між об'єктами зображення.

Статистичний аналіз просторового розподілу пікселів та спектральних коефіцієнтів за допомогою гістограм переважно застосовується для класифікації статичних текстур. Для аналізу динамічних текстур використовують методи, що базуються на кореляційному аналізі. Найбільш поширеною та простою в реалізації є стохастична модель. Фон зображення описують гістограмою розподілу значень кольору за величиною в базовій області, вільній від об'єктів. Отриману гістограму апроксимують функцією щільності розподілу ймовірності, найчастіше гаусовою. Основними параметрами такої моделі є середнє значення m та дисперсія σ . При цьому максимальне відхилення сигналу моделі приймають 2σ . Мінімальний поріг значення величини відхилення можна прийняти величину $\varepsilon_{tr} = 3\sigma$.

Як приклад реалізації вимірювальної системи, наведемо алгоритм розпізнавання зображення об'єктів із використанням стохастичної моделі:

$$if |u_{i,j} - m| > \varepsilon_v \text{ then } v_{i,j} = u_{i,j} \text{ else } v_{i,j} = 0 \quad (1)$$

де $u_{i,j}, v_{i,j}$ – елементи матриць заданого зображення та зображення об'єктів.

Методика побудови моделі та її застосування:

1. Фрагмент зображення фону, вільний від сторонніх предметів, розміром $n_x n_y = 80 \times 80$ пікселів використано як базовий для того, щоб знайти статистичні параметри фону.

2. На основі виразу (1) створюється зображення об'єктів. Виконується аналіз отриманих результатів. Зменшити похибку можна збільшивши порогове значення відбору, але, як показали чисельні експерименти, в цьому випадку втрачається якість зображення об'єктів. Таким чином, стохастична модель погано апроксимує фоновий сигнал та неспроможна повністю відділити шукані об'єкти від фону

Список використаних джерел:

1. Вовк С.М. Методи обробки зображень та комп'ютерний зір : навч. посіб. / С.М. Вовк, В.В. Гнатушенко, М.В. Бондаренко. – Д. : ЛІРА, 2016.

2. Кветний Р. М. Комп'ютерне моделювання систем та процесів. Методи обчислень. Частина 2 : навчальний посібник / [Р. Н. Кветний, І. В. Богач, О. Р. Бойко та інші]; за заг. ред. Р. Н. Кветного. – Вінниця : ВНТУ, 2013.

3. Кобилін О.А., Творошенко І.С. Методи цифрової обробки зображень: навч. посібник. – Харків: ХНУРЕ, 2021.

УДК 621.317

Лугових О.О., ст.викладач,

Наумчук В. А., студент

Державний університет «Житомирська політехніка»

ПОРІВНЯННЯ МЕТРОЛОГІЧНИХ ТА ЕКСПЛУАТАЦІЙНИХ ХАРАКТЕРИСТИК УЛЬТРАЗВУКОВИХ І ТУРБІННИХ ВИТРАТОМІРІВ ГАЗУ

Вибір типу вимірювача витрат газу є важливим етапом проектування систем обліку та контролю газових потоків. Він визначається вимогами до точності вимірювань, умовами експлуатації, діапазоном витрат, характеристиками робочого середовища, діаметром трубопроводу, а також економічною доцільністю застосування приладу. Найбільш поширеними у промисловій практиці є ультразвукові витратоміри (УВ) та турбінні витратоміри (ТВ), які суттєво відрізняються за принципом дії, конструктивними особливостями та експлуатаційними характеристиками [1].

Ультразвуковий вимірювач витрат газу працює на основі вимірювання різниці часу проходження ультразвукового сигналу за напрямком потоку та проти нього. За цією різницею визначається середня швидкість руху газу в трубопроводі, після чого за відомою площею перерізу труби обчислюється об'ємна витрата. Додатково, використовуючи дані про температуру, тиск та густину газу, може визначатися масова витрата [3].

У сучасних УВ часто застосовуються багатопроменеві схеми вимірювання (4, 6 або 8 акустичних каналів), що підвищує точність вимірювання та дозволяє враховувати нерівномірність профілю швидкостей у потоці [4].

Турбінний вимірювач витрат газу визначає витрату за частотою обертання турбіни, яка встановлена в потоці газу. Потік газу обертає лопатеве колесо турбіни, а швидкість його обертання пропорційна швидкості потоку. Частота обертання реєструється магнітним або індукційним датчиком і перетворюється в електричний сигнал, пропорційний витраті газу [1].

Принциповою відмінністю цих приладів є наявність або відсутність рухомих елементів. УВ не мають рухомих механічних частин, що забезпечує значно менший механічний знос, стабільність метрологічних характеристик упродовж тривалого часу та мінімальні потреби в технічному обслуговуванні [3]. У ТВ присутні турбіна, вал і

підшипникові вузли, які з часом зношуються та потребують періодичної перевірки або заміни [1].

За показниками точності УВ зазвичай забезпечують похибку вимірювання в межах $\pm 0,5$ – $1,0$ % у номінальному діапазоні витрат. У високоточних комерційних системах похибка може бути навіть меншою [4]. Для ТВ характерна похибка приблизно $\pm 1,0$ – $1,5$ %. Крім того, точність турбінних приладів може знижуватися з часом через зношування підшипників і механічних частин [1].

Важливим параметром є діапазон вимірювання (turndown ratio). УВ можуть працювати в широкому діапазоні витрат ($1:20$ – $1:100$), тоді як для турбінних приладів цей показник зазвичай становить $1:10$ – $1:20$ [3]. Це означає, що ультразвукові прилади краще підходять для систем зі значними коливаннями витрати газу.

Щодо гідравлічних характеристик, УВ створюють мінімальні втрати тиску, оскільки практично не перешкоджають руху потоку. ТВ мають більший гідравлічний опір через наявність турбіни в потоці, що може призводити до додаткових енергетичних втрат у системі [1].

Ще одним важливим фактором є чутливість до стану робочого середовища. ТВ більш чутливі до забруднення газу, наявності механічних частинок, пилу або конденсату, які можуть пошкоджувати лопаті турбіни або викликати заклинювання механізму [2]. УВ менш чутливі до таких факторів, оскільки вимірювання здійснюється без контакту з потоком [3].

Важливе значення мають також умови монтажу. Для забезпечення високої точності вимірювань необхідно дотримуватися вимог до довжини прямих ділянок трубопроводу перед і після витратоміра. Для ТВ ці вимоги зазвичай становлять 10 – 20 діаметрів труби перед приладом і 5 – 10 після нього [1]. УВ також потребують прямих ділянок трубопроводу, однак сучасні багатопроменеві моделі можуть працювати навіть за менш сприятливих умов потоку [4].

УВ можуть працювати в широкому діапазоні температур і тисків газу, що робить їх придатними для використання на магістральних газопроводах і в системах комерційного обліку природного газу [3]. ТВ частіше застосовуються в розподільчих мережах, газорегуляторних пунктах і промислових установках із відносно стабільними умовами роботи [1].

Ще однією перевагою УВ є можливість діагностики стану потоку та самого приладу. Багато сучасних моделей мають вбудовані системи самодіагностики, які можуть виявляти турбулентність потоку, зміну профілю швидкості або несправності датчиків [4].

З економічної точки зору ТВ зазвичай мають нижчу початкову

вартість, що робить їх привабливими для використання в невеликих або середніх системах обліку газу. Однак у довгостроковій перспективі ультразвукові прилади можуть бути вигіднішими через менші витрати на обслуговування та більший строк служби [1].

Таким чином, ультразвукові вимірювачі витрат газу доцільно застосовувати в системах комерційного обліку, на магістральних трубопроводах великого діаметра, у системах автоматизованого контролю та в умовах підвищених вимог до точності та надійності [3]. ТВ можуть бути економічно виправданими в системах зі стабільними режимами роботи, середніми діаметрами трубопроводів і помірними вимогами до точності [1].

У результаті проведеного аналізу було розглянуто основні особливості ультразвукових та турбінних вимірювачів витрат газу, їх принципи роботи, конструктивні характеристики та експлуатаційні параметри. Встановлено, що кожен із типів витратомірів має свої переваги та обмеження, які необхідно враховувати під час проєктування систем вимірювання та обліку газових потоків [2].

УВ характеризуються високою точністю вимірювань, широким діапазоном вимірювання, мінімальними втратами тиску та відсутністю рухомих механічних елементів. Це забезпечує високу надійність роботи приладу, стабільність метрологічних характеристик упродовж тривалого часу та зменшення витрат на технічне обслуговування. Такі прилади особливо ефективні у системах комерційного обліку природного газу, на магістральних трубопроводах великого діаметра та в умовах змінних режимів потоку [3].

ТВ відзначаються відносно простою конструкцією, достатньою точністю вимірювання та нижчою початковою вартістю. Вони широко застосовуються в розподільчих газових мережах, промислових установках і системах зі стабільними параметрами потоку. Однак наявність рухомих механічних елементів зумовлює їх більшу чутливість до забруднення робочого середовища та потребу в періодичному технічному обслуговуванні [1].

Вибір типу витратоміра повинен здійснюватися з урахуванням конкретних умов експлуатації, вимог до точності вимірювань, діапазону витрат газу, характеристик робочого середовища та економічної доцільності застосування приладу. Правильно обраний вимірювач витрат газу забезпечує надійність роботи системи обліку, підвищує точність контролю технологічних процесів та сприяє ефективному використанню енергетичних ресурсів [2].

У таблиці 1 наведено результати порівняння ультразвукових та турбінних витратомірів.

Таблиця 1

Результати порівняння ультразвукових та турбінних витратомірів

Критерій порівняння	Ультразвуковий витратомір	Турбінний витратомір
Принцип дії	Вимірює різницю часу проходження ультразвукового сигналу.	Визначає витрату за частотою обертання турбіни.
Наявність рухомих деталей	Немає рухомих механічних елементів.	Присутні турбіна та підшипникові вузли.
Точність (похибка)	Висока ($\pm 0,5$ – $1,0$ %), стабільна з часом.	Дещо нижча ($\pm 1,0$ – $1,5$ %), може знижуватись через знос.
Втрати тиску (опір)	Мінімальні (не перешкоджає руху потоку).	Більший гідравлічний опір.
Чутливість до забруднень	Менш чутливий до домішок.	Більш чутливий (домішки та конденсат можуть пошкодити механізм).
Умови потоку	Стабільні результати за змінних режимів потоку.	Стабільні результати за змінних режимів потоку.

Список використаних джерел

1. Метрологія та вимірювальна техніка : підручник / Поліщук Є.С., Дорожовець М.М., Яцук В.О. та ін. Львів : Бескид Біт, 2003. 544с.
2. Ловеїкін В.С., Ромасевич Ю.О., Човнюк Ю.В. Мехатроніка. Навчальний посібник. – К., 2012. - 357 с
3. ISO 9951 / ISO 17089: Стандарти для турбінних та ультразвукових лічильників газу (комерційний облік).
4. ISO 17089 (ДСТУ ISO 17089): Ультразвукові лічильники газу для промислового обліку та передачі прав власності.

УДК 621:317

*Магалецький Я.В., аспірант,
Подчашинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»
Безвесільна О.М., д.т.н., професор
Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»*

ЧАСТОТНИЙ ВИМІРЮВАЛЬНИЙ КАНАЛ КОМП'ЮТЕРИЗОВАНОЇ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ КОНТРОЛЮ МЕХАНІЧНИХ ПАРАМЕТРІВ АСИНХРОННИХ ДВИГУНІВ

В комп'ютеризованій інформаційно-вимірювальній системі (КІВС) контролю механічних параметрів асинхронних двигунів необхідно вимірювати частотно-часові параметри сигналів (період, частота) [1].

Алгоритм роботи частотного вимірювального каналу з мікропроцесорним управлінням, що дозволяє досліджувати періодичні процеси в широкому частотному діапазоні, є наступним. Спочатку настраюють апаратну і програмну частини на режим, наприклад, цифрового періодоміра. Потім вимірюють невідому частоту f_x і задаються потрібною похибкою квантування $\delta_{КЧ}$. На основі значень f_x і $\delta_{КЧ}$ визначають тривалість еталонного часового інтервалу [2]:

$$T_0 = \frac{1}{\delta_{КЧ} \cdot f_x} \cdot 100\%.$$

Як квантуючу частоту f_0 в мікропроцесорних частотомірах можна наприклад використовувати сигнал, що присутній на шинах управління (ШУ) мікропроцесорних систем (залежно від їх архітектури). Для переважної кількості недорогих мікроконтролерів $f_0 \approx 2$ МГц. Якщо значення T_0 і f_0 відомі, визначають критичну частоту $f_{xк}$. Якщо $f_x \leq f_{xк}$, то апаратну частину наструють на режим цифрового періодоміра і переходять до підпрограми вимірювання частоти в цьому режимі. У іншому випадку ($f_x > f_{xк}$) здійснюється режим цифрового частотоміра.

Структурна схема мікропроцесорного частотного вимірювального каналу, яка дозволяє реалізувати даний алгоритм, подана на рис. 1. Вона

УДК 004.7

*Рудич М.В., здобувач,
Духновська К.К., к.т.н.*

Київський національний університет імені Тараса Шевченка

МЕТОДИ ВІДНОВЛЕННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ДИФУЗІЙНИХ МОДЕЛЕЙ У ЗАДАЧАХ ЦИФРОВОЇ ОБРОБКИ СИГНАЛІВ

Дифузійні моделі базуються на двох взаємопов'язаних процесах: поступовому руйнуванню структури зображення шляхом додавання шуму та подальшому її відновленню. Основна ідея полягає в тому, що складну задачу генерації зображення можна розбити на послідовність простіших кроків.

Прямий процес дифузії полягає у поступовому додаванні випадкового шуму до зображення протягом дискретних кроків часу. На кожному кроці до пікселів додається шум, зазвичай змодельований нормальним розподілом, що призводить до поступової втрати структурної інформації. Цей процес формалізується як марковський ланцюг, у якому стан зображення на поточному кроці залежить лише від попереднього. Така властивість спрощує моделювання, оскільки не потребує врахування всієї історії перетворень. Важливу роль відіграє параметр, відомий як планувальник шуму, який визначає інтенсивність шуму на кожному кроці. Від його налаштувань залежить швидкість деградації зображення: при малих значеннях процес є плавним, при великих — структура руйнується швидше. Після достатньої кількості ітерацій зображення втрачає всі впізнавані ознаки та наближається до білого шуму [1].

Зворотний процес дифузії полягає у поетапному відновленні зображення зі стану шуму. Замість прямого відновлення пікселів модель навчається оцінювати шум, який було додано на кожному кроці прямого процесу.

На практиці використовується нейронна мережа (часто архітектура типу U-Net), яка на вході отримує зашумлене зображення та номер кроку, а на виході прогнозує компонент шуму. Отримана оцінка віднімається від поточного стану, що дозволяє отримати менш зашумлену версію зображення. Навчання моделі виконується шляхом мінімізації середньоквадратичної помилки (MSE) між передбаченим і реальним шумом, доданим у прямому процесі. Повторюючи цей процес багаторазово, модель поступово відновлює структуру зображення — від загальних контурів до дрібних деталей. Такий підхід дозволяє

ефективно реконструювати сигнал навіть за умов значного зашумлення [1][2].

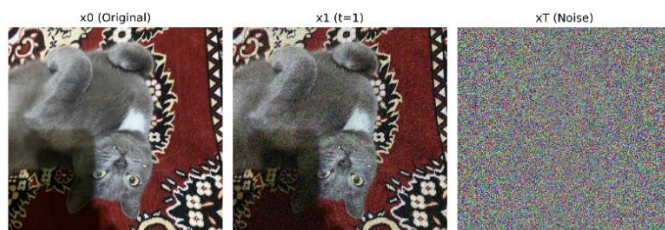


Рис.1. Ілюстрація прямого процесу у дифузійних моделях

Застосування. Однією з ключових задач є видалення шуму. У реальних системах, таких як відеоспостереження, зображення часто містять шум через низьку освітленість або обмеження сенсорів. Дифузійні моделі дозволяють відновлювати деталі зображення без суттєвих втрат якості, що підвищує точність подальшого аналізу. У медичних інформаційно-вимірювальних системах, зокрема при обробці рентгенівських або МРТ-зображень, важливо мінімізувати шум без спотворення структур. Дифузійні моделі забезпечують високу якість реконструкції, що є критичним для діагностики [2,3].

Ще одним важливим застосуванням є відновлення пошкоджених або відсутніх ділянок зображення (inpainting). Модель використовує контекст сусідніх областей для реконструкції відсутніх даних, що дозволяє ефективно відновлювати інформацію.

Висновок. Дифузійні моделі є ефективним підходом до відновлення зображень у задачах цифрової обробки сигналів. Їх основна перевага полягає у використанні поетапного процесу зашумлення та відновлення, що дозволяє отримувати високоякісні результати навіть за значного рівня шуму.

Список використаних джерел:

1. Ho J., Jain A., Abbeel P. Denoising diffusion probabilistic models // Advances in Neural Information Processing Systems. – 2020.
2. Song Y., Ermon S. Generative modeling by estimating gradients of the data distribution // Advances in Neural Information Processing Systems. – 2019.
3. Karras T., Aittala M., Laine S., et al. Elucidating the design space of diffusion-based generative models // Advances in Neural Information Processing Systems. – 2022.

УДК 621:317

*Свістельник О.С., аспірант,
Подчаїшинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ МІКРОПРОЦЕСОРНОЇ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ КОНТРОЛЮ ПАРАМЕТРІВ МІКРОКЛІМАТУ НА ПОЛІГРАФІЧНОМУ ВИРОБНИЦТВІ

Якість поліграфічної продукції безпосередньо залежить від стабільності параметрів мікроклімату виробничого приміщення. Відповідно до вимог стандарту ISO 12647-2 [1], температура повітря повинна підтримуватися у межах $(23 \pm 2) ^\circ\text{C}$, а відносна вологість – у діапазоні $(50 \pm 5) \%$ відносної вологості (ВВ). Порушення цих умов навіть на 3-5 % ВВ спричиняє деформацію паперового полотна та порушення суміщення фарб до 0,3 мм, що є неприпустимим при багатофарбовому офсетному друці [2]. Вплив вологості на геометричні характеристики паперу описується через рівноважний вологовміст: збільшення відносної вологості на 10 % ВВ спричиняє лінійне розширення паперу в поперечному напрямку на 0,2-0,5 %. Водночас зміна температури від $20 ^\circ\text{C}$ до $25 ^\circ\text{C}$ знижує динамічну в'язкість поліграфічних фарб на 15-20 % відповідно до рівняння Арреніуса, що порушує баланс фарба-вода та призводить до нерівномірного нанесення фарбового шару і виникнення відмарювання на зворотному боці аркуша. Нерівномірний просторовий розподіл параметрів мікроклімату у приміщенні – градієнт температури може досягати 3-5 $^\circ\text{C}$, а вологості – 8-12 % ВВ – додатково ускладнює підтримання стабільних умов виробництва [2].

Перший рівень системи – польовий – включає вимірювальні вузли на базі мікроконтролерів STM32 з цифровими сенсорами SHT31 (похибка температури $\pm 0,3 ^\circ\text{C}$, вологості $\pm 2,0 \%$ ВВ). Вузли розміщуються з кроком не більше 50 м² площі приміщення, що забезпечує рівномірне охоплення всього виробничого простору. Другий рівень – передачі даних – реалізований на основі протоколу MQTT із затримкою менше 200 мс; як транспортне середовище використовується Wi-Fi-інфраструктура підприємства без прокладання додаткових кабельних мереж. Третій рівень – зберігання та візуалізації – використовує часову базу даних InfluxDB та панель моніторингу Grafana, що забезпечує відображення поточних значень, довгострокових трендів і автоматичне

сповіщення персоналу при виході параметрів за допустимі межі.
Архітектуру системи наведено на рис. 1.

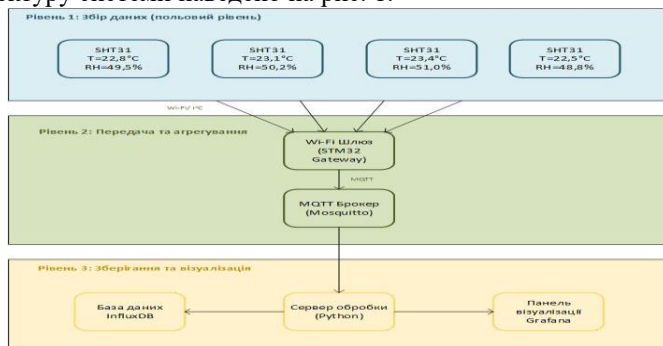


Рис. 1. Архітектура розподіленої інформаційно-вимірювальної системи контролю мікроклімату на поліграфічному виробництві

Математична модель вимірювального каналу враховує систематичну та випадкову складові похибки. Систематична складова для сенсора SHT31 не перевищує $\pm 0,2$ °C та $\pm 1,5$ % BB і визначається похибкою калібрування та нелінійністю передавальної характеристики. Оцінювання невизначеності за методологією GUM показує, що сукупна стандартна невизначеність каналу температури для сенсора SHT31 не перевищує 0,18 °C ($k = 1$), що повністю відповідає вимогам класу точності ISO 12647-2. Міжкалібрувальний інтервал для сенсорів становить 12 місяців, калібрування здійснюється на еталонних установках з точністю $\pm 0,05$ °C та $\pm 0,1$ % BB.

Результати аналізу підтверджують, що впровадження запропонованої ІВС забезпечує стабільність параметрів мікроклімату у межах норм ISO 12647-2 [1] та дозволяє знизити кількість браку поліграфічної продукції, пов'язаного з порушенням умов середовища, на 35-45 %.

Список використаних джерел:

1. ISO 12647-2:2013. Graphic technology — Process control for the production of halftone colour separations, proof and production prints. Part 2: Offset lithographic processes.
2. Kipphan H. Handbook of Print Media / H. Kipphan. – Berlin : Springer, 2001. – 1207 p.

УДК 621:317

*Ступак А.Г., аспірант,
Подчаїшинський Ю.О., д.т.н., професор,
Чепюк Л.О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ОЦІНКА ЕФЕКТИВНОСТІ СТИСНЕННЯ ЗОБРАЖЕНЬ В ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ МЕДИЧНОГО ЗАСТОСУВАННЯ

Порівняння ефективності дискретного косинусного (ДКП) та дискретного вейвлет-перетворення (ДВП) у системах стиснення медичних зображень за результатами стиснення тестового зображення за допомогою алгоритмів сімейства *LZ* або інших алгоритмів стиснення без втрат не дає однозначних оцінок кількісного виграшу того чи іншого перетворення при заданій якості. Запропоновано використати класичний підхід оцінки потенційної можливості стиснення джерела на основі обчислення його ентропії [1,2].

$$H = - \sum_i P(\hat{S}_i) \log_2 P(\hat{S}_i), \quad (1)$$

де $P(\hat{S}_i)$ – ймовірність появи коефіцієнта трансформації з величиною $\hat{S}_i$. Значення ентропії дозволяє оцінити потенційний коефіцієнт стиснення зображення за допомогою простого виразу $K_{cm} = 24/H$. У цифровій моделі реалізовано обчислення (9), де як джерело використана матриця коефіцієнтів трансформації по яскравості (Y) з розмірами, що відповідають розміру зображення.

Метрика SSIM, або індекс структурної подоби [1,2] є одним із критеріїв оцінки якості зображень і визначає ступінь подібності відповідних ділянок (вікон) зображень, що порівнюються. Різниця між двома вікнами x та y з розміром $N \times N$ [1]:

$$SSIM_{x,y} = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \quad (2)$$

де x , y – вікна оригінального та спотвореного зображень; μ_x , μ_y – середні значення координат пікселів у вікнах x та y ; σ_x , σ_y – середньоквадратичні відхилення; $\sigma_{x,y}$ – значення коваріації; c_1 , c_2 –

постійні коефіцієнти. Далі параметри усереднюються. Зазвичай, метрика (2) розрахована на вікно розміром 8×8 пікселів. Для аналізу всього зображення вікно зміщується на задану кількість пікселів послідовно по горизонталі та по вертикалі. Інтегральна оцінка визначається як [1]:

$$SSIM = \frac{1}{L} \sum_{l=1}^L SSIM_l, \quad (3)$$

де l – номер вікна; L – кількість вікон.

Значення (2) і (3) дорівнюють одиниці тільки при повному збігу параметрів. У табл. 1 наведено результати порівняння ДКП та ДВП за значенням ентропії H для заданих параметрів SSIM для різних типів медичних зображень.

Табл. 1. Ефективність ДКП та ДВП у цифровій моделі

SSIM	0,99	0,98	0,97	0,96	
«Хребет»					
Q	97	91	80	65	ДКП
<i>H</i>	8,21	5,32	3,75	2,87	
Q	90	78	65	49	ДВП
<i>H</i>	7,08	4,52	3,38	2,62	
«Дитина»					
Q	91	78	60	35	ДКП
<i>H</i>	3,93	2,58	1,88	1,45	
Q	84	66	42	13	ДВП
<i>H</i>	3,59	2,30	1,61	1,22	
«Рука»					
Q	96	81	56	16	ДКП
<i>H</i>	3,65	1,61	0,99	0,65	
Q	91	72	41	3	ДВП
<i>H</i>	3,22	1,45	0,83	0,54	

Список використаних джерел:

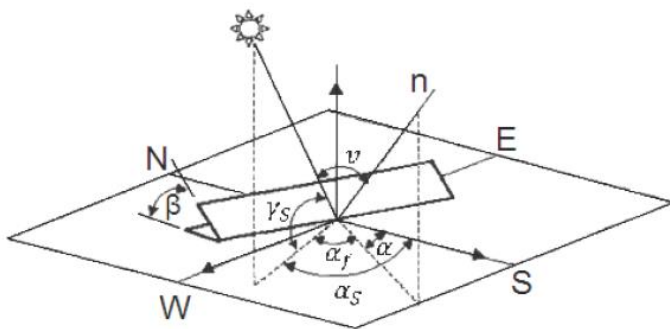
1. Lin W, Kuo C-CJ. Perceptual visual quality metrics: A survey. J Vis Commun Image Represent 2011; 22(4): 297-312.
2. Chandler D.M., Hemami S.S. VSNR: A WaveletBased Visual SignaltoNoise Ratio for Natural Images IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 9, SEPTEMBER 2007, pp. 2284–2298.

УДК 621:317

*Товстік С.О., аспірант,
Подчаїшинський Ю.О., д.т.н., професор
Державний університет «Житомирська політехніка»
Дерев'янюк О.В., к.п.н., доцент
Житомирський професійний ліцей*

ЕФЕКТИВНІСТЬ ЗАСТОСУВАННЯ СИСТЕМ СТЕЖЕННЯ ЗА РУХОМ СОНЦЯ ДЛЯ ФОТОЕЛЕКТРИЧНИХ МОДУЛІВ

Застосування систем стеження за Сонцем дозволить зменшити термін окупності системи та зменшити вартість виробленої електроенергії. Величиною, що впливає інтенсивність опромінення фотоелектричних модулів (ФМ), є кут падіння сонячних променів її поверхню. Застосування систем стеження дозволить змінювати кут залежно від положення Сонця, що збільшить кількість потужності, що прийшла на поверхню ФМ. Для розрахунку інтенсивності потоку сонячного випромінювання, що надходить на похилу поверхню, що поглинає промені, необхідно знати кути падіння сонячних променів на неї [1,2]. Рух сонця по небосхилу наведено на рис. 1.



n – нормаль до поверхні ФМ; γ_s – сонячна висота, град; α – азимут, град; α_s – сонячний азимут, град; α_f – горизонтальний кут тіні, град; $\nu(\beta, \alpha)$ – кут падіння сонячних променів по відношенню до нормалі, град; β – кут нахилу фотоелектричного модуля до горизонту, град.

Рис. 1. Рух сонця по небосхилу

У загальному вигляді випромінювання, що йде від сонця, являє собою суму падаючого та розсіяного випромінювання:

$$G_h(\beta, \alpha) = B_h(\beta, \alpha) + D_h(\beta, \alpha) + R_{gh}(\beta, \alpha) \quad (1)$$

Позаземний потік випромінювання на горизонтальну поверхню в певний період визначається за формулою (1), візьмемо період, що дорівнює 1 год :

$$G_h = I_0 \varepsilon \left(\frac{1}{2\pi} \right) \left[\sin \varphi \cdot \sin \delta \left(\frac{\pi}{12} \right) + \cos \varphi \cdot \cos \delta (\sin \omega_2 - \sin \omega_1) \right],$$

де I_0 – Сонячна постійна $I_0 = 1367$ Вт /м⁻²; ε – поправка до середньої сонячної відстані щодня, φ – широта місцевості, град; δ – спряження, град;; ω_1 і ω_2 – годинні кути на кінцях проміжку.

Безпосередньо визначити падаючий потік неможливо, тому його визначають як різницю позаземного і розсіяного випромінювання, приведенного до кута відмінювання в певний інтервал часу:

$$B_h(\beta, \alpha) = \frac{(G_h - D_h) \cdot \Delta T}{\sin \gamma_s} \cos(\beta, \alpha).$$

Розсіяне випромінювання береться як певна величина.

$$\varepsilon = 1 + 0,003344 \cos(J' - 0,048869),$$

де J' – день у градусах;

$$\delta = \sin^{-1} 0,3978 \sin[J' - 1,4 + 0,0355 \sin(J' - 0,0489)],$$

де

$$\omega_s = \cos^{-1}(-\tan \varphi \tan \delta),$$

$$\gamma_s = \sin^{-1}(\sin \varphi \sin \delta + \cos \varphi \cos \delta \cos \omega),$$

$$\alpha_F = \alpha_S - \alpha,$$

$$v(\beta, \alpha) = \cos^{-1}(\cos \gamma_s \cos \alpha_F \sin \beta + \sin \gamma_s \cos \beta).$$

На основі цього алгоритму розрахунку можна побудувати графіки, що відображають ефективність застосування систем стеження для даної місцевості.

Список використаних джерел:

1. Markvart T., Castaner L. Practical handbook of photovoltaics: fundamentals and applications. – NY: ELSEVIER, 2012. – 1204 p.
2. Остренко Д. О., Колларов О. Ю. Аналіз впливу кута нахилу сонячних панелей на роботу електричної мережі з використанням ВДЕ. Наукові праці ДонНТУ. Серія: «Електротехніка і енергетика». 2020. № 2(23). С. 70-76.

