

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УНІВЕРСИТЕТ "УКРАЇНА"**

Інститут комп'ютерних технологій

**КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ:
ОСВІТА І НАУКА**

Тези доповідей
XVI всеукраїнської конференції
м. Київ, 10 червня 2025 року

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УНІВЕРСИТЕТ "УКРАЇНА"**

Інститут комп'ютерних технологій

**КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ:
ОСВІТА І НАУКА**

**Тези доповідей
XVI всеукраїнської конференції
м. Київ, 10 червня 2025 року**

Київ - 2025

УДК 004
К63

Затверджено до друку

*Вченою радою Інституту комп'ютерних технологій
Відкритого міжнародного університету розвитку людини «Україна»
(протокол № 3 від 17.06.2025 р.)*

Відповідальний за випуск: Наталія ОДРІБЕЦЬ

Редакційна група Відкритого міжнародного університету розвитку людини «Україна»: Таланчук П.М. (головний редактор), Давиденко Г.В., Одрібець Н.В., Забара С.С., Додонов О.Г., Дуднік А.С., Писарчук О.О., Зеленський К.Х., Зайцев В.Г., Поліновський В.В., Тимошенко А.Г., Павленко В.І., Кіт Г.В., Павленко О.Ю.

Комп'ютерні технології: освіта і наука: тези доповідей XVI Всеукраїнської конференції (м. Київ, 10 червня 2025 р.). — К.: Університет «Україна», 2025. — 105 с.

ISBN 978-966-388-727-2

DOI: 10.36994/978-966-388-727-2-2025-105

У збірнику вміщено тези доповідей XVI Всеукраїнської конференції «Комп'ютерні технології: освіта і наука», в яких відображено сучасні тенденції у сфері комп'ютерних наук, інформаційних технологій та інших суміжних галузей. Інноваційні підходи в освіті та науці, актуальні проблеми інфокомунікаційних та комп'ютерних технологій, роль технологій у сучасному навчанні та дослідженнях, вплив інформаційних технологій на суспільство та бізнес.

Конференція відбулась в рамках реалізації наукових досліджень: «Метод захисту неструктурованої інформації на мобільних пристроях що використовуються в адаптивних кейс-менеджмент системах» № 0124U000025 та «Імітаційна модель навігації та дешифрування мап з дронів для точних геоінформаційних додатків» № 0124U000036.

ISBN 978-966-388-727-2

DOI: <https://doi.org/10.36994/978-966-388-727-2-2025-105>

© Університет «Україна», 2025

Програмний комітет конференції:

Голова:

Таланчук П.М. – д.т.н., проф., академік АПН України;

Члени:

Ольшанська О.А. - д.е.н., професор, проректор з наукової і міжнародної діяльності Університету «Україна»;

Одрібець Н.В. – к.ф.-м.н., доцент, директор Інституту комп'ютерних технологій Університету «Україна»;

Забара С.С. – д.т.н., професор, почесний директор Інституту комп'ютерних технологій Університету «Україна»;

Додонов О.Г. - д. т. н., професор, Інститут проблем реєстрації інформації НАН України;

Дуднік А.С. - д. т. н., професор, Київський національний університет імені Тараса Шевченка;

Писарчук О.О. – д. т. н., професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;

Зеленський К.Х. – д. т. н., професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;

Зайцев В.Г. - д. т. н., професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;

Тимошенко А.Г. – к.т.н., професор Університету «Україна»;

Павленко В.І. – к.ф.-м.н., доцент Університету «Україна»;

Кіт Г.В. – к.т.н., директор Івано-Франківської філії Університету «Україна»;

Організаційний комітет конференції:

Голова комітету:

Таланчук І.В. – перший проректор Університету «Україна»;

Заступник голови комітету:

Одрібець Н.В. – к.ф.-м.н., директор Інституту комп'ютерних технологій;

Члени комітету:

Дуднік А.С. - д. т. н., професор, Київський національний університет імені Тараса Шевченка;

Морозова І.В. – в.о. завідувача кафедри комп'ютерної інженерії;

Веденєва О.А. – в.о. завідувача кафедри інформаційних технологій та програмування;

Павленко В.І. – к.ф.-м.н., доцент Університету «Україна»;

Самарай В.П. – к.т.н., доцент Університету «Україна»;

Тимошенко А.Г. – к.т.н., професор Університету «Україна»;

Ізварін І.В. - к.т.н., доцент Університету «Україна»;

Авдалов Г.В. – ст.викл. Університету «Україна»;

Павленко О.Ю. – інженер-дослідник Університету «Україна»;

Молчанов А.О. – к.т.н., зав. лабораторії кіберфізичних систем імені Максима Петренка.

Зміст

<i>Таланчук П.М.</i> Вступне слово	8
<i>Авдалов Г.В., Самарай В.П.</i> Визначення ефективних гібридних криптографічних схем проти квантових загроз	10
<i>Авдалов Г.В., Самарай В.П.</i> Підходи до переходу на постквантову криптографію: аналіз документа nist ir 8547 (2024)	13
<i>Близнюк А.В., Писарчук О.О.</i> Математичне моделювання ризиків витоку даних з інформаційних систем.....	16
<i>Богун Р.І.</i> Інтегровані середовища розробки з підтримкою штучного інтелекту: нові можливості для вивчення програмування студентами	19
<i>Богущький А.І., Тимошенко О.М.</i> Використання штучного інтелекту для проєктування мікросервісної архітектури	21
<i>Борисенко О.С., Тимошенко А.Г.</i> Захист арі у хмарних додатках: ризики та підходи	23
<i>Бровченко Є.М., Самарай В.П.</i> Адаптивний метод захисту інформації в мобільних пристроях на основі поведінкової моделі	25
<i>Войтех Д.В., Тимошенко А.Г.</i> Порівняння алгоритмів мультиагентного навчання з підкріпленням для децентралізованого управління енергоспоживанням.....	28
<i>Григор'єв К.С., Грищенко В.Ю., Павленко В.І.</i> Архітектура дерін для децентралізованого зберігання персональних архівів із дотриманням вимог gdpr	30
<i>Грищенко В.Ю., Григор'єв К.С., Павленко В.І.</i> Техніко-економічна оцінка дерін-орієнтованої мережі зберігання персональних архівів	33
<i>Демидов А.С., Даценко І.П.</i> Аварійне відновлення у хмарних мережах. Використання aws global accelerator у сценарії аварійного відновлення.....	36
<i>Денисюк О., Павленко В.І.</i> Адаптивні методи оптимізації rag-систем в освітніх технологіях	39

<i>Дробіт Б.В., Тимошенко А.Г.</i> Автоматичне оцінювання письмових завдань студентів за допомогою гібридних семантичних підходів фінгерпринтування	41
<i>Дуднік А.С., Батрак О.Г.</i> Алгоритми позиціонування дрона за допомогою gps та машинного зору.....	43
<i>Ємець М.І., Даценко І.П.</i> Економіка довіри у віртуальних освітніх метавсесвітах як інструмент соціальної токенизації, nft-сертифікації та dao-управління.....	45
<i>Жиритовський О.А.</i> Аналіз недоліків сучасних мов програмування та проектування нової мовної парадигми	47
<i>Загорулько А.В., Павленко В.І.</i> Модульні сі/сd системи, переваги, архітектура та виклики.....	50
<i>Йовдій Г.Г.</i> Архітектура безпечного цифрового середовища для засуджених: пілотна модель «цифрова свобода»	52
<i>Мельников О.Ю., Грищук Д.В.</i> Розрахунок коефіцієнта ймовірності помилки в слові для використання в додатку для діагностики дислексії у дітей	55
<i>Мельников О.Ю., Канішев В.О.</i> Вебзастосунок для аналізу кольорової палітри сайтів для людей з порушенням кольоросприйняття.....	58
<i>Касілов Д.В., Писарчук О.О.</i> Розвиток штучного інтелекту в синтезі інформаційних систем	61
<i>Кошара А.В., Писарчук О.О.</i> Інтеграція платформ threat intelligence у сіem-системи для покращення виявлення кіберзагроз.....	65
<i>Левченко Л.І.</i> Використання штучного інтелекту в закладах вищої освіти.....	68
<i>Михайленко О.О.</i> Архітектура стійких мікросервісів: як проектувати на відмову	72
<i>Міронов Ю.Г.</i> Особливості zero-code підходу для створення веб-ресурсів.....	74
<i>Павлик В.Ю., Самарай В.П.</i> Генеративні ші-асистенти для адаптивних cad-інтерфейсів.....	76

<i>Podlesny S.</i>	
Ai-influenced transformation of higher education	79
<i>Одрібець Н.В.</i>	
Інтелектуальна система генерації тестових завдань з вищої математики	81
<i>Одрібець С.П.</i>	
Методологія побудови навчального розкладу з використанням цілочисельного програмування	83
<i>Рожков С.М., Павленко В.І.</i>	
Оптимізація партиціювання та індексації у високонавантажених базах даних у хмарних сервісах	85
<i>Рубаняк Т.М., Тимошенко О.М.</i>	
Удосконалення систем управління складською логістикою	88
<i>Топалов А.М.</i>	
Інформаційно-вимірювальна система екологічного моніторингу водного середовища на основі технологій ші та ір	91
<i>Фесенко А.О. Дуднік А.С.</i>	
Сучасний стан та перспективи розвитку квантових технологій	94
<i>Хрипко С.Л.</i>	
Використання блокчейн-технології для створення дистрибутивних додатків.....	96
<i>Шкітов А.А., Тимошенко А.Г.</i>	
Системно-порівняльний аналіз ефективності типових алгоритмів в оптимізації бізнес-процесів	99
<i>Юшко О.В., Самарай В.П.</i>	
Методи перетворення супутникових rgb зображень в ір у розрізі візуальної навігації бпла	103

ВСТУПНЕ СЛОВО

Шановні колеги, науковці, та студенти! Шановні розробники і воїни цифрового фронту!

Сьогодні ми відкриваємо XVI Всеукраїнську конференцію «Комп'ютерні технології: освіта і наука» — захід, що став не лише науковим форумом, а й дзеркалом змін, які переживає наша держава та весь світ у XXI столітті. Ця конференція проходить у час, коли знання перетворюється на силу, а технології — на зброю задля ПЕРЕМОГИ.

У представлених анотаціях — я бачу не просто наукові дослідження. Я бачу портрет нового покоління українських фахівців — людей, які будують цифровий щит нашої країни.

Дослідження, присвячене інтеграції децентралізованих ідентифікаторів та доказів з нульовим розголошенням, показує, як майбутнє Web3 може бути не лише зручним, а й безпечним. Це — інструмент цифрової незалежності, яка така ж важлива, як і енергетична чи економічна.

Анотації, що стосуються кіберзахисту, безпеки API в хмарних середовищах, SIEM-систем, нагадують нам, що в умовах постійних атак агресора на український кіберпростір — кожен програміст стає кібервоїном.

Роботи з напрямів мультиагентного навчання, управління енергоспоживанням, DePIN, автоматизації зберігання даних, — це вже сьогодні формує основу цифрової стійкості інфраструктури держави, яку не можна зруйнувати ракетами.

Дослідження, присвячені генеративному ШІ (штучного інтелекту), адаптації його до CAD-середовищ, візуальному аналізу для людей з особливостями сприйняття кольорів, інструментам для діагностики дислексії, — відкривають двері до доступної, інклюзивної, гуманної освіти, де кожен має шанс.

Важливо й те, що окремі анотації торкаються штучного інтелекту в освіті, критичного мислення студентів, впровадження постквантових криптоалгоритмів, автоматизації бізнес-рішень — тем, які знаходяться на вістрі глобальної наукової думки.

Ми бачимо, що конференція охоплює спектр найактуальніших викликів сучасності — від воєнного застосування штучного інтелекту та обробки супутникових даних до zero-code платформ і нових мов програмування. І це не абстрактні дослідження — це відповіді на реальні виклики, з якими стикається українське суспільство щодня.

Сьогодні український IT-фронт не менш важливий, ніж бойові дії на передовій. Саме ви — ті, хто створює технології, які забезпечують зв'язок на полі бою, точне цілевказання, безпечний обіг даних, а головне — стратегічну перевагу.

Після операції «ПАВУТИННЯ», яка стала символом нової епохи технологічної війни, навіть ті, хто не розумів значення цифрових інструментів, визнали: сучасна війна — це не лише дрони і ракети, а й алгоритми, дані, мережі, коди.

Ця операція відкрила очі суспільству на те, що перемога в XXI столітті неможлива без цифрового інтелекту, без синергії науки, інженерії, оборони та освіти.

Україна виборює своє майбутнє і на землі, і в кіберпросторі. Саме ви, учасники цієї конференції — викладачі, студенти, дослідники, практики — формуєте наукову, технічну і моральну спроможність нашої країни в епоху змін.

Я впевнений, що після нашої перемоги — а вона неодмінно буде — саме ви станете тими фахівцями, які збудують нову Україну:

відкрити, але безпечно захищену;

цифрову, але глибоко гуманістичну;

сучасну, але збережену для майбутніх поколінь.

Бажаю всім учасникам конференції плідної праці, змістовних дискусій, натхнення і нових ідей, які, можливо, вже завтра змінять хід історії.

Бажаю нашій конференції творчих звершень, нових наукових відкриттів, плідної співпраці та впевненого руху до перемоги – у науці, у технологіях, в Україні.

Слава Україні! Слава українському інтелекту! Слава тим, хто програмує перемогу! Щиро дякую за увагу!

Петро ТАЛАНЧУК

*доктор технічних наук, професор,
дійсний член Академії педагогічних наук України,
заслужений діяч науки і техніки України,
Президент Університету «Україна»*

ВИЗНАЧЕННЯ ЕФЕКТИВНИХ ГІБРИДНИХ КРИПТОГРАФІЧНИХ СХЕМ ПРОТИ КВАНТОВИХ ЗАГРОЗ

Авдалов Герман Вікторович

І курс, група КІ-24-1phd, спеціальність “Комп’ютерна інженерія”

Інститут комп’ютерних технологій Університету “Україна”, м Київ,

Україна

<https://orcid.org/0009-0007-7728-6659>

germannavdalov@gmail.com

Науковий керівник: Самарай В. П., к.т.н, с.н.с., доцент

samaraj@ukr.net

***Анотація.** Швидкий прогрес у розробці квантових комп’ютерів створює неминучу загрозу існуючим криптографічним стандартам. Гібридна криптографія, що поєднує класичні та постквантові алгоритми, є перспективним рішенням для забезпечення довгострокової безпеки даних. Пропонується п’ять ключових напрямків визначення та оцінки ефективності таких схем, фокусуючись на аспектах безпеки, продуктивності та адаптивності в умовах еволюції квантових загроз. Акцентується увага на необхідності розробки формальних методів верифікації, комплексного аналізу стійкості до гібридних атак, експериментальної оцінки продуктивності, створення адаптивних схем та стандартизації критеріїв оцінки.*

***Ключові слова:** гібридна криптографія, постквантова криптографія, квантові загрози, безпека, продуктивність, формальна верифікація.*

***Abstract.** The rapid progress in the development of quantum computers poses an imminent threat to existing cryptographic standards. Hybrid cryptography, which combines classical and post-quantum algorithms, is a promising solution for ensuring long-term data security. Five key areas for defining and evaluating the effectiveness of such schemes are proposed, focusing on aspects of security, performance, and adaptability in the context of the evolution of quantum threats. The emphasis is on the need to develop formal verification methods, comprehensive analysis of resistance to hybrid attacks, experimental performance evaluation, creation of adaptive schemes, and standardization of evaluation criteria.*

***Keywords:** hybrid cryptography, post-quantum cryptography, quantum threats, security, performance, formal verification.*

Вступ

Враховуючи стрімкий прогрес у квантових обчисленнях, що створює безпрецедентну загрозу сучасній криптографії, світ потребує надійних рішень для захисту даних. Гібридна криптографія, що поєднує перевірені класичні та новітні постквантові алгоритми, є найперспективнішим підходом для безпечного переходу до постквантової ери. Метою цього дослідження є визначення та обґрунтування ключових критеріїв та методик оцінки ефективності таких гібридних криптографічних схем. Створення комплексного підходу, який забезпечить

надійність, продуктивність та адаптивність цих систем перед майбутніми квантовими загрозами.

Формальні методи верифікації безпеки гібридних схем

Наразі оцінка безпеки гібридних криптосистем часто залежить від інтуїції або припущень про незалежність компонентів. Наша пропозиція полягає у розробці строгих математичних моделей та формальних методів доведення безпеки, які враховуватимуть потенційну взаємодію та залежності між класичними та постквантовими компонентами. Це забезпечить надійну основу для оцінки стійкості до гібридних атак, що поєднують квантові та класичні методи, дозволяючи виявляти вразливості, які можуть виникнути на стику двох парадигм.

Комплексний аналіз стійкості до різноманітних квантових атак

Ефективність гібридних схем має оцінюватися не лише з погляду відомих квантових алгоритмів (Шора, Гровера), але й з урахуванням потенційних ще не відкритих квантових атак, спрямованих саме на гібридну архітектуру. Пропонується моделювання та аналіз сценаріїв, де злоумисники можуть використовувати комбіновані квантово-класичні підходи для компрометації конфіденційності, цілісності та справжності. Це включає аналіз можливих атак на слабкішу з двох криптографічних примітивів, а також на протоколи їх поєднання.

Експериментальна оцінка продуктивності та практичності

Теоретична безпека повинна доповнюватися практичною застосовністю. Необхідно провести експериментальні дослідження продуктивності гібридних схем на різних апаратних платформах, оцінюючи обчислювальні витрати, використання пам'яті та затримку. Це дозволить ідентифікувати найбільш ефективні комбінації класичних та постквантових алгоритмів для конкретних застосувань (наприклад, IoT, хмарні сервіси, захист комунікацій), збалансуючи безпеку та ресурсомісткість.

Розробка адаптивних гібридних схем із динамічним вибором компонентів

Зважаючи на динамічний розвиток квантових технологій, статичні гібридні схеми можуть виявитися недостатньо гнучкими. Пропонується розробка адаптивних гібридних криптосистем, які зможуть динамічно змінювати склад компонентів залежно від рівня квантової загрози та доступних ресурсів. Наприклад, система може використовувати більш криптостійкі (але потенційно ресурсомісткі) постквантові алгоритми при зростанні загроз або наявності потужних квантових комп'ютерів і перемикатися більш ефективні класичні алгоритми за інших умов.

Стандартизація критеріїв та інструментів для порівняльної оцінки

Для сприяння широкому впровадженню гібридних рішень критично важлива розробка стандартизованих критеріїв та інструментів для їхньої порівняльної оцінки. Ці критерії повинні включати як рівень безпеки (класичної та квантової), так і практичні аспекти (продуктивність, вартість впровадження, легкість

інтеграції, сумісність). Створення спільних бенчмарків та фреймворків для тестування дозволить об'єктивно порівнювати різні гібридні підходи та прискорити вибір оптимальних рішень для промислових та державних застосувань.

Визначення ефективних гібридних криптографічних схем вимагає комплексного підходу, що охоплює глибокий теоретичний аналіз, практичне тестування та адаптивні стратегії. Запропоновані напрямки дослідження сприятимуть розробці надійних та життєздатних криптографічних рішень, що забезпечать захист даних у постквантовій ері. Інвестиції у ці напрямки є ключовими для підтримання стійкості кібербезпеки в умовах еволюції квантових обчислень.

Список використаних джерел

1. NIST. (2024). *Post-Quantum Cryptography Standardization*. Retrieved from <https://csrc.nist.gov/projects/post-quantum-cryptography>.
2. Mosca, M. (2018). *Quantum Safe Cryptography in an Era of Quantum Computers*. *IEEE Security & Privacy Magazine*, 16(5), 32-35.
3. Chen, L., Laine, P., & Zaverucha, G. (2017). *Post-Quantum Cryptography: State of the Art*. Springer.
4. Albrecht, M. R., & Breitner, P. (2018). *Implementing Hybrid Post-Quantum Cryptography*. In *Post-Quantum Cryptography* (pp. 3-18). Springer, Cham.
5. Міністерство цифрової трансформації України. (2021). *Стратегія цифрової трансформації сектору освіти і науки до 2030 року*.
6. Український інститут розвитку освіти. (2023). *Штучний інтелект в освіті: можливості та виклики. Аналітична доповідь*.
7. Röppelmann, E., & Güneysu, T. (2017). *Implementing Post-Quantum Cryptography: A Survey*. *ACM Computing Surveys (CSUR)*, 50(4), 1-36.

ПІДХОДИ ДО ПЕРЕХОДУ НА ПОСТКВАНТОВУ КРИПТОГРАФІЮ: АНАЛІЗ ДОКУМЕНТА NIST IR 8547 (2024)

Авдалов Герман Вікторович

*І курс, група KI-24-1phd, спеціальність “Комп’ютерна інженерія”
Інститут комп’ютерних технологій Університету “Україна”, м Київ,
Україна*

<https://orcid.org/0009-0007-7728-6659>

germannavdalov@gmail.com

*Науковий керівник: Самарай В. П., к.т.н, с.н.с., доцент
samaraj@ukr.net*

Анотація. У доповіді розглянуто ключові аспекти переходу до постквантових криптографічних стандартів на основі аналітичного звіту NIST IR 8547 (2024). Зокрема, окреслено ризики, пов’язані з квантово-вразливими алгоритмами, та визначено необхідність впровадження нових стандартів цифрового підпису й інкапсуляції ключів. Підкреслено роль гібридних рішень у перехідний період та зазначено вимоги до оновлення інфраструктури безпеки. Проаналізовано категорії криптографічної стійкості та графік відмови від застарілих алгоритмів до 2035 року. Особливу увагу приділено взаємодії державних і приватних структур для забезпечення надійного та безпечного впровадження PQС.

Ключові слова: криптографія; постквантова криптографія; криптографія з відкритим ключем; квантові обчислення.

Abstract. The paper explores key aspects of the transition to post-quantum cryptographic (PQC) standards based on the NIST IR 8547 (2024) report. It outlines the risks associated with quantum-vulnerable algorithms and emphasizes the adoption of new digital signature and key encapsulation mechanisms. The role of hybrid schemes during the transitional phase is highlighted, along with the need to upgrade cryptographic infrastructure. The study analyzes security categories and the proposed timeline for phasing out outdated algorithms by 2035. Special attention is given to the collaboration between public and private sectors to ensure a secure and efficient PQC implementation.

Keywords: cryptography; post-quantum cryptography; public key cryptography; quantum computing.

Вступ

Активний розвиток квантових обчислень створює безпрецедентні виклики для сучасної криптографії, зокрема для алгоритмів з відкритим ключем, таких як RSA, DSA та ECDSA, які десятиліттями забезпечували безпеку електронної комунікації, потенційно вразливі до атак із використанням квантових комп’ютерів, зокрема алгоритму Шора. У відповідь на цю загрозу Національний інститут стандартів і технологій США (NIST) ініціював розробку нових криптографічних стандартів, стійких до квантових атак. У листопаді 2024 року NIST опублікував внутрішній звіт IR 8547, який окреслює стратегію переходу до постквантової

криптографії (PQC) у федеральних системах та надає рекомендації для технологічної спільноти. Даний документ визначає перелік нових стандартів, пропонує графік відмови від застарілих алгоритмів та висвітлює технічні та організаційні аспекти впровадження PQC. Метою цього дослідження є аналіз положень звіту NIST IR 8547 та окреслення ключових кроків, необхідних для успішного переходу до постквантових криптографічних рішень.

Мета публікації NIST IR 8547

Забезпечити керівництво та дорожню карту для переходу від квантово-вразливих до квантово-стійких криптографічних стандартів у федеральних та комерційних інформаційних системах США.

Основні постквантові стандарти (FIPS)

FIPS 203: ML-KEM — схема інкапсуляції ключа на основі модульних решіток.

- FIPS 204: ML-DSA — цифровий підпис на базі решіток (CRYSTALS-DSA).
- FIPS 205: SLH-DSA — геш-підпис без збереження стану (SPHINCS+).

Проблематика переходу

- Очікувана тривалість переходу — 10–20 років.
- Потрібна модернізація інфраструктури: протоколів (TLS, SSH, IPsec), криптобібліотек (OpenSSL, BoringSSL), апаратних модулів (HSM, TPM), PKI, IT-додатків.

- Виклик щодо патентних обмежень і сумісності з наявними системами.

Гібридні рішення

- Тимчасове використання гібридних протоколів (PQC + класичні алгоритми) на етапі переходу.
- Підтримка NIST таких рішень для зменшення ризиків через недоліки в реалізації.

Категорії безпеки PQC

- NIST запроваджує 5 рівнів безпеки PQC відповідно до симетричних алгоритмів (AES, SHA-2/3).
- Наприклад, ML-DSA-87 (256 біт) відповідає категорії 5, що еквівалентно AES-256.

Пріоритетність переходу

- NSM-10 встановлює дедлайн — 2035 рік для повного переходу у федеральних системах.
- Окремі програми можуть потребувати прискореного переходу (TLS, S/MIME, підпис коду, автентифікація).

Методологія міграції

- Поступове виведення з обігу класичних алгоритмів.
- Визначення статусу алгоритмів як “прийнятний”, “застарілий”, “заборонений”, “застаріле використання”.
- Рефакторинг, тестування, перевірка на атаки через побічні канали.

Перехід до постквантової криптографії є стратегічно важливим кроком для гарантування безпеки інформаційних систем у майбутньому квантових обчислень. Звіт NIST IR 8547 окреслює комплексний і практично орієнтований підхід до міграції від вразливих алгоритмів до квантово-стійких рішень, визначаючи стандарти, часові рамки та пріоритетні напрями впровадження. Успішна реалізація цієї стратегії потребує активної участі державного і приватного секторів, оновлення інфраструктури безпеки та прийняття тимчасових гібридних рішень. Особливої уваги вимагає захист даних з довготривалим терміном зберігання, що підпадають під загрозу «збирати зараз — розшифрувати пізніше». Забезпечення криптографічної стійкості сьогодні є основою цифрової безпеки на найближчі десятиліття.

Список використаних джерел

2. NIST. (2024). <https://csrc.nist.gov/pubs/ir/8547/ipd>
3. NIST. (2024). <https://doi.org/10.6028/NIST.IR.8547.ipd>

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РИЗИКІВ ВИТОКУ ДАНИХ З ІНФОРМАЦІЙНИХ СИСТЕМ

Близнюк Артем Володимирович

II курс, група KI-23-1phd, спеціальність «Комп'ютерна інженерія»

Інститут комп'ютерних технологій Університету «Україна»

ORCID: <https://orcid.org/0009-0007-4461-5823>,

blizniykartem@gmail.com

Науковий керівник: **Писарчук О.О.**, доктор технічних наук, професор,
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: <https://orcid.org/0000-0001-5271-0248>,

platinumpa2212@gmail.com

Анотація. У тезах запропоновано концепцію математичного моделювання процесів витоку інформації з інформаційно систем, що враховує різні чинники. Модель базується на використанні технічних, поведінкових та інших показників і дозволяє кількісно оцінювати ризики витоку. Запропонована структура створює основу для подальшого застосування методів машинного навчання з метою розробки СППР на основі DLP-систем для виявлення та прогнозування інцидентів витоку інформації.

Abstract. The article presents the concept of mathematical modelling of information leakage processes from information systems, which takes into account various factors. The model is based on the use of technical, behavioural and other indicators and allows quantifying leakage risks. The proposed structure creates the basis for further application of machine learning methods to develop an IPSS based on DLP systems for detecting and predicting information leakage incidents.

Цифровізація державного управління та зростання обсягів обробки даних підсилюють проблему витоку конфіденційної інформації. В умовах складних кіберзагроз ключову роль відіграють DLP-системи, які потребують вдосконалення — зокрема, через впровадження математичних моделей, що враховують комплексні ризики. Поєднання інфологічних індикаторів із формалізованими методами оцінки загроз дає змогу створити більш гнучкі та ефективні механізми виявлення витоків.

Сьогодні у сфері інформаційної безпеки застосовуються ймовірнісні, статистичні та rule-based моделі для оцінки витоку даних у DLP-системах. Проте вони часто обмежені в адаптації до нових загроз. Сучасні підходи дедалі частіше включають машинне навчання та нечітку логіку, що дозволяє виявляти аномалії на ранніх етапах і формувати основи для систем підтримки прийняття рішень на базі DLP.

Математичне моделювання процесів витоку інформації ґрунтується на застосуванні ймовірнісних, статистичних методів, а також елементів теорії надійності та черг. Для кількісного опису процесів, які відбуваються під час витоку,

використовуються диференціальні рівняння, що дозволяють оцінити динаміку зміни обсягу викраденої інформації.

Одне з базових рівнянь моделі має вигляд:

$$\frac{dI}{dt} = -k \cdot I(t),$$

де $I(t)$ – обсяг інформації, що може бути викрадений за певний час; k – коефіцієнт витоку, залежний від рівня захищеності та умов середовища.

Сформуємо математичне представлення для трьох ключових чинників витоку інформації.

1. Ймовірність доступу до носія, функція часу та рівня захищеності:

$$P_a = f(t, S),$$

де t – час, протягом якого носій залишається без нагляду; а S – параметр захищеності.

2. Швидкість витоку:

$$v = g(I_0, T, D),$$

де I_0 – початковий обсяг інформації; T – час контакту; а D – рівень доступності носія для зловмисника.

3. Обсяг витоку, обчислюється як інтеграл швидкості витоку відносно часу:

$$V = \int_0^t v dt$$

Запропонована система рівнянь дає змогу оцінити як загальний обсяг втраченої інформації, так і ймовірність інциденту з урахуванням характеристик середовища, типу носія та поведінки користувача

Для розробки більш детального представлення математичної моделі витоку інформації необхідно також враховувати структурну модель компонентів захисту даних. передачі даних в інформаційних системах (рис. 1).



Рисунок 1 — Блоки структури моделі захисту інформації від витоку даних

Така концепція математичного моделювання враховує основні чинники ризику витоку інформації в DLP-системах і дозволяє кількісно оцінювати ймовірність та обсяг втрат даних. Вона є базою для подальшого застосування методів машинного навчання з метою розробки СППР.

Список використаних джерел:

1. Половінкін М.І., Глухов С.І., Черній Д.І., Пархоменко І.І. Алгоритм виявлення витоку інформації на основі перевірки статистичних гіпотез // Телекомунікаційні та інформаційні технології, 2024. – No 1(82). – С.95-105.
2. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. – К.: Вид. ДУІКТ, 2009. – 292 с.