УДК 004.93

*Федоренко І. О., здобувач,
Громико І. О., професор*

Харківський національний університет імені В. Н. Каразіна

АЛГОРИТМ БІСПЕКТРАЛЬНОЇ ОБРОБКИ ЗОБРАЖЕНЬ ДЛЯ АВТОМАТИЗОВАНОЇ СЕЛЕКЦІЇ АНОМАЛІЙ В УМОВАХ НИЗЬКОГО ТЕПЛОВОГО КОНТРАСТУ

Актуальним завданням сучасних систем дистанційного моніторингу є забезпечення надійної селекції об'єктів в умовах температурної рівноваги з фоном (ефект «теплового злиття»). Класичні моноспектральні довгохвильові інфрачервоні сенсори (LWIR) за таких умов втрачають інформативність. Для розв'язання цієї проблеми розроблено конвеєрний алгоритм цифрової обробки, який реалізує піксельне злиття даних теплового та ближнього інфрачервоного (NIR) діапазонів з активним підсвічуванням.

Запропонований конвеєр обробки відеопотоку структурно поділяється на етапи просторової синхронізації, фільтрації шумів, синтезу критерію аномальності та морфологічної сегментації.

На етапі попередньої обробки вирішується проблема апаратної зашумленості. З огляду на фізичні особливості мікроболометрів (схильність до утворення імпульсного шуму) та специфіку NIR-камер (генерація спекл-шуму від лазерного підсвічування), алгоритм застосовує нелінійну медіанну фільтрацію з апертурою 3×3 . Це дозволяє нівелювати локальні екстремуми інтенсивності без деградації високочастотних просторових компонент (контурів об'єктів), що є базовою вимогою для точного мультиспектрального аналізу [2].

Ключовою геометричною задачею є просторове суміщення кадрів. Через рознесення оптичних осей сенсорів алгоритм компенсує паралакс за допомогою матричного проективного перетворення простору (гомографії). Математична модель суміщення має вигляд:

$$s \begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = H \begin{bmatrix} x \\ y \\ 1 \end{bmatrix},$$

де x, y - координати пікселя у системі відліку NIR-сенсора,

x', y' - відповідні координати у проекції LWIR-сенсора,

H - матриця гомографії розмірністю 3×3 , отримана на етапі стереокалібрування,

s - масштабувальний коефіцієнт.

Для усунення похибок, пов'язаних із різною розрядністю АЦП сенсорів, виконується лінійна нормалізація гістограм інтенсивності до єдиного діапазону [0, 1].

Синтез результуючої маски базується на розрахунку критерію біспектральної невідповідності D . Цей показник кількісно оцінює ступінь порушення природної спектральної кореляції між тепловим випромінюванням та оптичним відбиттям об'єкта:

$$D(x, y) = |C_{LWIR}(x, y) - \alpha \cdot R_{NIR}(x, y)|,$$

де C_{LWIR} - нормований локальний тепловий контраст,

R_{NIR} - інвертований коефіцієнт відбиття у NIR-діапазоні,

α - адаптивний ваговий коефіцієнт освітленості.

На фінальному етапі до отриманої карти невідповідності застосовується порогова бінаризація з подальшою математичною морфологією (операція «Відкриття»). Послідовне виконання ерозії та дилатації гарантовано відсікає хибні піксельні кластери (флуктуації фону) та відновлює цілісну топологію цілі [3].

Завдяки математичному моделюванню та структурному аналізу розробленого конвеєра, теоретично обґрунтовано його високу обчислювальну ефективність. Використання лінійних матричних перетворень замість ресурсоємних згорткових нейромереж створює передумови для функціонування алгоритму в реальному часі на малопотужних вбудованих платформах, забезпечуючи високу ймовірність стійкої селекції аномалій у складних умовах спостереження.

Список використаних джерел:

1. Федоренко І. О. Біспектральний підхід до виявлення замаскованих об'єктів на основі поєднання теплових та ближніх інфрачервоних зображень. Інформаційні технології в сучасному світі: дослідження молодих вчених : матеріали Міжнар. наук.-практ. конф. молодих вчених, аспірантів і студентів. Харків : ХНЕУ ім. С. Кузнеця, 2026. С. 62.

URL:
https://repository.hneu.edu.ua/bitstream/123456789/38789/1/Студ_конф_I_C_2026+.pdf.

2. Gonzalez R. C., Woods R. E. Digital Image Processing. 4th ed. New York : Pearson, 2018. 1192 p.

3. Ma J., Ma Y., Li C. Infrared and visible image fusion methods and applications: A survey. Information Fusion. 2019. Vol. 45. P. 153–178.

УДК 004.92:655.3

Чинкує Камелія, здобувач

*Інститут поліграфії та медійних технологій НУ «Львівська
політехніка»*

АЛГОРИТМИ АВТОМАТИЧНОЇ РАСТЕРИЗАЦІЇ ВЕКТОРНОЇ ГРАФІКИ В ЗАДАЧАХ ПОЛІГРАФІЧНОГО ДРУКУ

Растреризація векторної графіки важливий етап підготовки друку, що визначає якість відтворення контурів при роздільній здатності 1200-2400 dpi. На відміну від екранного рендерингу (96 dpi), поліграфічний друк не допускає видимого аліасингу - артефактів у вигляді «сходинок» на діагональних лініях і розмитих країв на дрібних елементах. Це висуває принципово інші вимоги до точності алгоритмів перетворення, ніж у задачах комп'ютерної графіки загального призначення. Більшість векторних контурів у форматах PDF, SVG і PostScript описується кривими Без'є третього порядку: $P(t) = (1-t)^3P_0 + 3(1-t)^2tP_1 + 3(1-t)t^2P_2 + t^3P_3$, де $t \in [0, 1]$, P_0 та P_3 - кінцеві точки, P_1 та P_2 - опорні. Задача растреризації створюється як визначення ступеня покриття кожного пікселя сітки контуром, тобто обчислення інтеграла площі перетину піксельного квадрата $[i, i+1] \times [j, j+1]$ з ідеальною фігурою. Розв'язання інтеграла для довільних кривих Без'є є обчислювально нераціональним, тому на практиці застосовуються наближені методи.

Алгоритм Брезенхема виконує растреризацію відрізків за $O(n)$ операцій без множення та ділення через цілочисельну арифметику. Проте він є принципово бінарним: піксель або замальований повністю, або ні. При роздільній здатності 1200 dpi це приводить до чітко видимого аліасингу на діагональних елементах товщиною менше 0,3 мм. Для поліграфії такий результат є неприйнятним.

Алгоритм Ву відсторонює цей недолік через введення поняття дробового покриття: для кожного пікселя вздовж контуру обчислюється частка $\alpha \in [0, 1]$, що відображає ступінь його перекриття, після чого піксель фарбується з інтенсивністю $\alpha \cdot C$, де C - колір лінії. Це забезпечує плавне згладжування країв практично без зростання обчислювальної складності порівняно з Брезенхемом.

Також було розглянуто scan-line rendering з правилом заповнення, що використовується в інтерпретаторах PostScript та PDF. Для кожного горизонтального рядка пікселів обчислюються точки перетину контуру з прямою $y = \text{const}$, які сортується за x . Заповнення виконується між

парами точок перетину за правилом non-zero winding або even-odd. Це забезпечує правильну обробку самоперетинних контурів, особливо в замкнених гліфів із внутрішніми порожнинами.

Для порівняльного оцінювання сформовано тестовий набір поліграфічних символів різних гарнітур, що включало прямі штрихи, діагональні елементи, серифи та замкнені контури. Еталонне зображення отримано растеризацією при 9600 dpi з подальшим зменшенням до 1200 dpi методом Ланцоша.

Отримані результати: алгоритм Брезенхема - $SSIM = 0,81$, виразні артефакти на діагональних штрихах; алгоритм Ву - $0,94$, помітне покращення на тонких елементах; субдिवізія Без'є з суперсемплінгом $4\times - 0,97$; суперсемплінг $16\times - 0,99$ при чотириразовому збільшенні часу обчислень. Scan-line з алгоритмом Ву показав $SSIM = 0,95$ на замкнених контурах, що підтверджує його перевагу саме в цій категорії символів.

З'ясовано, що субдिवізія кривих Без'є з суперсемплінгом $4\times$ забезпечує оптимальний баланс точності та швидкості для поліграфічного друку при 1200 dpi. Алгоритм Брезенхема непридатний для якісної поліграфії через бінарну природу. Алгоритм Ву є прийнятним компромісом у задачах, де пріоритетом є швидкість. Перспективою подальших досліджень є GPU-реалізація субдिवізії Без'є в RIP-системах реального часу, що може скоротити час растеризації на порядок.

Список використаної джерел:

1. Li T.-M., Huang W., Aittala M., Durand F. Differentiable vector graphics rasterization for editing and learning // ACM Transactions on Graphics. 2020. Vol. 39, No. 6. P. 1–15.
2. Loop C., Blinn J. Resolution independent curve rendering using programmable graphics hardware // ACM SIGGRAPH 2005 Papers. 2005. P. 1000–1009.
3. Yap C. K. Complete subdivision algorithms. I: Intersection of Bezier curves // Proceedings of the Twenty-Second Annual Symposium on Computational Geometry. 2006. P. 217–226.
4. Tian X., Günther T. A survey of smooth vector graphics: Recent advances in representation, creation, rasterization, and image vectorization // IEEE Transactions on Visualization and Computer Graphics. 2022. Vol. 30, No. 3. P. 1652–1671.

УДК 004.93

*Юдіна Л.Г, аспірант,
Апенько Н.В, к.т.н., доцент
Національний університет «Київський авіаційний інститут»*

ВПЛИВ ГЕОМЕТРИЧНИХ ПАРАМЕТРІВ ЗЙОМКИ НА ТОЧНІСТЬ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ

Сучасний розвиток безпілотних літальних апаратів (БпЛА) сприяє їх широкому застосуванню у задачах моніторингу територій, картографування, екологічного контролю, а також у системах безпеки та пошуково-рятувальних операціях [1]. Одним із ключових напрямів використання БпЛА є автоматизований аналіз візуальних даних, що базується на методах комп'ютерного зору. Ефективність систем розпізнавання об'єктів значною мірою визначається якістю вхідних зображень. На відміну від стаціонарних систем спостереження, зображення, отримані з БпЛА, формуються в умовах динамічного середовища, що призводить до варіацій геометричних та фотометричних характеристик сцени. Це, у свою чергу, впливає на стабільність дескрипторів та точність ідентифікації об'єктів. У зв'язку з цим актуальною є задача дослідження впливу параметрів аерозйомки на характеристики візуальних даних і точність їх подальшого аналізу [2].

Процес формування зображень у системах на основі БпЛА визначається сукупністю параметрів, серед яких ключовими є висота польоту, кут нахилу камери, швидкість руху платформи, а також характеристики сенсорної системи. Зміна цих параметрів призводить до трансформації геометричної структури зображення, зміни масштабу об'єктів та появи додаткових спотворень. Зі збільшенням висоти польоту відбувається зменшення просторової роздільної здатності об'єктів, що проявляється у зниженні деталізації текстурних характеристик. Це призводить до зменшення кількості інформативних ознак, що використовуються для формування дескрипторів, а також до зниження їх стійкості.

Кут нахилу камери визначає рівень перспективних спотворень. При значних кутах виникає деформація геометричної структури сцени, що ускладнює процес встановлення відповідностей між зображеннями та призводить до зростання кількості помилкових класифікацій. Додатковим фактором є наявність шумів, зумовлених характеристиками сенсорної системи та впливом зовнішнього

середовища. Шум знижує контрастність локальних структур і негативно впливає на процес виділення ключових точок.

Таким чином, формування візуальних даних можна розглядати як стохастичний процес, у якому параметри аерозйомки визначають статистичні властивості дескрипторів зображень. Для формалізації впливу параметрів введемо вектор параметрів формування зображення: $x = (h, \theta, v, l, \sigma)$.

Точність автоматичного розпізнавання можна розглядати як функцію цих параметрів: $A = f(h, \theta, v, l, \sigma)$.

Для оцінювання сили впливу параметрів використовується

коефіцієнт кореляції:

$$r_{xy} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}}.$$

Отримані результати свідчать про наявність негативної кореляції між висотою польоту та точністю розпізнавання, що пояснюється зменшенням деталізації зображення. Аналогічна залежність спостерігається для кута нахилу камери та рівня шуму. Аналіз статистичних характеристик дескрипторів показав, що зі збільшенням висоти польоту зменшується середнє значення ознак та зростає дисперсія, що призводить до зниження стабільності дескрипторів. У свою чергу, це безпосередньо впливає на точність розпізнавання.

Таким чином, встановлено, що параметри аерозйомки формують якість візуальних даних та визначають ефективність алгоритмів комп'ютерного зору.

Список використаних джерел:

1. Mohammed, B. A., Stanovska, I., Kashkevich, S., Lebedynskyi, A., Vakulenko, Y., Protas, N., Klyuchak, O., Lastivka, O., Semenjuk, A., Kivshar, O. (2025). Development of a methodological approach for assessing the condition of complex organizational and technical systems. *Eastern-European Journal of Enterprise Technologies*, 2 (3 (134)), 47–53. <https://doi.org/10.15587/1729-4061.2025.326468>.
2. Kashkevich, S. (Ed.). (2025). *Decision support systems: mathematical support*. Kharkiv: TECHNOLOGY CENTER PC. <https://doi.org/10.15587/978-617-8360-13-9>.

Shcherbak A.Ye., postgraduate student
Oles Honchar Dnipro National University

REFLECTION-DECOUPLED ANALYSIS IN THE TDR SIGNAL DIGITAL PROCESSING PIPELINE

Time-domain reflectometry (TDR) is a widely adopted method for non-destructive characterisation of inhomogeneous materials, including soils, biological tissues, and composite structures. Its principle relies on launching a broadband electromagnetic pulse into a transmission-line probe immersed in the material under test and recording the reflected waveform. A single Fourier transform then converts this temporal record into the frequency-dependent complex dielectric permittivity (CDP) spectrum, covering a range from tens of megahertz to several gigahertz [1]. A critical challenge in this workflow is the sensitivity of the recovered spectrum to source instability, connector imperfections, and cable length variations – artefacts that corrupt the measured reflection coefficient and, consequently, the retrieved material parameters.

The classical approach to compensating for these systematic errors is the Dual Reflection Analysis (DRA) method [2]. DRA exploits the ratio of two successive reflections – the first from the air-material interface and the second from the probe termination – to cancel the source transfer function.

Reflection-Decoupled Analysis (RDA) addresses these limitations through the introduction of a dedicated Mismatched Section (MS) – a precisely characterised, geometrically stable segment of transmission line (typically air-filled or PTFE-filled) inserted between the feed cable and the measurement probe [3]. The dielectric properties of the MS are known a priori and do not change with environmental conditions, making the first reflection from the MS entrance a fully deterministic reference signal that encodes the instantaneous state of the source, the connector, and the entire feed cable. In every acquisition cycle, RDA processes two physically separated waveforms: the reference reflection $R_1(\omega)$ from the MS entrance and the measurement reflection $R_2(\omega)$ from the probe–material interface. Because $R_1(\omega)$ contains the complete source signature, the material-dependent reflection coefficient can be deconvolved as:

$$\rho(\omega) = R_2(\omega) / [R_1(\omega) \cdot H_{MS}(\omega)],$$

where $H_{MS}(\omega)$ is the analytically computed transfer function of the MS. This division effectively removes the source function from every measurement without the need for explicit calibration procedures such as the Short-Open-Load (SOL) protocol that is standard in vector network analysis.

The practical consequence is that RDA operates as a continuous, in-situ self-calibrating system [3].

Within a full TDR digital signal processing pipeline, RDA is positioned upstream of the inverse problem solver. The recommended pipeline architecture consists of the following sequential stages: (1) signal acquisition – synchronous averaging of N waveforms to suppress AWGN; (2) adaptive denoising – Savitzky-Golay or wavelet thresholding to preserve edge sharpness; (3) baseline correction – polynomial trend subtraction to remove DC drift; (4) windowing – Tukey window application before FFT to reduce spectral leakage; (5) RDA deconvolution – extraction of the clean reflection spectrum $\rho(\omega)$; (6) inversion – retrieval of CDP parameters via a hybrid optimisation algorithm.

The inclusion of RDA as stage 5 decouples the quality of the spectral estimate from cable-assembly variability. Laboratory tests reported in [3] demonstrate that RDA maintains CDP retrieval accuracy (relative error below 2 %) over cable length variations of up to 3 m and temperature shifts of ± 20 °C, conditions under which classical DRA degrades to errors exceeding 8 %. This robustness is of particular importance for embedded monitoring systems operating in field environments where controlled calibration is impractical.

The principal advantages of RDA are: single-shot self-calibration inherent to every measurement cycle; independence from probe length, enabling short probes in high-loss media; compatibility with low-cost TDR hardware, since the MS can be fabricated from standard semi-rigid coaxial cable. The main limitation is the increased complexity of the probe assembly and the requirement for accurate characterisation of $H_{MS}(\omega)$, which must account for the geometry and temperature dependence of the MS permittivity.

References:

1. Heimovaara T. J. Frequency domain analysis of time domain reflectometry waveforms. *Water Resources Research*. 1994. Vol. 30, No. 2. P. 189–199.
2. Mironov V. L., Dobson M. C., Kaupp V. H. et al. Generalized refractive mixing dielectric model for moist soils. *IEEE Trans. Geoscience Remote Sensing*. 2004. Vol. 42, No. 4. P. 773–785.
3. Huisman J. A., Sperl C., Bouten W., Verstraten J. M. Soil water content measurements at different scales. *Journal of Hydrology*. 2001. Vol. 245. P. 48–58.

Секція 7 КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ ТА РОБОТОТЕХНІКА

UDC 628.3:004.9

*Artem Prykhodko, student
Sumy State University*

AUTOMATION OF WASTEWATER TREATMENT PROCESSES USING DIGITAL TECHNOLOGIES

In modern conditions of increasing anthropogenic load on the environment, increasing the efficiency of wastewater treatment is of particular relevance. Traditional treatment methods are often characterized by significant energy consumption, lack of flexibility and dependence on the human factor. In this regard, the introduction of automated control systems based on digital technologies is a promising direction for improving the operation of treatment facilities.

Automation of wastewater treatment processes involves the use of sensors, controllers and software for continuous monitoring and control of technological parameters. Key indicators include the level of pollution, concentration of suspended solids, chemical oxygen demand, pH of the environment, temperature and others. The use of sensor systems allows you to receive data in real time, which significantly increases the accuracy of control and the speed of decision-making [1].

An important role is played by computer-integrated control systems that provide automatic regulation of the operation of pumps, aeration units, filters and other elements of the technological process. This allows you to optimize energy consumption, reduce resource losses and improve the quality of treatment. In addition, the use of optimization algorithms and artificial intelligence elements makes it possible to predict changes in the composition of wastewater and adjust equipment operating modes in advance [2].

One of the promising areas is the integration of Internet of Things (IoT) technologies, which provides remote monitoring and control of treatment systems. This is especially relevant for distributed facilities and small treatment plants. The use of cloud services allows you to accumulate and analyze large amounts of data, which helps to increase management efficiency [3].

Thus, automation of wastewater treatment processes using digital technologies helps to increase environmental safety, reduce energy consumption and improve the quality of treatment. Further development of this area is associated with the implementation of intelligent management

systems that ensure sustainable development of the water management complex.

References:

1. Ільків І. В. Методи і їх алгоритмична, програмна та технічна реалізація побудови інформаційної системи біологічного очищення стічних вод : дис. д-ра філософії : спец. 122 "Комп'ютерні науки" / Ільків Ігор Васильович. - Рівне : НУВГП, 2023. - 208 с.

2. Розганяєв В. О. Автоматизація процесу налагодження фільтрації рідин промисловими фільтрами. 2019. URL: <https://krs.chmnu.edu.ua/jspui/handle/123456789/552>, (дата звернення 18.03.2026).

3. Рішення IoT для водопостачання та водовідведення. URL: <https://www.se.com/ua/uk/work/solutions/for-business/water/> (дата звернення 20.03.2026).

UDC 681.121:681.324.06

***Pysarets Anna, Candidate of Technical Sciences, Associate Professor,
Pysarets Oleksandr, student
Igor Sikorsky Kyiv Polytechnic Institute***

COMPUTER-INTEGRATED SYSTEMS FOR THE ENERGY CARRIERS METERING

The rapid development of information technology facilitates the creation of computer-integrated systems and their implementation in many areas of human activity, from household organization to industrial production.

Typically, such systems have three-level architecture. The first level of such a structure contains sensors and actuators, the second level handles event processing (where information is stored and processed, and devices of the previous level are controlled), and the third level handles monitoring and remote control using the Internet [1].

The use of such systems allows for the collection, transmission, processing and analysis of data received from primary transducers. This, in turn, facilitates the acquisition of prompt and reliable information about the state of the controlled object or technological process, the adoption of optimal decisions, especially in the event of emergency situations, and increased management efficiency.

In this case, the controlled object may be a separate apartment in the living building, a private house, a public building, a microdistrict, an industrial enterprise, etc.

In particular, such systems are becoming widespread in the field of monitoring and controlling indoor microclimate parameters (temperature, humidity); lighting, including street lighting; power supply for electrical equipment; monitoring technological process parameters (temperature, pipeline pressure and its tightness), etc.

The applied data transmission technologies and the topology of the created systems are selected depending on the size of the control object, the number, purpose and location features of the primary transducers.

In the field of energy carriers metering, characterized by a large number of simultaneously connected remote devices, the most widely used wired and wireless technologies are RS-485, M-Bus, wM-Bus, LoRaWAN, NB-IoT [2, 3].

The specific features of the metering systems using at industrial enterprises include the need to integrate legacy equipment into a network that does not have wireless data transfer interface adapters, as well as the installation of sensors and actuators in hard-to-reach places.

In this case, a combined system is used, where wired data transmission technologies are used at the first level.

As a result, such system offers the advantages of all currently used data transmission technologies, namely [2 – 4]:

- High noise immunity and data security (accessing information requires physical access to the equipment or data buses);
- High reliability;
- Weather-independence;
- The ability to combine meters from different manufacturers in the network to measure different energy sources;
- Unlimited quantity of connected metering units;
- Speed and ease of deployment;
- Significant reduction in time and cost during the design, deployment, and operation of the system.

At the same time, issues of software vulnerabilities, information system leaks, vulnerability to cyber attacks, etc. remain relevant.

Practical issues of creating computer-integrated energy carriers metering systems in our country are presented in the report.

References:

1. Kozel V., Ivanchuk O., Drozdova I., Prykhodko O. Automation of the Protocol Selection Process for IoT Systems. *International Journal of Computing*. 2022. № 21(2). P. 251-257. DOI: 10.47839/ijc.21.2.2594
2. Писарець А. В., Писарець Є. В. Автоматизовані системи передачі показань від приладів обліку енергоносіїв. Частина 1. *Вісник КПІ. Серія приладобудування*. 2020. Вип. 59(1). С. 95–101. DOI: 10.20535/1970.59(1).2020.210037
3. Писарець А. В., Писарець Є. В. Автоматизовані системи передачі показань від приладів обліку енергоносіїв. Частина 2. *Вісник КПІ. Серія приладобудування*. 2020. Вип. 60(2). С. 79–86. DOI: 10.20535/1970.60(2).2020.221452
4. Pysarets A., IoT technologies in the energy carriers metering // Збірник матеріалів XXIII Міжнародної науково-технічної конференції "ПРИЛАДОБУДУВАННЯ: стан і перспективи", 14 – 15 травня 2024 р., м. Київ: ПБФ, НТУУ «КПІ», 2024. С. 302–305.

УДК 004.7

*Голуб Д. А, здобувач
Бондаренко В. В, викладач*

Черкаський національний університет імені Богдана Хмельницького

ТЕХНОЛОГІЇ ЗАНУРЕННЯ ЯК ФАКТОР ФОРМУВАННЯ ЕФЕКТУ ПРИСУТНОСТІ У VR

Перші згадки про створення віртуального середовища, що повністю імітувало б реальний світ, з'явилися в 1960-х роках, коли було розроблено перший прототип сучасних окулярів віртуальної реальності – Headsight. Пізніше фахівці Массачусетського університету створили додаток, що дозволяв здійснити віртуальну прогулянку містом Аспен, обираючи способи відображення місцевості.

Зі зростанням обчислювальних можливостей апаратного забезпечення та збільшення інтересу публіки до віртуальної реальності, з 2012 року індустрія віртуальної реальності почала свій стрімкий розвиток. Таким чином, з'явилися окуляри віртуальної реальності Oculus Rift, Meta Quest, Microsoft HoloLens, HTC Vive та подібні. Кожен із них прагнув створити програмно-апаратні рішення, здатні забезпечити повне занурення користувача у віртуальне середовище.

На сучасному етапі розвитку VR-технологій значна увага приділяється вирішенню проблеми досягнення високого рівня занурення та ефекту присутності. Занурення являє собою створення ефекту присутності у віртуальному середовищі завдяки технологіям, що імітують тактильні відчуття користувача, наприклад, вібрацію. Така технологія має назву haptics [1].

Гарним прикладом використання технології haptics для формування ефекту присутності у віртуальному середовищі можна навести фільм “Ready Player One” (Першому гравцеві приготуватись), знятий Стівеном Спілбергом за однойменним романом. У фільмі ефект присутності досягався за допомогою комбінації декількох технологій, які на сьогодні частково реалізуються у VR, серед яких:

1. Повнотілесний трекінг рухів – спеціальні датчики відстежують положення тіла користувача, дозволяючи його аватару у віртуальному середовищі точно повторювати рухи.
2. Тактильний зворотний зв'язок – рукавички або костюми передають відчуття дотику, ударів або вібрації при взаємодії з віртуальними об'єктами.
3. Бігові платформи – пристрої, що дозволяють користувачу ходити або бігати у віртуальному просторі, залишаючись на одному місці у фізичному середовищі.

4. Просторове аудіо – технологія тривимірного звуку, що дозволяє визначати напрямок і відстань до джерела звуку.

5. Високоякісне візуальне відображення – VR-шоломи з широким полем зору та стереоскопічним зображенням створюють реалістичну тривимірну сцену.

Разом ці технології утворюють відчуття повного занурення у віртуальне середовище, що дозволяє користувачеві сприймати його як реальний простір. Таким чином, можна змодельовати будь-яку реальну ситуацію у віртуальному середовищі та досліджувати поведінку користувача в умовах, максимально наближених до реальності.

Однак для досягнення такого ефекту необхідні високі апаратні обчислювальні потужності, а також високий рівень реалістичності елементів віртуального середовища, що досягається створенням високоякісних тривимірних моделей, текстур, анімацій тощо. У зв'язку з цим розробники намагаються шукати баланс між рівнем реалістичності сцени та продуктивністю системи.

Розвиток технологій занурення стає ключовим фактором у формуванні переконливого відчуття присутності у віртуальному середовищі. Поєднання технологій імітації тактильних відчуттів, високоякісних віртуальних середовищ, просторового аудіо та систем повнотілесного трекінгу дозволить створювати реалістичні віртуальні світи, що не будуть відрізнятися від реального світу. Подальші перспективи використання цих середовищ будуть включати в себе застосування VR у навчанні, тренуванні, науці тощо, роблячи користувацький досвід більш захопливим.

Список використаних джерел:

1. Bottoni P., Cifani S., Kanev K., Moraru D., Nakamura A., Marini M. R. Towards a More Realistic VR Experience: Merging Haptic Gloves with Precision Gloves [Electronic resource]. 2026. URL: <https://doi.org/10.48550/arXiv.2602.15833> (date of access: 15.03.2026).

УДК 528.7:629.735.33

**Барабаш В.В., здобувач,
Ткачук Д.Ю., аспірантка**

Державний університет «Житомирська політехніка»

РОЗРОБКА СИСТЕМИ АВТОМАТИЧНОГО КАРТОГРАФУВАННЯ МІСЦЕВОСТІ З ВИКОРИСТАННЯМ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У сучасних умовах цифрової трансформації особливої актуальності набувають засоби оперативного збору, обробки та аналізу геопросторових даних. Одним із найбільш перспективних напрямів у цій сфері є використання безпілотних літальних апаратів для автоматизованого картографування місцевості. Такі системи забезпечують отримання високодеталізованих аерофотознімків, що можуть бути використані для побудови ортофотопланів, тривимірних моделей території та цифрових карт різного призначення.

Традиційні підходи до картографування, зокрема наземні геодезичні вимірювання та супутникова зйомка, характеризуються достатньою точністю, проте часто потребують значних часових і фінансових витрат.

Запропонована система включає кілька функціонально пов'язаних компонентів: безпілотний літальний апарат з цифровою камерою, навігаційний модуль GNSS/IMU, програмне забезпечення для планування польотної місії, канал передавання даних та обчислювальний модуль фотограмметричної обробки. На етапі підготовки користувач задає межі ділянки дослідження, висоту польоту, параметри перекриття знімків і режим фотографування. На основі цих даних формується маршрут автоматичного обльоту території. Під час виконання польотного завдання БПЛА здійснює послідовне фотографування поверхні через визначені просторові інтервали або в заданих координатах. Кожен кадр супроводжується метаданими про географічне положення, орієнтацію платформи та висоту польоту. Це створює передумови для подальшої геоприв'язки зображень і точного відновлення просторової структури місцевості.

Обробка отриманих аерофотознімків передбачає послідовне виконання декількох етапів: вирівнювання зображень, визначення спільних опорних точок, побудову щільної хмари точок, формування цифрової моделі рельєфу або поверхні, ортореєстрацію та зшивання знімків в єдиний ортофотоплан. У результаті формується просторово узгоджений набір даних, придатний для подальшого аналізу у геоінформаційних системах. Важливим параметром якості

аерознімання є просторовий розмір пікселя на місцевості, який у спрощеному вигляді визначається співвідношенням:

$$\text{GSD} = (\text{H} \times \text{p}) / \text{f},$$

де GSD - просторова роздільна здатність знімка на місцевості; H - висота польоту; p - фізичний розмір пікселя матриці камери; f - фокусна відстань об'єктива.