ІНТЕГРОВАНІ СЕРЕДОВИЩА РОЗРОБКИ З ПІДТРИМКОЮ ШТУЧНОГО ІНТЕЛЕКТУ: НОВІ МОЖЛИВОСТІ ДЛЯ ВИВЧЕННЯ ПРОГРАМУВАННЯ СТУДЕНТАМИ

Роман БОГУН

кандидат фізико-математичних наук,
доцент кафедри інформаційних технологій та програмування
Інституту комп'ютерних технологій

Відкритого міжнародного університету розвитку людини «Україна» (Київ)
bohun.roma@gmail.com

Abstract. *The rapid infusion of AI into development environments is fundamentally reshaping the very philosophy of programming education. For a student, an AI assistant becomes a personal tutor: code gets written faster, its quality improves, and complex problems are no longer quite so daunting. But there is a flip side to this coin—an urgent need to teach students not just to blindly copy, but to critically dissect the logic behind the generated code. This shift inevitably transforms the educator's role, moving them from being a simple transmitter of knowledge to a navigator who guides students in their ethical interactions with the AI world. Ultimately, proficiency with these tools is no longer just an advantage; it has become a core requirement for any IT professional.*

Анотація. *Стрімке проникнення ШІ в середовища розробки кардинально змінює саму філософію навчання програмістів. Для студентів ШІ-помічник — це персональний тьютор: код пишеться швидше, якість росте, а складні задачі вже не так лякають. Але виникає і зворотний бік медалі: гостра потреба навчити студентів не копіювати сліпо, а критично аналізувати логіку згенерованого коду. Це неминуче трансформує роль викладача, перетворюючи його з транслятора знань на навігатора, що вчить етичній взаємодії зі світом ШІ. Зрештою, володіння цими інструментами — вже не перевага, а ключова вимога для будь-якого IT-фахівця.*

Інтегровані середовища розробки (IDEs) з підтримкою штучного інтелекту (ШІ), зокрема GitHub Copilot, Cursor, Windsurf та інші відкривають нові можливості для персоналізованого навчання програмування, що підтверджується результатами емпіричних досліджень у різних освітніх контекстах [1; 2; 3]. Практичне використання ШІ як тьютора або асистента демонструє зростання якості студентських проєктів, підвищення продуктивності та зменшення когнітивного навантаження [4; 5]. Водночас, дослідники звертають увагу на необхідність критичного осмислення ролі ШІ в освітньому процесі, зокрема щодо формування довіри до результатів генерації коду та збереження мотивації до самостійного мислення [6; 1]. Це вимагає адаптації навчальних стратегій, які поєднують переваги автоматизації з розвитком алгоритмічного мислення та етичної відповідальності.

Згідно з аналітичними звітами, кількість користувачів ШІ-помічників зростає експоненційно, а компанії-розробники інвестують рекордні ресурси в їх розвиток. За словами генерального директора Microsoft Сат'я Наделли, станом на 2025 рік до 30% коду в компанії вже генерується за допомогою ШІ. IDE з підтримкою ШІ дедалі активніше використовуються не лише у професійній розробці, а й у навчальному процесі. Ці інструменти забезпечують студентам доступ до

інтелектуальної підтримки в реальному часі: автозаповнення коду, генерація функцій, пояснення логіки, дебаг і рефакторинг. Особливо ефективними ці інструменти є на початкових етапах навчання, коли студенти стикаються з типовими труднощами — синтаксичними помилками, нерозумінням логіки алгоритмів, браком прикладів.

Роль викладача зазнає тектонічних зсувів: замість простого ретранслятора знань з'являється фасилітатор, що вчить студентів мистецтву критичного діалогу з ШІ, допомагаючи відрізнити корисну генерацію від цифрового шуму. Це не якась далека теорія. Інструменти на кшталт GitHub Copilot вже сьогодні дають змогу перетворити кожен практичну роботу на такий тренажер відповідальності та аналітики.

Отже, думати про ШІ в середовищах розробки лише як про кнопку «зроби добре» — це глибоко помилковий підхід. Насправді, це ціла екосистема для тренування аналітичного мислення, де студент вчиться не просто писати код, а й ставити правильні запитання, верифікувати чужі рішення та захищати власні. І коли рішення такого рівня, як GitHub Copilot, відкривають вільний доступ через програму GitHub Education, не скористатися цим — це зробити стратегічну помилку в підготовці майбутніх фахівців. Безперечно, це кидає нам виклик. Потрібно буде переглянути застарілі методики оцінювання та адаптувати навчальні плани, але сам імпульс для освітньої трансформації вже не зупинити.

Список використаних джерел

1. Alanazi M., Soh B., Samra H., Li A.L.C. The Influence of Artificial Intelligence Tools on Learning Outcomes in Computer Programming: A Systematic Review and Meta-Analysis // *Computers*. 2025. Vol. 14, No. 5. Article 185. DOI: <https://doi.org/10.3390/computers14050185>.

2. Gardella N., Pettit R., Riggs S.L. Performance, Workload, Emotion, and Self-Efficacy of Novice Programmers Using AI Code Generation // *Proceedings of the 2024 Conference on Innovation and Technology in Computer Science Education*, Vol. 1, ITiCSE 2024. Milan, Italy, 2024. P. 290–296. DOI: <https://doi.org/10.1145/3649217.3653615>.

3. Avramovic S., Avramovic I., Wojtusiak, J. Exploring the Impact of GitHub Copilot on Health Informatics Education // *Applied Clinical Informatics*. 2024. Vol. 15, No. 5. P. 1121–1129. DOI: <https://doi.org/10.1055/a-2414-7790>.

4. Timcenko O. Case Study: Using Artificial Intelligence as a Tutor for a Programming Course // *2024 21st International Conference on Information Technology Based Higher Education and Training (ITHET)*. Paris, France, 2024. DOI: <https://doi.org/10.1109/ITHET61869.2024.10837624>.

5. Mesaros G.O. Learning Web Development Using GitHub Copilot in and Outside Academia: A Blessing or a Curse? // *Interdisciplinary Description of Complex Systems*. 2024. Vol. 22, No. 3. P. 355–359. DOI: <https://doi.org/10.7906/indecs.22.3.10>.

Shah A., Chernova A., Tomson E., Porter L., Griswold W.G., Raj A.G.S. Students' Use of GitHub Copilot for Working with Large Code Bases // *Proceedings of the 56th ACM Technical Symposium on Computer Science Education, SIGCSE TS 2025*, Vol. 1. Pittsburgh, PA, 2025. P. 1050–1056. DOI: <https://doi.org/10.1145/3641554.3701800>

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОЄКТУВАННЯ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Богуцький Андрій Ігорович

*II курс, група KI-23-1phd, спеціальність «Комп'ютерна інженерія», Інститут комп'ютерних технологій
Університету «Україна».*

ORCID: <https://orcid.org/0009-0006-9458-8838>

bohutskyi_ak22@nuwm.edu.ua

*Науковий керівник: Тимошенко О.М., к.ф.-м.н., доцент,
Інститут комп'ютерних технологій Університету «Україна».*

***Анотація.** Однією з ключових подій початку 20-х років XXI століття стала поява загальнодоступного генеративного штучного інтелекту (ШІ). У галузі комп'ютерних технологій його вплив відчутний особливо сильно. Всього за кілька років ключові технологічні гіганти перейшли від використання ШІ як допоміжного інструменту для спеціалістів до заміни працівників ним самим. Слідом за великими компаніями тренд відчувають і малі компанії. Це часто стосується рутинних процесів пошуку помилок, перевірки лексики коду, написання документації, тестування та іншого. Деякі ШІ-моделі станом на початок 2025 року здатні виконувати роботу програміста початкового рівня за значно меншу плату, що значно впливає на витрати бізнесу.*

Правильне використання спеціально тренуваних моделей виглядає перспективним для оптимізації процесів розробки програмного забезпечення (ПЗ). Зокрема, однієї з ключових проблем: збільшення вартості розробки та складності впровадження змін з часом.

***Abstract.** One of the key inventions of the early 20s of the 21st century was the emergence of publicly available generative artificial intelligence (AI). In the field of computer technology, its impact is significant. In just a few years, key tech giants have moved from using AI as an auxiliary tool for specialists to replacing employees with it. Following the trend set by big companies, small companies are also experiencing it. This often concerns routine processes of finding bugs, checking code vocabulary, writing documentation, testing, etc. As of early 2025, some AI models are capable of performing the work of an entry-level programmer for a much lower price, which significantly affects business costs.*

Proper use of specially trained models looks promising for optimizing software development processes. Especially, one of the key problems is the increase in development costs and the complexity of implementing changes over time.

Проектування систем ПЗ на основі мікросервісної архітектури є основною задачею програмістів високого рівня. Інструменти, які використовуються на ранніх етапах проектування, мають суттєвий вплив на надійність, продуктивність і простоту підтримки системи. В епоху стрімкого розвитку фреймворків, важливість вибору правильного інструменту є запорукою швидкої та якісної розробки

програмного продукту з подальшим масштабуванням та розширенням функціональності.

Основні завдання при проєктуванні мікросервісів включають визначення меж розподілу та відповідальності окремих сервісів, а також взаємодії між ними. Ці завдання передбачають прийняття критично важливих рішень, пов'язаних з декомпозицією сервісів, протоколами зв'язку та загальною архітектурною структурою. Побудова систем з нуля вимагає балансу між відповідною деталізацією сервісів та мінімізацією міжсервісної комунікації. Погано спроектовані системи ризикують мати архітектурні антипатерни, такі як надмірна кількість зв'язків або високу зв'язність класів, які перешкоджають підтримці та масштабованості.

Генеративний ШІ став перспективним інструментом для розв'язання цих проблем шляхом автоматизації та вдосконалення проєктування мікросервісної архітектури, особливо для розробки нового програмного забезпечення. Технології машинного навчання (ML) та обробка природної мови (NLP) допомагають у критично важливих завданнях проєктування, таких як аналіз вимог, побудові діаграм, створення контрольних списків, написання супровідної документації та прийнятті архітектурних рішень. Розробник у цей час може сфокусуватись на розв'язанні значущих проблем. Таким чином за однаковий проміжок часу, фахівець з допомогою ШІ виконує більший обсяг роботи без втрати якості результату.

Алгоритм SEMGROMI використовує NLP для ідентифікації мікросервісів на основі семантичної подібності історій користувачів. Поряд із цим, для аналізу структури системи також застосовується алгоритм кластеризації методом K-середніх для поділу даних на однорідні групи, що дозволяє знаходити приховані структури в монолітних системах і спрямовувати процес декомпозиції на мікросервіси. Проте ефективність цих методів значною мірою залежить від якості вхідних даних, а точне визначення оптимальної кількості кластерів є критично важливим для отримання змістовної сегментації. Ця технічна основа підкреслює ключову роль штучного інтелекту в автоматизації та оптимізації проєктування мікросервісів.

Важливо розуміти, що генеративний ШІ не здатен придумати щось кардинально нове. Інформація якою він оперує обмежується загальнодоступними джерелами. Об'єм цих джерел гігантський, і на відміну від людини, він здатен за короткий проміжок часу запропонувати типові та ефективні рішення для вирішення бізнес-задачі, аргументуючи вибір тих чи інших технологій. Проте він може не врахувати специфіки домену або нюансів та обмежень, які досвідчений інженер відчуває з досвіду.

Людство поки що не досягнуло рівня агентного ШІ, який би міг самостійно планувати дії та приймати рішення, тому фінальне слово у розв'язанні задач за людиною, проте генеративний ШІ є та буде потужним інструментом в її руках.

ЗАХИСТ API У ХМАРНИХ ДОДАТКАХ: РИЗИКИ ТА ПІДХОДИ

Борисенко Олександр Сергійович

III курс аспірантури, група KI-22-1phd, спеціальність “Комп’ютерна інженерія”

Інститут комп’ютерних технологій Університету “Україна”

Науковий керівник: Тимошенко А.Г., к.т.н., проф.,

Інститут комп’ютерних технологій Університету “Україна”

Анотація. У роботі досліджено актуальні ризики безпеки, що виникають при використанні API у хмарних додатках, а також розглянуто сучасні технічні підходи до їх захисту. Особливу увагу приділено автентифікації, авторизації, обмеженню запитів (rate limiting), журналюванню та контролю доступу. Розглянуто специфіку реалізації безпеки API в середовищі AWS з використанням таких інструментів, як Amazon API Gateway, AWS WAF, IAM, а також шифрування даних та контроль стану API.

Abstract. This paper examines current security risks associated with the use of APIs in cloud applications and explores modern technical approaches to mitigating them. Special focus is placed on authentication, authorization, rate limiting, logging, and access control. The implementation of API protection in AWS is discussed, including tools such as Amazon API Gateway, AWS WAF, IAM, data encryption, and API health monitoring.

У сучасних хмарних додатках API (інтерфейс прикладного програмування) є ключовим компонентом, через який здійснюється взаємодія між сервісами, мобільними застосунками та веб-інтерфейсами. Разом із цим API є частою мішенню атак через публічну доступність, високий рівень динаміки та складність контролю доступу. Основні загрози включають:

1. Несанкціонований доступ: У разі відсутності належної автентифікації або авторизації зломисник може отримати повний доступ до функціоналу API. У середовищі AWS для цього рекомендується застосовувати AWS IAM, авторизацію на основі токенів (OAuth 2.0) або використання Amazon Cognito.

2. Передача незашифрованих даних: Відсутність TLS/SSL призводить до перехоплення конфіденційної інформації. Всі API-запити мають передаватися виключно через HTTPS.

3. Перевантаження API (DoS, API abuse): Масове надсилання запитів може вивести сервіс з ладу. Для захисту необхідно застосовувати механізми rate limiting та throttling, доступні через Amazon API Gateway.

4. Ін’єкційні атаки (наприклад, SQL/NoSQL injection, command injection): Вони можливі при недостатньому валідуванні введення користувачем. AWS WAF дозволяє створювати правила фільтрації, що блокують шкідливі запити на рівні API Gateway.

5. Недостатній аудит та журналювання: Відсутність моніторингу унеможливує виявлення інцидентів безпеки. AWS CloudTrail забезпечує повну історію запитів до API, а AWS CloudWatch — моніторинг та сповіщення.

Окрім того, важливо впроваджувати принцип найменших привілеїв при доступі до API, використовуючи IAM policy, що чітко визначають дозволені дії для кожного користувача чи сервісу. Для розгортання API можна також застосовувати механізм API keys з обмеженим терміном дії та контрольованим доступом.

У середовищі AWS найбільш безпечна архітектура API включає:

- Використання Amazon API Gateway для централізованого контролю доступу;
- Інтеграцію з Lambda або іншими безсерверними компонентами для виконання бізнес-логіки;
- Захист за допомогою AWS WAF та авторизаційних механізмів (IAM, JWT, OAuth);
- Журналювання та сповіщення за допомогою CloudTrail і CloudWatch;
- Шифрування конфіденційних даних у транзиті та на зберіганні.

В умовах стрімкого зростання використання мікросервісної архітектури в хмарних додатках, API стає не лише інструментом взаємодії між сервісами, але й потенційною вразливістю. Інциденти, пов'язані з небезпечними API-запитами, можуть призвести до витоку персональних даних, неавторизованого доступу до внутрішніх систем або порушення роботи додатків. Саме тому необхідно застосовувати не лише автентифікацію запитів, а й контроль контексту доступу, зокрема методів, джерел і частоти звернень.

Захист API у хмарному середовищі є критичним аспектом забезпечення загальної кібербезпеки хмарного застосунку. Завдяки використанню спеціалізованих сервісів AWS можна реалізувати комплексний підхід до безпеки API, що включає автентифікацію, обмеження запитів, фільтрацію загроз, аудит дій та моніторинг, забезпечуючи надійний захист від сучасних атак.