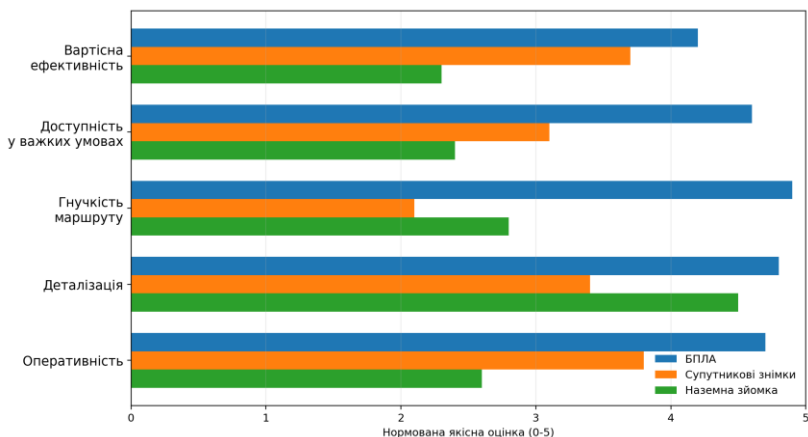


Рис.1. Ілюстративне порівняння підходів до картографування за ключовими якісними показниками

Застосування безпілотних літальних апаратів у системах автоматичного картографування є перспективним напрямом розвитку сучасних геоінформаційних технологій. Поєднання автоматизованого планування місії, аерофотознімання та фотограмметричної обробки забезпечує отримання актуальних і високодеталізованих просторових даних.

Список використаних джерел:

1. Ковальчук І. М., Мельник А. С. Застосування безпілотних літальних апаратів у геодезії та моніторингу територій // Геоінформатика. – 2020. – №3. – С. 52–58.
2. OpenDroneMap. OpenDroneMap Documentation. URL: <https://www.opendronemap.org/>

УДК 629.735.33:004.93

*Біленький І.О., здобувач,
Добржанський О.О., к. т. н., доцент
Державний університет «Житомирська політехніка»*

РОЗРОБКА СИСТЕМИ АВТОМАТИЧНОЇ ПОСАДКИ БПЛА З ВИКОРИСТАННЯМ ВІЗУАЛЬНИХ МАРКЕРІВ

Інтенсивне впровадження БПЛА у логістиці, моніторингу територій, аграрному секторі та рятувальних операціях актуалізує задачу забезпечення їх точної та безпечної посадки. На завершальному етапі польоту використання лише супутникової навігації не гарантує необхідної точності через похибки позиціонування, затримки вимірювань і можливі втрати сигналу. У зв'язку з цим перспективним є застосування засобів комп'ютерного зору, здатних забезпечити локальне високоточне наведення БПЛА на посадковий майданчик.

Метою роботи є розробка підходу до автоматичної посадки БПЛА на основі візуальних маркерів, який передбачає виявлення маркера у відеопотоці з бортової камери, оцінювання його просторового положення відносно камери та формування керуючих сигналів для корекції траєкторії польоту. Як маркер доцільно використовувати ArUco-мітки, оскільки вони мають контрастну геометричну структуру, високу завадостійкість і дозволяють надійно визначати положення та орієнтацію об'єкта у просторі.

Функціональну структуру запропонованої системи наведено на рис. 1. Відеодані з бортової камери надходять до модуля комп'ютерного зору, у якому виконується детектування ArUco-маркера та оцінювання вектора зміщення посадкової платформи відносно БПЛА. Далі на основі отриманих координат формується вектор похибки, який використовується регулятором для побудови керуючих впливів на автопілот. Такий підхід забезпечує поступове вирівнювання апарата над маркером і зменшує відхилення від заданої точки посадки.

Математична модель визначення положення маркера може бути подана рівнянням проєкції:

$$s \cdot p = K[R|t]P,$$

де p – координати точки маркера на зображенні; K – матриця внутрішніх параметрів камери; R і t – матриця обертання та вектор перенесення, що описують положення камери відносно маркера; P – координати точки маркера у світовій системі координат. На основі оцінених параметрів формується вектор похибки $e = [\Delta x, \Delta y, \Delta z, \Delta \psi]^T$, який використовується для корекції положення, висоти та курсу БПЛА на етапі заходу на посадку.

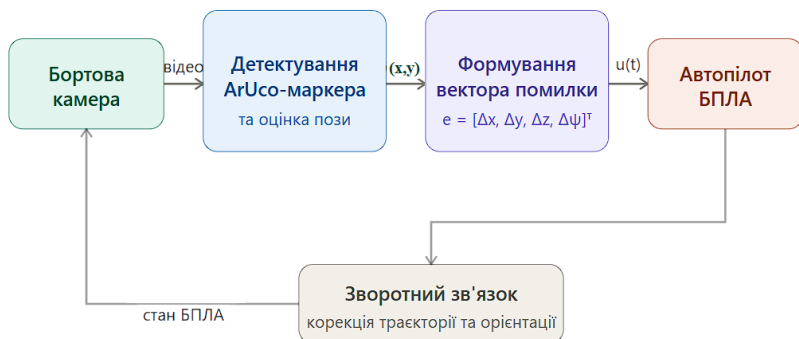


Рис.1. Структурна схема системи автоматичної посадки БПЛА

Очікуваними перевагами запропонованого підходу є підвищення точності посадки на обмежені платформи, зниження залежності від супутникових навігаційних систем і підвищення надійності роботи в умовах часткового зашумлення або нестабільного сигналу GPS. Практична реалізація системи може бути корисною для автономних безпілотних платформ, що працюють у міських умовах, на промислових об'єктах або у важкодоступних районах. Подальші дослідження доцільно спрямувати на моделювання роботи алгоритму, експериментальну перевірку точності посадки та оцінювання стійкості системи до зміни освітлення, висоти й кута огляду камери.

Список використаних джерел:

1. Xin, L., Tang, Z., Gai, W., Liu, H. Vision-Based Autonomous Landing for the UAV: A Review. *Aerospace*, 2022, 9(11), 634. DOI: 10.3390/aerospace9110634. URL: <https://www.mdpi.com/2226-4310/9/11/634>
2. Semerikov, S.O., Nechypurenko, P.P., Vakaliuk, T.A. et al. Vision-Based Autonomous UAV Landing: A Comprehensive Review of Technologies, Techniques, and Applications. *Journal of Intelligent & Robotic Systems*, 2025, 111, 115. DOI: 10.1007/s10846-025-02314-4. URL: <https://link.springer.com/article/10.1007/s10846-025-02314-4>
3. Lv, M., Fan, B., Fang, J., Wang, J. Autonomous Landing of Quadrotor Unmanned Aerial Vehicles Based on Multi-Level Marker and Linear Active Disturbance Reject Control. *Sensors*, 2024, 24(5), 1645. DOI: 10.3390/s24051645. URL: <https://www.mdpi.com/1424-8220/24/5/1645>

УДК 629.735.33:681.5

Василевський Д.В., здобувач,

Кравчук А.Р., доцент

Державний університет «Житомирська політехніка»

ДОСЛІДЖЕННЯ МЕТОДІВ ЕНЕРГОЕФЕКТИВНОГО КЕРУВАННЯ БЕЗПІЛОТНИМИ АПАРАТАМИ ПІД ЧАС ВИКОНАННЯ ТРИВАЛИХ МІСІЙ

Безпілотні літальні апарати (БПЛА) набули широкого застосування у задачах моніторингу, картографування, пошуково-рятувальних операціях, сільському господарстві та системах технічного спостереження. Разом із розширенням сфер їх використання зростають вимоги до тривалості автономного польоту, надійності виконання місії та раціонального використання бортового енергетичного ресурсу. Одним із головних обмежень ефективності БПЛА залишається обмежена ємність акумуляторних батарей, а збільшення запасу енергії за рахунок зростання маси елементів живлення не завжди є доцільним, оскільки це погіршує льотні характеристики платформи. У зв'язку з цим особливою актуальності набуває розроблення методів керування, які забезпечують мінімізацію енерговитрат без втрати якості виконання польотного завдання.

У межах дослідження виходимо з того, що енергоспоживання БПЛА визначається не лише параметрами силової установки, а й профілем швидкості, інтенсивністю маневрування, стабілізаційними відхиленнями, зовнішніми збуреннями та структурою маршруту. Одним із ключових чинників енергоефективності є швидкість польоту. Залежність питомих енерговитрат від швидкості має нелінійний характер і зазвичай містить мінімум, що відповідає енергоефективному режиму. На малих швидкостях зростають витрати на підтримання стійкості та підйомної сили, а на великих – аеродинамічні втрати через збільшення лобового опору. Цю залежність наведено на рис. 1. Отже, вибір швидкості поблизу мінімуму питомих енерговитрат є важливою умовою підвищення тривалості місії.

Важливим напрямом підвищення енергоефективності є також оптимізація траєкторії руху. Раціональне планування маршруту дає змогу скоротити довжину шляху, зменшити кількість зайвих маневрів і врахувати вплив рельєфу, вітрових збурень та обмежень повітряного простору. Для цього можуть застосовуватися методи динамічного програмування, генетичні та евристичні алгоритми, орієнтовані на мінімізацію енерговитрат за збереження безпеки польоту та часових вимог місії.

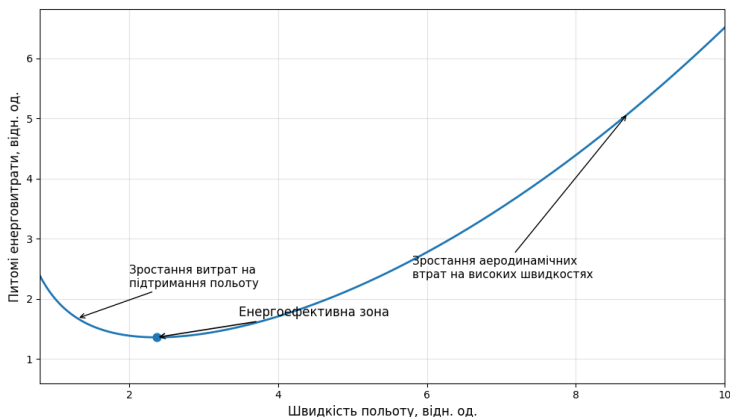


Рис.1. Залежність питомих енерговитрат БПЛА від швидкості польоту

Перспективним напрямом є застосування адаптивних систем керування, здатних змінювати параметри польоту відповідно до поточного стану БПЛА та зовнішніх умов. На основі даних інерціальних, навігаційних, барометричних і аерометричних датчиків система може коригувати швидкість, просторове положення та режими роботи двигунів для зниження енерговитрат. Додатковий ефект забезпечує використання методів машинного навчання, що дають змогу прогнозувати енергоспоживання та формувати ефективні стратегії керування з урахуванням попередніх польотних даних.

Підвищення енергоефективності БПЛА під час тривалих місій досягається завдяки поєднанню оптимального швидкісного режиму, раціональної траєкторії, адаптивного керування та інтелектуального аналізу польотної інформації. Реалізація цих підходів сприяє збільшенню тривалості автономної роботи, підвищенню надійності виконання місії та зменшенню навантаження на бортову енергосистему. Подальші дослідження доцільно зосередити на розробленні інтегрованих систем прогнозування енергоспоживання в реальному часі.

Список використаних джерел:

1. Zeng Y., Xu J., Zhang R. Energy Minimization for Wireless Communication with Rotary-Wing UAV. arXiv, 2018. arXiv:1804.02238. URL: <https://arxiv.org/pdf/1804.02238>
2. Beigi P., Rajabi M. S., Aghakhani S. An Overview of Drone Energy Consumption Factors and Models. arXiv, 2022. arXiv:2206.10775. URL: <https://arxiv.org/pdf/2206.10775>

УДК 629.735.33:004.93

*Захарчук Г.А., здобувач,
Ткачук А.Г., к. т. н., доцент
Державний університет «Житомирська політехніка»*

РОЗРОБКА СИСТЕМИ АВТОМАТИЧНОГО СТЕЖЕННЯ БПЛА ЗА РУХОМИМ ОБ'ЄКТОМ

БПЛА активно впроваджуються в задачі моніторингу, патрулювання, відеоспостереження та супроводу динамічних об'єктів. Одним із ключових завдань у таких системах є забезпечення стійкого автоматичного стеження за об'єктом в умовах змінної освітленості, часткових перекриттів, фонових завад і маневрування самого носія. Традиційні підходи, що базуються на ручному керуванні або спрощених методах сегментації зображення, мають обмежену точність і недостатню робастність у реальних експлуатаційних умовах. У зв'язку з цим актуальним є створення інтегрованої системи, яка поєднає алгоритми комп'ютерного зору з контуром автоматичного керування польотом.

Запропонована система має чотириланкову архітектуру. Перша ланка представлена бортовою камерою БПЛА, яка формує потік RGB-зображень із частотою до 60 кадр/с. Друга ланка – обчислювальний модуль Jetson Nano, на якому реалізовано алгоритми комп'ютерного зору. Для первинної локалізації цільового об'єкта використовується нейромережева детекція, а для міжкадрового супроводу – кореляційний трекер CSRT. Така комбінація дає змогу зменшити обчислювальне навантаження та підвищити стійкість системи при короточасних втратах детекції.

На основі координат обмежувального прямокутника визначається центр об'єкта:

$$x_c = \frac{x_{\min} + x_{\max}}{2}, \quad y_c = \frac{y_{\min} + y_{\max}}{2}$$

де W і H – ширина та висота кадру відповідно. Отримані величини характеризують зміщення об'єкта в полі зору камери та використовуються як сигнали похибки для системи керування.

Третя ланка архітектури реалізована на польотному контролері Pixhawk, який формує керуючі сигнали за PID-законом:

$$u(t) = K_p e(t) + K_i \int e(t) dt + K_d \frac{de(t)}{dt}$$

де $e(t)$ – поточна похибка позиціонування об'єкта в кадрі, K_p , K_i , K_d – коефіцієнти пропорційної, інтегральної та диференціальної складових. Команди керування передаються через протокол MAVLink. Четверта

ланка включає виконавчі органи БПЛА – безщіткові двигуни, за допомогою яких здійснюється просторова корекція за каналами Pitch, Roll і Yaw.

Оцінювання ефективності запропонованої системи виконано в симуляційному середовищі Gazebo із підключенням Software In The Loop. Як об'єкт стеження використовувався рухомий наземний робот зі швидкістю до 2 м/с. У ході 50 експериментів визначено, що середня квадратична похибка центрування не перевищує 18 пікселів за умови прямолінійного руху об'єкта та 34 пікселі під час зміни траєкторії. Затримка від моменту надходження відеокадру до формування керуючого сигналу становила не більше 85 мс, що свідчить про придатність системи до роботи в режимі, близькому до реального часу.



Рис.1. Порівняння середньої квадратичної похибки центрування та Затримка обробки відносно порогу реального часу

Отримані результати підтверджують ефективність інтеграції методів комп'ютерного зору із системою автоматичного керування БПЛА. Поєднання алгоритмів детекції та трекінгу забезпечує стійке супроводження рухомого об'єкта в динамічних умовах. Перспективами подальших досліджень є використання інфрачервоних камер для роботи в умовах недостатньої освітленості, а також застосування фільтра Калмана для прогнозування траєкторії цілі та згладжування керуючих впливів.

Список використаних джерел:

1. Tang, G.; Ni, J.; Zhao, Y.; Gu, Y.; Cao, W. *A Survey of Object Detection for UAVs Based on Deep Learning*. Remote Sensing, 2024, 16(1), 149. DOI: 10.3390/rs16010149. URL: <https://www.mdpi.com/2072-4292/16/1/149>
2. He, Y.; Chao, C.; Zhang, Z.; Guo, H.; Ma, J. *UAV Visual Object Tracking Based on Spatio-Temporal Context*. Drones, 2024, 8(12), 700. DOI: 10.3390/drones8120700. URL: <https://www.mdpi.com/2504-446X/8/12/700>

УДК 629.735.33:681.5

*Любченко І.В., здобувач,**Кравчук А.Р., доцент**Державний університет «Житомирська політехніка»*

МОДЕЛЮВАННЯ СИСТЕМИ СТАБІЛІЗАЦІЇ КВАДРОКОПТЕРА З ВИКОРИСТАННЯМ PID-РЕГУЛЯТОРА

Сучасні квадрокоптери широко застосовуються в аерофотозйомці, моніторингу територій, сільському господарстві, рятувальних операціях і наукових дослідженнях. Однією з ключових умов їх ефективного функціонування є забезпечення стійкого польоту та точного відпрацювання керуючих команд. Оскільки квадрокоптер є динамічно нестійкою системою, для підтримання його орієнтації у просторі необхідно використовувати алгоритми автоматичного керування, здатні компенсувати зовнішні збурення та внутрішні динамічні відхилення.

У роботі розглянуто математичне моделювання системи стабілізації квадрокоптера на основі PID-регулятора. Метою дослідження є побудова моделі керування, що забезпечує стабілізацію орієнтації апарата за каналами крену, тангажу та ристання, а також аналіз впливу параметрів регулятора на динаміку перехідних процесів. Керування положенням квадрокоптера здійснюється шляхом зміни швидкостей обертання чотирьох електродвигунів, унаслідок чого формуються керуючі моменти відносно осей roll, pitch та yaw. Для оцінювання поточного стану використовуються дані інерціального вимірювального модуля, до складу якого входять акселерометри та гіроскопи.

У спрощеному вигляді динаміка обертального руху описується рівнянням:

$$J\ddot{\varphi}(t) = M(t)$$

де J – момент інерції, $\varphi(t)$ – кутове відхилення, $M(t)$ – керуючий момент.

PID-регулятор формує керуючий сигнал за законом:

$$u(t) = K_p e(t) + K_i \int e(t) dt + K_d \frac{de(t)}{dt}$$

де $e(t)$ – похибка регулювання, а K_p , K_i , K_d – коефіцієнти пропорційної, інтегральної та диференціальної складових.

Пропорційна складова забезпечує швидку реакцію на поточну похибку, інтегральна – зменшує статичну помилку, а диференціальна – покращує демпфування та знижує перерегулювання. У моделі регулятори налаштовувалися окремо для кожного каналу стабілізації, що дозволяє незалежно керувати орієнтацією апарата.

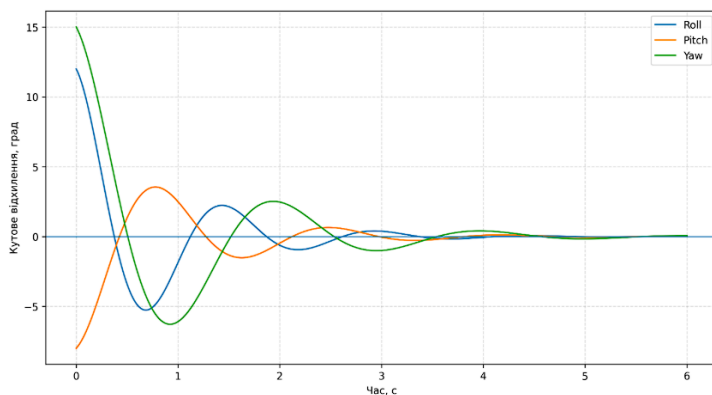


Рис.1. Перехідні процеси стабілізації квадрокоптера за каналами roll, pitch та yaw при PID-регулюванні

Результати моделювання показали, що використання PID-регулятора забезпечує ефективне повернення квадрокоптера до заданого положення після початкового відхилення. Перехідні процеси мають затухаючий характер, а амплітуда коливань зменшується з часом, що свідчить про стійкість системи. Найкращі показники досягаються за узгодженого вибору коефіцієнтів K_p , K_i та K_d , коли забезпечуються достатня швидкодія та мінімальне перерегулювання.

Отримана модель може бути використана як основа для подальшої розробки систем автоматичного керування БПЛА. Перспективним напрямом є застосування адаптивних та інтелектуальних методів керування для підвищення точності стабілізації в умовах змінного зовнішнього середовища.

Список використаних джерел:

1. Lopez-Sanchez, I.; Moreno-Valenzuela, J. PID control of quadrotor UAVs: A survey. *Annual Reviews in Control*. 2023. Vol. 56. Article 100900. DOI: 10.1016/j.arcontrol.2023.100900.
2. Gün, A. Attitude control of a quadrotor using PID controller based on differential evolution algorithm. *Expert Systems with Applications*. 2023. Vol. 229, Part B. Article 120518. DOI: 10.1016/j.eswa.2023.120518.

УДК 621.311:004.85

*Манзевитий В., здобувач,
Покляченко О.В., старший викладач
Державний університет «Житомирська політехніка»*

ПРОГНОЗУВАННЯ ЕЛЕКТРОСПОЖИВАННЯ В ЕНЕРГЕТИЧНИХ СИСТЕМАХ ІЗ ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Сучасний розвиток енергетичних систем супроводжується зростанням нерівномірності та варіативності електроспоживання, що обумовлено інтеграцією відновлюваних джерел енергії, цифровізацією електромереж, зміною режимів роботи споживачів і впливом зовнішніх факторів, зокрема метеорологічних. За таких умов підвищуються вимоги до точності прогнозування електричного навантаження, оскільки саме якісний прогноз є основою для оперативного диспетчерського керування, оптимізації режимів генерації, зменшення резервів потужності та підвищення надійності функціонування енергосистеми.

Прогнозування електроспоживання зазвичай поділяють на короткострокове, середньострокове та довгострокове. Короткострокове прогнозування охоплює часовий інтервал від кількох годин до кількох діб і використовується для оперативного керування режимами роботи енергосистеми. Середньострокове прогнозування застосовується для планування технічного обслуговування, ремонтів та балансування ресурсів на горизонті від кількох тижнів до місяців. Довгострокове прогнозування орієнтоване на стратегічне планування розвитку енергетичної інфраструктури та оцінювання перспектив зміни попиту.

Традиційні статистичні методи, зокрема авторегресійні моделі типу ARIMA, ефективні для аналізу стаціонарних часових рядів, однак часто виявляються недостатньо гнучкими для опису складних нелінійних залежностей, характерних для сучасних енергетичних даних. У зв'язку з цим дедалі ширше застосовуються методи машинного навчання, здатні виявляти приховані закономірності у великих масивах даних та враховувати вплив багатьох факторів одночасно.

Для побудови моделей прогнозування використовують історичні дані про споживання електроенергії, часові мітки, календарні ознаки, метеорологічні параметри, а також, за потреби, соціально-економічні показники. Серед класичних алгоритмів машинного навчання найбільш поширеними є метод опорних векторів, дерева рішень, випадковий ліс та градієнтний бустинг. Для задач, у яких необхідно враховувати часову структуру ряду, особливий інтерес становлять рекурентні нейронні

мережі, зокрема архітектура LSTM, яка забезпечує моделювання довгострокових часових залежностей та знижує втрати інформації під час обробки послідовностей.

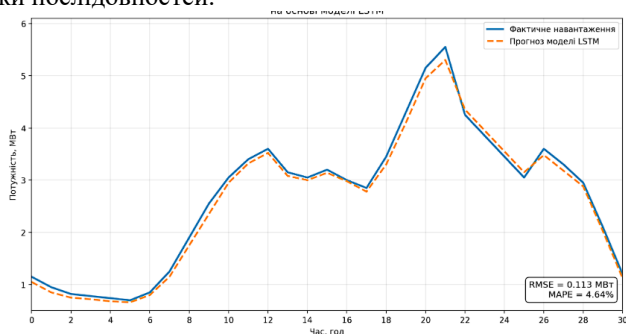


Рис. 1. Результати короткострокового прогнозування електроспоживання на основі моделі LSTM: порівняння фактичних і прогнозованих значень навантаження.

Процес побудови системи прогнозування включає збір, очищення та нормалізацію даних, формування інформативних ознак, вибір архітектури моделі, її навчання та валідацію. Якість прогнозу оцінюється за допомогою метрик похибки, серед яких найбільш уживаними є RMSE та MAPE. Отримані результати можуть бути інтегровані в автоматизовані системи керування для підтримки прийняття рішень у реальному часі.

Використання методів машинного навчання для прогнозування електроспоживання дає змогу підвищити точність оцінювання навантаження, оптимізувати режими роботи генерувальних потужностей, знизити витрати на паливо та підвищити ефективність інтеграції накопичувачів енергії й відновлюваних джерел. Отже, інтелектуальні методи аналізу даних є перспективним напрямом розвитку сучасної енергетики, а подальші дослідження мають бути спрямовані на підвищення точності, адаптивності та інтерпретованості прогнозних моделей.

Список використаних джерел:

1. Guo W., Che L., Shahidehpour M., Wan X. Machine-Learning based methods in short-term load forecasting. *The Electricity Journal*. 2021. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1040619020301767>.
2. Dewangan F., Abdelaziz A.Y., Biswal M. Load Forecasting Models in Smart Grid Using Smart Meter Information: A Review. *Energies*. 2023;16(3):1404. URL: <https://www.mdpi.com/1996-1073/16/3/1404>

УДК 004.896:004.93

*Антонюк О., здобувач,
Ткачук А.Г., к. т. н., доцент
Державний університет «Житомирська політехніка»*

ІНТЕЛЕКТУАЛЬНА СИСТЕМА АВТОНОМНОЇ НАВІГАЦІЇ МОБІЛЬНОГО РОБОТА НА ОСНОВІ КОМП'ЮТЕРНОГО ЗОРУ

У робототехніці важливою задачею є автономна навігація мобільних роботів без участі оператора. Такі системи застосовують у виробництві, логістиці, охороні та сервісі. Традиційні засоби навігації не завжди ефективні в закритих приміщеннях і часто є дорогими, тому перспективним рішенням є використання комп'ютерного зору на основі камери. Метою роботи є розроблення інтелектуальної системи автономної навігації мобільного робота на основі візуальних даних. Для цього передбачено отримання та обробку зображення, виявлення перешкод і формування команд керування рухом.

Принцип роботи системи полягає у послідовному опрацюванні візуальної інформації, що надходить з камери мобільного робота в режимі реального часу. На початковому етапі здійснюється захоплення відеопотоку та поділ його на окремі кадри для подальшого аналізу. Далі виконується попередня обробка зображення, яка включає фільтрацію шумів, покращення контрасту та стабілізацію візуальних характеристик сцени.

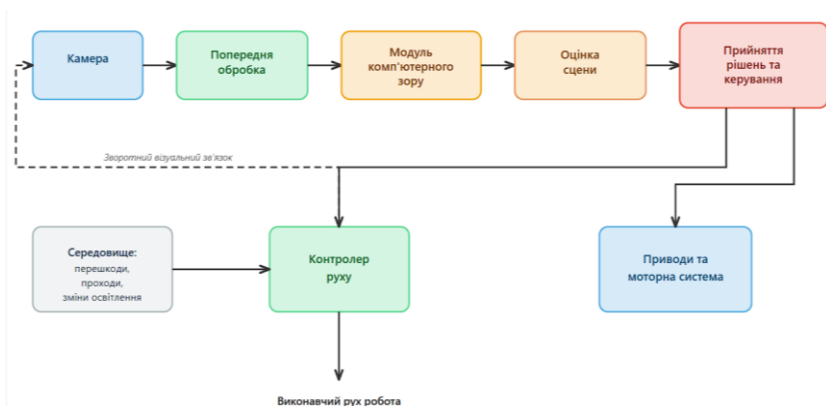


Рис. 1. Структурна схема інтелектуальної системи автономної навігації

Це дає змогу зменшити вплив зовнішніх завад, зокрема нерівномірного освітлення або дрібних візуальних спотворень, і

підвищити точність розпізнавання об'єктів. Після цього система переходить до етапу виділення інформативних елементів зображення, зокрема контурів, меж об'єктів та зон, що можуть відповідати потенційним перешкодам на шляху руху. На основі аналізу їхнього положення, форми та розмірів формується уявлення про поточний стан навколишнього середовища. Якщо центральна частина траєкторії залишається вільною, система генерує команду на подальший прямолінійний рух. У разі виявлення перешкоди виконується оцінювання доступного простору зліва та справа від робота, після чого обирається найбезпечніший напрямок обходу. Якщо ж безпечний маршрут відсутній, формується команда на зупинку.

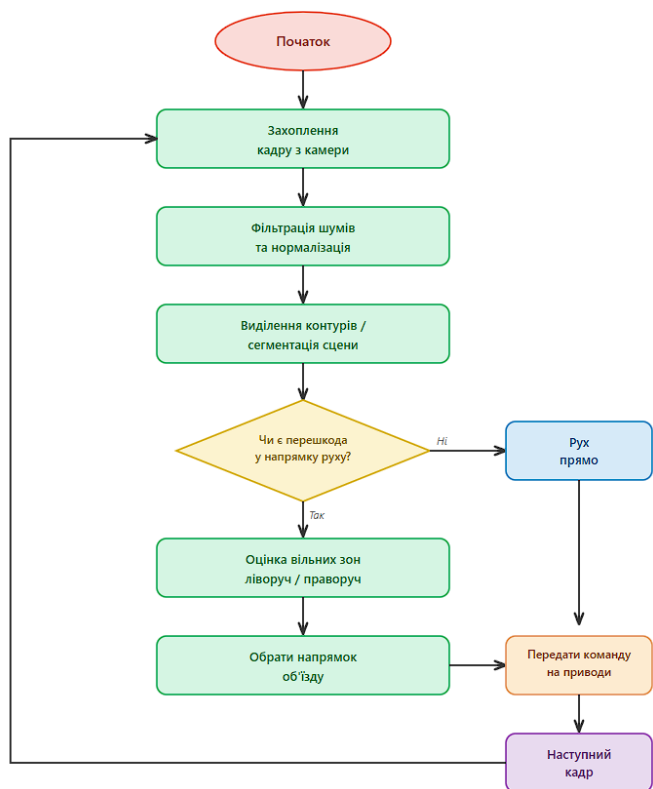


Рис.2. Блок-схема алгоритму автономної навігації

Наукова цінність роботи полягає у застосуванні методів комп'ютерного зору для реалізації недорогої та гнучкої системи

автономної навігації. Практична цінність полягає в можливості використання розробленого підходу в мобільних роботах освітнього, сервісного та промислового призначення. Експериментальна перевірка показала, що робот здатний орієнтуватися в приміщенні, виявляти перешкоди та змінювати траєкторію руху залежно від умов середовища.

Застосування комп'ютерного зору для автономної навігації мобільного робота є перспективним напрямом розвитку сучасних інтелектуальних робототехнічних систем. Подальше вдосконалення може бути пов'язане з використанням нейронних мереж і додаткових сенсорів для підвищення точності навігації.

Список використаних джерел:

1. Marroquín, A., García, G., Fabregas, E., Aranda-Escolástico, E., Fariás, G. Mobile Robot Navigation Based on Embedded Computer Vision. *Mathematics*, 2023, 11(11), 2561.
2. Katona, K., Neamah, H. A., Korondi, P. Obstacle Avoidance and Path Planning Methods for Autonomous Navigation of Mobile Robot. *Sensors*, 2024, 24(11), 3573.
3. Wang, S., Ahmad, N. S. AI-based approaches for improving autonomous mobile robot localization in indoor environments: A comprehensive review. 2025.
4. Rodríguez-Martínez, E. A., Flores-Fuentes, W., Achakir, F., Sergiyenko, O., Murrieta-Rico, F. N. Vision-Based Navigation and Perception for Autonomous Robots: Sensors, SLAM, Control Strategies, and Cross-Domain Applications—A Review. *Eng*, 2025, 6(7), 153.

УДК 681.5

*Вернидуб Б.Д., здобувач,
Кравчук А.Р., доцент,
Пуховський Є.С., д.т.н., професор
Державний університет «Житомирська політехніка»*

РОЗРОБКА СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ РІВНЕМ РІДИНИ В РЕЗЕРВУАРІ

Розробка системи автоматичного керування рівнем рідини в резервуарі є актуальним завданням промислової автоматизації, оскільки стабілізація рівня рідини належить до ключових умов надійного функціонування багатьох технологічних процесів у харчовій, хімічній та енергетичній галузях. Відхилення рівня від заданого значення може спричиняти порушення режимів роботи обладнання, погіршення якості продукції, зниження ефективності технологічного процесу та виникнення аварійних ситуацій. У зв'язку з цим доцільним є застосування автоматизованої системи керування, яка забезпечує безперервний контроль рівня рідини, його порівняння із заданим значенням та формування відповідного керуючого впливу на виконавчі механізми.

Об'єктом керування в такій системі є резервуар із рідиною, який характеризується інерційними властивостями, оскільки зміна рівня відбувається не миттєво, а в часі під впливом вхідних і вихідних потоків. Для вимірювання поточного значення рівня можуть застосовуватися ультразвукові або гідростатичні датчики, які забезпечують достатню точність і надійність контролю. Обробка виміряного сигналу та реалізація алгоритму регулювання здійснюються за допомогою програмованого логічного контролера або мікропроцесорної системи. Керуючий вплив передається на виконавчі механізми, зокрема на частотно-регульований електропривод насоса або електропривідну засувку, що дає змогу змінювати подачу рідини відповідно до поточних умов роботи системи.

З огляду на динамічні властивості об'єкта для забезпечення необхідної точності та стійкості доцільно використовувати ПІД-регулятор, закон керування якого описується виразом:

$$u(t) = K_p e(t) + K_i \int e(t) dt + K_d \frac{de(t)}{dt}, \text{ де } e(t) = h_{\text{зад}} - h(t)$$

Пропорційна складова забезпечує швидку реакцію системи на виникнення відхилення, інтегральна – усуває статичну похибку в усталеному режимі, а диференціальна – враховує швидкість зміни регульованої величини та підвищує якість перехідного процесу за рахунок зменшення перерегулювання.



Рис.1. Схема апаратної реалізації системи автоматичного керування

Функціонування системи автоматичного керування реалізується циклічно. На початковому етапі виконується ініціалізація датчиків і керуючого модуля, після чого система переходить у режим безперервного опитування вимірювального каналу. Отримане значення рівня порівнюється із заданим, на основі чого визначається похибка регулювання. Якщо поточний рівень відповідає встановленому режиму, насос працює в режимі підтримання або вимикається. У разі наявності відхилення контролер обчислює керуючий сигнал за ПІД-алгоритмом і подає його на виконавчий механізм, який змінює інтенсивність подачі або відведення рідини. Після цього цикл повторюється, що забезпечує безперервне автоматичне підтримання рівня в заданих межах.

Розроблена система може застосовуватися у водоочисних, харчових, хімічних та енергетичних установках, де потрібне точне регулювання рівня рідини. Її використання підвищує стабільність технологічних процесів, зменшує вплив людського фактора та забезпечує надійну роботу обладнання.

Список використаних джерел:

1. Achu Govind K.R., Mahapatra, S. *Improving precision and robustness in level control of coupled tank systems: A tree seed optimization and μ -analysis approach*. Results in Control and Optimization, 2024.

УДК 681.51:631.544.4

*Зіновчук О., здобувач,
Добржанський О.О., к.т.н., доцент
Державний університет «Житомирська політехніка»*

РОЗРОБКА СИСТЕМ АВТОМАТИЧНОГО КЕРУВАННЯ МІКРОКЛІМАТОМ У ТЕПЛИЦІ

Розробка систем автоматичного керування мікрокліматом у теплицях є важливим напрямом підвищення ефективності сучасного аграрного виробництва. Забезпечення оптимальних умов для росту рослин, таких як температура, вологість повітря, освітленість та рівень вуглекислого газу, безпосередньо впливає на врожайність, якість продукції та енергоефективність тепличних комплексів. На відміну від традиційного ручного контролю, автоматизовані системи дозволяють підтримувати стабільні параметри середовища незалежно від зовнішніх умов і мінімізують вплив людського фактора.

Типова структура системи автоматичного керування мікрокліматом включає сенсорну підсистему, що здійснює збір даних про параметри середовища (температура, вологість, освітленість, концентрація CO₂), виконавчі механізми (вентилятори, обігрівачі, системи зрошення, штори затінення) та центральний контролер, який реалізує алгоритми управління. Контролер аналізує отримані дані та формує керуючі сигнали для підтримання заданих параметрів у межах оптимальних значень.

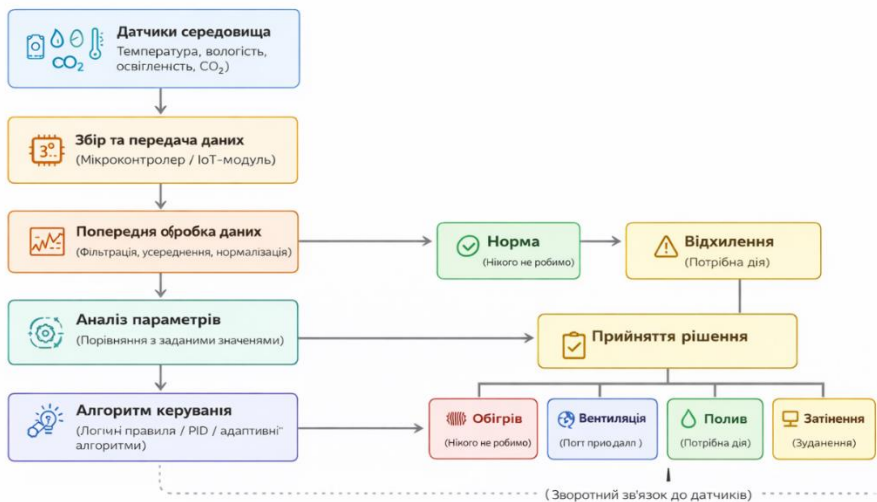


Рис.1. Структурна схема контролю мікрокліматом

У процесі функціонування система здійснює безперервний моніторинг стану мікроклімату та порівняння поточних показників із заданими значеннями. У разі виявлення відхилень за температурою, вологістю чи концентрацією вуглекислого газу негайно формується сигнал на контролер, який керує відповідним обладнанням. Це може реалізовуватися за допомогою включення систем крапельного поливу, відкриття вентиляційних фрамуг, активації теплогенераторів, систем туманоутворення або фітоосвітлення. На практиці це дозволяє автоматизувати підтримку ідеальних умов для росту рослин, оптимізувати витрати електроенергії та води, а також попередити розвиток хвороб, викликаних порушенням температурно-вологісного режиму.

Додатковою перевагою автоматизованих систем є можливість накопичення та аналізу історичних даних. Збір інформації про параметри мікроклімату та реакцію системи дозволяє оптимізувати режими роботи обладнання, прогнозувати зміни умов та підвищувати ефективність використання ресурсів. На основі цих даних можуть реалізовуватися адаптивні алгоритми керування, що враховують фазу росту рослин та сезонні особливості.

Інтеграція сучасних технологій, таких як Інтернет речей, хмарні сервіси та мобільні додатки, розширює функціональні можливості систем керування мікрокліматом. Це дозволяє здійснювати віддалений моніторинг і керування, отримувати сповіщення про аварійні ситуації та забезпечувати більш гнучке налаштування параметрів.

Впровадження систем автоматичного керування мікрокліматом у теплицях сприяє підвищенню врожайності, зниженню витрат ресурсів та забезпеченню стабільної якості продукції. Використання сучасних технологій автоматизації створює передумови для розвитку «розумного» сільського господарства та підвищення конкурентоспроможності аграрного сектору.

Список використаних джерел:

1. Chen, S. *A Review of Environmental Control Strategies and Models for Modern Agricultural Greenhouses* (2025).
2. Sacaleanu, D. I. та ін. *IoT-Enhanced Decision Support System for Real-Time Greenhouse Microclimate Monitoring and Control* (2024).
3. Tang, R., Aridas, N. K., Abu Talip, M. S. *Design of Wireless Sensor Network for Agricultural Greenhouse Based on Improved Zigbee Protocol* (2023).
4. Mahmood, F., Govindan, R., Bermak, A., Yang, D., Al-Ansari, T. *Data-driven robust model predictive control for greenhouse temperature control and energy utilisation assessment* (2023).

УДК 004.056:621.311

*Катков А.О., здобувач,
Покляченко О.В., старший викладач
Державний університет «Житомирська політехніка»*

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ОБ'ЄКТАМИ ЕЛЕКТРОЕНЕРГЕТИКИ

Сучасні об'єкти електроенергетики функціонують на основі комп'ютеризованих систем управління, зокрема SCADA-систем, автоматизованих систем диспетчерського керування та локальних підсистем контролю технологічних процесів. Поглиблення цифровізації, інтеграція таких систем у корпоративні мережі та використання віддаленого доступу підвищують ефективність керування енергетичними об'єктами, проте одночасно суттєво збільшують рівень кіберризиків. Наслідком реалізації кіберзагроз можуть стати порушення технологічних режимів, зниження надійності електропостачання, пошкодження обладнання та виникнення масштабних аварійних ситуацій.

До основних кіберзагроз для комп'ютеризованих систем управління в електроенергетиці належать несанкціонований доступ, шкідливе програмне забезпечення, атаки типу відмови в обслуговуванні, компрометація каналів передачі даних, а також цілеспрямовані атаки на об'єкти критичної інфраструктури. Особливу небезпеку становлять складні тривалі цільові атаки, які характеризуються прихованим проникненням у систему, закріпленням у мережі та подальшим впливом на технологічні процеси або інформаційні ресурси.

Метою дослідження є аналіз основних підходів до забезпечення кібербезпеки комп'ютеризованих систем управління об'єктами електроенергетики та визначення ефективних методів підвищення їх захищеності. Базовими напрямками захисту є сегментація мережевої інфраструктури, впровадження засобів виявлення та запобігання вторгненням, застосування криптографічного захисту даних, регулярне оновлення програмного забезпечення, а також реалізація рольового контролю доступу до ресурсів системи.

Одним із ключових принципів побудови захищеної інфраструктури є концепція багаторівневого захисту Defense in Depth, що передбачає формування декількох взаємодоповнювальних рубежів безпеки. Такий підхід дає змогу зменшити ймовірність успішної реалізації атаки навіть у разі компрометації окремого елемента системи. Додаткового значення набувають засоби моніторингу в реальному часі, аналізу журналів подій та виявлення аномальної активності, зокрема із застосуванням методів

машинного навчання, що підвищує оперативність виявлення потенційних інцидентів.

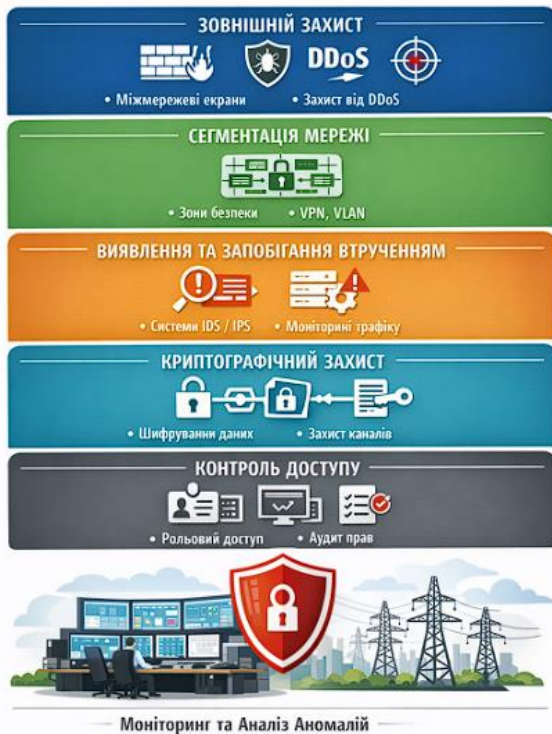


Рис.1. Ключові рівні багаторівневого кіберзахисту систем керування в електроенергетиці

Забезпечення кібербезпеки комп'ютеризованих систем управління в електроенергетиці є комплексним науково-технічним завданням, яке потребує узгодженого поєднання технічних, програмних та організаційних заходів. Реалізація сучасних підходів до захисту сприяє підвищенню стійкості енергетичної інфраструктури, надійності функціонування об'єктів електроенергетики та зниженню ризику кіберінцидентів.

Список використаних джерел:

1. Abdelkader, S., Amissah, J., Kinga, S., Mugerwa, G., Emmanuel, E., Mansour, D.-E. A., Bajaj, M., Blazek, V., Prokop, L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in Engineering, 2024.

УДК 629.735.33:004.93

*Кондур С.В., здобувач,
Ткачук Д.Ю., аспірантка
Державний університет «Житомирська політехніка»*

СИСТЕМА АВТОМАТИЧНОГО ВИЯВЛЕННЯ ТА ЛОКАЛІЗАЦІЇ ЛЮДИНИ ДРОНОМ У ПОШУКОВИХ ОПЕРАЦІЯХ

Швидкість і точність є визначальними чинниками ефективності пошуково-рятувальних операцій. Використання безпілотних літальних апаратів суттєво розширює можливості рятувальних служб, забезпечуючи оперативне обстеження великих і важкодоступних територій. Водночас традиційний підхід, за якого оператор вручну аналізує відеопотік з камери дрона, є виснажливим і знижує концентрацію уваги, що підвищує ймовірність пропуску об'єкта пошуку. Перспективним рішенням є застосування систем автоматичного виявлення на основі штучного інтелекту, які використовують методи комп'ютерного зору та глибокого навчання для аналізу зображень у реальному часі. Поєднання RGB-камери та тепловізійного сенсора забезпечує ефективне виявлення людини за різних умов спостереження, зокрема в темний час доби, за складного рельєфу або часткового маскування рослинністю.

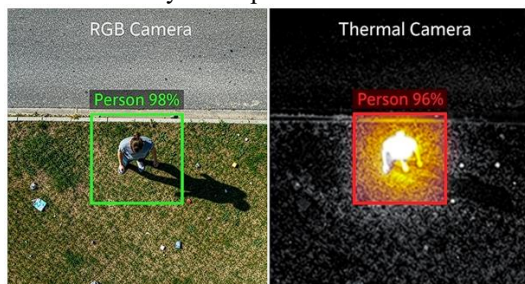


Рис.1. Виявлення людини за допомогою оптичного та тепловізійного сенсорів

Після успішного розпізнавання об'єкта на кадрі, критичним етапом є його точна геолокація. Система автоматично розраховує географічні координати знайденої людини. Для цього використовуються дані з GPS-модуля дрона, його висота (альтиметр), а також кут нахилу камери та орієнтація БПЛА у просторі (дані IMU). Згенеровані координати миттєво передаються на пульт управління рятувальної групи у вигляді мітки на цифровій мапі.

Застосування автоматизованого підходу суттєво зменшує час, необхідний для виявлення постраждалих, та нівелює вплив людського фактора. Згідно з результатами моделювання, використання нейромережових алгоритмів підвищує ймовірність виявлення об'єкта в умовах лісистій місцевості на значний відсоток порівняно з ручним візуальним пошуком [1].

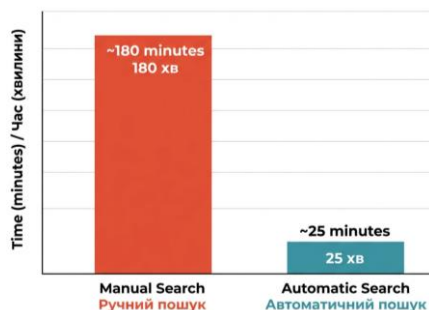


Рис. 2 Порівняння часу обстеження території (хв/кв. км)

Порівняльний аналіз методів пошуку з використанням БПЛА засвідчує суттєву перевагу автоматизованих систем на основі RGB-камери та тепловізора над ручним моніторингом оператором. В умовах відкритої місцевості вдень точність автоматизованого виявлення досягає 96 %, тоді як за ручного спостереження становить близько 75 %. У нічний час та за складних умов ефективність ручного моніторингу різко знижується, тоді як автоматизована система зберігає високі показники виявлення понад 85 %. Додатковими перевагами автоматизованого підходу є відсутність впливу людського фактора, обробка даних у режимі реального часу та підвищена точність визначення координат об'єкта. Ефективність такої системи залежить від продуктивності бортового обчислювального модуля або стабільності каналу зв'язку, якості сенсорів і рівня попереднього навчання моделі на спеціалізованих наборах даних. Інтеграція автоматизованих систем пошуку у практику рятувальних підрозділів є перспективним напрямом підвищення оперативності реагування та ефективності пошуково-рятувальних операцій.

Список використаних джерел:

1. R. Gašiorowski, et al. "Search and Rescue Operations Using Drones and Computer Vision." – IEEE Access. URL: <https://ieeexplore.ieee.org/> (дата звернення: 19.03.2026).

УДК 681.5:621.311

*Шпаківський, здобувач,
Ткачук А.Г., к. т. н., доцент
Державний університет «Житомирська політехніка»*

ПОБУДОВА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ КЕРУВАННЯ ЕЛЕКТРИЧНИМ НАВАНТАЖЕННЯМ ПРОМИСЛОВИХ ЕНЕРГЕТИЧНИХ КОМПЛЕКСІВ

Сучасні промислові енергетичні комплекси потребують впровадження комп'ютеризованих систем керування електричним навантаженням, орієнтованих на підвищення енергоефективності, стабілізацію режимів електроспоживання та зниження експлуатаційних витрат. Побудова таких систем базується на інтеграції засобів мікропроцесорної техніки, інформаційно-вимірювальних пристроїв і програмно-апаратних платформ у єдине інформаційне середовище підприємства. Це забезпечує безперервний моніторинг параметрів електроспоживання, оперативний аналіз навантаження та автоматичне регулювання режимів роботи енергетичного обладнання в реальному часі.

Актуальність впровадження комп'ютеризованих систем зумовлена нерівномірністю графіків електричного навантаження на більшості промислових підприємств, що призводить до перевищення договірних лімітів потужності та збільшення фінансових витрат. Ефективним рішенням є застосування тривірневої ієрархічної архітектури, у якій нижній рівень представлений інтелектуальними датчиками та багатофункціональними лічильниками, що здійснюють вимірювання потужності, енергії та показників якості електроенергії. Середній рівень формують програмовані логічні контролери та комунікаційні шлюзи, які реалізують збір даних, локальну обробку інформації та алгоритми автоматичного обмеження або перерозподілу навантаження в критичних режимах. Верхній рівень включає серверні засоби, SCADA-платформи та програмне забезпечення для візуалізації, архівування, диспетчерського аналізу й планування енергоспоживання.

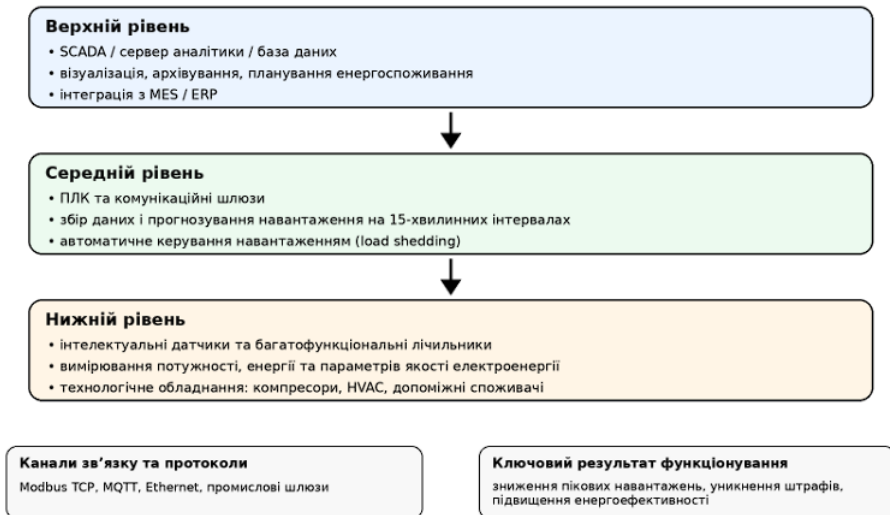


Рис. 1. Архітектура тривірневої КСКЕН для моніторингу, прогнозування та автоматичного керування електричним навантаженням

Практична реалізація системи доцільна на базі контролерів із підтримкою промислових протоколів обміну даними, зокрема Modbus TCP або MQTT, що забезпечує інтеграцію енергетичного обладнання із загальною системою управління підприємством. Основу функціонування становить прогнозування електричного навантаження на коротких часових інтервалах з подальшим автоматичним коригуванням режимів роботи допоміжних споживачів без порушення основного технологічного процесу. Такий підхід дозволяє перейти від пасивного обліку електроенергії до активного керування попитом, що формує передумови для впровадження принципів Smart Grid на рівні окремого промислового об'єкта.

Список використаних джерел:

1. Yasmin, R., Bors, D., et al. A Survey of Commercial and Industrial Demand Response Flexibility with Energy Storage Systems and Renewable Energy. Sustainability, 2024, 16(2), 731.
2. Eckhoff, J., Wadhwa, S., Fette, M., Wulfsberg, J. P., Wanigasekara, C. Electrical Load Forecasting in the Industrial Sector: A Literature Review of Machine Learning Models and Architectures for Grid Planning. Energies, 2026, 19(2), 538.

УДК 629.735.33:004.93:004.8

*Яременко Д., здобувач,
Ткачук Д.Ю., аспірантка
Державний університет «Житомирська політехніка»*

РОЗРОБКА СИСТЕМИ УНИКНЕННЯ ПЕРЕШКОД ДЛЯ АВТОНОМНОГО ДРОНА З ВИКОРИСТАННЯМ ГЛИБИННОГО НАВЧАННЯ

Стрімкий розвиток безпілотних літальних апаратів зумовлює підвищення вимог до надійності, автономності та адаптивності навігаційних систем. Одним із ключових завдань автономного польоту є своєчасне виявлення та уникнення перешкод у динамічному й неструктурованому середовищі. Традиційні підходи, що ґрунтуються на класичних методах обробки зображень або використанні простих сенсорів, характеризуються обмеженою точністю, недостатньою швидкістю та низькою стійкістю до змін умов експлуатації. У зв'язку з цим перспективним напрямом є застосування методів глибокого навчання, які забезпечують підвищення робастності системи та її здатності функціонувати в реальному середовищі.

Метою роботи є розробка системи уникнення перешкод для автономного дрона на основі алгоритмів глибокого навчання, здатної забезпечувати навігацію в режимі реального часу без попередньої побудованої карти середовища. Об'єктом дослідження є процес автономної навігації БПЛА в середовищі з перешкодами, а предметом – методи та алгоритми глибокого навчання для виявлення перешкод і коригування траєкторії польоту.

Запропонована система побудована на основі архітектури YOLOv8, адаптованої для обробки даних RGB-D-камери. Вхідними даними є потік кольорових зображень і карта глибини, що формуються в реальному часі. На основі їх аналізу система виділяє вільні та небезпечні зони простору, після чого модуль планування траєкторії генерує керуючі сигнали для польотного контролера. Для побудови безпечної траєкторії використано поєднання методу потенційних полів і прогностичної моделі руху дрона, що дозволяє враховувати як статичні, так і динамічні перешкоди. Програмна реалізація інтегрована з PX4 та ROS2, що забезпечує модульність і можливість адаптації до різних типів безпілотних платформ.

Оцінювання ефективності системи виконувалося в середовищі Gazebo за сценаріями різного рівня складності. Результати моделювання показали, що система забезпечує успішне уникнення перешкод у 94,7 % випадків при швидкості польоту до 8 м/с, а затримка між виявленням перешкоди та формуванням керуючого сигналу не

перевищує 35 мс. Це підтверджує придатність розробленого рішення до застосування в системах реального часу. Порівняно з традиційними підходами запропонована система демонструє вищу точність виявлення та кращу адаптивність до складних умов середовища.

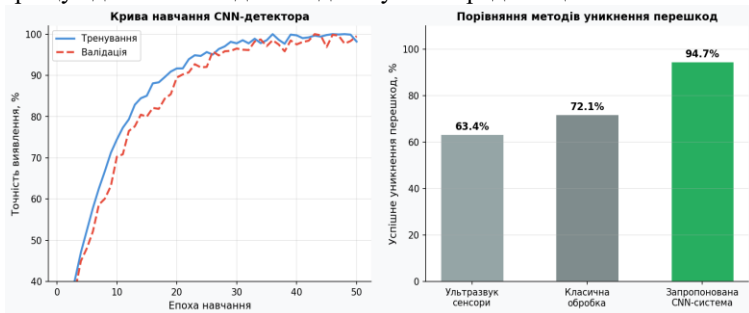


Рис.2. Порівняння ефективності методів уникнення перешкод та крива навчання CNN

Наукова новизна роботи полягає у розробленні методу комбінованої обробки RGB-D-даних із використанням полегшеної нейронної мережі, оптимізованої для вбудованих обчислювальних платформ. Практична цінність розробки полягає у можливості її застосування в пошуково-рятувальних операціях, інспекції інфраструктури та автономній доставці. Запропонований підхід забезпечує ефективну навігацію БПЛА в невідомому середовищі та має переваги за показниками точності, швидкодії й адаптивності.

Список використаних джерел:

1. Dai X., Mao Y., Huang T., Qin N., Huang D., Li Y. Automatic obstacle avoidance of quadrotor UAV via CNN-based learning. *Neurocomputing*. 2020. Vol. 402. P. 346–358. DOI: 10.1016/j.neucom.2020.04.020.
2. Xue Z., Gonsalves T. Vision Based Drone Obstacle Avoidance by Deep Reinforcement Learning. *AI*. 2021. Vol. 2, No. 3. P. 366–380. DOI: 10.3390/ai2030023.
3. Katkuri A. V. R., Madan H., Khatri N., Abdul-Qawy A. S. H., Patnaik K. S. Autonomous UAV navigation using deep learning-based computer vision frameworks: A systematic literature review. *Array*. 2024. Article 100361. DOI: 10.1016/j.array.2024.100361.
4. Debnath D., Vanegas F., Sandino J., Hawary A. F., Gonzalez F. A Review of UAV Path-Planning Algorithms and Obstacle Avoidance Methods for Remote Sensing Applications. *Remote Sensing*. 2024. Vol. 16, No. 21. Article 4019. DOI: 10.3390/rs16214019.

УДК 681.5:621.316.1

*Токовий Д.А., здобувач,
Покляченко О.В., старший викладач*
Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНА СИСТЕМА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В РОЗПОДІЛЬНИХ МЕРЕЖАХ

Сучасні розподільні електричні мережі працюють в умовах зростання частки нелінійних навантажень, силовій електроніки та розосередженої генерації, що ускладнює забезпечення належної якості електричної енергії. Відхилення напруги, гармонічні спотворення, несиметрія фаз і провали напруги негативно впливають на надійність роботи обладнання та зумовлюють додаткові економічні втрати. Тому актуальним є впровадження автоматизованих систем, здатних у режимі реального часу контролювати показники якості електроенергії та формувати керуючі впливи для їх нормалізації. Метою роботи є розробка автоматизованої системи забезпечення якості електричної енергії в розподільних мережах, що поєднує засоби вимірювання, обробки даних, оцінювання параметрів мережі та автоматичного керування компенсувальними пристроями. Запропонований підхід забезпечує безперервний моніторинг параметрів мережі, виявлення відхилень і автоматичне формування рішень щодо стабілізації напруги, зменшення гармонічних спотворень і підвищення симетрії фазних навантажень.

Функціональна структура системи включає підсистему вимірювання, комунікаційну підсистему, аналітичний модуль, модуль прийняття рішень та виконавчу підсистему. На нижньому рівні використовуються цифрові аналізатори якості електроенергії, інтелектуальні лічильники та датчики струму й напруги, що здійснюють синхронізований збір миттєвих і усереднених значень параметрів мережі. На середньому рівні реалізується передавання даних до контролера або SCADA-системи, де виконуються розрахунок показників якості та ідентифікація аварійних або передаварійних режимів. Верхній рівень забезпечує формування керуючих сигналів для регулювання положення відпаса трансформатора, ввімкнення батарей статичних конденсаторів, активних фільтрів гармонік, компенсаційних пристроїв типу STATCOM або алгоритмів керування навантаженням.

Відповідно до сучасних стандартів контролю якості електричної енергії система повинна забезпечувати вимірювання та інтерпретацію таких параметрів, як частота мережі, діюче значення напруги, флікер, провали та перенапруги, перерви електропостачання, несиметрія

напруг, гармоніки та інтергармоніки. Для оцінювання рівня гармонічних спотворень може використовуватися показник повного коефіцієнта гармонічних спотворень напруги:

$$THD_U = \frac{\sqrt{\sum_{n=2}^N U_n^2}}{U_1} \cdot 100\%$$

де U_1 – діюче значення основної гармоніки напруги, U_n – діючі значення вищих гармонік. Застосування такого показника дає змогу кількісно оцінити ступінь спотворення синусоїдальної форми напруги та використовувати його як один із критеріїв прийняття керуючих рішень. Для комплексної оцінки стану мережі доцільно використовувати інтегральний критерій якості електричної енергії:

$$J = w_1 \left(\frac{\Delta U}{\Delta U_{\text{доп}}} \right)^2 + w_2 \left(\frac{THD_U}{THD_{U,\text{доп}}} \right)^2 + w_3 \left(\frac{k_{2U}}{k_{2U,\text{доп}}} \right)^2$$

де ΔU – відхилення напруги від номінального значення; THD_U – коефіцієнт гармонічних спотворень; k_{2U} – коефіцієнт несиметрії; w_1, w_2, w_3 – вагові коефіцієнти відповідних показників. Мінімізація критерію J дає змогу реалізувати автоматичний вибір керуючих дій залежно від характеру порушення. Наприклад, при перевищенні допустимого відхилення напруги система може змінювати коефіцієнт трансформації або підключати компенсувальні засоби, а при зростанні гармонічних спотворень – активувати фільтрокомпенсувальні пристрої.