АДАПТИВНИЙ МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ В МОБІЛЬНИХ ПРИСТРОЯХ НА ОСНОВІ ПОВЕДІНКОВОЇ МОДЕЛІ

Бровченко Євген Миколайович

III курс, група КІ-22-1phd, спеціальність «Комп'ютерна інженерія»

Інститут комп'ютерних технологій Університету «Україна»

Науковий керівник: Самарай В. П., к.т.н., с.н.с., доцент

Інститут комп'ютерних технологій Університету «Україна»

***Анотація.** Робота присвячена проблемі використання мобільного пристрою в умовах активного впливу та захист неструктурованої інформації. Увага приділена використанню мобільного пристрою як частини інформаційної системи та можливі заходи щодо захисту інформації від протиправних дій. Була проведена робота по вивченню проблеми в реальних умовах використання та взаємодії. Пропонується модель алгоритму адаптивного захисту інформації. В основу моделі покладена ідея динамічної адаптації системи.*

***Ключові слова:** мобільний пристрій; захист інформації; неструктурована інформація; кібербезпека.*

ADAPTIVE INFORMATION PROTECTION METHOD IN MOBILE DEVICES BASED ON BEHAVIORAL MODEL

***Abstract.** The work is devoted to the problem of using a mobile device in conditions of active influence and protection of unstructured information. Attention is paid to the use of a mobile device as part of an information system and possible measures to protect information from illegal actions. Work was carried out to study the problem in real conditions of use and interaction. A model of the adaptive information protection algorithm is proposed. The model is based on the idea of dynamic adaptation.*

***Key words:** mobile device; security; information protection; user interaction with a mobile device; adaptive security.*

Мобільний пристрій містить багато різноманітної інформації чи даних. Природа та важливість цієї інформації може бути різною, але захист має пріоритетне значення. Враховуючи динаміку розвитку та невизначеність деяких процесів, перед інженерами та розробниками стоїть важке та важливе завдання по захисту інформаційних систем та забезпеченню надійної роботи. Мобільний пристрій можна вважати найбільш проблематичною складовою. Цей пристрій має ряд переваг та особливостей. Робота присвячена проблематиці використання мобільних пристроїв та захисту неструктурованої інформації. Неструктурована інформація може бути у вигляді текстових документів, електронних листів, фотографій, відео, записів голосу та іншого контенту, який зберігається на мобільних пристроях. До основних проблем можна віднести: втрата або крадіжка мобільного пристрою; вразливості операційної системи та програмного забезпечення; недостатній рівень шифрування та недостатній рівень складності паролів; нехтування

кібергігієною. Існуючи інженерно-архітектурні рішення не завжди виконують поставлену задачу та можуть мати проблеми з інтеграцією. Аналіз прикладної області та результати дослідження говорять про те що є попит на швидкі та ефективні рішення щодо безпеки інформаційних систем в цілому та мобільного пристрою зокрема. Лише комплексний підхід може забезпечити ефективне рішення. Адаптивний захист передбачає використання різних методів і технологій, таких як шифрування, біометричні ідентифікатори, інтелектуальні системи виявлення загроз. Включає в себе постійне оновлення і покращення методів захисту, оскільки загрози постійно еволюціонують, і необхідно підлаштовувати захисні механізми під нові виклики. Користувачі мобільних пристроїв повинні бути активно включені в процес адаптивного захисту, слідкувати за оновленнями, використовувати паролі, підтримувати резервне копіювання і відповідати на попередження щодо безпеки. Розробники програмного забезпечення для мобільних пристроїв мають велику відповідальність щодо забезпечення безпеки інформації, і вони повинні включати адаптивні захисні механізми в свої додатки і платформи. Процес вимагає поєднання технічних, організаційних та освітніх заходів для досягнення максимальної ефективності. Забезпечення адаптивного захисту інформації на мобільних пристроях є ключовою умовою для збереження приватності і безпеки користувачів у цифровому світі. Може бути покращений завдяки співпраці між виробниками, науковцями, законодавцями та споживачами для розвитку більш безпечних інформаційних середовищ.

Захист інформації на мобільному пристрої засновано на поєднанні технологічних нововведень та підвищенні обізнаності користувачів з питань кібербезпеки. Деякі напрямки розвитку включають застосування штучного інтелекту (AI) та машинного навчання. AI може допомогти в розробці розширених механізмів захисту, що автоматично виявляють аномальні або підозрілі дії та блокують потенційні загрози. Біометрична автентифікація, покращення технологій біометричної автентифікації, таких як розпізнавання обличчя, відбитків пальців, можуть забезпечити більш надійний захист інформації. Застосування блокчейн-технологій, блокчейн може відігравати важливу роль у забезпеченні безпеки інформації, оскільки він дозволяє зберігати дані розподілено та захищено від змін. Розвиток квантово-стійких алгоритмів шифрування, з розвитком квантових комп'ютерів створюється потреба в нових алгоритмах шифрування, які можуть витримати потужність квантового злому. Приватність за замовчуванням (Privacy by Design), проектування мобільних пристроїв та застосунків з врахуванням приватності користувачів сприятиме захисту інформації на мобільних пристроях. Освіта та обізнаність користувачів, підвищення обізнаності користувачів щодо кібербезпеки та навчання їх ефективним методам захисту інформації на мобільних пристроях допоможе зменшити ризик виникнення інцидентів, пов'язаних з безпекою. Розвиток законодавства та нормативної бази, вдосконалення законодавства та нормативної бази у галузі кібербезпеки сприятиме створенню надійного середовища для захисту інформації. Захист інформації на мобільних пристроях спиратиметься на комбінації

технологічного прогресу, навчання користувачів та співпраці між різними сторонами, такими як розробники, постачальники послуг та законодавці. Забезпечення безпеки та приватності даних в цифровому світі залишається пріоритетом, оскільки кількість мобільних пристроїв та їх використання продовжують зростати.

Сучасній користувач мобільних пристроїв має певні вимоги що стосуються на ергономіку та рівень інформаційної обізнаності. Розвиток галузі в цілому вимагає швидких, надійних та ефективних рішень що потрапляють не лише в економічну площину а й площину кібербезпеки. Використання мобільних пристроїв може адаптуватися до швидких сучасних потреб безпеки організації та може бути легко налаштований відповідно до конкретних вимог. Мобільний пристрій є зручним і доступним для багатьох користувачів, він зазвичай знаходиться поруч з користувачем і може використовуватися як додатковий елемент безпеки.

Список використаних джерел:

1. Бровченко Є.М., Самарай В.П. Метод захисту інформації на мобільних пристроях на основі адаптивної поведінкової моделі. Інфокомунікаційні та комп'ютерні технології, 2(08), Київ, 2024. С. 33–39. <https://doi.org/10.36994/2788-5518-2024-02-08-04>

ПОРІВНЯННЯ АЛГОРИТМІВ МУЛЬТИАГЕНТНОГО НАВЧАННЯ З ПІДКРІПЛЕННЯМ ДЛЯ ДЕЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ

Войтех Д.В.

2 курс, група KI-23-1phd, спеціальність «Комп'ютерна інженерія»,
Інститут комп'ютерних технологій Університету «Україна».

<https://orcid.org/0009-0003-8997-5495>

Науковий керівник: Тимошенко А.Г., к.тех.н., доцент,
Інститут комп'ютерних технологій Університету «Україна»

<https://orcid.org/0000-0003-0954-3186>

Анотація. У роботі представлено порівняльний аналіз популярних алгоритмів мультиагентного навчання з підкріпленням, що застосовуються для децентралізованого керування енергоспоживанням домогосподарств. Розглянуто підходи від незалежного Q-навчання до централізованого навчання з децентралізованим виконанням (MADDPG, QMIX, MAPPO). Аналіз включає їх здатність до координації, стійкість до часткової спостережуваності та ефективність у стандартних симуляційних середовищах, зокрема CityLearn. Особливу увагу приділено практичним аспектам: стабільності навчання, чутливості до гіперпараметрів та масштабованості. Зроблено висновки щодо доцільності використання тих чи інших підходів у задачах управління енергоспоживанням у розподілених мережах.

Abstract. This study presents a comparative analysis of popular multi-agent reinforcement learning algorithms applied to decentralized household energy control. Methods range from independent Q-learning to centralized training with decentralized execution, including MADDPG, QMIX, and MAPPO. The analysis covers coordination capabilities, robustness under partial observability, and performance in standard benchmarks such as CityLearn. Practical aspects are also examined, including training stability, hyperparameter sensitivity, and scalability. The study concludes with recommendations on which MARL approaches are best suited for decentralized energy management tasks in smart grids.

Сучасні електромережі потребують потужних інтелектуальних засобів координації розподілених енергетичних ресурсів для зниження пікових навантажень та ефективною інтеграції відновлюваних джерел [1]. Централізоване керування в таких системах обмежене через алгоритмічну складність задачі та ризики порушення конфіденційності даних [2]. Мультиагентне навчання з підкріпленням (MARL) є перспективною парадигмою для побудови децентралізованого керування, де домогосподарства виступають автономними агентами з власними локальними спостереженнями та цілями [3].

MARL-алгоритми. Незалежне Q-навчання (IQL) може бути ефективним при ретельному підборі функції винагороди, однак є вразливим до нестационарності. DDPG підходить для безперервного простору дій, але незалежне навчання погано забезпечує координацію між агентами. Метод PPO демонструє стабільне навчання в кооперативних задачах середньої складності [4]. MADDPG реалізує централізоване навчання з децентралізованим виконанням (CTDE),

використовуючи централізовану модель-критика для покращення координації агентів. Метод QMIX факторизує глобальну Q-функцію на локальні компоненти, що дозволяє агентам діяти автономно з урахуванням глобальної мети. MAPPO поєднує централізовану функцію цінності з незалежними політиками і добре масштабується у багатобудинкових сценаріях [4].

Результати симуляцій. У середовищі CityLearn MARL-алгоритми, зокрема MAPPO, демонструють зниження функції втрат на 10–12% порівняно з базовими контролерами [4]. Для невеликих систем незалежні агенти часто є достатньо ефективними, проте зі зростанням розмірності модельованої системи перевагу отримують CTDE-підходи [3]. У GridLearn та схожих середовищах моделювання параметрів передавальних електромереж MARL також дозволяє досягти суттєвого покращення показників, таких як стабільність напруги [4].

Практичні виклики. Навчання агентів у симуляційному середовищі вимагає значних обчислювальних ресурсів. Off-policy алгоритми (наприклад, DDPG, QMIX) дозволяють ефективніше використовувати дані і досягати очікуваних результатів за меншу кількість епізодів, проте вони схильні до нестабільності під час навчання [3]. On-policy методи (наприклад, MAPPO) є стабільнішими, але вимагають більше симуляцій для досягнення тієї ж якості. Часткова спостережуваність та зміни в поведінці інших агентів ускладнюють збіжність, тому часто застосовують рекурентні мережі для кращого збереження стану. У великих системах централізовані моделі-критики погано масштабуються, проте алгоритми на кшталт QMIX адресують цю проблему завдяки поєднанню локальних оцінок агентів [4].

MARL-алгоритми ефективно координують розподілені енергетичні ресурси в умовах децентралізованого керування. Прості підходи (IQL, PPO) краще працюють у невеликих системах за умови якісного підбору функції винагороди, однак CTDE-методи (MADDPG, QMIX, MAPPO) мають переваги в масштабованості та стабільності. Гібридні стратегії, які поєднують попереднє планування та навчання, є перспективним напрямом. Подальші дослідження мають зосереджуватись на проблемах якості даних, переносу агентів в реальні умови та стабільності навчання.

Список використаних джерел

1. Farhangi H. The path of the smart grid. IEEE Power and Energy Magazine, 2010, Vol. 8, No. 1, P. 18–28.
2. Fang X. et al. Smart grid – The new and improved power grid: A survey. IEEE Communications Surveys & Tutorials, 2012, Vol. 14, No. 4, P. 944–980.
3. Zhang K., Yang Z., Basar T. Multi-agent reinforcement learning: A selective overview of theories and algorithms. Handbook of Reinforcement Learning and Control, 2019, P. 321–384.
4. Vázquez-Canteli J. R., Nagy Z. Reinforcement learning for demand response: A review of algorithms and modeling techniques. Applied Energy, 2019, Vol. 235, P. 1072–1089.

АРХІТЕКТУРА DEPIN ДЛЯ ДЕЦЕНТРАЛІЗОВАНОГО ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ АРХІВІВ ІЗ ДОТРИМАННЯМ ВИМОГ GDPR

Григор'єв Костянтин Сергійович

*III курс, група KI-22-1phd, спеціальність «Комп'ютерна Інженерія»,
Інститут комп'ютерних технологій Університету «Україна»,
ORCID: <https://orcid.org/0009-0004-4212-6661>*

Грищенко Вадим Юрійович

*III курс, група KI-22-1phd, спеціальність «Комп'ютерна Інженерія»
Інститут комп'ютерних технологій Університету «Україна»,
ORCID: <https://orcid.org/0009-0004-4212-6661>, komarda47@gmail.com
Науковий керівник: **Павленко В.І.**, к.ф.-м.н., доцент,
Інститут комп'ютерних технологій Університету «Україна»
ORCID: <https://orcid.org/0000-0002-3958-0415>, pavlenko.v@i.ua*

Анотація. Експоненційне зростання обсягів персонального цифрового контенту вимагає надійних рішень для конфіденційного, довгострокового й нормативно сумісного зберігання даних. Централізовані хмарні сервіси створюють ризики втрати контролю, витоків даних і складності з реалізацією прав користувачів, зокрема «права на забуття». У цій роботі запропоновано децентралізовану архітектуру зберігання персональних архівів, побудовану на парадигмі *Decentralized Physical Infrastructure Network (DePIN)*. Система об'єднує кодоване знищення (*erasure coding*), постквантове шифрування та модель відкликання доступу через *capability*-токени, що забезпечує повну відповідність вимогам GDPR. Запропонований механізм *Shard-Proof Pseudonymization (SPP)* дає змогу видаляти дані без порушення незмінності блокчейну.

DePIN-Based Architecture for GDPR-Compliant Decentralized Personal Archives

Abstract. *The exponential growth of user-generated digital content demands robust, privacy-respecting, and resilient storage solutions. Centralized cloud services, while convenient, introduce risks such as data breaches, surveillance, and limited user control. This paper presents a decentralized storage architecture based on the Decentralized Physical Infrastructure Network (DePIN) paradigm. It leverages erasure coding, post-quantum encryption, and a revocable capability access model to achieve compliance with General Data Protection Regulation (GDPR) mandates, particularly the right to erasure. A key contribution is the novel Shard-Proof Pseudonymization (SPP) mechanism that enables secure content revocation without compromising the immutability of blockchain records.*

Зі зростанням цифровізації особисте життя людини супроводжується накопиченням великих обсягів чутливої інформації: фото, документи, медичні записи, творчі проекти. За оцінками IDC, до 2025 року світовий обсяг даних перевищить 180 зетабайт, значна частина яких — персональні дані [1].

Сучасні централізовані хмарні рішення, як-от Google Drive чи iCloud, забезпечують зручність, але втрачають довіру через відсутність прозорості, ризики централізованих збоїв та неможливість реалізації «права на забуття» у відповідності до Регламенту ЄС про захист персональних даних (GDPR) [2], [3].

Запропонована система базується на чотирьох функціональних шарах:

Клієнтський шар: Файли діляться на частини (4 МБ), шифруються за допомогою Kyber-1024, кодується методом Reed–Solomon ($n = 20$, $k = 14$) і розповсюджуються між вузлами.

Шар зберігання (DePIN): Дисковий простір надається вузлами-учасниками за винагороду у вигляді токенів. Вузли ранжуються за доступністю та пропускнуою здатністю.