Особливістю автоматизованої системи є циклічний принцип функціонування. На першому етапі здійснюється вимірювання параметрів мережі в контрольних вузлах. Далі виконується нормалізація, фільтрація та аналітична обробка даних, після чого формується висновок про поточний рівень якості електричної енергії. У разі виявлення відхилень модуль керування визначає тип порушення, обирає оптимальний спосіб корекції та передає команду виконавчим пристроям. Після реалізації керуючого впливу здійснюється повторний контроль параметрів, що забезпечує замкнений контур автоматизованого регулювання. Такий підхід дозволяє перейти від пасивного моніторингу до активного керування якістю електроенергії у розподільній мережі.

Список використаних джерел:

1. IEC. IEC 61000-4-30:2025. Electromagnetic compatibility (EMC) – Part 4-30: Testing and measurement techniques – Power quality measurement methods. 2025.

УДК 004.8:530.12:004.056

*Кучма Ю.В., к.т.н., доцент,
ТОВ Приватний вищий навчальний заклад «УНІВЕРСИТЕТ
СУЧАСНИХ ТЕХНОЛОГІЙ»*

МОДЕЛЮВАННЯ НЕЛІНІЙНОЇ ДИНАМІКИ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ НА КВАНТОВИХ СИМУЛЯТОРАХ

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням складності інформаційних процесів, які реалізуються в кіберфізичних, розподілених та інтелектуальних системах. Такі процеси вирізняються високою розмірністю простору станів, наявністю багаторівневих зворотних зв'язків, стохастичних збурень і взаємодією когерентних та некогерентних компонентів. У класичних обчислювальних середовищах точне моделювання подібних процесів у режимі реального часу є обмеженим через експоненційне зростання обчислювальної складності [1].

У цьому контексті квантові симулятори розглядаються як перспективна обчислювальна платформа, здатна відтворювати динаміку складних систем на фундаментальному фізичному рівні. Їх використання відкриває нові можливості для формалізованого аналізу нелінійних інформаційних процесів, зокрема тих, що виникають у задачах кібербезпеки, адаптивного керування, криптографічного захисту та підтримки прийняття рішень у динамічних середовищах.

Актуальність дослідження також зумовлена необхідністю розроблення узагальненого математичного апарату, який дозволяє поєднати квантову динаміку, класичні алгоритми керування та адаптивні механізми оптимізації в межах єдиної моделі [2].

Квантові симулятори призначені для відтворення еволюції відкритих квантових систем з урахуванням шумових процесів, дисипації та керованих нелінійних ефектів. На відміну від універсальних квантових комп'ютерів, симулятори орієнтовані на дослідження конкретних класів динамічних систем і дозволяють більш ефективно використовувати обмежені квантові ресурси.

У задачах моделювання інформаційних процесів квантові симулятори забезпечують природну реалізацію багатовимірних просторів станів і операторної динаміки. Це дозволяє адекватно описувати як когерентні інформаційні потоки, так і некогерентні процеси втрат, завад і атак. Особливу роль відіграє можливість врахування стан-залежних ефектів, що є характерною ознакою адаптивних інформаційних систем [3].

1. Математичні засади моделювання нелінійної динаміки.

Для формалізованого опису нелінійної адаптивної динаміки інформаційних процесів вводиться багатовимірний простір станів, який задається як тензорний добуток гільбертових просторів окремих підсистем

$$\mathcal{H} = \bigotimes_{i=1}^N \mathcal{H}_i, \quad (1)$$

де $\mathcal{H}_i$ – гільбертів простір відповідає i -тій підсистемі, а N – визначає їх кількість. Така структура дозволяє моделювати ієрархічні взаємодії між підсистемами та враховувати як локальні, так і колективні ефекти [4].

2. Простір керування та адаптивні механізми

Адаптивна перебудова динаміки реалізується через параметричний простір керування $\mathcal{U}$, який визначає множину допустимих операторів впливу на систему

$$\mathcal{U} = \{\hat{K}(t) \in \mathcal{L}(\mathcal{H})\}, \quad (2)$$

де $\hat{K}(t)$ – оператор керування, що модулює еволюцію стану системи відповідно до поточного стану та історії вимірювань. Представлений простір формалізує адаптивні алгоритми керування.

Важливо наголосити, що ключовим елементом цього математичного апарата є щільнісний оператор $\hat{\rho}(t)$, який визначає стан системи в багатовимірному гільбертівському просторі $\mathcal{H}$. Саме використання щільнісного оператора дозволяє формально враховувати суперпозиції, квантову когерентність, а також ефекти декогеренції, що виникають через взаємодію з оточенням і шумові процеси.

Другим ключовим компонентом є оператор керування $\hat{K}(t)$, який формалізує динамічне втручання класичної підсистеми в еволюцію квантового стану. Параметричний простір керування $\mathcal{U}$ визначає множину допустимих операторів і дозволяє математично формалізувати адаптивні алгоритми, що реагують на поточний стан системи та історію квантових вимірювань. Наявність такого оператора забезпечує нелінійний контур зворотного зв'язку, у якому результати вимірювань активно впливають на подальшу динаміку системи.

3. Рівняння еволюції та нелінійні ефекти.

Рівняння еволюції системи враховує як когерентну еволюцію через стан-залежний гамільтоніан, так і дисипативні та адаптивні ефекти через оператори.

$$\frac{d\hat{\rho}(t)}{dt} = -i [\hat{H}(t, \hat{\rho}), \hat{\rho}(t)] + D[\hat{\rho}(t)] + F(\hat{\rho}(t), \hat{K}(t)), \quad (3)$$

де $\hat{H}(t, \hat{\rho})$ – стан-залежний гамільтоніан, $D[\hat{\rho}(t)]$ – дисипативний оператор, $F(\hat{\rho}(t), \hat{K}(t))$ – оператор нелінійного адаптивного впливу.

Така модель відображає використання інформації про стан системи для корекції подальшої еволюції, що є характерним для інтелектуальних і самоналаштовуваних інформаційних систем.

4. Цільова функція оптимізації.

Для кількісної оцінки ефективності керування вводиться цільова функція

$$J[\hat{K}(t)] = \int_0^T \text{Tr} \{ \hat{\rho}(t) \hat{O}_{\text{target}} \} dt - \lambda \int_0^T \| \hat{K}(t) \|^2 dt \rightarrow \max, \quad (4)$$

де $\hat{O}_{\text{target}}$ – оператор цільової характеристики, λ – коефіцієнт штрафу за ресурси, T – кінцевий час моделювання.

Така постановка дозволяє аналізувати компроміс між досягненням заданих інформаційних властивостей і вартістю керування.

5. Варіаційні алгоритми та дискретизація керування

Практична реалізація оптимального керування на квантових симуляторах здійснюється з використанням варіаційних квантово-класичних алгоритмів.

Дискретизація операторів керування через градієнтне оновлення забезпечує реалізацію варіаційних алгоритмів, які є квантово-класичними гібридними схемами адаптивного управління

$$\hat{K}_{n+1} = \hat{K}_n + \eta \frac{\partial J[\hat{K}_n]}{\partial \hat{K}_n}, \quad (5)$$

де n – номер дискретного кроку, η – адаптивний крок, $\partial J / \partial \hat{K}_n$ – градієнт цільової функції.

Отже, запропонований математичний апарат забезпечує формалізоване моделювання високорозмірних, нелінійних та адаптивних інформаційних процесів в умовах динамічної невизначеності, дозволяючи оцінювати стійкість криптографічних механізмів, оптимізувати параметри захищених каналів та досліджувати сценарії активної протидії. При цьому результати квантових вимірювань та адаптивні дії класичних операторів формують нелінійний контур зворотнього зв'язку [4], що забезпечує контекстно-залежну перебудову алгоритмічних і протокольних рішень у режимі реального часу, підвищуючи живучість та стійкість інформаційних і комунікаційних систем.

Необхідно зазначити, що комплексне поєднання квантових і класичних компонентів [5], створює теоретичну основу для побудови адаптивних алгоритмів оптимізації та високопродуктивних квантово-класичних симуляторів, дозволяючи аналізувати ефективність,

стійкість і адаптивність систем у складних кібербезпекових середовищах.

Таким чином, запропонований підхід формує платформу для моделювання, аналізу та оптимізації нелінійних інформаційних процесів, інтегруючи методи квантового моделювання з класичними алгоритмами керування з перспективою для підвищення стійкості, живучості та безпеки інформаційних мереж у динамічних умовах загроз.

Список використаних джерел:

1. Живилю, Є., & Кучма, Ю. (2025). DEEP LEARNING-МОДЕЛЬ ПРОГНОЗУВАННЯ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ БЕЗПЕКИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 589–601. <https://doi.org/10.28925/2663-4023.2025.31.1050>
2. NIST: Post-Quantum Cryptography (PQC) Project і NIST Releases First 3 Finalized Post-Quantum Encryption Standards, <https://csrc.nist.gov/projects/post-quantum-cryptography>.
3. Фесенко, Т., & Калашнікова, Ю. (2025). ФЕДЕРАТИВНА GNN-ХАІ МОДЕЛЬ ПРОГНОЗУ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У ZERO TRUST-СЕРЕДОВИЩІ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 602–619. <https://doi.org/10.28925/2663-4023.2025.31.1049>
4. Zhyvylo, Y., & Kuchma, Y. (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. Collection “Information Technology and Security”, 13(2), 162–177. <https://doi.org/10.20535/2411-1031.2025.13.2.344591>
5. Фесенко, Т., та Калашникова, Ю. (2025). Математичні аспекти спільного застосування алгоритму AES та стеганографічних методів у захисті ключів автентифікації. Збірник «Інформаційні технології та безпека», 13 (2), 178–191. <https://doi.org/10.20535/2411-1031.2025.13.2.344592>.

УДК 530.145:004.8:004.056:517.9

Живило Є.О., к.н. з держ.упр., доцент

*Національний університет «Полтавська політехніка імені Юрія
Кондратюка»*

НЕЛІНІЙНІ КВАНТОВІ ІНФОРМАЦІЙНІ ПРОЦЕСИ В АДАПТИВНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ НОВОГО ПОКОЛІННЯ

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням складності електронно-комунікаційних систем, зокрема тих, що використовуються в критично важливих інфраструктурах та мережах Сил оборони і безпеки України. Інтенсивна цифровізація, перехід до сервісно-орієнтованих і розподілених архітектур, інтеграція гетерогенних мереж зв'язку, а також зростаюча роль автоматизованих систем підтримки прийняття рішень формують принципово нові вимоги до стійкості, надійності та безпеки обчислювальних процесів.

Додатковим чинником ускладнення є постійна дія багатофакторної невизначеності, що включає випадкові шумові процеси, цілеспрямовані кібернетичні та фізичні атаки, обмеженість обчислювальних і енергетичних ресурсів, а також динамічну зміну топології та параметрів мереж [1]. У таких умовах класичні підходи до проєктування та аналізу інформаційних систем дедалі частіше виявляються недостатніми, що стимулює пошук нових парадигм обчислень і керування.

Одним із перспективних напрямів є використання квантових та гібридних квантово-класичних технологій. Розвиток квантових обчислень, квантових комунікацій і постквантових криптографічних механізмів зумовлює необхідність формування математичних моделей, здатних адекватно описувати еволюцію квантових станів у відкритих, керованих і адаптивних системах [2]. Особливого значення набувають нелінійні квантові інформаційні процеси, які виникають унаслідок взаємодії системи з середовищем, процедур вимірювання та контурів зворотного зв'язку.

У класичній квантовій механіці еволюція ізольованої системи описується лінійним рівнянням Шредінгера або, у випадку змішаних станів, лінійним рівнянням фон Неймана. Проте реальні обчислювальні системи є відкритими та функціонують у взаємодії з середовищем, що призводить до появи дисипації, декогеренції та стохастичних ефектів. Додатково, в адаптивних системах результати вимірювань використовуються для корекції подальшої еволюції, формуючи контури активного зворотного зв'язку.

Саме наявність таких контурів зворотного зв'язку є ключовою причиною виникнення ефективної нелінійності квантової динаміки. Нелінійність у цьому контексті не суперечить фундаментальним постулатам квантової механіки, а є наслідком умовної еволюції стану, параметричної залежності гамільтоніана від поточного стану та адаптивного керування процесами вимірювання й обробки інформації.

Таким чином, нелінійні квантові інформаційні процеси слід розглядати як природний інструмент опису функціонування адаптивних обчислювальних систем нового покоління, у яких квантова динаміка, інформаційні потоки та алгоритми керування утворюють єдину взаємопов'язану систему.

Простір станів та адаптація. Нехай стан складеної квантової системи описується щільнісним оператором

$$\rho(t) \in D(H), \quad H = \bigotimes_{i=1}^N H_i, \quad (1)$$

де H – гільбертів простір складеної системи, а $D(H)$ – множина допустимих квантових станів. Такий підхід дозволяє коректно враховувати як чисті, так і змішані стани, а також ефекти декогеренції та шуму. За цих умов адаптація в системі реалізується через вектор керування

$$\mathbf{u}(t) \in \mathcal{U} \subset \mathbb{R}^m \quad (2)$$

визначає параметри гамільтоніана, операторів вимірювання, а також характеристики квантових каналів і класичних обчислювальних процедур. На відміну від статичних схем керування, у розглянутому підході вектор $\mathbf{u}(t)$ формується динамічно на основі поточного стану системи та результатів проміжних вимірювань. Це забезпечує можливість оперативної реакції на зміну зовнішніх умов і внутрішнього стану системи.

Узагальнене рівняння нелінійної квантової динаміки. Для опису еволюції стану адаптивної квантової системи доцільно використовувати узагальнене нелінійне рівняння Ліндблада, у якому як унітарна, так і дисипативна частини динаміки можуть залежати від стану системи

$$\begin{aligned} \frac{d\rho(t)}{dt} = & -i \left[H_0 + \sum_j u_j(t) H_j + H_{nl}(\rho(t)), \rho(t) \right] + \\ & + \sum_k \gamma_k(\rho(t), \mathbf{u}(t)) (L_k(\rho(t)) \rho L_k^\dagger(\rho(t)) - \frac{1}{2} \{L_k^\dagger L_k, \rho\}) \end{aligned} \quad (3)$$

де H_0 – базовий гамільтоніан, H_j – керуючі гамільтоніани, $H_{nl}(\rho)$ – стан-залежний нелінійний гамільтоніан, $L_k(\rho)$ та $\gamma_k(\rho, \mathbf{u})$ визначають нелінійні дисипативні процеси та вплив середовища.

Така модель дозволяє врахувати вплив керуючих дій, умовних вимірювань і нелінійних ефектів, що виникають у процесі адаптації.

Нелінійний характер рівняння відображає використання інформації про стан системи для корекції її подальшої еволюції. З математичної точки зору це призводить до ускладнення аналізу стійкості та оптимальності, проте водночас відкриває можливості для більш гнучкого й ефективного керування квантовими інформаційними процесами.

Постановка задачі оптимального керування. Виконання завдання у межах запропонованої моделі є синтез закону адаптивного керування $\mathbf{u}^*(t)$, який забезпечує оптимальну еволюцію стану $\rho(t)$ протягом інтервалу часу $t \in [0, T]$, починаючи з $\rho(0) = \rho_0$. Тому цільова функція має вигляд:

$$J(\mathbf{u}) = \mathbb{E}[\Phi(\rho(T), \rho_{target}) + \int_0^T (\mathcal{C}(\rho(t)) + \lambda \mathcal{R}(\mathbf{u}(t))) dt], \quad (4)$$

де Φ – відхилення кінцевого стану від цільового, $\mathcal{C}(\rho)$ – поточний функціонал якості (когерентність, ентропія, точність обчислень), $\mathcal{R}(\mathbf{u})$ – регуляризація витрат ресурсів, а λ – коефіцієнт компромісу між точністю та витратами керування. Саме введення інтегральної цільової функції дозволяє систематично аналізувати компроміси між ефективністю обчислень, стійкістю до зовнішніх впливів і вартістю керування. Це є особливо важливим для систем оборонного призначення, де ресурси є обмеженими, а вимоги до надійності та безпеки – критично високими [3].

Інтеграція з варіаційними квантовими алгоритмами та квантовими нейромережами. У випадку варіаційних квантових алгоритмів стан системи параметризується як

$$\rho(\theta) = U(\theta)\rho_0 U^\dagger(\theta), \quad (5)$$

де θ – вектор варіаційних параметрів. Оновлення θ на основі вимірювань реалізує нелінійну адаптацію системи відповідно до цільової функції. Аналогічні погляди застосовуються й у квантових нейромережах, де параметри керування інтерпретуються як вагові коефіцієнти, а нелінійність динаміки відіграє роль функцій активації. Отже це створює передумови для використання квантових методів машинного навчання в задачах обробки інформації, прогнозування та підтримки прийняття рішень у складних динамічних середовищах.

Розглянутий підхід формує теоретичне підґрунтя для розроблення адаптивних квантових і гібридних квантово-класичних обчислювальних систем, орієнтованих на роботу в умовах інтенсивних зовнішніх збурень і загроз. Зокрема, він може бути використаний для аналізу та синтезу систем захищеного зв'язку, квантово-стійких механізмів автентифікації, а також інтелектуальних систем керування в оборонних інформаційних інфраструктурах.

Подальші дослідження доцільно спрямувати на вивчення стійкості запропонованих моделей до різних класів атак [4], розроблення чисельних методів розв'язання нелінійних рівнянь квантової динаміки та експериментальну верифікацію ефективності адаптивних квантових алгоритмів у реальних або наближених до реальних умовах функціонування.

Список використаних джерел:

1. International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 24760-1:2025 Information security, cybersecurity and privacy protection – A framework for identity management. Part 1: Core concepts and terminology (3rd ed.). <https://www.iso.org/standard/24760-1>.
2. Фесенко, Т., та Калашникова, Ю. (2025). Математичні аспекти спільного застосування алгоритму AES та стеганографічних методів у захисті ключів автентифікації. Збірник «Інформаційні технології та безпека», 13 (2), 178–191. <https://doi.org/10.20535/2411-1031.2025.13.2.344592>.
3. Фесенко Т., Калашнікова Ю. Використання Cisco SecureX для SOC-автоматизації. *Системи управління, навігації та зв'язку*. 2025. № 4 (82). С. 138–143. DOI: <https://doi.org/10.26906/SUNZ.2025.4.138>. URL: <https://journals.nupp.edu.ua/sunz/article/view/4119> (дата звернення: 04.02.2026).
4. NIST: Post-Quantum Cryptography (PQC) Project і NIST Releases First 3 Finalized Post-Quantum Encryption Standards, <https://csrc.nist.gov/projects/post-quantum-cryptography>.

УДК 519.718

*Сеснедес Гарсія П.Д., наук. співробітник,
Сеснедес Гарсія Н.В., наук. співробітник*

Інститут проблем математичних машин і систем НАН України

ОЦІНКА ЗАЛИШКОВОГО РЕСУРСУ ТРУБОПРОВОДІВ З УРАХУВАННЯМ КОРОЗІЙНИХ ЗОН

Запропонована методологія прогнозування залишкового ресурсу трубопроводів базується на застосуванні ймовірнісно-фізичної моделі відмов, що використовує статистичні або прогнозні дані для визначення її параметрів. Модель описується дифузійно-монотонним *DM*-розподілом і дозволяє визначати як наробіток до граничного стану за заданою ймовірністю, так і ймовірність відмови за заданий період.

За обмеженої або відсутньої статистики застосовуються альтернативні підходи для визначення параметрів *DM*-розподілу: детерміністичний метод стандарту API 570 [1] для прогнозування швидкості розвитку дефекту та підхід ASME B31G [2] для встановлення граничного значення його розміру. За цими методами визначають розрахунковий тиск руйнування і оцінюють допустимість дефекту відносно робочого тиску. Для кородованого трубопроводу граничний стан визначається глибиною корозії або товщиною стінки і використовується як критерій відмови при ймовірнісному моделюванні часу його досягнення. Це значення застосовується у моделі дифузійно-монотонного *DM*-розподілу відмов за ДСТУ 8646:2016 для оцінки залишкового ресурсу об'єкта.

Практична реалізація підходу базується на оцінці допустимості корозійного дефекту за модифікованою методикою рівня 1 відповідно до стандарту ASME B31G. Для цього з урахуванням коефіцієнта форми дефекту z_c визначається фактор Фоліаса M , який залежить від довжини дефекту L , номінального діаметра труби D та товщини стінки wt .

$$M = \begin{cases} \sqrt{1 + 0,6275z_c - 0,003375z_c^2}, & z_c \leq 50 \\ 0,032z_c + 3,3, & z_c \geq 50 \end{cases}, \text{ де } z_c = \frac{L^2}{Dwt} \quad (1)$$

Далі визначається рівень напруження S_F , що призводить до відмови, на основі глибини корозії d та напруги потоку $S_{flow} = SMYS + 68,95$ МПа [2], де $SMYS$ – мінімальна межа плинності. Допустимість дефекту визначається умовою, що прогнозований тиск руйнування перевищує робочий тиск P_O з урахуванням коефіцієнта безпеки $SF \approx 1,39$ [2].

$$\left(S_{flow} \left[\frac{1 - 0,85(d/wt)}{1 - 0,85(d/wt)/M} \right] 2wt / D \right) \geq (SF \cdot P_O) \quad (2)$$

Для оцінки придатності об'єкта з урахуванням плину часу необхідно визначити швидкість розвитку дефекту за детерміністичним методом відповідно до API 570 на основі параметрів d та L , після чого проводиться прогноз зміни розмірів дефекту та перевірка умов придатності об'єкта для подальшої експлуатації за ASME B31G.

Вищеописані методи дозволяють визначити залежність прогнозованого тиску руйнування від розмірів дефекту та строку експлуатації. За результатами цієї серії розрахунків встановлюється глибина дефекту d_f , при якій умова (2) порушується, що свідчить про недопустимість подальшої експлуатації трубопроводу відповідно до вимог ASME B31G.

Для застосування ймовірно-фізичного методу прогнозування залишкового ресурсу на основі дифузійно-монотонного DM -розподілу відмов визначаються параметри форми v та масштабу μ . Для цього на дефектній ділянці виконують вимірювання товщини стінки у $n = 30$ рівномірно розташованих сегментах P_i по окружності та вздовж об'єкта, наприклад за допомогою оптичних 3D-сканерів або глибиномірів, що дозволяє врахувати вплив окружних напружень. Параметри DM -розподілу визначаються класичними методами на основі вимірювань товщини стінки: масштаб μ розраховується за граничним значенням d_f , наробітком τ та середньою швидкістю дефекту з урахуванням лише ненульових значень P^* (n^* – кількість елементів), а параметр форми v – через коефіцієнт варіації глибин корозії вибірки P^* .

Оцінка залишкового ресурсу здійснюється за кумулятивною функцією наробітку до граничного стану $\Phi(z)$, яка залежить від параметрів масштабу μ та форми v і визначає ймовірність відмови до часу t :

$$F(t) = DM(t; \mu; v) = \Phi\left(\frac{t-\mu}{v\sqrt{\mu t}}\right), \text{ де } \Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z e^{-\frac{u^2}{2}} du \quad (3)$$

Параметри масштабу μ та форми v визначають ймовірність досягнення граничного стану $\Phi(z)$ для заданих наробітків t , що дозволяє оцінити залишковий ресурс, наробіток до граничного стану за заданою ймовірністю та ймовірність відмови за певний період.

Список використаних джерел:

1. API 570: Piping Inspection Code: In-service Inspection, Rating, Repair, and Alteration of Piping Systems, 5th ed. Washington, DC: American Petroleum Institute, 2024.
2. ASME B31G: Manual for Determining Remaining Strength of Corroded Pipelines. New York: American Society Mechanical Engineers, 2023.

УДК 004.032.26:658.562

*Моргун Є., здобувач
Добржанський О.О., к. т. н., доцент
Пуховський Є.С. д.т.н., професор
Державний університет «Житомирська політехніка»*

НЕЙРОМЕРЕЖЕВА СИСТЕМА ВИЯВЛЕННЯ ДЕФЕКТІВ У ПРОМИСЛОВИХ ОБ'ЄКТАХ

В умовах Industry 4.0 автоматизований контроль якості є важливою складовою підвищення ефективності та конкурентоспроможності промислових підприємств. Перспективним напрямом є застосування методів глибокого навчання, які забезпечують точне виявлення, локалізацію та класифікацію дефектів поверхні в режимі реального часу. Метою роботи є розробка нейромережевої системи контролю, придатної для використання безпосередньо у виробничих умовах.

Залежно від особливостей виробництва та характеру дефектів доцільно застосовувати різні архітектури нейронних мереж. Для задач швидкої локалізації дефектів у високошвидкісних виробничих процесах ефективними є одноетапні детектори сімейства YOLO, які забезпечують оперативне виявлення пошкоджених ділянок у вигляді обмежувальних рамок. У випадках, коли критичним є точне визначення геометричних параметрів дефекту, наприклад площі корозії, довжини тріщини чи форми пошкодження, доцільно використовувати сегментаційні архітектури U-Net або Mask R-CNN, які дають змогу класифікувати кожен піксель зображення та отримувати точну маску дефекту.

За умов обмеженої кількості розмічених даних перспективним є використання методів виявлення аномалій без учителя. У цьому разі модель навчається на зображеннях бездефектних зразків, а відхилення виявляються за помилкою реконструкції або за відхиленням локальних ознак від еталонного розподілу. До таких підходів належать згорткові автоенкодери, memory-bank методи та моделі на основі нормалізуючих потоків. Їх застосування є особливо доцільним у тих галузях, де отримання великого набору розмічених прикладів дефектів є ускладненим або економічно недоцільним.

Ефективність нейромережевої системи слід оцінювати не лише за загальною точністю класифікації, а й за спеціалізованими метриками, що враховують якість локалізації та дисбаланс класів. Для задач детекції та сегментації важливою є метрика Intersection over Union:

$$IoU = \frac{A_{overlap}}{A_{union}}$$

де $A_{overlap}$ – площа перетину прогнозованої та еталонної областей, A_{union} – площа їх об'єднання.

Для комплексної оцінки якості класифікації доцільно використовувати F1-міру, яка визначається як гармонійне середнє між точністю та повнотою:

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

З метою підвищення стійкості моделі до реальних виробничих умов у процес навчання доцільно включати аугментацію даних, зокрема додавання шуму, розмиття руху, варіювання експозиції, колірної температури та геометричні перетворення. Це сприяє підвищенню узагальнювальної здатності моделі та забезпечує її надійне функціонування в умовах пилу, вібрацій, нестабільного освітлення та інших виробничих завод.

Для практичного впровадження системи доцільним є застосування підходів Edge AI, за яких нейромережевий висновок виконується безпосередньо поблизу джерела даних. Такий підхід дає змогу зменшити затримки передавання інформації, знизити навантаження на мережеву інфраструктуру та забезпечити роботу системи в режимі реального часу. Підвищення продуктивності апаратної реалізації досягається шляхом оптимізації моделі, зокрема квантування, зменшення розрядності обчислень і скорочення надлишкових параметрів.

Список використаних джерел:

1. Ma, Y., Yin, J., Huang, F., Li, Q. *Surface defect inspection of industrial products with object detection deep networks: a systematic review*. Artificial Intelligence Review, 2024, Vol. 57, Article 333. DOI: 10.1007/s10462-024-10956-3.

УДК 004.032.26

*Раданович В.Я., здобувачка,
Ткачук Д.Ю., аспірантка,
Крижанівська І.В., к.т.н., доцент
Державний університет «Житомирська політехніка»*

ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ ДЛЯ ПРОГНОЗНОГО ОБСЛУГОВУВАННЯ ЕЛЕКТРИЧНИХ ДВИГУНІВ НА ОСНОВІ ВІБРАЦІЙНИХ ТА ЕЛЕКТРИЧНИХ СИГНАЛІВ

Прогнозне обслуговування в енергоінформаційних мережах (Predictive Maintenance) ґрунтується на аналізі великих обсягів даних, що надходять від сенсорів та відображають фізичні процеси функціонування обладнання. Одним із перспективних напрямів є застосування нейронних мереж для аналізу часових рядів вібраційних сигналів і параметрів споживання струму електричними двигунами, зокрема асинхронними електродвигунами, які є найбільш поширеними в промислових енергосистемах, а також синхронними машинами та електроприводами промислового призначення.



Рис.1. Структурна схема нейромережевої системи прогнозного обслуговування електричних двигунів

Застосування таких моделей дозволяє виявляти приховані закономірності деградації елементів обладнання та прогнозувати момент виникнення відмови до її фактичного прояву. Аналіз вібраційних і електричних сигналів забезпечує можливість діагностування характерних дефектів, зокрема пошкоджень підшипників, дисбалансу ротора, міжвиткових замикань обмоток та деградації ізоляції.

На відміну від традиційних підходів контролю стану, таких як спектральний або пороговий аналіз, нейронні мережі здатні моделювати складні нелінійні залежності між режимами роботи, зовнішніми впливами та технічним станом обладнання на основі історичних даних, що включають як повні цикли до відмови, так і цензуровані спостереження.

Для задач прогнозування технічного ресурсу застосовуються неймережеві моделі, що поєднують методи глибинного навчання та виживального аналізу. Такі підходи дозволяють оцінювати функції ризику відмови та визначати залишковий ресурс обладнання (Remaining Useful Life) з урахуванням як статичних характеристик двигуна, так і часової динаміки вібраційних і електричних сигналів.