Шар консенсусу та аудиту: Побудований на Substrate-базованому блокчейні; хеші фрагментів зберігаються з періодичним оновленням.

Шар контролю доступу: Впроваджено capability-токени, які забезпечують селективний доступ до даних і можливість криптографічного відкриття доступу.

Псевдонімізація фрагментів (SPP)

Запропоновано механізм Shard-Proof Pseudonymization (SPP), що використовує подвійну хеш-функцію для розриву зв'язку між фрагментами даних і публічними записами у блокчейні. Це забезпечує:

1. Неможливість повторної ідентифікації;
2. Виконання статті 17 GDPR без порушення незмінності даних.

Постквантовий криптографічний стек

Вперше в системах зберігання даних для споживачів застосовано Kyber-1024 для шифрування та Dilithium-5 для підпису токенів доступу [4], [5]. Це забезпечує стійкість до квантових атак.

У межах прототипу було розгорнуто 100 вузлів Raspberry Pi 5 у 5 географічних регіонах. Отримано такі результати:

Надійність: 99.9994% за симуляцію впродовж 5 років.

Затримка: 37 с на завантаження, 2.9 с на отримання даних.

Вартість: \$53/ТБ/рік проти \$276 у AWS S3.

Право на забуття: 100% видалення протягом 72 годин після відкриття доступу.

Розроблена модель загроз гарантує безпеку навіть при частковому контролі фрагментів з боку злоумисника ($f < n - k$):

Sybil-атаки: Блокуються стейкінгом і QoS-рейтинговою системою.

Витік метаданих: Унеможливлено завдяки SPP.

Несанкціонований доступ: Забезпечено обмеженими в часі токенами.

Робота демонструє, що децентралізовані архітектури зберігання можуть відповідати найсучаснішим вимогам щодо безпеки, конфіденційності та нормативного регулювання. В основі запропонованої системи — поєднання постквантової криптографії, псевдонімізації, децентралізованої економіки (DePIN) та аудитованого контролю доступу.

Майбутні дослідження можуть включати масштабування на гетерогенне обладнання, інтеграцію з конфіденційними обчисленнями (Confidential Computing) і розробку механізмів стабілізації токенів для комерційного застосування.

Література.

1. IDC, “Global DataSphere Forecast 2023–2027,” International Data Corporation, 2023.
2. European Parliament, “Regulation (EU) 2016/679 (GDPR),” Official Journal of the EU, 2016.
3. K. Moosavi, A. Narayanan, “Blockchain Privacy and the GDPR,” Computer Law & Security Review, vol. 49, 2023.
4. National Institute of Standards and Technology (NIST), “FIPS 203: CRYSTALS-Kyber,” Draft Standard, 2024.
5. E. Alkim et al., “Dilithium in Practice,” Proc. ACM CCS, 2024.

ТЕХНІКО-ЕКОНОМІЧНА ОЦІНКА DEPIN-ОРІЄНТОВАНОЇ МЕРЕЖІ ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ АРХІВІВ

Грищенко Вадим Юрійович

III курс, група KI-22-1phd, спеціальність «Комп'ютерна Інженерія»
ORCID: <https://orcid.org/0009-0004-4212-6661>, komarda47@gmail.com

Григор'єв Костянтин Сергійович

III курс, група KI-22-1phd, спеціальність «Комп'ютерна Інженерія»
ORCID: <https://orcid.org/0009-0004-4212-6661>, prizma2098@gmail.com

Інститут соціальних технологій Університету «Україна»

Науковий керівник: **Павленко В.І.**, к.ф.-м.н., доцент,

Інститут комп'ютерних технологій Університету «Україна»

ORCID: <https://orcid.org/0000-0002-3958-0415>, pavlenko.v@i.ua

***Анотація.** У роботі представлено економічну та технічну оцінку децентралізованої архітектури зберігання персональних архівів, побудованої на основі *Decentralized Physical Infrastructure Network (DePIN)*. Система використовує модель токен-стимульованої участі, за якої користувачі надають власні ресурси зберігання в обмін на винагороду. Порівняльний аналіз з провідними централізованими та децентралізованими платформами показує значне зниження вартості зберігання при збереженні високої надійності, швидкості доступу та відповідності нормативним вимогам (зокрема *GDPR*).*

Economic and Technical Evaluation of DePIN-Powered Archive Storage Networks

***Abstract.** This paper presents an economic and technical assessment of a decentralized personal archive storage architecture based on the *Decentralized Physical Infrastructure Network (DePIN)*. The system employs a token-incentivized participation model, in which users contribute their own storage resources in exchange for rewards. A comparative analysis with leading centralized and decentralized platforms demonstrates a significant reduction in storage costs while maintaining high reliability, access speed, and compliance with regulatory requirements, particularly the *General Data Protection Regulation (GDPR)*.*

Цифрова епоха супроводжується зростаючою потребою у масштабованому, безпечному та економічно ефективному зберіганні персональних даних. Традиційні централізовані сервіси, такі як AWS S3, OneDrive чи Google Cloud, пропонують стабільність, однак їх вартість, ризики централізації та недостатня підтримка нормативних вимог стають дедалі критичнішими [1, 2].

Новітні децентралізовані платформи, зокрема Storj, Filecoin, Arweave, частково розв'язують проблему з довготривалим зберіганням, однак демонструють обмеження в енергоспоживанні, швидкодії та підтримці динамічного видалення даних [3, 4]. У цьому контексті підхід DePIN, що об'єднує інфраструктуру фізичних вузлів із блокчейн-механізмами аудиту, пропонує новий рівень ефективності.

Для оцінки ефективності було створено прототипну мережу на базі 100 вузлів Raspberry Pi 5 (8 ГБ RAM, 2 ТБ SSD), розташованих у 5 географічних регіонах. Пропускна здатність обмежувалася до 100 Мбіт/с для моделювання типових домашніх умов. Використано Reed–Solomon-кодування (20/14), Kyber-1024 для шифрування та Substrate-базований блокчейн для аудиту.

Платформа підтримує відкличні capability-токени, що дозволяють відкликати доступ до даних без фізичного знищення записів у ланцюжку блоків, забезпечуючи відповідність вимогам GDPR (ст. 17) [5].

Економічна ефективність показана в таблиці 1.

Таблиця 1.

Платформа	Річна вартість зберігання (1 ТБ)
DePIN Archive	\$53
Storj v1.77	\$78
AWS S3 Standard	\$276

DePIN забезпечує до 80% економії порівняно з AWS, що критично важливо для довготривалого архівування великих обсягів даних.

Затримка завантаження (1 ГБ): 37 с (DePIN), 44 с (Storj), 26 с (AWS)

Середній час отримання: 2.9 с (DePIN), 3.6 с (Storj), 1.8 с (AWS)

Швидкість завантаження (Мбіт/с): 210 (DePIN), 165 (Storj), 320 (AWS)

DePIN демонструє меншу варіативність затримки, ніж Storj, завдяки багатоточковому вибору фрагментів і кешуванню на вузлах.

Довгострокова надійність (5 років): 99.9994%

Стійкість до виходу вузлів: до 35% одночасних втрат

Споживання енергії (Вт·год/ГБ): 0.95 (DePIN), 1.4 (Storj), 0.8 (AWS)

DePIN показує найкраще співвідношення енергоефективності та децентралізації.

Основні переваги DePIN-архітектури:

- Стимулювання участі: економіка токенів винагороджує вузли з високою доступністю.

- **Регуляторна відповідність:** забезпечено псевдонімізацію та відкликання доступу згідно GDPR.

- **Гнучкість:** можна інтегрувати з хмарними сервісами та edge-сховищами.

Обмеження:

- **Волатильність токенів:** потребує стабілізаційних механізмів.

- **Залежність від домашніх мереж:** впливає на затримки.

- **Прототипна масштабованість:** система потребує подальшого тестування в реальному середовищі.

Проведений аналіз підтверджує, що **DePIN-орієнтоване зберігання** є **конкурентоспроможним** як з технічної, так і з економічної точки зору. Значне зниження вартості зберігання, прийнятна затримка доступу, енергоефективність та підтримка регуляторних норм роблять запропоновану архітектуру привабливою для широкого впровадження.

Майбутні роботи повинні зосередитись на розширенні мережі, інтеграції конфіденційних обчислень (Confidential Computing) і моделюванні сталості економіки токенів.

Література.

1. B. Mell, P. Grance, “The NIST Definition of Cloud Computing,” NIST SP 800-145, 2011.
2. M. Schneier, Data and Goliath, 2nd ed., Norton, 2022.
3. D. Vorick, L. Champine, “Sia: Simple Decentralized Storage,” White Paper, 2022.
4. S. Williams, “Arweave: A Protocol for Economically Sustainable Information Permanence,” 2020.
5. European Parliament, “Regulation (EU) 2016/679 (GDPR),” Official Journal of the EU, 2016

АВАРІЙНЕ ВІДНОВЛЕННЯ У ХМАРНИХ МЕРЕЖАХ. ВИКОРИСТАННЯ AWS GLOBAL ACCELERATOR У СЦЕНАРІЇ АВАРІЙНОГО ВІДНОВЛЕННЯ

Демидов Антон Сергійович

II курсу, група KI-22-1phd, спеціальність 123 «Комп'ютерна інженерія»

<https://orcid.org/0009-0009-7986-9203>, anton89d@gmail.com

Відкритий міжнародний університет розвитку людини «Україна», м. Київ
Науковий керівник: Даценко І. П., к.т.н.

Анотація: У роботі розглянуто використання AWS Global Accelerator як інструменту аварійного відновлення в хмарних мережах. Підкреслюється важливість зменшення часу відновлення (RTO) та втрати даних (RPO). Наведено приклад використання багаторегіональної архітектури з AWS Global Accelerator. Проведено тести із застосуванням Apache Benchmark, результати яких показали значне зменшення затримок. Описано конфігурацію інфраструктури через Terraform. Зроблено висновок про ефективність AWS Global Accelerator у забезпеченні безперервності бізнесу.

DISASTER RECOVERY IN CLOUD NETWORKS. USING AWS GLOBAL ACCELERATOR IN DISASTER RECOVERY SCENARIOS.

Abstract: This paper explores the use of AWS Global Accelerator as a disaster recovery tool in cloud networks. It highlights the importance of minimizing Recovery Time Objective (RTO) and data loss (RPO). A multi-region deployment example using AWS Global Accelerator is presented. Apache Benchmark tests demonstrated significantly lower latency and better performance. The infrastructure configuration is described using Terraform. The conclusion affirms AWS Global Accelerator's efficiency in ensuring business continuity.

У роботі досліджено застосування AWS Global Accelerator для аварійного відновлення у хмарних обчислювальних середовищах. Показано, що сервіс дозволяє значно зменшити час відновлення (RTO) завдяки перенаправленню трафіку до найближчого працездатного регіону AWS. Описано використання двох регіонів (us-east-1 та us-west-2), кожен з яких має власні балансувальники навантаження та резервну інфраструктуру.

AWS Global Accelerator конфігурується за допомогою Terraform. Створено дві групи кінцевих точок з маршрутизацією трафіку та перевітками здоров'я. Автоматичне перемикання відбувається у разі недоступності одного з регіонів.

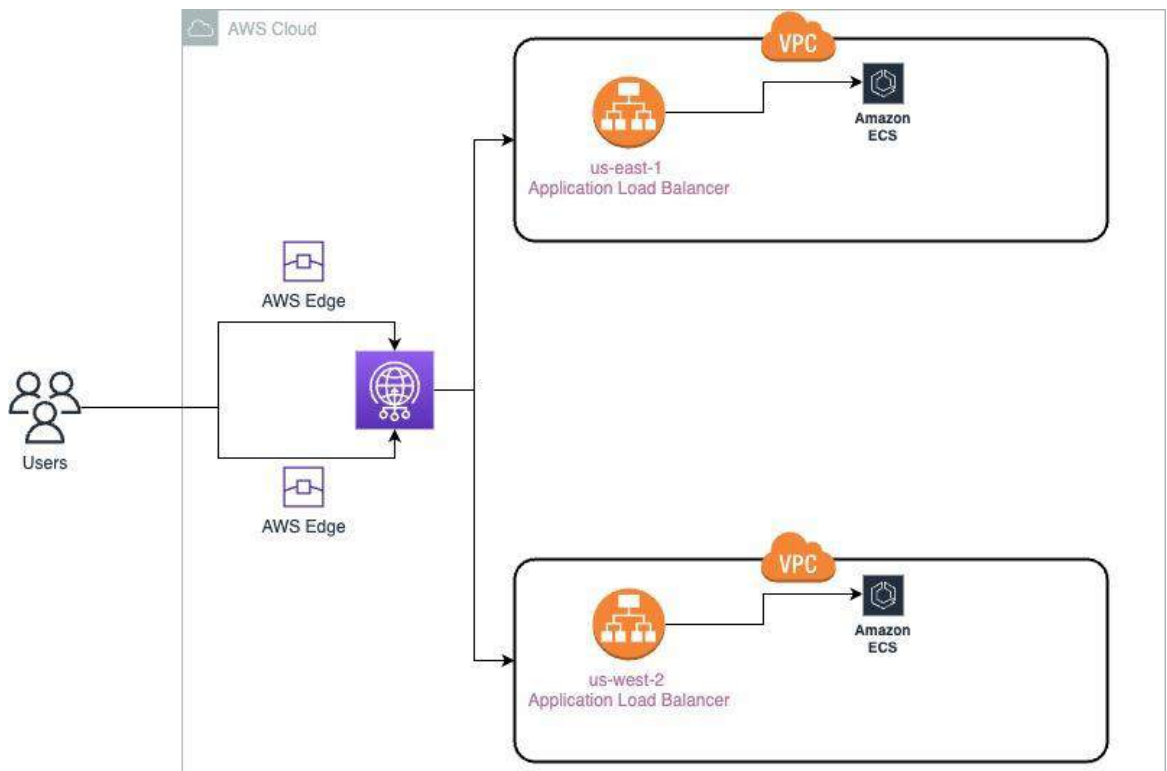


Рис 1. Крос-регіональна архітектура програмного додатка

Результати тестування за допомогою Apache Benchmark демонструють, що середній час відповіді був нижчим при використанні Global Accelerator порівняно з безпосереднім доступом до регіональних адрес.

Для 95% запитів час відповіді через Global Accelerator становив 528 мс, тоді як у регіонів — понад 1200 мс. Це підтверджує доцільність його застосування в сценаріях з високими вимогами до доступності.

Таблиця 1. Результати тестування Global Accelerator

Відсоток запитів, оброблених протягом певного часу (мс)	us-east-1 регіон	us-west-2 регіон	Global Accelerator
50	387	270	269
66	393	290	277
75	406	326	291
80	411	354	335
90	495	480	403
95	1395	1262	528
98	2225	1604	1400
99	3411	2208	1456
100	3411	2209	1456

AWS Global Accelerator підвищує надійність хмарної архітектури, зменшує час простою та є ефективним компонентом стратегії аварійного відновлення.

Список літератури.

АДАПТИВНІ МЕТОДИ ОПТИМІЗАЦІЇ RAG-СИСТЕМ В ОСВІТНІХ ТЕХНОЛОГІЯХ

Денисюк Олександр

2 курс, група KI-23-1phd, спеціальність «Комп'ютерна інженерія»

Інститут комп'ютерних технологій Університету «Україна»

<https://orcid.org/0009-0002-4814-5121>, saszko@gmail.com

Науковий керівник: **Павленко Володимир**, к.ф.-м.н.,

<https://orcid.org/0000-0002-3958-0415>, pavlenko.v@i.ua

Анотація. Сучасні системи генеративного штучного інтелекту створюють нові можливості для трансформації освітніх процесів. Особливу увагу привертають системи Retrieval-Augmented Generation (RAG), які поєднують векторний пошук з генеративними здібностями великих мовних моделей. Проте існуючі реалізації характеризуються недостатньою ефективністю пошуку та субоптимальним формуванням контексту, що обмежує їх застосування в освіті. У роботі розроблено методи оптимізації комбінованого пошуку та формування контексту для підвищення ефективності навчальних процесів. Експериментальні дослідження демонструють покращення швидкості пошуку на 14%, підвищення якості формування контексту на 9% та зростання релевантності результатів на 8%.