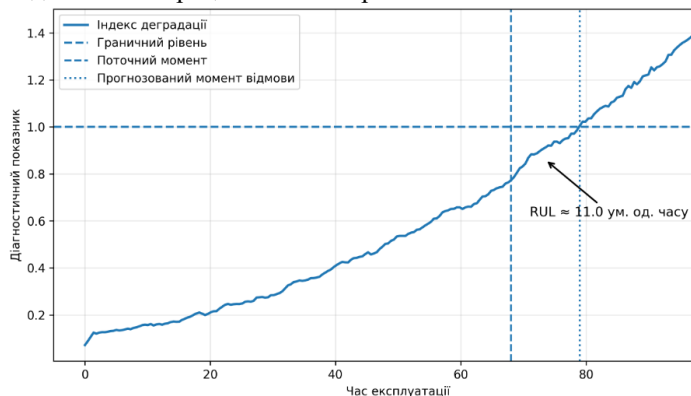


Рис.2. Приклад прогнозування залишкового ресурсу електродвигуна

Практичне впровадження зазначених підходів сприяє підвищенню надійності електромеханічних систем, зменшенню кількості аварійних зупинок та оптимізації витрат на технічне обслуговування, що забезпечує перехід від регламентного та реактивного обслуговування до інтелектуальних прогнозних стратегій.

Список використаних джерел:

1. Shadi, M. R., Mirshekali, H., Tahavori, M., Shaker, H. R. Survival Models for Predictive Maintenance and Remaining Useful Life in Sensor-Enabled Smart Energy Networks: A Review. *Sensors*, 2026, 26(6), 1915. DOI: 10.3390/s26061915.
2. Hamani, K., Kuchar, M., Kubatko, M., Kirschner, S. Advancements in Induction Motor Fault Diagnosis and Condition Monitoring: A Comprehensive Review. *Sensors*, 2025, 25(19), 5942. DOI: 10.3390/s25195942.
3. Ayankoso, S., Dutta, A., He, Y., et al. Performance of vibration and current signals in the fault diagnosis of induction motors using deep learning and machine learning techniques. *Structural Health Monitoring*, 2024/2026, 25(1), 196–212. DOI: 10.1177/14759217241289874.

УДК 629.1.03

Чумакевич В. О., к. т. н., доцент,

Пулеко І. В., к. т. н., доцент,

Оріщук І. О., ст. викладач

Оніщенко О. О., ст. викладач

Житомирський військовий інститут ім. С. П. Корольова,

Національний університет «Львівська політехніка»

Державний університет «Житомирська політехніка»

ЗАСТОСУВАННЯ ПРЯМОГО КЕРУВАННЯ МОМЕНТОМ АСИНХРОННОГО ДВИГУНА В РУШІЙНИХ СИСТЕМАХ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ

Використання наземних транспортних засобів з електричними двигунами, до недавнього часу, обмежувалось електричними рушіями на залізницях, міському електротранспорті тощо. Сьогодні в наше сьогодення зайшов цілий пласт безпілотних систем, які в якості рушія мають електричні двигуни. Здебільшого вони приводяться в рух двигунами постійного струму (ДПС) та синхронними двигунами змінного струму (СД). Окремим напрямком є використання brushless motor (скорочено BLDC двигуни). Використання асинхронних двигунів змінного струму (АСД) залишається не розповсюдженим, хоча відомі проєкти електротракторів, міського електротранспорту, де тяговими двигунами виступають саме АСД.

Важливою складовою частиною електроприводу є система керування. Завдяки стрімкому розвитку транспортної мехатроніки, асинхронні двигуни позбувся основних своїх недоліків: складність та висока вартість систем керування з плавною зміною швидкості обертання ротора, відносно менший (порівняно з двигунами постійного струму) крутний момент тощо.

На рис. 1. показана система електропривода наземного роботизованого комплексу (НРК), яка має власне бортове джерело електроенергії, силовий перетворювач, на який приходять сигнали керування, та можуть бути трансмісія та диференціал. При безпосередньому приводі останніх два елементи відсутні.

В сучасному тяговому електроприводі є перспективним заміна двигунів постійного струму на дешевші асинхронні. Для керування асинхронними двигунами широко використовується пряме керування моментом. Завданням прямого керування моментом є забезпечення швидкої реакції електромагнітного моменту на керуючий сигнал. На відміну від складніших систем векторного керування, де зміна моменту здійснюється дією на струм статора, який є керуючою величиною, в системі DTC керуючою величиною є потокощеплення статора. Зміна

потоцщеплення досягається оптимальною роботою силового перетворювача, який керує асинхронним двигуном.

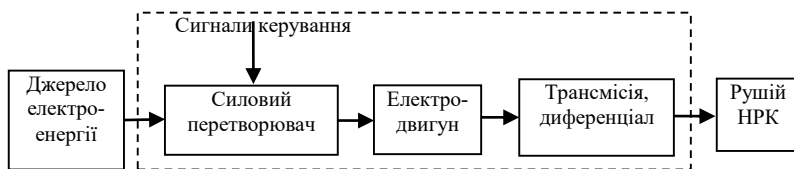


Рис. 1. Загальна структура електропривода НРК

Для математичного моделювання електропривода за принципом прямого керування двигуна використовуємо рівняння рівноваги напруги статора в нерухомій системі координат:

$$\vec{U}_{s\alpha\beta} = R_s \vec{I}_{s\alpha\beta} + \frac{d}{dt} \vec{\psi}_{s\alpha\beta},$$

та електромагнітного моменту двигуна, які записані через потоцщеплення статора і ротора у нерухомій системі координат:

$$M_d = \frac{3}{2} Z_p \frac{k_s}{\sigma L_r} (\psi_{s\alpha} \psi_{r\beta} - \psi_{s\beta} \psi_{r\alpha}),$$

де $\psi_{s\alpha}, \psi_{r\beta}$ – потоцщеплення статора та ротора у нерухомій системі координат.

Проведені моделювання підтвердили можливість використання прямого керування моментом асинхронного двигуна як привода рушія НРК. Воно забезпечує швидку реакцію електромагнітного моменту на керуючий сигнал.

Список використаних джерел:

1. Янко А. С., Михайличенко О. В., Крук О. І. Оптимальні алгоритми автоматичного керування робототехнічною платформою, які забезпечують її високу продуктивність та надійність функціонування. Системи управління, навігації та зв'язку. Збірник наукових праць. 2025. №2. С. 70-75. DOI: 10.26906/SUNZ.2025.2.070.
2. Simon M.G., Fodor D. Comparative Analysis of Field Oriented Control and Direct Torque Control Through Simulation in MATLAB Simulink for an Automotive Drive Motor. Engineering Proceedings. 2024; Vol. 79(1) P. 33. <https://doi.org/10.3390/engproc2024079033>

УДК 004.9:005.6:330.4

Яцук Ю.Л., аспірант

Навчально-науковий інститут «Українська інженерно-педагогічна академія» Харківського національного університету імені В. Н. Каразіна

ВПЛИВ КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ НА УПРАВЛІННЯ ПРОЦЕСАМИ В СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМАХ

Використання комп'ютерно-інтегрованих технологій при управлінні процесами в соціально-економічних системах є надзвичайно актуальним і має істотний вплив на різні аспекти функціонування таких систем, незалежно від їх масштабу. Сучасні тенденції цифровізації свідчать про зростання ролі інформаційних технологій як ключового інструменту трансформації управлінських підходів і підвищення ефективності економічних процесів.

Використання комп'ютерно-інтегрованих технологій дозволяє автоматизувати багато рутинних завдань всередині соціально-економічних систем, що підвищує їх ефективність та збільшує продуктивність. Зокрема, застосування інформаційних систем і технологій штучного інтелекту дає змогу оптимізувати управління проєктами, зменшити людський фактор і підвищити точність прийняття рішень.

Перехід до електронної документації, використання програм для автоматизації створення документів, управління договорами та іншими аспектами документообігу спрощує зберігання, доступ і обмін інформацією. Умови цифрової економіки формують нові підходи до взаємодії між суб'єктами господарювання, що базуються на інтегрованих цифрових платформах.

Використання комп'ютерних програм та баз даних дозволяє проводити більш точний аналіз функціонування соціально-економічних систем. Методи обробки великих даних і аналітичні інструменти сприяють підвищенню обґрунтованості управлінських рішень, що підтверджується сучасними дослідженнями у сфері аналізу економічних процесів.

Застосування технологій для захисту конфіденційної інформації та забезпечення кібербезпеки є надзвичайно важливим у світі, де дедалі більше процесів переходять в електронний формат. Соціально-технічні підходи до моделювання безпеки дозволяють враховувати як технічні, так і організаційні аспекти захисту інформації.

Комп'ютерно-інтегровані технології дозволяють підприємствам як різновиду соціально-економічних систем працювати масштабовано та

реалізовувати продукцію або надавати послуги незалежно від географічного розташування. Це сприяє формуванню глобалізованих ринків та підвищенню конкурентоспроможності підприємств.

Впровадження штучного інтелекту та інших інноваційних технологій сприяє покращенню прогнозування, аналізу та прийняття рішень.

Управління процесами на підприємстві як різновиді соціально-економічних систем включає використання комп'ютерно-інтегрованих технологій для підвищення ефективності управління.

Інтеграція комп'ютерно-інтегрованих технологій дозволяє впроваджувати адаптивні системи управління, здатні самонавчатися та вдосконалюватися на основі накопичених даних, що є одним із ключових напрямів розвитку сучасних соціально-економічних систем.

Використання комп'ютерно-інтегрованих технологій при управлінні процесами на підприємстві як різновиді соціально-економічних систем сприяє підвищенню ефективності діяльності, забезпечуючи швидкий доступ до інформації, автоматизацію процесів, економію ресурсів, оптимізацію прогнозування та підвищення конкурентоспроможності на ринку.

Список використаних джерел:

1. Мельник А.О., Кинаш Ю.Є. Розробка підсистеми автоматизованого управління відносинами з клієнтами малого бізнесу // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2024. № 54. С. 27–35. URL: <https://cit.lntu.edu.ua/index.php/cit/article/view/521/621> (дата звернення: 24.03.2026).

2. Bahi A., Gharib J., Gahi Y. Integrating generative AI for advancing agile software development and mitigating project management challenges // International Journal of Advanced Computer Science and Applications. 2024. Vol. 15, No. 3. URL: <https://thesai.org/Publications/ViewPaper?Volume=15&Issue=3&Code=IJACSA&SerialNo=6> (дата звернення: 24.03.2026).

3. Yushkevych O., Sharko V., Stavroiani S., Makatora D., Yevtushenko Y. Innovative development of economic systems in the digitalization conditions // Management Theory and Studies for Rural Business and Infrastructure Development. 2024. Vol. 46, No. 1. P. 23–30. URL: <https://reference-global.com/article/10.15544/mts.2024.03> (дата звернення: 24.03.2026).

УДК 621.365:681.5:004.89

*Люта А. В., к.т.н., доцент
Донбаська державна машинобудівна академія*

МОДЕРНІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ПРИВОДОМ ПЕРЕМІЩЕННЯ ЕЛЕКТРОДІВ ДУГОВОЇ СТАЛЕПЛАВИЛЬНОЇ ПЕЧІ З ВИКОРИСТАННЯМ НЕЧІТКОГО КОНТРОЛЕРА

Ключову роль в металургійній галузі грає сталеплавлення. На виробництво сталі в усьому світі витрачається близько 60 % енергії. В енергетичний період розплаву металу в печі трапляється багато електричних та електромеханічних збурень, які впливають на якість процесу плавки, на стабільність горіння електричних дуг, що призводить до збільшення енерговитрат та часу виплавки металу.

Експериментально встановлено, що при експлуатаційних коротких замикань (при падіннях шматків шихти і т. п.) виникають електродинамічні зусилля між гнучкими кабелями трьох фаз. Після зникнення експлуатаційних коротких замикань гнучких кабелів (ГК) коливаються з частотами вільних згасаючих коливань. При цьому змінюються відстані між фазами, що призводить до відповідної зміни взаємних індуктивностей фаз. Тому в струмах фаз виникають відповідні модульовані затухаючі коливання, які порушують нормальну роботу регуляторів переміщення електродів дугової сталеплавильної печі [1]. Таким чином, електроди також починають здійснювати поздовжні коливання. Такі коливальні процеси в ДСП можуть викликати резонанс системи і виникнення незатухаючих коливань. Такі аварійні режими можуть тривати десятки хвилин, оскільки за одну плавку може відбуватися до 200 коротких замикань. Електрохемічні коливання ГК, а, отже, і поздовжні коливання графітованих електродів, які створюються за рахунок зворотних зв'язків за струмом і напругою регуляторів переміщення електродів (РПЕ), викликають зниження втомної міцності елементів системи, а також можуть призвести до руйнування графітованих електродів, що призводить до витрати енергії, збільшення часу розплавлення металу і зниження продуктивності печі. Завдання компенсації коливань гнучких кабелів і буде вирішуватися в даній роботі.

Метою роботи є збільшення ефективності роботи дугової сталеплавильної печі шляхом поліпшення стабільності горіння електричних дуг при наявності збурювальних впливів.

Досягнення мети в роботі проводиться за рахунок компенсації збурювальних впливів шляхом модернізації системи управління приводом переміщення електродів дугової сталеплавильної печі.

Розроблений спосіб компенсації електромеханічних коливань гнучких кабелів наведено на рисунку 1 [2].

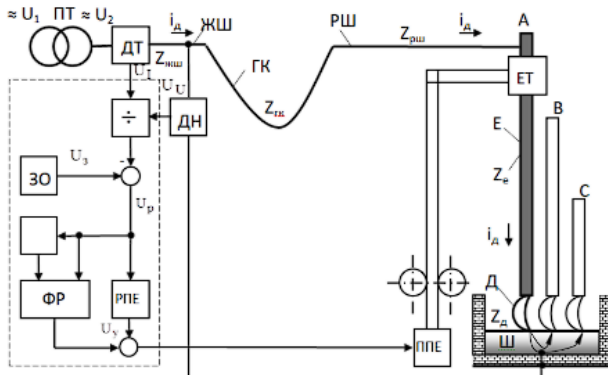


Рис.1. Структурна схема удосконаленої системи управління приводом переміщення електродів ДСП для однієї фази

На рисунку 1 були прийняті такі позначення: ПТ – пічний трансформатор; ЖШ – жорстка шина; ГК – гнучкий кабель; РШ – рухома шина; ЕД – електродотримачі; Е – електрод; Д – дуга; Ш – шихта; ДТ – датчик струму дуги; ДН – датчик напруги фази; РПЕ – регулятор переміщення електрода (П, ПІ або ПІД); ФР – фаззі-регулятор; ЗО – задатчик опору; ППЕ – привід переміщення електродів; А, В, С – фази А, В, С; U_U – сигнал з датчика напруги фази; U_I – сигнал з датчика струму дуги; U_Z – сигнал, пропорційний повного опору дуги; U_p – сигнал неузгодженості; $\dot{U}_p$ – похідна сигналу неузгодженості; U_f – сигнал на виході фаззі-регулятора; U_y – сигнал управління; $U_{y_{уд}}$ – сигнал управління в удосконаленій системі.

Список використаних джерел:

1. Khoshkhoo H. An efficient power control scheme for electric arc furnaces using online estimation of flexible cable inductance / H. Khoshkhoo, S. H. N. Sadeghi, R. Moini, H. A. Talebi // Computers & Mathematics with Applications. – Volume 62, Issue 12, December 2011, Pages 4391–4401.

Люта А.В. Удосконалення системи управління приводом переміщення електродів дугової сталеплавильної печі з використанням нечіткого контролера / А. В. Люта, О. В. Суботін, Я. І. Петрухін // Modern engineering and innovative technologies. International periodic scientific journal, 2026. – URL: <https://www.sworldjournal.com/index.php/swj/issue2026>

УДК 004.45:004.89

*Дейнеко А.О, здобувач**Духновська К.К, к.т.н.**Державний університет «Житомирська політехніка»*

СИСТЕМА РЕАЛЬНОГО ЧАСУ ДЛЯ КЕРУВАННЯ АВТОНОМНИМ АГЕНТОМ

Інтенсивний розвиток концепції Internet of Everything (IoE) зумовлює необхідність створення надійних та швидкодіючих програмних інтерфейсів для віддаленого управління автономними пристроями. Традиційні підходи до побудови таких систем часто спираються на архітектуру REST та класичний протокол HTTP, що створює значний мережевий оверхед при поллінгу (polling) і не забезпечує достатньої швидкодії для передачі телеметрії мобільних об'єктів у режимі реального часу. Відповідно, актуальним завданням є розробка клієнт-серверних рішень на базі повнодуплексних протоколів зв'язку, інтегрованих з ефективними алгоритмами навігації.

Метою даної роботи є розробка програмного комплексу, який складається з інтерактивної веб-панелі керування та бекенд-сервера, здатного розраховувати оптимальні траєкторії руху інтелектуального агента з урахуванням динамічних перешкод та безперервно транслювати його стан.

Запропонована система базується на розподіленій клієнт-серверній архітектурі. Серверна частина реалізована мовою Python з використанням мікрофреймворку Flask [1] та бібліотеки Eventlet для асинхронної обробки з'єднань. Стан автономного агента в будь-який момент часу формалізується вектором стану S :

$$S = \{x, y, B, status\},$$

де x, y — поточні координати об'єкта на дискретній сітці, B — рівень заряду акумулятора у відсотках, $status$ — поточний стан виконання задачі. Двосторонній обмін вектором S між сервером та клієнтом здійснюється через протокол WebSocket у форматі JSON із частотою оновлення 2 Гц, що забезпечує консистентність даних [2].

Клієнтська частина побудована на базі JavaScript-фреймворку Vue.js [3]. Візуалізація робочого простору у вигляді карти зайнятості (Occupancy Grid Map) реалізована за допомогою технології HTML5 Canvas. Це дозволяє оптимізувати рендеринг двовимірної сітки без переважання DOM-дерева браузера.

Базовим алгоритмом пошуку найкоротшого шляху обрано алгоритм A^* ($A - Star$). На кожній ітерації алгоритм розширює вузол сітки n , який мінімізує цільову функцію $f(n)$ [4]:

$$f(n) = g(n) + h(n),$$

де $g(n)$ — фактична вартість пройденого шляху від старту, а $h(n)$ — евристичне наближення відстані до цілі. Для забезпечення руху агента у восьми напрямках (включаючи діагональні переміщення) як евристику застосовано евклідову метрику:

$$h(n) = \sqrt{(x_n - x_g)^2 + (y_n - y_g)^2}.$$

Використання структури даних «бінарна купа» (binary heap) для зберігання відкритого списку вершин дозволило досягти часової складності алгоритму $O(E \log V)$, де V — кількість вільних клітинок, а E — кількість можливих переходів. Особливістю реалізованого навігаційного модуля є механізм динамічного перепланування маршруту. У разі зміни топології карти оператором безпосередньо під час руху об'єкта, система автоматично перевіряє валідність залишку шляху і, за необхідності, ініціює розрахунок нової траєкторії в обхід перешкоди. Додатково в системі імплементовано кінематичну модель енергоспоживання об'єкта. Зміна рівня заряду ΔB при переміщенні між суміжними вузлами n_i та n_{i+1} розраховується за формулою:

$$\Delta B = k * d(n_i, n_{i+1}),$$

де k — базовий коефіцієнт енергоспоживання, а d — просторова відстань між вузлами. Таким чином, діагональні кроки мають більшу вартість $\approx 1,414$ і відображаються у пропорційно більших витратах ресурсу. При досягненні критичного рівня заряду алгоритм забезпечує автоматичне повернення агента на координати базової станції для підзарядки.

Розроблений програмний комплекс успішно демонструє можливість ефективного управління автономним агентом у реальному часі через веб-інтерфейс. Подальший розвиток проєкту передбачає розширення серверної архітектури для забезпечення мультиагентної взаємодії (Swarm Robotics) та інтеграцію алгоритмів оптимізації траєкторій.

Список використаних джерел:

1. Grinberg M. Flask Web Development: Developing Web Applications with Python. – O'Reilly Media, 2018. – 316 p.
2. The WebSocket API (WebSockets) [Електронний ресурс] // MDN Web Docs. – URL: https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API
3. Vue.js: The Progressive JavaScript Framework [Електронний ресурс] // Офіційна документація Vue.js. – URL: <https://vuejs.org/>
4. Hart P. E., Nilsson N. J., Raphael B. A Formal Basis for the Heuristic Determination of Minimum Cost Paths // IEEE Transactions on Systems Science and Cybernetics. – 1968. – Vol. 4, No. 2. – P. 100–107.

УДК 004.032.26:629.735.33

*Ткачук В.Ю., здобувач
Добржанський О.О. к.т.н., доцент
Державний університет «Житомирська політехніка»*

НЕЙРОМЕРЕЖЕВІ МЕТОДИ ПРОГНОЗУВАННЯ ЕНЕРГЕТИЧНОГО СТАНУ БПЛА ДЛЯ РЕАЛІЗАЦІЇ АВТОНОМНОЇ СИСТЕМИ ЗАРЯДЖАННЯ

Обмежений енергетичний ресурс акумуляторних батарей залишається одним із головних чинників, що стримує тривале автономне функціонування безпілотних літальних апаратів. Для місії у динамічних умовах недостатньо лише контролювати поточну напругу батареї, оскільки реальний енергетичний стан БПЛА визначається сукупністю показників, зокрема рівнем заряду, станом здоров'я батареї, залишковим ресурсом, температурними умовами, профілем навантаження та режимом польоту. Сучасні дослідження у сфері авіаційних батарей підкреслюють, що саме інтелектуальні методи оцінювання цих параметрів дають змогу підвищити надійність енергетичного менеджменту в БПЛА та створюють основу для автономного прийняття рішень щодо повернення, посадки й підзарядження.

Метою роботи є розробка нейромережевих методів прогнозування енергетичного стану БПЛА для реалізації автономної системи заряджання, здатної у реальному часі оцінювати залишковий енергетичний ресурс і формувати рішення про перехід до режиму автоматичного повернення та заряджання. Запропонований підхід передбачає використання бортових даних про струм, напругу, температуру акумулятора, тягове навантаження, швидкість польоту, просторове положення апарата та параметри місії. На основі цих даних нейромережева модель повинна прогнозувати не лише поточний рівень заряду, а й часовий горизонт безпечного виконання місії, що є критично важливим для систем автономного енергетичного керування.

Функціонально система складається з бортової сенсорної підсистеми, модуля збору телеметрії, нейромережевого модуля прогнозування, блоку прийняття рішень та автономної зарядної станції. Для задач прогнозування доцільно використовувати рекурентні й часові архітектури, зокрема LSTM, Temporal Convolutional Network, Transformer-подібні моделі або гібридні physics-informed підходи, оскільки вони краще враховують нелінійну динаміку батареї та змінний

характер польотного навантаження. Вектор енергетичного стану БПЛА можна подати у вигляді:

$$x_k = [SOC_k, SOH_k, RUL_k, T_k, P_k]^T$$

де SOC_k – рівень заряду акумулятора, SOH_k – стан його деградації, RUL_k – залишковий корисний ресурс, T_k – температура, P_k – поточне енергоспоживання. Тоді нейромережева модель прогнозування може бути описана узагальненим співвідношенням:

$$\hat{x}_{k+1} = f_{\theta}(x_k, u_k, z_k)$$

де u_k – керуючі та польотні параметри, z_k – телеметричні вимірювання, f_{θ} – параметризована нейромережева модель. На основі прогнозованого значення SOC та оціненого енергетичного резерву система визначає момент, коли подальше виконання місії стає недоцільним, і генерує команду на автономне повернення до зарядної платформи.

Ключовою перевагою такого підходу є перехід від реактивного контролю батареї до прогнозного енергетичного керування. На відміну від порогових алгоритмів, що реагують лише на вже наявне зниження напруги, нейромережевий модуль враховує історію навантаження, характер маневрування, зовнішні умови та деградаційні процеси батареї. Це дає змогу завчасно ініціювати процедуру повернення, уникати глибокого розряду, зменшувати ризик аварійної посадки та підвищувати загальну безпеку автономного польоту. Практична цінність запропонованого рішення особливо зростає для БПЛА, що працюють у режимі довготривалого моніторингу, інспекції інфраструктури, логістики або пошуково-рятувальних операцій.

Для реалізації повністю автономного циклу енергозабезпечення прогнозний модуль має бути інтегрований із системою автоматичного докування та заряджання. Сучасні огляди показують, що такі системи базуються на поєднанні алгоритмів точного наведення, візуального позиціонування, сенсорного злиття та контактних або безконтактних механізмів підзаряджання. Тому нейромережеве прогнозування енергетичного стану доцільно розглядати як верхній рівень прийняття рішень, який визначає момент активації сценарію повернення, тоді як нижній рівень забезпечує безпечну посадку, зчеплення із платформою та подальше відновлення енергетичного ресурсу.

Список використаних джерел

1. Osman A. A., Mistarihi M. Z., Ramadan M., Ghazal M., Alkhedher M. A. *Review and Bibliometric Analysis of Intelligent Techniques for Advanced Battery State Estimation in Aviation Propulsion Systems*. Results in Engineering. 2025. Vol. 27. Art. 106741. DOI: 10.1016/j.rineng.2025.106741.
2. Zhao T., Zhang Y., Wang M., Feng W., Cao S., Wang G. *A Critical Review on the Battery System Reliability of Drone Systems*. Drones. 2025. Vol. 9, No. 8. Art. 539. DOI: 10.3390/drones9080539.
3. Duan M. et al. *PIDNN: A Hybrid Intelligent Prediction Model for UAV Battery Degradation*. Batteries. 2026. Vol. 12, No. 4. Art. 124. DOI: 10.3390/batteries12040124.

УДК 621.317

**Безвесільна О.М., д.т.н., професор,
Ткачук А.Г., к.т.н., доцент,
Толочко Т.О., ст.викладач,
Гриневич М.С., аспірант**

*Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського»
Державний університет «Житомирська політехніка»*

ІНТЕЛЕКТУАЛЬНА ДОСЛІДНИЦЬКА СИСТЕМА ДЛЯ ВИМІРЮВАНЬ КОРИСНИХ КОПАЛИН

Інтелектуальна дослідницька система може бути використана для проведення вимірювань корисних копалин на літальних апаратах (ЛА) у геології, геодезії та в інших галузях науки і техніки.

Відомі системи подібного типу мають такі основні недоліки [1,2]: на них при використанні на ЛА діє вертикальне прискорення, яке у 10^3 перевищує корисний сигнал прискорення сили тяжіння (ПСТ) або гравітаційної аномалії; частота власних коливань таких систем обирається довільною, тому при їх роботі необхідно використовувати додаткові фільтри низьких частот, які ускладнюють схему, зменшують її надійність і вносять додаткові похибки вимірювань; в алгоритмах роботи відомих систем відсутня поправка від впливу кутової швидкості обертання Землі; відомі системи мають великі залишкові похибки від впливу вертикального прискорення, значні інструментальні похибки та ін.

Суттєвими недоліками відомих систем є низькі точність та надійність вимірювання аномалій прискорення сили тяжіння (ПСТ) у процесі пошуку корисних копалин.

У даній статті поставлено задачу підвищення точності та надійності дистанційного пошуку корисних копалин шляхом використання інтелектуальної дослідницької системи.

Поставлену задачу вирішуємо створенням авіаційної інтелектуальної дослідницької системи для вимірювань прискорення сили тяжіння, що містить гравіметр у герметичному корпусі з двома каналами, у кожному з яких встановлено по одному чутливому елементу, виходи яких з'єднані із входом суматора, вихід якого з'єднано з входом підсилювача із захисним кільцем, вихід якого з'єднано через цифровий модуль із входом бортового комп'ютера, який з'єднано із попередньо навченим інтелектуальним Fuzzy-модулем, вихід якого є виходом інтелектуальної дослідницької системи, в якій новим є те, що в якості чутливих елементів гравіметра використані

п'єзоелектричні елементи, що є ідентичними і виконаними у вигляді п'єзопластин, між п'єзопластинами розміщена загальна інерційна маса, що через пружини прикріплена до центрів верхньої та нижньої п'єзопластин п'єзоелектричних елементів, а виходи п'єзопластин обох каналів з'єднані з входами суматора.

Гравіметр має потужний вихідний сигнал у 6-8 В. Таку потужність досягають, зокрема, завдяки меншому числу елементів та використанню однієї інерційної маси. Також на потужність впливає використання в якості чутливих елементів п'єзоелектричних елементів, що видають більш точний і потужний сигнал та на роботу яких значно менше впливають шуми та наводки під'єднуючих кабелів, резонанси. У гравіметрі відсутні інструментальні похибки залишкової неідентичності конструкції однакових п'єзопластин від впливу змін температури, вологості та тиску зовнішнього середовища, похибки акселерометрів системи стабілізації гравіметра: систематичні похибки дрейфу, похибки масштабних коефіцієнтів, похибки виставлення осей чутливості. Гравіметр не потребує додаткових компонентів: спеціального джерела живлення, додаткового високочутливого вторинного перетворювача з великим вхідним опором, тобто він має більшу надійність. Результати вимірювання ПСТ автоматично аналізуються в інтелектуальному Fuzzy-модулі, попередньо навченому за сигналом гравітаційної аномалії Δg розпізнавати види корисних копалин, що містить базу нечітких правил та лінгвістичних змінних і формує логічний висновок щодо наявності та виду корисних копалин. Інтелектуальний Fuzzy-модуль дозволяє здійснювати обробку множини вимірювальних даних у режимі реального часу під час руху літального апарату. Також інтелектуальний Fuzzy-модуль слугує для компенсації похибок вимірювання аномалій прискорення сили тяжіння, які з'являються в акселерометрів системи стабілізації гравіметра. Тому час, що витрачається на обробку вимірювальних даних, суттєво скорочується, а якість результатів підвищується.

Список використаних джерел

1. Патент на корисну модель 151618. Інтелектуальна гравіметрична система / Черепанська І. Ю., Безвесільна О.М., Сазонов А.Ю., Киричук Ю.О.; заявник і патентовласник Національний технічний університет України "КПІ імені Ігоря Сікорського". – u 2022 01565; заявл. 16.05.2022; надр. 17.08.2022, Бюл. №33.

Безвесільна О.М. Перетворювачі фізичних величин. Технічні засоби автоматизації / Підручник. – НПО «Пріоритети»: Київ. 2019 – 809 с.