ADAPTIVE METHODS FOR OPTIMIZATION OF RAG SYSTEMS IN EDUCATIONAL TECHNOLOGIES

Abstract. Modern generative artificial intelligence systems create new opportunities for transforming educational processes. Particular attention is drawn to Retrieval-Augmented Generation (RAG) systems, which combine vector search capabilities with generative abilities of large language models. However, existing implementations are characterized by insufficient search efficiency and suboptimal context formation, limiting their application in education. The work develops methods for optimizing combined search and context formation to improve learning process efficiency. Experimental studies demonstrate improvement in search speed by 14%, enhancement of context formation quality by 9%, and increase in result relevance by 8%.

Методологія дослідження

Методологія включає системний аналіз існуючих методів векторного пошуку та RAG-архітектур, математичне моделювання процесів формування контексту, експериментальні дослідження на корпусі з 5,000 навчальних матеріалів. Критичний аналіз передбачає оцінку підходів з точки зору швидкодії, якості відповідей та релевантності для освітніх цілей.

Вступ

Сучасна освіта вимагає інтелектуальних систем, здатних оперативно забезпечувати доступ до релевантної навчальної інформації, адаптованої до індивідуальних потреб здобувачів освіти. Традиційні методи інформаційного пошуку часто ігнорують семантичний контекст запитів, що негативно позначається на якості результатів і гальмує навчальний процес. Водночас моделі генеративного

штучного інтелекту, зокрема архітектури RAG, відкривають нові горизонти в розробці адаптивних освітніх платформ. Однак їх широке впровадження стримується через обмеження в швидкодії, неефективне формування контексту та недостатню інтеграцію педагогічних критеріїв. Цим обумовлюється актуальність дослідження.

Основні результати дослідження

При розробці ефективних RAG-систем для освітніх застосунків дослідники постають перед ключовими викликами: оптимізація векторного пошуку для навчального контенту, забезпечення семантичної цілісності при сегментуванні матеріалів, балансування між точністю та швидкістю, адаптація алгоритмів ранжування та інтеграція педагогічних критеріїв у метрики оцінки.

Розроблено адаптивний алгоритм гібридного ранжування, який інтегрує семантичну подібність із статистичними методами релевантності:

$$S(x_{ij}) = \alpha \cdot \text{sim_cos}(q_v, x_{ij}) + \beta \cdot \text{BM25}(q, c_{ij})$$

де α та β - адаптивні вагові коефіцієнти, що налаштовуються відповідно до типу освітнього контенту, q_v - векторне представлення запиту, x_{ij} - вектор документного фрагменту. Запропоновано метод динамічного сегментування документів, який адаптується до структури навчального матеріалу та забезпечує збереження семантичної цілісності з урахуванням педагогічних принципів. Розроблено багаторівневу систему кешування, яка оптимізує швидкість доступу до найбільш запитуваного контенту на основі навчальних траєкторій студентів.

Створено спеціалізовані метрики оцінки якості RAG-систем для освіти, що враховують релевантність, доступність матеріалу, структурованість подачі інформації та відповідність навчальним цілям.

Експериментальне тестування на корпусі з 5,000 документів різних форматів демонструє: підвищення швидкості пошуку на 14%, покращення якості формування контексту на 9% за метриками ROUGE та BERTScore, зростання релевантності на 8% за експертними оцінками педагогів ($p < 0.05$).

Практичне впровадження здійснено в освітній платформі для курсу "Розробка інтелектуальних систем на основі великих мовних моделей", що підтверджує ефективність методів у реальному навчальному середовищі. Результати вказують на значний потенціал адаптивних RAG-систем для цифровізації освіти через персоналізацію доступу до знань та створення інтелектуальних освітніх асистентів.

Список використаних джерел:

1. Rothman D. Transformers for Natural Language Processing and Computer Vision: Explore Generative AI and Large Language Models with Hugging Face, ChatGPT, GPT-4V, and DALL-E 3. 3rd ed. Packt Publishing, 2024. 728 p.
2. Weng C., Wang W. LangChain: Develop LLM-powered Applications with Python. O'Reilly Media, 2024. 450 p.
3. Wu T., Bommasani R., Liang P. Building Production-Ready LLM Applications: From Prototyping to Deployment. Manning Publications, 2024. 375 p.
4. Zhang A., Lau J. Practical Large Language Models: Building Production-Ready Systems with Modern LLM Technologies. Springer, 2024. 400 p.

**АВТОМАТИЧНЕ ОЦІНЮВАННЯ ПИСЬМОВИХ ЗАВДАНЬ СТУДЕНТІВ
ЗА ДОПОМОГОЮ ГІБРИДНИХ СЕМАНТИЧНИХ ПІДХОДІВ
ФІНГЕРПРИНТУВАННЯ
USING HYBRID SEMANTIC FINGERPRINTING METHODS IN THE
ESTIMATION PROCESS OF STUDENT WRITING ASSIGNMENTS**

Дробіт Б.В.

*2 курс, група KI-23-1phd, спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій університету «Україна».
Науковий керівник: Тимошенко А.Г., к.т.н., доцент,
Інститут комп'ютерних технологій Університету «Україна».*

***Анотація.** У роботі розглядається використання фінгерпринтів як методу структурного та семантичного аналізу програмного коду в контексті оцінювання практичних завдань у сфері інформаційних технологій. Найбільш релевантним у випадку поточного дослідження є як дискурсивні структури, так і великомасштабні мовні моделі, як наприклад BERT. Студентський текст спочатку підлягає парсингу у синтаксичному дереві залежностей, або RST-дереві. Наступним чином відбувається перетворення його у фінгерпринт за допомогою інкрементальної хеш-функції з мінімізацією колізії. Парсована структура далі підлягає нормалізації з метою видалення непотрібних конструкцій та зберігається у вигляді легкого XML-орієнтованого формату із застосуванням індексації для управління доступом до окремих вузлів. Як наслідок, семантичне BERT-вкладання створюється для кожного сегмента-кандидата. З метою отримання локального контексту, вкладаються не повні документи, натомість менші текстові фрагменти, а перевірка того, чи збігаються структурно подібні піддерева також з точки зору семантичності, обчислюється косинусна подібність між векторами, які відповідають семантичним вкладанням та студентським відповідям*

Викладення матеріалу дослідження. Головна проблема у межах поточної дискусії полягає у семантичній, або синтаксичній схожості текстових елементів у письмових відповідях та подальше визначення, чи є ці відповіді ідентичними, частково схожими, або повністю відмінними у порівнянні з еталонними відповідями. У цьому відношенні, фінгерпринти слугують в якості спеціальних вказівників того, яким чином та чому студентська відповідь відхиляється від них, виходячи з рамок аргументації, логічної послідовності, структури викладу та семантичної відповідності.

Система, яка вирішуватиме описану проблему має спеціалізуватися не лише на виявленні плагіату, але також враховувати альтернативні допустимі форми вираження відповіді, логічні невідповідності та інноваційні аргументації. Існує широкий вибір належних методів семантичного фінгерпринтування. Найбільш релевантним у випадку поточного дослідження є як дискурсивні структури, так і великомасштабні мовні моделі, як наприклад BERT (Bidirectional Encoder Representations from Transformers – двоспрямовані кодувальні відображення з трансформерів). Оскільки а-ні синтаксичний парсинг, а-ні BERT-вкладання не є результативним наодинці, існує необхідність їхнього поєднання. Складність полягає у різних за своєю суттю репрезентаціях цих підходів, оскільки синтаксичні

дерева структурують інформацію ієрархічним чином, в той час як трансформерні моделі створюють щільні високорозмірні вектори.

Студентський текст спочатку підлягає парсингу у синтаксичному дереві залежностей, або RST-дереві (Rhetorical structure theory – теорія риторичної структури). Наступним чином відбувається перетворення його у фінгерпринт за допомогою інкрементальної хеш-функції з мінімізацією колізії (алгоритм Рабіна-Карпа) [1]. Риторична структура представляється в якості збалансованої послідовності символів на базі слів Дика довжини n , представлених як рядок символів $S=s_1+s_2+\dots+s_n$, де кожен символ відповідає кодованому токєну (наприклад, '(' = 1, ')' = 2). Таким чином, хеш-функція Рабіна-Карпа представляється так:

$$H(S) = (\sum_{i=1}^n s_i \cdot b^{n-i}) \bmod q \quad (1)$$

Парсована структура далі підлягає нормалізації з метою видалення непотрібних конструкцій та зберігається у вигляді легкого XML-орієнтованого формату із застосуванням індексації для управління доступом до окремих вузлів [2]. Кожний фрагмент піддерева фінгерпринтується у вигляді кортежу, який містить структурне зважування, хеш-значення та посилання на первинний вузол. Через масиви суфіксів або B^+ дерева індексуються тільки ті піддерева, які знаходяться вище значення мінімальної ваги, що здійснюється для ефективного пошуку подібностей. Цей індекс виконує функцію першої ланки фільтрації з метою обмеження потенційних збігів перед семантичним аналізом.

Як наслідок, семантичне BERT-вкладання створюється для кожного сегмента-кандидата. З метою отримання локального контексту, вкладаються не повні документи, натомість менші текстові фрагменти, а перевірка того, чи збігаються структурно подібні піддерева також з точки зору семантичності, обчислюється косинусна подібність між векторами t_1 та t_2 , які відповідають семантичним вкладанням та студентським відповідям, відповідно:

$$\text{sim}(t_1, t_2) = (\|t_1\| \cdot \|t_2\|) / (t_1 \cdot t_2) \quad (9)$$

де $t_1 \cdot t_2$ позначає скалярний добуток векторів, а $\|t_1\| \cdot \|t_2\|$ – їхні евклідові норми. Результат функції хоча і відповідає $\text{sim} \in [-1, 1]$, але у контексті трансформерних вкладень значення найчастіше лежать у межах $[0, 1]$, тому що вектори піддаються нормалізації, що дає можливість сприймати результат в якості ступеня семантичної близькості.

У підсумку, система здатна генерувати автоматичну оцінку письмових результатів студентів з поясненням відхилень від еталонного матеріалу з оглядом на аргументацію, структура тексту та змістовну відповідність, таким чином забезпечуючи педагогів допоміжним зворотнім зв'язком.

Список літератури

1. Ansyari T., Abdullah D., Rosnita L. Plagiarism detection application for computer science student theses using cosine similarity and Rabin-Karp. *International Journal of Engineering, Science and Information Technology*, 2024. Vol. 5(1). PP. 185–194. DOI:10.52088/ijesty.v5i1.686.
2. Kustiawan Y., Ghauth K. Dynamic ReLab: A binary path-based labeling scheme for dynamic XML data. *IEEE Access*, 2025. PP. 1–1. DOI:10.1109/ACCESS.2025.3541398.

АЛГОРИТМИ ПОЗИЦІОНУВАННЯ ДРОНА ЗА ДОПОМОГОЮ GPS ТА МАШИННОГО ЗОРУ

Дуднік А.С.

д.т.н., професор, Київський національний університет ім. Тараса Шевченка,
Інститут комп'ютерних технологій Університету «Україна».

Батрак О.Г.

2 курс, група КІ-23-1phd, спеціальність «Комп'ютерна інженерія»
Інститут комп'ютерних технологій Університету «Україна».

Анотація. У сучасному техногенному середовищі безпілотні літальні апарати (БПЛА) активно впроваджуються в різні галузі — від агропромислового комплексу до оборонної сфери, від кінематографії до екологічного моніторингу. Ключовим фактором ефективного функціонування таких систем є точне просторове позиціонування. Основними методами навігації виступають глобальні навігаційні супутникові системи (GNSS), зокрема GPS, а також технології комп'ютерного зору. Їхнє поєднання дозволяє значно підвищити точність, надійність та автономність функціонування БПЛА.

Abstract. In today's high-tech environment, unmanned aerial vehicles (UAVs) are being actively integrated across various sectors — from agriculture and defense to filmmaking and environmental monitoring. A key factor in the effective operation of such systems is accurate spatial positioning. The primary methods of navigation include Global Navigation Satellite Systems (GNSS), particularly GPS, as well as computer vision technologies. Their combination significantly enhances the precision, reliability, and autonomy of UAV operations.

Позиціонування за допомогою GPS. Система GPS забезпечує визначення географічних координат із точністю до кількох метрів. У дронах GPS-модулі використовуються для реалізації автоматичної навігації, стабілізації позиції у повітрі, автоповернення в точку старту, а також побудови патрульних маршрутів. Для підвищення точності застосовують розширені алгоритмічні підходи, зокрема фільтр Калмана, диференціальну корекцію RTK та метод Dead Reckoning.

Математична модель фільтра Калмана. Нехай вектор стану дрона в 2D-просторі має вигляд:

$$\mathbf{x}_k = \begin{bmatrix} x_k \\ y_k \\ v_{x,k} \\ v_{y,k} \end{bmatrix}$$

де x_k, y_k — положення, $v_{x,k}, v_{y,k}$ — компоненти швидкості.

Модель переходу:

$$x_k = A \cdot x_{k-1} + w_{k-1}, \quad w_{k-1} \sim \mathcal{N}(0, Q).$$

При кроці $\Delta t = 1$:

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Модель вимірювання: $z_k = H \cdot x_k + v_k$, $v_k \sim \mathcal{N}(0, R)$,

$$\text{де } H = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Основні етапи фільтрації Калмана

Прогноз стану: $x_{k|k-1} = A \cdot x_{k-1|k-1}$.

Прогноз коваріації похибки: $P_{k|k-1} = A \times P_{k-1|k-1} \times A^T + Q$.

Калманівський коефіцієнт: $K_k = P_{k|k-1} \cdot H^T \cdot (H \cdot P_{k|k-1} \cdot H^T + R)^{-1}$.

Оновлення стану: $x_{k|k} = x_{k|k-1} + K_k \cdot (z_k - H \cdot x_{k|k-1})$

Оновлення дисперсії: $P_{k|k} = (I - K_k \cdot H) \cdot P_{k|k-1}$.

Чисельний приклад. Початковий стан: $x_0 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$, $P_0 = I$.

Вимірювання: $z_1 = \begin{bmatrix} 1.1 \\ 0.9 \end{bmatrix}$, $R = 0.01 \cdot I$, $Q = 0.001 \cdot I$.

Комп'ютерний зір як альтернатива GPS. Комп'ютерний зір виступає ефективною альтернативою GPS у ситуаціях, коли супутниковий сигнал відсутній або нестабільний. Завдяки методам машинного зору дрони можуть орієнтуватися в просторі шляхом аналізу візуальної інформації з камер. Серед ключових технологій варто виділити Visual Odometry (VO), алгоритми Simultaneous Localization and Mapping (SLAM), включаючи MonoSLAM, StereoSLAM і Visual-Inertial SLAM, а також сучасні підходи на основі глибокого навчання. До прикладів реалізації таких систем належать ORB-SLAM і DROID-SLAM. Найбільш надійними вважаються гібридні навігаційні системи, які поєднують дані від GPS, комп'ютерного зору (CV) та інерціальних сенсорів (IMU).

Перевагами таких рішень є підвищена надійність при втраті одного з каналів, висока точність позиціонування на малих висотах та здатність до автоматичного перемикавання між режимами залежно від зовнішніх умов. Попри значні успіхи, залишаються певні виклики: потреба в обчислювальних ресурсах для обробки відеопотоку, чутливість алгоритмів CV до змін освітлення, а також затримки обробки даних. Перспективними напрямками розвитку є інтеграція з мережами 5G, використання локальних маяків, глибоке сенсорне злиття та впровадження спеціалізованих графічних процесорів для опрацювання нейромереж у реальному часі.

Сучасні алгоритми позиціонування БПЛА на основі GNSS і машинного зору є критично важливими для автономного функціонування дронів. Їх поєднання забезпечує гнучкість, точність і надійність навігації, а інтеграція штучного інтелекту та сенсорного злиття відкриває нові горизонти застосування в умовах складної просторової динаміки.

ЕКОНОМІКА ДОВІРИ У ВІРТУАЛЬНИХ ОСВІТНІХ МЕТАВСЕСВІТАХ ЯК ІНСТРУМЕНТ СОЦІАЛЬНОЇ ТОКЕНІЗАЦІЇ, NFT-СЕРТИФІКАЦІЇ ТА DAO-УПРАВЛІННЯ

TRUST ECONOMY IN VIRTUAL EDUCATIONAL METAVERSES AS A TOOL FOR SOCIAL TOKENIZATION, NFT CERTIFICATION, AND DAO GOVERNANCE

Ємець Максим Ігорович

III курс, група KI-22-1phd, спеціальність «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «Україна»,
ORCID: <https://orcid.org/0009-0006-6111-9672>

maxemets.g@gmail.com

Науковий керівник: **Даценко І. П.**, к.т.н. ,

Відкритий міжнародний університет розвитку людини «Україна»

Анотація. У тезах розглянуто економіку довіри у віртуальних освітніх метавсесвітах. Аналізується токенизація взаємодії та її роль у мотивації. NFT і SBT використано для цифрової сертифікації знань. DAO-моделі подано як альтернативу централізованому управлінню. Наголошено на перспективності децентралізованих освітніх екосистем. **Ключові слова:** Освітній метавсесвіт, токенизація, NFT-сертифікація, DAO-управління.

Abstract. The paper examines the trust economy in virtual educational metaverses. It explores tokenized interaction as a motivational mechanism. NFTs and SBTs are used for digital knowledge certification. DAOs are considered an alternative to centralized governance. Decentralized educational ecosystems are emphasized as promising. **Keywords:** Educational metaverse, tokenization, NFT-certification, DAO-governance.

Вступ. Сучасні освітні системи перебувають на порозі радикальних трансформацій завдяки впровадженню метавсесвітів — інтерактивних віртуальних просторів, які поєднують освітні технології з децентралізованими інструментами Web3. В умовах цифрової революції особливого значення набуває економіка довіри, що базується на токенизації взаємодії, використанні NFT для сертифікації та DAO-моделей управління. Ці інновації створюють нові можливості для прозорості, безпеки та ефективності освітніх процесів, підвищуючи мотивацію учасників і розширюючи доступ до якісної освіти у віртуальному середовищі.

Токенизація взаємодії як механізм мотивації та контролю якості. Токенизація у віртуальних освітніх метавсесвітах виступає ефективним інструментом мотивації та забезпечення якості навчання. За допомогою цифрових токенів створюються системи винагород, які заохочують студентів і викладачів до активної участі та підтримки високих стандартів. Peer-to-peer оцінювання дозволяє учасникам взаємно оцінювати якість робіт, підвищуючи прозорість і довіру до процесу. Мікронагороди у вигляді токенів стимулюють постійну активність, а індекси репутації формують довіру та визначають статус користувачів у спільноті. Приклади таких систем можна знайти в Ed3-проектах Open Campus і EduDAO, де токенизація підтримує як мотивацію, так і децентралізоване управління, підвищуючи ефективність освітнього процесу.

NFT-сертифікація як інструмент доказу знань. NFT-сертифікація у віртуальних метавсесвітах забезпечує надійний, прозорий та незмінний спосіб

підтвердження освітніх досягнень. Використання soulbound tokens (SBT) дозволяє закріпити знання за конкретним індивідом, підвищуючи довіру та персоналізацію сертифікатів. Переваги NFT/SBT включають безпечне збереження, легку верифікацію та портативність освітніх результатів, що робить їх доступними для інтеграції у різні платформи та ринки праці. Втім, існують проблеми, зокрема ризики плагіату, анонімність деяких користувачів та обмежена доступність технологій для частини студентів.

DAO-управління у віртуальних освітніх спільнотах. Децентралізовані автономні організації (DAO) є революційною моделлю управління, яка трансформує традиційні адміністративні підходи в освітніх метавсесвітах. DAO базуються на технології блокчейн і смарт-контрактах, що забезпечує автоматизацію процесів прийняття рішень, прозорість та незмінність дій, зменшуючи ризик корупції або маніпуляцій. Головна перевага DAO полягає у децентралізації влади: всі учасники освітнього процесу — студенти, викладачі, адміністрація — мають рівні права голосу у формуванні правил, оцінці якості освіти, розподілі ресурсів та розвитку спільноти. Це створює систему колективної відповідальності, яка стимулює активну участь і підвищує мотивацію через відчуття впливу на освітній процес. З педагогічної точки зору, DAO виступає як інноваційна модель, що підтримує демократичне управління знаннями, розвиває навички критичного мислення, співпраці та самоорганізації у студентів і викладачів. Завдяки прозорості всіх транзакцій і рішень у блокчейні, підвищується довіра між учасниками, що є ключовим фактором для ефективного навчання у віртуальному середовищі. Практичні кейси, такі як платформи EduDAO чи Open Campus, демонструють, що DAO дозволяє адаптувати освітні програми в реальному часі відповідно до потреб спільноти, інтегрувати зворотній зв'язок та підтримувати стійку екосистему самоосвіти. Такий підхід мінімізує бюрократичні бар'єри і сприяє розвитку інклюзивності, де кожен голос має значення. Таким чином, DAO-управління у віртуальних освітніх метавсесвітах не лише підвищує якість і доступність освіти, але й формує нові соціальні та педагогічні практики, що відповідають викликам цифрової епохи.

DAO-управління у віртуальних освітніх метавсесвітах забезпечує прозорість, децентралізацію та колективну відповідальність, що підвищує ефективність навчального процесу та сприяє формуванню інноваційних педагогічних практик у цифровому середовищі.

Список використаних джерел:

1. Buterin V., Hitzig Z., Weyl G. Decentralized Society: Finding Web3's Soul. *Papers.ssrn.com*. 11.05.2022. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763
2. Chohan U. W. Decentralized Autonomous Organizations (DAOs): Their Present and Future. *Papers.ssrn.com*. 04.12.2017. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055

АНАЛІЗ НЕДОЛІКІВ СУЧАСНИХ МОВ ПРОГРАМУВАННЯ ТА ПРОЕКТУВАННЯ НОВОЇ МОВНОЇ ПАРАДИГМИ

Жиритовський О. А.

аспірант, Інститут комп'ютерних технологій
Відкритий міжнародний університет розвитку людини «Україна»,
м. Київ, вул. Львівська, 23, e-mail: i.am.zhirik@gmail.com

***Анотація.** Аналізуються недоліки сучасних мов програмування з точки зору зручності використання для програмістів. Розглянуто проблеми читабельності, надмірної формальності в оголошенні змінних, обмежень синтаксису та недоліки об'єктно-орієнтованого підходу. Багато з існуючих концепцій застаріли і не відповідають сучасним потребам. Запропоновано критерії, яким має відповідати ідеальна мова програмування: простота, гнучкість, відсутність зайвих формальностей і зосередженість на алгоритмічній суті.*

***Abstract.** The shortcomings of modern programming languages are analyzed from the perspective of usability for programmers. Issues such as readability, excessive formality in variable declarations, syntax limitations, and drawbacks of the object-oriented approach are considered. Many existing concepts are outdated and do not meet current needs. Criteria for an ideal programming language are proposed: simplicity, flexibility, absence of unnecessary formalities, and a focus on the algorithmic essence.*

Вступ

Комп'ютер виконує програми, що складаються з машинних команд – низькорівневих інструкцій, що безпосередньо обробляються центральним процесором. Проте ці інструкції є надто складними для сприйняття людиною, тому з'явилися мови програмування, які є проміжною ланкою між людиною та комп'ютером. Мета мов програмування – зробити опис алгоритмів інтуїтивно зрозумілим і придатним для трансляції у машинний код.

Синтаксис – це набір правил, які визначають форму правильно записаних конструкцій у мові програмування. Ідеальна мова мала б поєднувати зручність для програміста та ефективність виконання на комп'ютері. На практиці спостерігається певний компроміс: мови з простим і зручним синтаксисом зазвичай є інтерпретованими та працюють повільніше, тоді як мови ближчі до системного рівня забезпечують високу швидкодію, але є складнішими в освоєнні та використанні.

Типові проблеми сучасних мов програмування

1. Читабельність і порядок опису. Багато мов змушують програміста писати код у певному порядку – наприклад, спочатку описати всі функції, які викликаються пізніше. Це знижує зручність читання, адже логіка програми часто виявляється "внизу файлу", а зверху – технічні деталі;

2. **Складність декларацій змінних.** У багатьох мовах потрібно явно оголошувати змінні та їх типи. Це додає надмірної формальності: програміст змушений повідомляти компілятору те, що для нього очевидно;

3. **Неповнота мовних конструкцій.** Деякі мови не мають зручних механізмів для реалізації певних алгоритмічних патернів. Наприклад, відмова від оператора goto як поганого стилю створила ситуації, коли елегантного виходу з вкладених циклів просто не існує. Альтернативи або складніші, або менш читабельні;

4. **Надлишкова абстракція.** У багатьох мовах програмування активно використовуються конструкції для обробки колекцій даних, які приховують деталізацію окремих кроків – наприклад, замість звичайного циклу застосовуються спеціальні функції чи вирази. Такий підхід робить код коротшим, але часто менш зрозумілим, особливо якщо розглядати програму як послідовність чітких дій. Крім того, велика кількість подібних викликів може знижувати продуктивність, адже кожен з них – це додаткова обробка та витрати процесорного часу;

5. **Застарілі концепції об'єктно-орієнтованого програмування (ООП).** Деякі концепції ООП втратили свою актуальність. Наприклад, поліморфізм через приведення до базового типу часто можна замінити простішими структурами, а саме – масивами, що містять об'єкти різних типів. Наслідування теж нерідко ускладнює логіку програми: потрібно вирішувати, які методи ховати, які відкривати, як уникати конфліктів між батьківськими й дочірніми класами. Простішим підходом є композиція – тобто включення одного об'єкта всередину іншого;

6. **Обмеження синтаксису.** У багатьох мовах існують обмеження на те, де можна оголошувати змінні, де дозволений повноцінний код, а де лише окремі оператори. Це додає зайвих обмежень у процесі мислення та проектування програми.

Критерії побудови ідеальної мови програмування

На основі викладеного вище можна сформулювати невеликий перелік вимог до ідеальної мови:

1. **Простий та лаконічний синтаксис,** орієнтований на людину, а не на машину;

2. **Програма має подаватися у вигляді алгоритму,** тобто описувати послідовність елементарних кроків для вирішення певної задачі;

3. **Оптимальний набір конструкцій мови.** Набір мовних елементів повинен бути невеликим, але достатнім для опису всіх алгоритмів;

4. **Деревовидна структура програми:** функції, класи та простори імен повинні мати можливість вкладатися одне в одне. Це підвищить гнучкість структури програми та її організацію;

5. **Спрощене оголошення змінних.** Для оголошення змінної достатньо просто присвоїти їй значення – без окремої декларації чи вказання типу. Кожна змінна може бути локальною в межах блоку, в якому її створено. Так само вона може бути глобальною для вкладених внутрішніх блоків. Щоб відрізнити локальну змінну від глобальної, доцільно позначати глобальні змінні спеціальним символом на початку їхнього імені;

6. Автоматизоване управління пам'яттю. Після завершення використання змінних або об'єктів, мова має самостійно вивільняти зайняту пам'ять без участі програміста;

7. Явна типізація параметрів функцій. Типи параметрів функцій мають бути чітко вказані безпосередньо в сигнатурі функції для покращення читабельності та розуміння логіки програми. Важливо, щоб типи можна було описувати прямо під час оголошення функції, а не окремо в іншому місці.

Більшість існуючих мов програмування були створені в контексті обмежень свого часу: дефіцит апаратних ресурсів, жорсткі вимоги до ефективності, відсутність належних інструментів. Сучасний комп'ютерний світ змінився, настав час переосмислити синтаксис і концепції, які вважаються нормою. Ідеальна мова програмування має поєднувати простоту для людини з продуктивністю для комп'ютера.

МОДУЛЬНІ CI/CD СИСТЕМИ, ПЕРЕВАГИ, АРХІТЕКТУРА ТА ВИКЛИКИ

Загорулько А. В.

*II курс, група KI-23-1phd, спеціальність «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «Україна»
<https://orcid.org/0009-0004-9478-5642>, azago85@gmail.com*

Павленко В. І., к. ф.-м. наук, Відкритий міжнародний університет
розвитку людини «Україна»
<https://orcid.org/0000-0002-3958-0415>, pavlenko.v@i.ua

Анотація. Модульні CI/CD системи є сучасним підходом до автоматизації життєвого циклу розробки програмного забезпечення, що забезпечує гнучкість, масштабованість і ефективність. Завдяки побудові на основі незалежних або слабо пов'язаних модулів, такі системи дозволяють легко адаптувати окремі етапи конвеєра до нових вимог і технологій. Ключовими перевагами є можливість повторного використання компонентів, швидка інтеграція інновацій і мінімізація впливу змін. Водночас впровадження таких систем вимагає ретельного управління залежностями, безпеки та моніторингу. Цей підхід стає дедалі більш поширеним у середовищах із високими вимогами до швидкості релізів та надійності програмного забезпечення.

Ключові слова: CI; CD; програмне забезпечення; SDLC.

Abstract. Modular CI/CD systems represent a modern approach for SDLC automation, providing flexibility, scalability, and efficiency. Built on independent or loosely coupled components, these systems allow individual pipeline stages to be adapted easily to new requirements and technologies. Key advantages include reusability of components, fast integration of innovations, and minimized impact of changes. However, successful implementation requires careful management of dependencies, security, and monitoring. This approach is becoming increasingly popular in environments with high demands for release velocity and software reliability.

Keywords: CI; CD; software; SDLC.

Вступ

CI/CD (Continuous Integration / Continuous Deployment) є основою сучасної DevOps-інфраструктури та забезпечує автоматизацію життєвого циклу розробки програмного забезпечення (SDLC). Сучасні вимоги до гнучкості, масштабованості та швидкості релізів стимулюють перехід до модульних CI/CD архітектур.

Модульна CI/CD система — це система, побудована з незалежних або слабо пов'язаних компонентів (модулів), кожен з яких виконує конкретну функцію (наприклад, збірка, тестування, розгортання, моніторинг). Основна мета модульної архітектури - це забезпечення гнучкості, повторного використання та масштабованості CI/CD процесу.

Переваги модульного підходу

- Заміна або оновлення окремих модулів без впливу на всю систему.
- Швидка інтеграція нових технологій.
- Можливість комбінування модулів від різних постачальників.