Секція 8 СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У БІОМЕДИЦИНІ

УДК 004.932:616.5

*Ветров А.О., магістрант,
Нікітчук Т.М., к.т.н., доцент
Державний університет «Житомирська політехніка»*

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ДІАГНОСТИКИ ДЕГІДРАТАЦІЇ ШКІРИ

Стрімкий прогрес у сфері комп'ютерного зору та мобільних обчислень відкриває можливість створення інтелектуальних систем для об'єктивної неінвазивної оцінки стану шкіри у побутових умовах. Бар'єрна функція епідермісу визначається натуральним зволожувальним фактором (NMF) та ліпідним бар'єром міжклітинного матриксу, а її цілісність оцінюють показником трансепідермальної втрати води (TEWL): $4\text{--}10 \text{ г}/(\text{м}^2 \cdot \text{год})$ у нормі проти понад $15 \text{ г}/(\text{м}^2 \cdot \text{год})$ при порушенні бар'єру. Золотим стандартом діагностики є корнеометрія, що ґрунтується на зміні діелектричної проникності ($\epsilon \approx 80$ для води проти $\epsilon < 7$ для ліпідів), яка залишається недоступною широкому колу пацієнтів через вартість апаратного комплексу. Водночас AI-моделі, навчені на зображеннях видимого спектру, прогнозують вологість рогового шару з похибкою $4,7 \text{ AU}$ проти $10,7 \text{ AU}$ базових підходів [1], що відкриває принципову можливість скринінгу смартфоном.

Метою даного дослідження є розробка прототипу мобільного додатку для автоматизованої класифікації ступеня дегідратації шкіри за фотозображенням. Об'єктом дослідження виступає процес аналізу текстури шкіри за цифровими знімками, а предметом – методи комп'ютерного зору (LBP, GLCM, Gabor-фільтри) та мобільно-орієнтовані архітектури згорткових нейронних мереж (EfficientNet-B0, MobileNetV3-Large), оптимізовані засобами TensorFlow LiteRT з INT8-квантизацією.

Фізіологічне обґрунтування вибору GLCM полягає в тому, що зниження гідратації рогового шару порушує десмосомальний дигест, спричиняючи мікролущення та формування нерівного мікрорельєфу поверхні. Відшаровані лусочки шкіри («виступаючі» частини) відбивають падаюче світло, тоді як проміжки між ними («западини») залишаються у тіні, породжуючи різкі переходи між яскравими та

темними пікселями. Ці переходи GLCM фіксує як показник Contrast ($\sum P(i,j) \cdot (i-j)^2$), що виступає статистичним проксі-маркером стану гідратації, а не безпосереднім вимірювачем вмісту води. Необхідно враховувати епістемологічне обмеження методу: гіперпігментація, зокрема веснянки та меланінові утворення, дає статистично схожий відгук формули [2], тому для мінімізації хибних спрацювань передбачено попередню сегментацію пігментних областей та перехресну валідацію з LBP і Gabor-каналами.

Для навчання мережі застосовується двоетапна стратегія. На етапі попереднього навчання (pretraining) використовуються відкриті дерматологічні датасети ISIC Archive та HAM10000, що містять понад 70 000 зображень, для формування в базових шарах узагальнених уявлень про текстуру шкіри. Параметри цих шарів фіксуються, після чого здійснюється донавчання на власній клінічній вибірці ($n \geq 200$ суб'єктів) з корнеометричними мітками: понад 40 AU відповідає нормі, 30–40 AU – сухій шкірі, менше 30 AU – критичній сухості. Такий підхід подолає семантичну розбіжність між джерелом (онкологія) та ціллю (гідратація), оскільки базові шари кодують інваріантні до патології ознаки [3]. Замість статистично нерелевантного Гауссового шуму для аугментації застосовуються фізіологічно обґрунтовані методи: синтез мікрорельєфу лушення та варіація кута освітлення. Архітектура EfficientNet-B0 демонструє точність 91,84% на ISIC 2018 при 0,39G FLOPs [4], а після LiteRT INT8-квантизації забезпечує inference-затримку 5,90 мс при чотирикратному зменшенні розміру моделі з втратою точності менше 1% [5].

Перспективним доповненням є каскадна архітектура CNN та VLM за принципом CLIN-LLM [6], де CNN виступає першим етапом, встановлюючи клас гідратації за тривірневою шкалою з оцінкою невизначеності методом Monte Carlo Dropout. Встановлений діагноз фіксується як незмінний системний промт для VLM, яка генерує рекомендації щодо догляду та питного режиму виключно в межах заданого класу, без самостійного перегляду діагнозу, що повністю усуває ризик медичних галюцинацій, рівень яких у загальних VLM сягає 17,8% [7].

Прототип реалізує чотириетапний алгоритм роботи. На першому етапі AR-інтерфейс і TOF/LiDAR-сенсор верифікують відстань 15–20 см, а кнопка знімку блокується при значенні ISO понад 400; ця вимога є технічною необхідністю, оскільки мережа після ISIC-pretraining набуває гіперчутливості до мікроконтрастних переходів, і сенсорний шум при високому ISO може хибно класифікуватись як мікролушення. На другому етапі здійснюється попередня обробка засобами GrayWorld

та засобами адаптивного вимірювання (CLANE) і виділення гібридних текстурних дескрипторів GLCM+LBP. Третій етап передбачає класифікацію з відображенням рівня впевненості, а четвертий – генерацію персоналізованих рекомендацій через каскадну VLM.

Такий підхід робить додаток надійним інструментом для об'єктивного скринінгу стану шкіри в побутових умовах.

У ході дослідження розроблено концепцію та функціональний прототип мобільного додатка для неінвазивної діагностики дегідратації шкіри. Запропонований підхід, що базується на комбінації текстурних дескрипторів GLCM та мобільно-орієнтованих нейронних мереж, дозволяє досягти високої діагностичної точності (понад 91%) при мінімальних апаратних витратах. Використання Edge AI та методів квантизації забезпечує високу швидкість обробки даних (до 5,90 мс) та конфіденційність медичної інформації користувача.

Перспективи подальших досліджень спрямовані на інтеграцію даних з датчиків вологості та температури навколишнього середовища для корекції прогнозу рівня TEWL у реальному часі, вдосконаленні каскадних архітектур, розробці фізіологічно обґрунтованих методів аугментації для навчання моделей на рідкісних типах патологічних мікрорельєфів шкіри, що дозволить підвищити стійкість системи до різних умов освітлення, та проведенні розширених випробувань на більшій вибірці ($n > 500$) із паралельним використанням еталонних корнеометрів для фіксації динаміки відновлення бар'єрної функції епідермісу.

Список використаних джерел:

1. Kim, Y., et al. (2023). AI model improves stratum corneum moisture content prediction from visible-light images. *Skin Res. Technol.*, 29(7), e13384.
2. Bielecka, A., et al. (2023). Quantitative assessment of hyperpigmentation using GLCM. *PubMed*, PMID 37629289.
3. Minh, D., et al. (2025). Self-supervised pretraining vs. ImageNet transfer learning for dermatological diagnosis. *arXiv*, 2505.16773.
4. Tan, M., & Le, Q. V. (2019). EfficientNet: Rethinking model scaling for CNNs. *ICML, PMLR* 97, 6105–6114.
5. Hu, M., & Yang, X. (2023). Attention-driven lightweight model for skin lesion detection. *arXiv*, 2308.02119.
6. Rahman, M., et al. (2025). CLIN-LLM: Safety-constrained hybrid framework for clinical diagnosis. *arXiv*, 2510.22609.
7. Shi, Z., et al. (2024). GMAI-MMBench: Multimodal evaluation benchmark for medical AI. *NeurIPS*.

*Камінський Д.О., магістрант,
Льовкін В.М., к.т.н. доцент
Національний університет «Запорізька політехніка»*

РОЗРОБКА ПРИКЛАДНОЇ ПРОГРАМИ ВИЗНАЧЕННЯ ВИПАДКІВ ПНЕВМОНІЇ НА ОСНОВІ ЗАСОБІВ МАШИННОГО НАВЧАННЯ ТА ВЕБФРЕЙМВОРКУ

Традиційний аналіз рентгенівських знімків залежить від людського фактору: втоми лікаря та суб'єктивності сприйняття, що може призводити до помилок. Нерідко сам доступ до медичних послуг може бути ускладненим, зважаючи на недостатню кількість медичних працівників. Це може не бути критичним фактором у випадку критичних станів, однак, коли спостерігаються тільки легкі симптоми, то візит до лікаря може відкладатись, стан пацієнта може ускладнюватися, а своєчасні заходи можуть бути не задіяні.

У цьому контексті автоматизація процесу аналізу медичних зображень за допомогою засобів машинного навчання є критично важливою задачею, яка дозволяє створити допоміжний інструмент для підтримки прийняття рішень лікарями.

Досить велика кількість сучасних досліджень присвячена визначенню випадків пневмонії. Сучасні підходи до аналізу медичних зображень базуються на використанні згорткових нейронних мереж, або convolutional neural network (CNN).

Розробку прикладної програми для виявлення випадків пневмонії було виконано на основі технологічного стеку, що включає мову програмування Python, фреймворк Django, бібліотеку Django REST Framework для забезпечення реалізації самої програмної системи як вебзастосунку, бібліотек TensorFlow і Keras для реалізації глибоких нейронних мереж.

Розроблена програмна система надає ряд функцій для пацієнта, лікаря та адміністратора, щоб забезпечити зручність підтримки роботи над виявленням випадків пневмонії та інформуванням про такі виявлені випадки.

Для пацієнта надається можливість:

- перегляду діагнозів та висновків, які були зафіксовані лікарем;
- перегляду рентгенівських знімків, які належать самому пацієнту;
- перегляду списку зафіксованих медичних випадків та відповідних статусів роботи над цими випадками.

Для адміністратора системи надається можливість:

- перегляду загальної статистики роботи програмної системи;

- перегляду записів усіх користувачів системи, змінювання даних їх профілів;

- керування моделлю класифікації випадків пневмонії на основі перезапуску навчання моделей штучних нейронних мереж різних архітектур, перегляду та керування збереженими чекпоінтами для створених моделей класифікації стосовно їх використання під час безпосередньо оброблення рентгенівських знімків;

- перегляду статистики підтвердження та скасування автоматизованих діагностувань випадків пневмонії лікарями.

Для лікаря надається можливість:

- перегляду списку доступних для лікаря медичних випадків;
- внесення нового і редагування існуючого медичного випадку;
- завантаження до вмісту медичного випадку рентгенівських знімків, внесення анотацій;
- пошуку серед всіх доступних лікарю медичних випадків за заданим ним пацієнтом;
- перегляду рентгенівських знімків та результатів, які було отримано після автоматичного розпізнавання;
- встановлення шляхом підтвердження та змінювання на той, який лікар вважає адекватним, остаточного діагнозу за рентгенівським знімком.

Для експериментального дослідження було використано набір даних з відкритого джерела Kaggle [1], що містить 5 863 рентгенівські зображення. На основі даного набору даних було проведене дослідження з застосуванням моделей:

- AlexNet;
- VGG19;
- ResNet50;
- MobileNetV2;
- DenseNet121.

Програмне забезпечення було використано для проведення експериментального дослідження, де ці моделі були порівняні. Модель AlexNet має найвищу точність розпізнавання на рівні 0,9628. У свою чергу найменші результати продемонструвала модель DenseNet121. Так точність моделі склала 0,9386.

Список використаних джерел:

1. Mooney P. Chest X-Ray Images (Pneumonia). URL: <https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia> (дата звернення: 25.03.2026).

УДК 004.9:61

*Яковишен П.О., аспірант,
Тужанський С.Є., к.т.н., доцент
Вінницький національний технічний університет*

ІМІТАЦІЙНА ОЦІНКА ВПЛИВУ АСИНХРОННОСТІ ДЖЕРЕЛ ДАНИХ НА СИНХРОНІЗАЦІЮ ТЕЛЕМЕДИЧНИХ СИГНАЛІВ

Анотація. в роботі розглянуто проблему синхронізації телемедичних сигналів від асинхронних джерел у розподілених системах. Оцінено вплив початкового часового зсуву та дрейфу годинників на точність синхронізації. Запропоновано модель асинхронності та виконано порівняння підходів до вирівнювання часових міток. Результати підтверджують необхідність врахування характеру асинхронності при виборі методів синхронізації.

Ключові слова: телемедичні системи, синхронізація сигналів, асинхронність, часові мітки, розподілена обробка.

Вступ. Розвиток телемедичних систем супроводжується переходом до розподіленої обробки даних, що поєднує периферійні пристрої, локальні вузли та хмарні сервіси. Це дозволяє зменшити затримки та навантаження на мережу. Водночас така архітектура ускладнює синхронізацію даних, оскільки сигнали можуть надходити з різних джерел із різними часовими характеристиками. Точність аналізу стану пацієнта залежить від узгодженості цих даних [1, 2].

Основною причиною порушення синхронізації є початковий часовий зсув і дрейф годинників джерел, що може призводити до значних похибок.

Методика та результати дослідження. Метою роботи є імітаційна оцінка впливу асинхронності джерел даних на точність синхронізації телемедичних сигналів у розподілених системах. Дослідження виконано шляхом моделювання двох потоків біомедичних сигналів (ECG – 250 Гц, PPG – 50 Гц) тривалістю 1200 с. Асинхронність описано афінною моделлю локального годинника, що враховує початковий часовий зсув і дрейф (0-150 ppm), який зумовлює лінійне накопичення похибки часу [3, 4].

Для синхронізації застосовано подійне вирівнювання на основі крос-кореляції та підхід з урахуванням дрейфу, що передбачає оцінювання як зсуву, так і масштабування часу. Як метрику використано залишкову похибку синхронізації.

Отримані результати показують, що за відсутності дрейфу подійне вирівнювання забезпечує низьку похибку (~8 мс), однак зі зростанням дрейфу його ефективність істотно знижується. Натомість методи з

урахуванням дрейфу забезпечують стабільну точність ($\approx 8\text{--}10$ мс) у всіх сценаріях, що підтверджує визначальний вплив характеру асинхронності джерел на ефективність синхронізації.

Висновки. Проведене дослідження показало, що початковий часовий зсув і дрейф локальних годинників суттєво впливають на точність синхронізації телемедицини сигналів.

Подійне вирівнювання є ефективним лише за відсутності або незначного дрейфу, тоді як у складніших умовах доцільним є використання методів, що враховують зміну частоти годинника.

Отримані результати підтверджують необхідність адаптивного вибору методів синхронізації з урахуванням характеристик джерел даних і умов функціонування телемедицини систем

Список використаних джерел:

1. Тужанський С. Є., Яковишен П. О. Аналіз методів передавання даних у телемедицини системах. Оптико-електронні інформаційно-енергетичні технології. 2024. № 47(1). С. 222–232. [Електронне джерело]. Режим доступу: <https://doi.org/10.31649/1681-7893-2024-47-1-222-232>

2. Alenoghena C. O., Ohize H. O., Adejo A. O., Onumanyi A. J., Ohiohin E. E., Balarabe A. I., Okoh S. A., Kolo E., Alenoghena B. Telemedicine: A Survey of Telecommunication Technologies, Developments and Challenges. Journal of Sensor and Actuator Networks, 12(2):20, 2023. [Електронне джерело]. Режим доступу: <https://doi.org/10.3390/jsan12020020>

3. IEEE Standard 1588-2008. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (Precision Time Protocol, PTP). Institute of Electrical and Electronics Engineers, 2008. [Електронне джерело]. Режим доступу: <https://standards.ieee.org/standard/1588-2008.html>

4. Mills D. L. Network Time Protocol Version 4: Protocol and Algorithms Specification. RFC 5905, Internet Engineering Task Force (IETF), 2010. [Електронне джерело]. Режим доступу: <https://www.rfc-editor.org/rfc/rfc5905>

Секція 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Заїка Д. В., Кобилін І. О.	Оптимізація алгоритмів коду у відеоіграх: сучасні тенденції та проблеми ефективності	3
Сосновська Є. Р., Осипова О. І.	Розробка програмного забезпечення для автоматизованого збору та аналізу даних ринку нерухомості	5
Царева О. С., Цап Д. І.	Енергоефективність програмного коду: аналіз сучасних тенденцій	7
Підкаура О. А.	Застосування алгоритму IDA* з використанням pattern database для оптимального розв'язання кубика Рубіка	9
Кльонов А. С., Колосовський А. С..	Застосування методу градієнтного спуску у виборі швидкості в моделі машинного навчання	11
Глинчук Л. Я.	Застосування великих мовних моделей для автоматичної генерації технічної документації під час реінжинірингу інформаційних систем	13
Іщенко Д. Г.	Інтеграція практик DevOps в управління життєвим циклом системи складської логістики	15
Бондарчук М. Ю., Горобець С. М.	Моделювання процесу розповсюдження забруднюючих речовин в атмосфері	17
Єрмаков В. А., Косенко С. І.	Огляд сучасних методів статистичного аналізу медичних даних	19
Шибасєва Н. О., Рудніченко М. Д., Шведов Д. В.	Аналіз сучасних підходів управління обробкою неконвенційних даних у транспортних системах	21
Закусило В. В.	Розробка системи тренування швидкого набору тексту з автоматичним аналізом помилки на основі лінгвістичних метрик подібності	23
Аблець А. В., Тронь В. В.	Гібридна фізично-інформована нейромережа для прогнозу споживаної потужності млина напівсамоподрібнення на годину вперед	25
Лупаренко О.	Комп'ютерне моделювання та аналіз динамічних режимів нелінійних систем у середовищі MATLAB	27

Нагорнюк О. А.	Математичне та програмне забезпечення розрахунку зон дії передавачів перешкод радіоканалам безпілотних літальних апаратів	29
Пономаренко А. В., Зайко Т. А.	Проблеми та перспективи інтелектуального опрацювання великих даних у розподілених системах діагностування	31
Мох Н. С., Корщенко В. С.	Порівняльний аналіз використання оперативної пам'яті масивами NumPy та стандартними списками Python	33
Трибюк В. О., Фант М. О.	Реалізація поведінкового шаблону стратегія для обробки взаємодій користувачів з об'єктами платформи Симулятор орбітальних механік	35
Жеребцов Д. В., Сергійко В. М., Бродський Ю. Б.	Тридіагоналізація стрічкових симетричних матриць	37
Сухарський С. С., Малашонок Г. І.	Архітектура Deep Q-Network як метод глибинного навчання з підкріпленням	39
Гирилович Д. С.	Актуальність та аналіз методів прогнозування врожайності сільськогосподарських культур	41
Яковенко В. Б., Пількевич І. А.	Гібридний метод статичного аналізу асимптотичної складності потоків виконання коду	43
Киселевич В. В.	Аналіз існуючих POS-систем управління	45
Держанівський А. О., Піонтківський В. І.	Оптимізація методу аналітичного моделювання орбітального руху при розв'язанні рівняння Кеплера із застосуванням алгоритму Ньютона-Рафсона	47
Жеребцов Д. В., Сергійко В. М., Локтікова Т. М.	Застосування принципів F.I.R.S.T. у написанні unit-тестів	49
Козлик С. О., Концидайло А. М.	Дослідження принципів побудови та проектування вебсервісу для бронювання житла	53
Пилипенко Є. В., Локтікова Т. М., Кушнір Н. О.	Атаки типу prompt injection на LLM-системи та методи захисту	55
Тороп М. Д., Чижмотря О. В.		57

Тороп М. Д., Чижмотря О. В.	Автоматизація тестування вебзастосунків з використанням LLM- агентів	59
Ботвін О. Ю., Кушнір Н. О.	Android-додаток для розвитку словникового запасу користувачів	61
Суханов Д. О., Безнос Д. В.	Структурно-функціональна організація навчальної системи наскрізного проектування цифрових автоматів	63
Усатий Т. Р.	Моделювання поведінки користувачів у вебсистемах малого бізнесу на основі аналізу клікстріму	67
Лавренчук С. О., Льовкін В. М.	Розробка програмного забезпечення навчання дизайнерів-модельєрів	69
Тушак В. С., Чижмотря О. В.	Інформаційна фрагментація у діяльності CFD-трейдера та засоби її подолання	71
Тушак В. С., Чижмотря О. В.	Поведінкові помилки та роль статистичного аналізу у прийнятті торгових рішень	73
Дрожаж В. Т., Концидайло А. М.	Особливості тестування вебплатформи для пошуку роботи або стажування	75
Лаєтін Д. А., Чижмотря О. Г.	Утилітарні класи Bootstrap vs семантичний CSS: вплив на швидкість розробки та підтримку проекту	77
Демчук О. В., Чижмотря О. В.	Адаптивний алгоритм тест-підбору дозвілля	79
Davydov V., Chyzhmotria O.	Personalized music recommendations based on user behavior analytics	81
Царук К. А., Чижмотря О. В.	Забезпечення інформаційної безпеки вебплатформи для організації волонтерської діяльності	83
Каштан С. С.	Математичне моделювання квазіідеальних течій у складних гідросистемах на основі числових методів комплексного аналізу	85
Васянович О. А., Морозов А. В.	Автоматизована генерація mock-даних у розробці стрімінгових сервісів	87
Царук К. А., Чижмотря О. В.	Розробка вебплатформи для організації волонтерської діяльності	89
Швець Д. В., Котов І. А., Карабут Н. О.	Механізми поліморфної адаптації Java- патернів під специфічні архітектури операційних систем	91

Демчук О. В., Чижмотря О. В.	Гейміфікація як інструмент утримання користувачів	93
Білотіл Я. О., Чижмотря О. В.	Генезис логістичної невизначеності та дефіцит адаптивності в архітектурах сучасних TMS	95
Білотіл Я. О., Чижмотря О. В.	Гібридизація методів ансамблевого навчання та рекурентних нейроструктур у задачах мінімізації часових відхилень	97
Білотіл Я. О., Чижмотря О. В.	Обґрунтування реактивної data-архітектури та вибір інструментального стека інтелектуальної логістичної платформи	99
Ігнатенко С. І., Чижмотря О. В.	Метод проєкційного текстування: аналоги та методи покращення	101
Ігнатенко С. І., Чижмотря О. В.	Інтеграція штучного інтелекту у процес рендерингу: перспективи та виклики	103
Дубина О. Ю., Льовкін В. М.	Розробка програмного забезпечення моніторингу стану худоби	105
Горобець В. І., Льовкін В. М.	Розробка програмного забезпечення прогнозування групової динаміки людських ресурсів підприємства	107
Захарова О. А.	Адаптивне формування тренувальних програм у мобільному застосунку «Тренер»	109
Сухарський С. С., Малашонок Г. І.	Тридіагоналізація стрічкових симетричних матриць	111
Денисенко Д. О., Єфремов Ю. М.	Проектування UX/UI-інтерфейсу веб-платформи для медіаконтенту	113
Денисенко Д. О., Єфремов Ю. М.	Веб-платформа для рецензування фільмів та серіалів	115
Петров Д. В., Єфремов Ю. М.	Веб-платформа читання ранобе	117
Петров Д. В., Єфремов Ю. М.	Архітектура системи персоналізації в веб-платформах для читання ранобе	119
Мінайленко В. Ю., Єфремов Ю. М.	Вебплатформа для торгівлі годинниками та аксесуарами з підтримкою аукціону та обміну	121
Мінайленко В. Ю., Єфремов Ю. М.	Проектування клієнтської частини вебплатформи для торгівлі годинниками на основі бібліотеки React	123

Секція 2. КОМП'ЮТЕРНА ІНЖЕНЕРІЯ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ

ІНФОРМАЦІЇ

Калашнікова Ю.В.	Нелінійні хвильові механізми передавання та обробки інформації в квантово-фотонних мережах	125
Баленко Г.І., Дячук О.Ю., Окунькова О.О.	Підходи UTM та Security Fabric у гетерогенних мережевих середовищах: порівняльний аналіз Cisco-рішень та Open-Source стеку	127
Приходько Д.С., Дячук О.Ю.	Аналіз методів та засобів виявлення вразливостей IT-інфраструктури на основі OpenVAS	131
Онищук О.О.	Дослідження ефективності SEO-оптимізації веб ресурсів на базі CMS WordPress	133
Фесенко Т.М.	Квантово-класичні гібридні алгоритми розв'язування нелінійних задач у високопродуктивних інформаційних системах	135
Живило Є.О.	Нелінійні квантові інформаційні процеси в адаптивних обчислювальних системах нового покоління	139
Кучма Ю.В.	Моделювання нелінійної динаміки інформаційних процесів на квантових симуляторах	143
Магалецька В.В.	Інформаційні технології на основі нелінійних квантових моделей	147
Поліновський В.В.	Хаотична та нелінійна динаміка як інструмент підвищення стійкості та безпеки інформаційних систем	149
Рубін Е.Ю.	Нелінійне керування відкритими квантовими системами в кіберфізичних та IoT-орієнтованих інформаційних технологіях	151
Ланчевич А.І., Балацька В.С., Полотай О.І.	Архітектура інтеграції блокчейн-технологій у підсистему аудиту комплексних систем захисту інформації	153
Пірог О.В., Шелуха О.О.	Формування системи управління інформаційною безпекою малого IT-підприємства в умовах підготовки до сертифікації ISO/IEC 27001	155
Жержерунов П.Ю., Шматко О.В.	Efficient Zero-Knowledge Proof Circuits for the SM3 Hash Function in Resource-Constrained Blockchain Systems	157
Кожихов К.О., Шматко О.В.	Enhancing Credit Scoring with Hybrid Quantum Machine Learning Architectures	159

Мостовий О.С.	Розподілений SMT-аналіз вразливостей бінарних файлів архітектури ARM64 на НРС-кластерах	161
Makovskiy I.Yu., Netrebko R.V.	Analysis of Regulatory and International Standards for the Formation of Security Profiles for Automated Systems	163
Ніколаєнко М.В., Шелуха О.О.	Моделювання інтегрованої системи контролю доступу для медичного закладу	165
Капранчук В.М., Шелуха О.О.	Дослідження якості та безпеки Wi-Fi мереж із використанням програмного сніффера	167
Левченко В.О., Миша М.А., Петляк Н.С.	Інтеграція штучного інтелекту в процес аудиту інформаційної безпеки	169
Костєрев Д.С., Шельвестер В.Я.	Роль оцінки ризиків у системі авторизації з безпеки автоматизованих систем класу "3", де обробляється інформація, що становить державну таємницю	171
Баленко Г.І., Брага В.Ю., Дячук О.Ю., Колощук М.С.	Інтелектуальна взаємодія протоколів OSPF та EIGRP: дослідження механізмів редистрибуції маршрутів у середовищах EVE-NG та Cisco Packet Tracer	173
Адамчук Р.С., Дячук О.Ю.	Програмна підсистема генерації, моніторингу та аналізу подій кібербезпеки на основі логів мережевого обладнання Cisco	177
Макаревич С.О., Дячук О.Ю., Колощук М.С.	Забезпечення захищеної маршрутизації в OSPF-мережах із використанням технологій VPN	181
Сергєєв В.М., П'ятаченко В.Ю.	Симуляція атак підміни координат у навігаційних даних для тестування моделей машинного навчання	183
Плахтій М.О.	Нелінійна постквантова автентифікація в федеративних системах	185
Пунько Х.М., Вовк Р.Б.	Методологічні аспекти забезпечення безпеки веборієнтованих інформаційних систем	187
Охрімчук В.В., Охрімчук І.А.	Метод виявлення повільних DDoS-атак	189
Аннюк П.Б., Вовк Р.Б.	Еволюція та архітектурні особливості інтелектуальних систем виявлення вторгнень у сучасному кіберпросторі	191
Штукований М.О., Духновська К.К.	Машинне навчання для виявлення семантичних помилок у коді	193
Трофімов О.С.	Метод комбінованого шифрування даних в хмарних середовищах	195

Габорець О.А.	Фішинг як базовий детермінант соціальної інженерії в системі кібербезпеки	197
Гончаров М.О., Малахов С.В.	Спиральні розгортки блоків вихідних даних як спосіб захисту стеганографічного контенту	201
Кравчук В.С., Дорогий Я.Ю.	Метрики ефективності захисту від кіберзагроз	205
Кравчук В.С., Дорогий Я.Ю., Цуркан В.В.	Критерій ефективності захисту від кіберзагроз	208
Макарик А.С., Фальковський І.Г.	Обґрунтування підходів до оптимізації застосування GPO з урахуванням архітектури та масштабу домену мережі	211
Слободянюк А.О., Бродський Ю.Б., Росіїнський Ю.М.	Системний моніторинг серверних і мережевих компонентів інформаційної інфраструктури як чинник забезпечення її стабільності	213
Зубелевич Д.І., Вандалович В.П.	Методи виявлення та протидії атакам на ланцюжки постачання у відкритому програмному забезпеченні	215
Добришин Ю.Є.	Загрози та ризики інформаційної безпеки у хмарних обчисленнях	217
Дричак Б.Я., Вовк Р.Б.	Методологія забезпечення стійкості глибоких нейронних мереж у інформаційно-комп'ютерних системах	219
Гладченко О.В., Луценко Н.О.	Особливості забезпечення кіберзахисту мережевої інфраструктури в умовах сучасних ризиків	221
Berdov V. V., Nechyporenko O.V.	Vehicle active safety computer system	225
Корнійчук В.В.	Проблеми та методи проєктування мережевих протоколів	227
Остапець Д.О., Русакевич С.Р.	Огляд і аналіз методів та засобів генерації випадкових чисел	229
Чекун М.А., Панченко В.І.	Розробка програмного комплексу для ієрархічного моделювання архітектур EOM	231
Красовський В.І., Шелуха О.О.	Дослідження ефективності передачі відеоданих у гетерогенних мережах з використанням кодека H.265+ та механізмів QoS	233
Адамчук Р.С., Дячук О.Ю., Колошук М.С.	Методи автоматизованого збору та аналізу даних з Telegram-спільнот у задачах OSINT	235

Лелета В.Р., Колошук М.С., Дячук О.Ю.	Використання штучного інтелекту для виявлення DDoS-атак у мережах корпоративного рівня	237
Ковальчук О.М., Колошук М.С., Дячук О.Ю.	Аналіз використання SOAR-платформ для автоматизації реагування на кіберінциденти	241
Martseniuk Y.	Building a Service Catalogue for Cloud Security	243
Гнатюк В.О.	Система аналізу мережевого трафіку з використанням методів машинного навчання для задач SIGINT	249
Шевченко А.Є., Ядуха Д.В.	Аналіз стійкості модифікованої криптосистеми AJP5-1 з узагальненими числами Мерсенна до атак на основі решіток	251
Ковальчук А.В., Ядуха Д.В.	Побудова модифікації постквантового механізму інкапсуляції ключа на основі AJP5	254
Литвинець Б.В., Шушура О.М.	Мінімізація впливу шахрайства та протидія зашумленню даних у системах кредитного скорингу	257
Боцанюк І.М., Головня О.С.	Адаптивна модель підвищення стійкості систем виявлення фішингу	259
Щур Н.О.	Криптографічна гнучкість у сучасних інформаційних системах	261
Палагін В.В., Івченко О.В., Палагіна О.А., Воробкало О.К.	Методи AI/ML для аналізу та нейтралізації кібератак на VLAN	263
Палагін В.В., Гончаров А.В., Пташкін Р.Л.	Методологія апаратного реінжинірингу та криміналістичного аналізу обчислювальних платформ	265
Остапеч Д.О., Панін Д.В., Пірогов Д.А.	Огляд джерел ентропії для генерування випадкових чисел	267
Дзюба В.В.	Розробка та навчання компактних мовних моделей для застосування в освітніх системах та кібербезпеці	269
Соловей В.А.	Офлайн конфіденційна комунікація без адресації у координатній криптографії	271
Соловей В.А.	Метаданонеітральні канали комунікації та крах моделі спостереження	273
Соловей В.А.	Моделювання онтологічно замкнених каналів зв'язку у координатній криптографії	275

Соловей В.А.	Еволюційні імпліцитні канали передачі інформації у координатній криптографії	277
Соловей В.А.	Фазово-еволюційні криптографічні системи: формальна безключова модель	279
Соловей В.А.	Координатне кодування у динамічно еволюціонуючих криптографічних просторах	281
Соловей В.А.	Логічна автентифікація без паролів	283
Соловей В.А.	Парадигма формування експоненційно стійких шифрокодів у координатній криптографії	285
Дячук О.Ю., Колошук М.С.	Використання алгоритму TurboQuant для підвищення ефективності систем моніторингу мережесих подій	287
Пятаков О.О., Колошук М.С.	Порівняльний аналіз можливостей GitHub CodeQL та OWASP ZAP в умовах DevSecOps-конвєєра	289
Хохлов М.О.	Вимоги стандартизації інформаційно-комунікаційної системи моніторингу ситуаційного центру	291
Рудюк Б.М.	Порівняльний аналіз GlobalProtect, Cisco Secure Client та FortiClient для захищеного віддаленого доступу в умовах кіберзагроз	293
Єфіменко А.А.	Адаптація методології DevOps для підвищення ефективності та безпеки IoT-систем	295
Сердійчук І.С., Єфіменко А.А.	Архітектурні рішення для моніторингу та розподілу ресурсів шлюзів безпеки гетерогенної мережі	297
Опанасенко Є.Р., Єфіменко А.А.	Оцінка впливу архітектури веб-додатку на частоту хибнопозитивних спрацювань при скануванні вразливостей	299
Опанасенко Є.Р., Бродський Ю.Б., Росіїнський Ю.М.	Аналіз та оцінювання ефективності застосування сканера OWASP ZAP на прикладі веб-додатку DVWA	301
Грищенко Д.С., Колошук М.С., Окунькова О.О.	Дослідження ефективності використання IAM-платформ для управління доступом у корпоративних інформаційних системах	303
Млинський Б.М., Дячук О.Ю., Колошук М.С.	Особливості забезпечення відмовостійкості в розподілених мережесих системах: аналіз проблеми Split-Brain та порівняння з автономними архітектурами	305
Лелета В.Р., Маєвський О.В., Бродський Ю.Б.	Інтелектуальний агент для аналітичної підтримки ситуаційного центру в задачах моніторингу надзвичайних подій	308

Левицька Т.О.	Кібербезпека та захист інтелектуальних алгоритмічних систем у криптовалютному трейдингу	310
Колошук М.С., Дячук О.Ю., Окунькова О.О.	Використання ADEM для виявлення аномалій та потенційних кіберзагроз у розподілених мережах	313
Миколайчук В. В.	DNSSEC як засіб захисту від DNS-спуфінгу в хмарній платформі Azure	316

Секція 3. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Коротун О.В., Чернець К.А.	Огляд сучасних кулінарних рекомендаційних систем	318
Галух А.О., Бондарчук В.О., Онищук О.О.	Порівняння протоколу http і технології websocket у сучасних вебсистемах	320
Венгловська Ю.В.	Вплив комп'ютерних ігор на креативність	322
Шабуня Д.Є., Шеховцова В.І.	Підходи до розробки IT-сервісу з організації та проведення заходів волонтерської організації	324
Романенко С.О.	Інтелектуальна адаптація інтерфейсів Користувача на основі поведінкової аналітики та методів машинного навчання	326
Лі Н.Д., Кобилін І.О.	Гібридний метод виявлення дублікатів Workflow для loga-моделей на основі структурного та поведінкового аналізу	328
Хіхло І.Д., Кунуп Т.В.	Використання штучного інтелекту в інформаційних системах	330
Кожанов А.Є., Євланов М.В.	Вдосконалення методу синтезу опису архітектури інформаційної системи	332
Кунуп Т.В., Сидоров Ю.М.	Administrator utility: утиліта централізованого керування системними обмеженнями Windows	334
Кунуп Т.В., Білоусов Д.О.	Експертна система для прогнозування рівня забруднення повітря у місті	336
Воловецький В.Б.	Програмне забезпечення для прогнозування ускладнень на газосховищах	338
Кунуп Т.В., Іванчиков О.І.	Особливості використання wmsystem для оптимізації управління складськими процесами	340
Лисенко А.Я., Грінченко Г.С.	Розробка інформаційної системи підтримки прийняття рішень для кваліметричного оцінювання ризиків енергетичних об'єктів	342

Горпiнiч I.O., Зайко Т.А.	Інтелектуальні методи забезпечення безпекитранзакційних даних та виявлення шахрайства	344
Казначєєва А.В.	Модель оцiнки та прогнозування енергоспоживання iot-пристроїв з урахуванням змiн зовнiшнього середовища	347
Прасол Н.С., Марчук Г.В.	Семантичний пошук вакансiй у вебпорталах працевлаштування на основi augmented generation	354
Олексюк О.С., Марчук Г.В.	Застосування навчання з пiдкрiпленням для побудови iнтелектуального автопiлота в авiасимуляторi	356
Мандрик О.В., Марчук Г.В.	Ігровий штучний iнтелект у симуляторах для моделювання реалiстичних сценарiїв	358
Одарченко Р.С., Ассаул О.Ю., Ищук К.І.	Оцiнка пiдходiв до оцiнки цифрової зрiлостi пiдприємств	360
Мойсєєв М.Г.	Методика iнтелектуального аналізу соцiальної активностi користувачiв для формування персонiфiкованих маркетингових стратегiй	362
Лазаренко М.В., Руднiченко М.Д., Шибєєва Н.О.	Аналіз iєрархiчних агентних моделей обробки мультимодальних даних в процесах розпiзнавання образiв	364
Панюшкін А.Ю., Руднiченко М.Д.	Розробка концепцiї системи вирiшення завдань нелiнійної оптимiзацiї на базi алгоритмiв ройового iнтелекту	366
Тимошенко Д.О., Руднiченко М.Д.	Аналіз сучасних малих мовних моделей для автоматизацiї процесiв асистування в онлайн-зустрiчах	368
Шведов Д.В.	Розробка алгоритму побудови гiбридних моделей iнтелектуального аналізу фiнансових ризикiв у сферi довгострокових iнвестицiй	370
Шумейко К.П.	Інтеграцiя методiв багатовимiрного аналiзу мультимодальних даних у задачах керування гiдроакустичними процесами	372
Зленський А.О.	Методологiчні пiдходи побудови адаптивних систем iнтелектуальних агентiв для задач аналізу та iдентифiкацiї об'єктiв	374
Голуб Д.К., Вишняк М.Ю.	Методи кореляцiї запитiв та вiдповiдей при асинхроннiй взаємодiї з apache kafka	376

Коротун О.В., Пасічник В.О.	Сучасні підходи та технології побудови інтелектуальної системи аналізу фізичного стану людини	378
Коротун О.В., Пасічник В.О.	Проектування та програмна реалізація інтелектуальної системи аналізу фізичного стану людини	380
Картамишев Д.О.	Мова програмування go у задачах автоматизації інфраструктурних процесів розподілених інформаційних систем	382
Гладченко О.В., Коваленко К.А.	Системний аналіз великих даних у фінансовому секторі	384
Сокорчук І.П.	Ефективне використання стандартних утиліт linux для пошуку дублікатів файлів	386
Батраченко С.М., П'ятаченко В.Ю.	Інформаційна система підтримки прийняття рішень для аналізу харчових звичок на основі android-додатка	388
Шумейко К.П.	Використання fusion-моделі для аналізу мультимодальних даних	390
Єдкін Д.Я. Сябрук. І.М.	Інтелектуальна CRM-система підтримки ветеринарного прийому з автоматичною рекомендацією препаратів за діагнозом	393
Гладченко О.В., Цикулова А.Е.	Автоматизація виробничих процесів як фактор підвищення конкурентоспроможності малого бізнесу	396
Гітіс В.Б., Флюд Д.В.	Інформаційна система для керування групами розмінування	400
Леус В.О., Савіцький Р.С.	Методи структуризації та збереження даних у системах візуального конструювання вебресурсів	402
Кунуп Т.В., Савранський Р.В.	Інформаційні технології та архітектурні рішення у системах спортивного менеджменту	404
Корецький Ю.І., Савіцький Р.С.	Порівняльний аналіз архітектурних патернів ізоляції даних у мультитенантних хмарних застосунках	406
Минець О.Р., Калита Н.І.	Ігровий discord-бот з автоматизованою системою монетизації та управлінням ієрархією користувачів	408
Берник А.О., Гришанович Т.О.	Розробка веборієнтованої системи бронювання залізничних квитків на основі клієнт-серверної архітектури	410
Pototskyi Maksym, Gamayun Igor, Kopp Andrii	Framework for testing small language models ability to assess bpmn quality	412
Гладченко О.В., Мітла М.О.	Моделювання процесів обробки даних у сучасних інформаційних системах	414

Савчук О.І.	Сучасні підходи та виклики у використанні машинного навчання для аналізу даних	416
Селіванов М.В., Пархоменко А.В.	Інтелектуальні методи та засоби проєктування інтерфейсів комп'ютерних систем	418
Фриз С.П., Авсієвич Р.О., Дацько Д.В.	Комплекс мультисенсорної розвідки в умовах розумного поля бою	420
Бабарицький Д.О., Білова Т.Г.	Формування системи аналітичних показників для виявлення аномалій у публічних закупівлях	422
Любиченко О.В., Горобець С.М.	Методи підвищення достовірності оцінок в системах рейтингування	424
Поздняков О.А., Пархоменко А.В.	Оцінювання невизначеності великих мовних моделей при генерації мігрованого користувацького апар-коду	426
Бадігон В.О., Петросян А.Р.	Розробка біометричної системи контролю доступу на базі архітектури edge-to-cloud	428
Штиль М.Р., Петросян Р.В.	Інтелектуальна система контролю доступу на основі біометричної ідентифікації облич в умовах обмежених ресурсів	430
Otreshko Ivan, Luchnoi Roman, Litvinova Uliya, Kopp Andrii	Datadriven approach to syntactic gateway quality analysis of business process models	432
Гладич Р. І.	Цифровізація процесів управління та супроводу наукової діяльності в умовах інформаційного середовища	434
Лебедєв О.Є., Глазок О.М.	Програмний засіб автоматизованого коментування у telegram-каналів	436
Мельников О.Ю., Пархоменко Ю.Д.	Розробка модульної системи керування поведінкою камери в середовищі unity	438
Шкільнюк Д.О., Коротун О.В.	Огляд різновидів міні-ігор	440
Дунай Д.А., Нікуліна О.М.	Інтеграція фізикоінформованих нейронних мереж в архітектуру iot-систем у контексті стратегії green it	442
Немеровський А.О., Коротун О.В.	Опис технології жанру tower Defense	444
Базалей В.А.	Використання просторово-статистичного підходу для оцінки пасажиропотоку під час автобусних перевезень	446
Жданюк М.Р., Марчук Г.В.	Адаптивна псевдовипадкова генерація у іграх як інструмент керування ігровим досвідом	448

Білокур С.Р.	Хмарні технології у побудові корпоративних інформаційних систем	450
Боданов Є.С., Глазок О.М.	Масштабування в kubernetes на основі спеціалізованого інтелектуального оператора	452
Гаврилюк А.Р.	Оцінка продуктивності розподілених cloudedge архітектур	454
Шевчук О.О., Гаврилюк А.Р.	Методи оптимізації маршрутів доставки в інформаційних системах логістики	456
Бондар В.С., Усата О.Ю.	Застосування фреймворку next.js для розробки системи рекомендацій відеоконтенту	458
Богачкін Ф.О.	Розробка інтелектуальної системи моніторингу зайнятості столів на основі iot та відеоаналітики	460
Прокоп'єв Д.М., Тітов С.В.	Інтелектуальна система для діагностики та моніторингу стану пацієнта	462
Даншина С.Ю.	Геопросторовий аналіз транспортної аварійності	464
Попко А.К., Ніколаско А.Ю.	Архітектура програмної системи моніторингу промислового обладнання	466
Камишан П.С., Кобилін І.О.	Моделі багатокритеріального Ранжування релевантності інформаційних блоків у мобільних системах супроводу	468
Kaimachnikova V.S.	Software modeling of in-memory vector Indexing performance for retrieval-augmented generation (rag) systems	470
Остапєць Я.Д.	Огляд інтелектуальних методів управління технологічними процесами на залізничних станціях	473
Бондарєв А.С., Г'ятченко В.Ю.	Аналіз методів обробки неповних даних для веборієнтованої системи підтримки прийняття рішень на основі машинного навчання	476
Катюха А.А.	Проектування та реалізація вебзастосунку Для просування відеоігор	478
Шкаруба А.В.	Онлайн сервіс для динамічної візуалізації даних	480
Петрівський В.Я., Мельник М.О.	Штучний інтелект у медичній діагностиці	482
Krasnokutskaya I.V., Hatsenko D.O.	High-performance data processing technologies in modern information systems based on gpu	484
Розбицький Р.Е., Петросян Р.В.	Порівняльний аналіз javascript-пантаймів у мікросервісній архітектурі	486

Татаренко Н.С., Петросян Р.В.	Аналіз використання groxtoх ve у середовищі homelab на споживчому обладнанні	488
Васьківська Д.С., Доровська С.О., Глазок О.М.	Застосування графових нейронних мереж у проектуванні інтегральних схем	490
Целуєв В.О., Савіцький Р.С.	Методи захисту персональних даних користувачів у геймерських соціальних мережах	492
Целуєв В.О., Савіцький Р.С.	Real-time комунікація у ігровій платформі засобами websocket	494
Черниш М., Коротун О.В.	Опис методів адаптивного керування поведінкою ші-агентів у файтингах	496
Залозний О.А., Савіцький Р.С.	Організація зберігання повідомлень, сповіщень та дій користувачів у вебплатформі аніме й манги	498
Безкоровайний В.В., Сирятський В.В.	Моделювання процесу багатокритеріального оцінювання програмного забезпечення для технологій дистанційної освіти	500
Вербіцький О.І.	Концепція інформаційної системи "психолог онлайн"	502
Кузнецов Д.О., Євланов М.В.	Управління бізнес-вимогами як ключовий фактор успішності проєктів: методичний аспект	504
Pushkar Anton, Yahup Kateryna, Kopp Andrii	Towards ml-driven architectural solution for preventing malicious sql transactions	506
Осауленко І.А.	Сучасні тенденції розвитку аналітичних проєктів з використанням штучного інтелекту	508
Васянович О.А., Морозов А.В.	Архітектура рекомендаційних систем в умовах відсутності статистики взаємодій	510
Tetyana Neroda	Determining priority factors for printing order execution through big data predictive analytics	512
Кисіль К.О.	Імпульсні нейронні мережі з гібридним кодуванням для обробки потокових даних у реальному часі	514
Красношاپка М.М., Одарченко Р.С.	Формування вимог до інформаційної системи підбору науково-педагогічних працівників закладів освіти	516

Секція 4. ЕЛЕКТРОНІКА, ЕЛЕКТРОННІ КОМУНІКАЦІЇ, ПРИЛАДОБУДУВАННЯ ТА РАДІОТЕХНІКА

Мельник А.О.	Статистичне оцінювання та побудова довірчих інтервалів для імпульсної перехідної функції	518
Пятін І.С., Бойко Ю.М.	RL мобільні телекомунікації з LDPC кодуванням	520
Залевський В.Й., Сидорчук О.Л., Волянський Є.А. Бобронніков А.С.	Зменшення радіолокаційної помітності антенних систем	522
	Створення модифікованих методів оцінки стану комфорту людини в житловому приміщенні з використанням моделі PMV	524
Андреев О.В.	Завадостійкий модем передавання команд керування рухомим об'єктом	526
Єгоян В.Б., Бурмістров С.В., Бондаренко В.В.	Апаратно-програмний комплекс ІОТ-сигналізації: інтеграція сучасних радіотехнічних та комунікаційних рішень	528
Жабський С.О., Снитюк С.О., Христинець Н.А.	Аналіз продуктивності та ресурсів пам'яті у проектуванні інформаційних систем на Arduino UNO	530
Соболенко С.О., Дубина О.Ф., Заєць Ю.О., Пивовар О.П.	Проблемні питання формування каналів зв'язку в підрозділах SHORAD	532
Горбачов І.О., Литвинюк О.М., Гнатюк В.О.	Метод прогнозування завантаження та розподілу ресурсів в телекомунікаційних системах	534
Карашук Н.М., Андріє Т.В.	Умова вибору частоти повторення зондувальних сигналів для усунення спільних неоднозначностей визначення кутових координат та дальності PCA	536
Кондратюк В.А., Макієвський О.А., Ципоренко В.В.	Система добового контролю чадного газу з використанням трансивера NRF24L01 та ESP8266	538
Підкаменний О.М., Ципоренко В.В.	Розроблення системи моніторингу присутності та переміщення в приміщенні на базі ІОТ технологій	540
Пономаренко І.С.,	Розробка омметра на основі Arduino	542

Ципоренко В.Г.	UNO	
Сорокін Д.А., Зилевіч М.О.	Фактори техногенного та геометричного впливу на точність локалізації об'єктів у мережах LORA	544
Горшенін О.Є.,	Аналіз характеристик методу навігації БПЛА за полем радіовипромінювань від низькоорбітальних телекомунікаційних космічних апаратів: досягнення та недоліки	546
Клочко К.А., Журавель Р.В., Завгородній Д.А., Куропятник Б.В., Ломоносов М.С.	Інтегрована ІОТ-система моніторингу та керування інфраструктурою населених пунктів	548
Віктор Гнатюк, Левон Петросян	Метрики операційної резильєнтності для оцінювання телекомунікаційних мереж на основі Network Digital TWIN	550
Клочко К.А., Коваленко Д.В., Вантух М.В., Черняков М.Є., Лан В.В.	ІОТ-система моніторингу інфраструктури та екологічного стану населених пунктів	552
Бугайов М.В.	Двоканальний метод амплітудного пеленгування з компенсацією рівня шуму	554

Секція 5. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Шуліка О. С.	Цифрові освітні сервіси як засіб формування професійної компетентності майбутніх учителів інформатики	556
Куцан А. В.	Створення та впровадження інтерактивного освітнього контенту	559
Казаков Н. С., Ніжегородцев В. О.	Аналіз сучасних прототипів інтерфейсів комерційних вебсередовищ освітніх послуг	561
Матвієнко Л. Г.	Мультимодальні цифрові платформи у викладанні іноземних мов у закладах вищої освіти	563
Будзінська О. О.	Принципи семантичного аналізу даних у цифровому освітньому середовищі та	567

Дягилева О. С., Юрженко А. Ю., Свирида В. С., Кононова О. С.	його вплив на систему управління інформаційною безпекою Використання платформи Discourse у морській освіті та підготовці	569
Слісаренко Р. В., Дейнеко Ж. В.	Модель представлення та інтерпретації результатів тематичного аналізу для віртуального асистента дистанційного навчання	571
Тітарчук С. В., Малежик П. М.	Метод оптимізації доступу до архівних документів у системах електронного документообігу з урахуванням потреб освітнього процесу	573
Ушаткіна С. О.	Інформаційно-комунікаційні технології як засіб формування навчальної мотивації здобувачів освіти	575
Філіпчук М. П., Мельничук Н. І., Філіпчук О. І.	Побудова та візуалізація деяких різновидів графів	577
Ястребова А. В., Вакалюк Т. А.	Необхідність розробки вебсистеми з оптимізації управління науковою роботою здобувачів ступеня доктор філософії	579
Хомочкін А. П., Мигун А. О., Красношлик О. Ю.	Дослідження впливу коливань магнітного поля, що виникають під час навчального процесу в момент перебування учнів школи в укритті	581
Зварич О. Л., Вовк Р. Б.	Методологічні засади впровадження адаптивних систем навчання у вищій освіті на основі штучного інтелекту	583
Косовський С. Б., Кобилін І. О.	Впровадження VR-технологій в освітній процес: можливості та виклики	585
Кривонос О. М.	Персоналізація навчання програмування на основі адаптивних цифрових середовищ	587
Олексієнко А. О., Вовк Р. Б.	Методологія підготовки інженерів програмного забезпечення в умовах імплементатії генеративного штучного інтелекту	589
Сікора Я. Б.	Концепція «human-in-the-loop» у	591

Карман О. С., Малежик П. М. Чінкує П.	цифровій освіті VR-технології як частина комп'ютерної 3D-графіки та їх застосування в навчанні Інтелектуальна VR/AR-платформа з адаптивним навчанням на основі штучного інтелекту	593 595
Смотр О. О.	Інтелектуальні системи підтримки прийняття рішень для стратегічного управління освітою у сфері цивільного захисту	597
Довгаль І. А.	Інформаційно-комунікаційні технології як інструмент опанування професійної англійської мови майбутніми інженерами-металургами	599
Шевчук П. Г., Гиндич І. Є.	Міжнародна STEM-програма FIRST LEGO League та навчання інформатики у ЗЗСО	601
Безкоровайний В. В., Кисельова О. Б., Щербак І. В. Сокорчук І. П.	Адаптація комп'ютерних мереж при впровадженні технологій індивідуалізації навчання Будова автоматизованого робочого місця викладача для освітнього процесу в дистанційній формі	605 607
Михайлюк О. В.	Методи збору та обробки даних про стан сервісів у операційній системі Windows	609

Секція 6. ЦИФРОВА ОБРОБКА СИГНАЛІВ ТА ЗОБРАЖЕНЬ В АВТОМАТИЗОВАНИХ ТА ІНФОРМАЦІЙНО- ВИМІРЮВАЛЬНИХ СИСТЕМАХ

Андрікевич С.А., Щербатюк А.В., Тужанський С.Є.	Метод покращення зображень очного дна на основі фазового підходу	611
Бугайов М.В., Поздняков В..	Метод просторово-спектрального оброблення групових акустичних сигналів гвинтомоторних літальних апаратів	613
Горобець О.С., Подчашинський Ю.О., Чепок Л.О.	Методи визначення якості поверхні облицювальних виробів з природного каменю	615
Григоренко І.В., Лашков А.Г.	Удосконалена комп'ютеризована вимірювальна система для контролю	617

Григоренко І.В., Лиска С.В., Григоренко С.М. Зімчук І.В., Шапар Т.М.	виготовлення макаронних виробів Комп'ютеризована система контролю виробництва твердого сиру	619
Іващев Д.В., Герасимов В.В., Король А.В. Іщенко О.С., Подчашинський Ю.О., Чепюк Л.О.	Алгоритм комплексованої фільтрації вимірювань в супутникових системах навігації безпілотних літальних апаратів Виявлення та інтерполяція пропусків у телеметричних даних моніторингу палива транспортних засобів Порівняльний аналіз датчиків вимірювання рівня рідини в комп'ютеризованих інформаційно- вимірювальних системах	621 623 625
Левицький А.В., Подчашинський Ю.О., Єфіменко Н.А., Чепюк Л.О. Лугових О.О., Наумчук В.А.	Статистичні методи аналізу зображень з інформацією про геометричні параметри та параметри руху об'єктів Порівняння метрологічних та експлуатаційних характеристик ультразвукових і турбінних витратомірів газу	627 629
Магалецький Я.В., Безвесільна О.М., Подчашинський Ю.О., Чепюк Л.О.	Частотний вимірювальний канал комп'ютеризованої інформаційно- вимірювальної системи контролю механічних параметрів асинхронних двигунів	633
Рудич М.В., Духновська К.К.	Методи відновлення зображень на основі дифузійних моделей у задачах цифрової обробки сигналів	635
Свістельник О.С., Чепюк Л.О.	Метрологічне забезпечення мікропроцесорної інформаційно- вимірювальної системи контролю параметрів мікроклімату на поліграфічному виробництві	637
Ступак А.Г., Подчашинський Ю.О., Чепюк Л.О.	Оцінка ефективності стиснення зображень в інформаційно- вимірювальних системах медичного застосування	639
Товстік С.О., Подчашинський Ю.О.,	Ефективність застосування систем стеження за рухом сонця для	641

Дерев'янка О.В. Федоренко І. О., Громико І. О.	фотоелектричних модулів Алгоритм біспектральної обробки зображень для автоматизованої селекції аномалій в умовах низького теплового контрасту	643
Чінкує Камелія	Алгоритми автоматичної растеризації векторної графіки в задачах поліграфічного друку	645
Юдіна Л.Г., Апенько Н.В.	Вплив геометричних параметрів зйомки на точність розпізнавання об'єктів	647
Shcherbak A. Ye.	Reflection-decoupled analysis in the tdr signal digital processing pipeline	649

Секція 7. КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ ТА РОБОТОТЕХНІКА

Prykhodko A.	Automation of wastewater treatment processes using digital technologies	651
Pysarets A., Pysarets O.	Computer-integrated systems for the energy carriers metering	653
Голуб Д. А., Бондаренко В. В.	Технології занурення як фактор формування ефекту присутності у VR	655
Барабаш В. В., Ткачук Д. Ю.	Розробка системи автоматичного картографування місцевості з використанням безпілотних літальних апаратів	657
Біленький І. О., Добржанський О. О.	Розробка системи автоматичної посадки БПЛА з використанням візуальних маркерів	659
Василевський Д. В., Кравчук А. Р.	Дослідження методів енергоефективного керування безпілотними апаратами під час виконання тривалих місій	661
Захарчук Г. А., Ткачук А. Г.	Розробка системи автоматичного стеження БПЛА за рухомим об'єктом	663
Любченко І. В., Кравчук А. Р.	Моделювання системи стабілізації квадрокоптера з використанням PID- регулятора	665
Манзевитий В., Покляченко О. В.	Прогнозування електроспоживання в енергетичних системах із використанням методів машинного навчання	667
Антонюк О., Ткачук А. Г.	Інтелектуальна система автономної навігації мобільного робота на основі	629

Вернидуб Б. Д., Кравчук А. Р., Пуховський Є. С.	комп'ютерного зору Розробка системи автоматичного керування рівнем рідини в резервуарі	672
Зіновчук О., Добржанський О. О.	Розробка систем автоматичного керування мікрокліматом у теплиці	674
Катков А. О., Покляченко О. В.	Забезпечення кібербезпеки комп'ютеризованих систем управління об'єктами електроенергетики	676
Кондур С. В., Ткачук Д. Ю.	Система автоматичного виявлення та локалізації людини дроном у пошукових операціях	678
Шпаківський, Ткачук А. Г.	Побудова комп'ютеризованих систем керування електричним навантаженням промислових енергетичних комплексів	680
Яременко Д., Ткачук Д. Ю.	Розробка системи уникнення перешкод для автономного дрона з використанням глибинного навчання	682
Токовий Д. А., Покляченко О. В.	Автоматизована система забезпечення якості електричної енергії в розподільних мережах	684
Кучма Ю. В.	Моделювання нелінійної динаміки інформаційних процесів на квантових симуляторах	686
Живило Є. О.	Нелінійні квантові інформаційні процеси в адаптивних обчислювальних системах нового покоління	690
Сеспедес Гарсія П. Д., Сеспедес Гарсія Н. В.	Оцінка залишкового ресурсу трубопроводів з урахуванням корозійних зон	694
Моргун Є., Добржанський О. О., Пуховський Є. С.	Нейромережева система виявлення дефектів у промислових об'єктах	696
Раданович В. Я., Ткачук Д. Ю., Крижанівська І. В.	Застосування нейромереж для прогнозного обслуговування електричних двигунів на основі вібраційних та електричних сигналів	698
Чумакевич В. О., Пулеко І. В., Орішук І. О., Оніщенко О. О.	Застосування прямого керування моментом асинхронного двигуна в рушійних системах наземних роботизованих комплексів	700

Ящук Ю. Л.	Вплив комп'ютерно-інтегрованих технологій на управління процесами в соціально-економічних системах	702
Люта А. В.	Модернізація системи управління приводом переміщення електродів дугової сталеплавильної печі з використанням нечіткого контролера	704
Дейнеко А. О., Духновська К. К.	Система реального часу для керування автономним агентом	706
Ткачук В. Ю., Добржанський О. О.	Нейромережеві методи прогнозування енергетичного стану БПЛА для реалізації автономної системи заряджання	708
Безвесільна О. М., Ткачук А. Г., Толочко Т. О., Гриневич М. С.	Інтелектуальна дослідницька система для вимірювань корисних копалин	710

Секція 8. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У БІОМЕДИЦИНІ

Ветров А.О., Нікітчук Т.М.	Розробка мобільного додатку на основі штучного інтелекту для діагностики дегідратації шкіри	712
Камінський Д.О., Льовкін В.М.	Розробка прикладної програми визначення випадків пневмонії на основі засобів машинного навчання та вебфреймворку	715
Яковишен П.О., Тужанський С.Є.	Імітаційна оцінка впливу асинхронності джерел даних на синхронізацію телемедичних сигналів	717

Наукове видання

**Тези XVI Міжнародної
науково-технічної конференції
«Інформаційно-комп'ютерні технології»**

Житомир, 02-03 квітня 2026 р.

Відповідальний за випуск:

Ю.В. Венгловська