- Безперервне вдосконалення процесів, передбачає можливість оптимізації окремих етапів конвеєра без ризику для всієї CI/CD системи.
- Легкість масштабування.

Архітектурні підходи

- Мікросервісна архітектура конвейерів – кожен етап (збірка, тестування, розгортання) може бути реалізований, як окремий мікросервіс.
- Оркестрація – централізований координатор використовується для керування окремими модулями.
- Підтримка API, необхідна для можливості реалізації модулів та розширення функціональних можливостей за рахунок залучення сторонніх вендорів.

Виклики та ризики

- Складність у координації модулів, потребує надійного оркестратора.
- Забезпечення цілісності конвейера, потребує наявності механізму контролю залежностей між модулями.
- Розподілена структура ускладнює централізоване управління та потребує надійної системи безпеки та контролю доступу.

Модульний підхід до проектування CI/CD систем є еволюційною відповіддю на зростаючі вимоги до SDLC, а саме забезпечення гнучкості, швидкості, надійності, масштабованості та підтримки розгортання на різних типах хмарних та приватних середовищ.

Список літератури

1. Загорулько, А. В., & Павленко, В. І. (2024). Архітектура ефективної ci/cd-системи для програмних рішень, заснованих на msa. Інфокомунікаційні та комп'ютерні технології, 1(07), 56-60. <https://doi.org/10.36994/2788-5518-2024-01-07-07>, 141–145. <https://doi.org/10.1109/SCC.2019.00033>, 763–768. <https://doi.org/10.1109/incit63192.2024.10810646>, 1–7. <https://doi.org/10.1145/3194760.3194768>

АРХІТЕКТУРА БЕЗПЕЧНОГО ЦИФРОВОГО СЕРЕДОВИЩА ДЛЯ ЗАСУДЖЕНИХ: ПІЛОТНА МОДЕЛЬ «ЦИФРОВА СВОБОДА»

Йовдій Георгій Георгійович

Анотація. У тезі представлено інноваційну модель «Цифрова свобода» — інфраструктуру контрольованого, але відкритого доступу до Інтернету для засуджених, яка поєднує апаратно-програмні технології моніторингу з дотриманням прав людини. Основна мета — створення безпечного цифрового каналу для дистанційного навчання, працевлаштування та комунікації без ризику для суспільної безпеки. Запропонована технічна архітектура дозволяє забезпечити повноцінну цифрову взаємодію ув'язнених, не вдаючись до жорсткої фільтрації чи цензури.

Abstract. The paper presents the pilot concept of “**Digital Freedom**” — a secure, monitored internet access model for incarcerated individuals in Ukraine. Unlike traditional restrictions or whitelist-based systems, this approach introduces a **controlled but open access gateway**, allowing prisoners to engage in online education, remote work, and communication under full behavioral logging and non-invasive monitoring. The technical architecture is based on VPN tunneling, static IP binding, DPI/NGFW traffic analysis, and proxy-based behavioral analytics — all without accessing private messages or violating privacy laws. The system ensures transparency, accountability, and adaptability while minimizing risks to public safety. The model emphasizes **responsibility over restriction**, offering digital access as a progression-based privilege, not a blanket right. This initiative aims to reintegrate inmates into society through **digital literacy, professional development, and structured interaction** — both during incarceration and after release. The concept is scalable, cost-efficient, and compliant with national legislation and international human rights standards. Ultimately, “**Digital Freedom**” **transforms access into a tool for growth, not a threat**, and provides a new framework for rehabilitative justice in the digital age.

1. Вступ: чому цифровий доступ — це безпека, а не загроза

Ізоляція від Інтернету в сучасному світі дорівнює виключенню з соціального, економічного та освітнього життя. Засуджені в Україні сьогодні позбавлені не лише зв'язку, а й права на цифрову адаптацію. У XXI столітті це не покарання — це цифрове відчуження, яке суперечить як міжнародним стандартам, так і логіці ресоціалізації.

2. Суть моделі: доступ без ризику

Концепція моделі базується на принципі: **не whitelist-доступ до кількох сайтів, а повноцінний, але контрольований шлюз із аналітичним моніторингом.** Користувач (засуджений) має змогу вільно користуватись інтернетом — у межах правового поля — а всі його дії проходять через багаторівневу систему технічного аналізу.

3. Технічна архітектура: як це працює

3.1. VPN-шлюз із централізованим журналюванням

Увесь трафік проходить через локальний VPN-контур, який:

- забезпечує з'єднання з мережею за унікальним ID-користувача;

- автоматично фіксує спроби доступу до заборонених ресурсів;
- зберігає повний лог активності без втручання в зміст повідомлень (HTTPS не декодується).

3.2. Статична IP-ідентифікація та логування

Кожен засуджений отримує власну IP-адресу, яка зв'язана з його обліковим записом. Це дозволяє:

- формувати **персональний цифровий профіль**;
- аналізувати темпи розвитку (кількість годин на навчальних платформах, інтерес до працевлаштування);
- побудувати **прогнозну модель ризиків** (наприклад, через виявлення раптових змін у поведінці).

3.3. DPI / NGFW-моніторинг

Інфраструктура оснащується DPI (Deep Packet Inspection) та NGFW (Next-Generation Firewall), що:

- відслідковують мережеву поведінку;
- не читають зміст зашифрованих повідомлень;
- формують **аналітичну картину цифрової активності**, яку можуть використовувати куратори, психологи, соціальні працівники.

3.4. Проксі-сервер для поведінкової аналітики

- Всі сесії логуються;
- Зберігається тривалість, тип контенту, динаміка запитів;
- Працює **алгоритм оцінки залученості**, який може бути підставою для збільшення або обмеження доступу.

4. Юридичне підґрунтя: де право — там і технологія

Проект базується на:

- **ст. 53 Конституції України (право на освіту);**
- **ст. 26 Загальної декларації прав людини (доступ до освіти — без дискримінації);**
- **резолуції A/HRC/32/13 Ради ООН з прав людини, яка закликає надати Інтернет навіть ув'язненим;**
- **потребі змінити ст. 110 Кримінально-виконавчого кодексу, що сьогодні фактично забороняє цифрову присутність.**

5. Масштабування: просто, ефективно

Система може бути впроваджена в будь-якій установі завдяки тому, що:

- базується на **стандартному обладнанні (router + proxy + VPN-сервер)**;
- використовує **open-source** інструменти логування та моніторингу (наприклад, ELK stack, OpenVPN, Zabbix);
- підтримується спільнотою ІТ-фахівців, волонтерів, освітян.

6. Людський вимір: контроль — не репресія

Моніторинг не застосовується для покарання. Його роль:

- дати адміністрації сигнал: хто активно навчається, хто втрачає інтерес;
- підтримати прогрес, а не карати за відхилення;
- дозволити самому засудженому побачити, як його дії фіксуються і що змінюється.

Це **цифрова відповідальність** як новий етап соціальної взаємодії.

7. Інновація

Модель «Цифрова свобода» — це перша в Україні ініціатива, що:

- **поєднує архітектуру цифрової безпеки з етикою прав людини;**
- відкриває доступ до інтернету **не як пільгу**, а як результат індивідуального прогресу;
- пропонує **супровід після звільнення** — ті самі акаунти, ті самі платформи, той самий простір розвитку.

Це не про Wi-Fi у камерах. Це про **зв'язок із життям**, у якому вже живе решта світу.

Інтернет сам по собі нікого не змінить — але **контрольований доступ із моніторингом, аналітикою та зворотним зв'язком** здатен зробити більше, ніж будь-яка заборона: він створює **реальні умови для повернення**, а не лише формальні шанси.

Цифрова свобода — це архітектура, в якій держава не ізолює, а супроводжує.

Список бібліографії:

1. Конституція України – <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Кримінально-виконавчий кодекс України, ст. 110 – <https://zakon.rada.gov.ua/laws/show/1129-15>
3. UN Human Rights Council Resolution A/HRC/32/13 (2016) – <https://digitallibrary.un.org/record/845728>
4. Загальна декларація прав людини, стаття 26 – <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
5. UNICRI Report (2024): Digital Rehabilitation in Prisons – <https://unicri.it/Publications/Digital-Prisons-2024>
6. Federal Bureau of Prisons (USA): TRULINCS – <https://www.bop.gov/inmates/trulincs.jsp>
7. Telio Group (EU): Prison Communication Systems – <https://www.telio.com/en/>
8. Fortinet: Next Generation Firewall (NGFW) – <https://www.fortinet.com/resources-campaign/next-generation-firewall>
9. Cisco: Deep Packet Inspection (DPI) Overview – <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html>
10. Наказ МОН №1116 (2021) – [https://zakon.rada.gov.ua/laws/show/z1202-](https://zakon.rada.gov.ua/laws/show/z1202-21)

РОЗРАХУНОК КОЕФІЦІЄНТА ЙМОВІРНОСТІ ПОМИЛКИ В СЛОВІ ДЛЯ ВИКОРИСТАННЯ В ДОДАТКУ ДЛЯ ДІАГНОСТИКИ ДИСЛЕКСІЇ У ДІТЕЙ

Мельников О.Ю., Гришук Д.В.,
Донбаська державна машинобудівна академія

Анотація. Розглянуто проблему дислексії у дітей та необхідність її автоматизованої діагностики. Описано метод розрахунку коефіцієнта ймовірності помилки в слові на основі типових і фактичних помилок дітей. Запропоновано лінійну регресійну модель із використанням бази даних Access. Реалізація здійснена у середовищі Lazarus з інтерактивним візуальним підходом до складних слів.

Abstract. The problem of dyslexia in children and the need for its automated diagnosis is considered. A method for calculating the error probability coefficient in a word based on typical and actual errors made by children is described. A linear regression model using an Access database is proposed. The implementation is carried out in the Lazarus environment with an interactive visual approach to highlighting complex words.

За даними Міжнародної асоціації дислексії [1] 12% населення мають дислексію. Дислексія визначається як стійка нездатність опанувати навичку читання при нормальному рівні інтелекту в оптимальних умовах навчання [2].

В Україні лише у 2017 році почали розглядати дислексію, як порушення, що потребує корекції й тому ґрунтовних досліджень та науково-обґрунтованих методик для корекційної роботи з такими дітьми ще немає. Але певні зрушення в цьому напрямку все ж є і дислексія вже активно діагностується. Кількість продіагностованих дітей з цим порушенням щороку збільшується, що свідчить про надзвичайну актуальність даної проблеми [3, с.156].

Одним з напрямів діагностики дислексії є аналіз типових помилок, які допускає дитина під час читання. Для цього потрібно розробити інструменти, що дозволять не лише фіксувати помилки, а й на основі накопичених даних будувати моделі, які оцінюють складність конкретних слів для дитини з дислексією [4].

Одним з таких інструментів є коефіцієнт ймовірності помилки в слові, який можна обчислити на основі статистики помилок, пов'язаних із цим словом. Такий підхід дозволить автоматизувати оцінку складності матеріалу для дитини та виявити «проблемні» слова ще до початку тестування.

Для розрахунку коефіцієнта ймовірності помилки використовується база даних Access з кількома взаємопов'язаними таблицями:

- завдання – містить правильні відповіді для кожного завдання;
- типові помилки – містить помилкові відповіді на завдання за типами дислексії;
- виконані завдання – фіксує відповіді дітей, які відрізняються від правильних.

Ключова таблиця для розрахунку – це "Типові помилки". У ній містяться типові помилки по кожному з завдань з вказанням типу дислексії, для якого

характерна ця помилка. Таким чином, накопичується статистика помилок за 5 категоріями дислексії: оптична, мнестична, фонетична, аграматична, семантична.

Коефіцієнт ймовірності помилки в слові розраховується за допомогою лінійної регресійної моделі [5], у якій кожен тип помилки виступає як незалежна змінна. Модель має вигляд:

$$y = b_0 + b_1 \cdot x_1 + b_2 \cdot x_2 + b_3 \cdot x_3 + b_4 \cdot x_4 + b_5 \cdot x_5 + b_6 \cdot x_6 \quad (1)$$

де:

$x_1 - x_6$ – кількість помилок відповідного типу (для конкретного слова);

$b_1 - b_6$ – вагові коефіцієнти, що відображають важливість кожного типу помилки;

b_0 – вільний член (середнє значення помилок без урахування конкретного типу);

y – прогнозована ймовірність помилки в слові.

Коефіцієнти $b_1 - b_6$ обчислюються автоматично за методом найменших квадратів на основі інформації з бази даних. Зокрема:

– коефіцієнти $b_1 - b_5$ визначаються з використанням таблиці «Типові помилки», де накопичено статистику помилок за 5 видами дислексії;

– коефіцієнт b_6 оцінюється за таблицею «Виконані завдання», що містить фактичні помилки дітей.

Регресійні коефіцієнти обчислюються на основі суми добутків, квадратів та середніх значень. Модель оновлюється щоразу при запуску додатка.

Додаток реалізовано в середовищі візуального програмування Lazarus. При відкритті форми з блоком завдань тестування має виконуватись наступний алгоритм:

1. Завантажуються усі типові та фактичні помилки з бази даних.
2. Розраховуються коефіцієнти регресії ($b_1 - b_6$).
3. Для кожного завдання виконуються SQL-запити до бази даних, щоб отримати статистику помилок ($x_1 - x_6$).
4. На основі $x_1 - x_6$ та коефіцієнтів $b_1 - b_6$ обчислюється ймовірність помилки.
5. Якщо ймовірність перевищує поріг, то розмір шрифту для цього завдання змінюється (з 15 на 20), що візуально підкреслює складні слова.

Цей підхід дозволяє зробити інтерфейс динамічним та чутливим до накопичених даних і не вимагає ручної оцінки кожного слова.

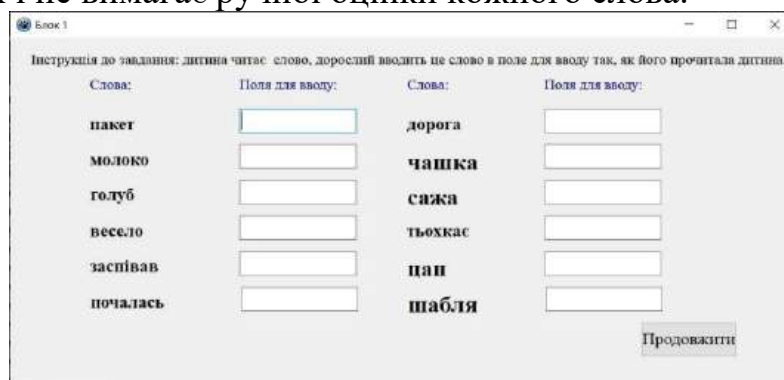


Рисунок 1 – Блок завдань тесту з врахуванням коефіцієнту ймовірності помилки

Список літератури

1. International Dyslexia Association [Електронний ресурс]. – URL: <http://www.dyslexiaida.org>.
2. Іноді низька успішність дітей у школі має пояснення: що з цим робити? [Електронний ресурс]. – URL: https://galinfo.com.ua/news/inodi_nyzka_uspishnist_ditey_u_shkoli_maie_royasnennya_shcho_z_tsym_robity_407073.html.
3. Логопедія. Підручник. / За ред. М.К. Шеремет. – К.: Видавничий Дім «Слово», 2010. – 376 с.
4. Мельников О. Ю., Грищук Д. В. Програмне забезпечення для попередньої діагностики дислексії у дітей // Automation of Technological and Business Processes. – Одеса: ОНТУ, 2024. – № 16 (2). – С. 81–87. – DOI: <https://doi.org/10.15673/atbp.v16i2.2843>
5. Гончаренко В. М. Статистика: навчальний посібник. – К.: Видавничий дім «Кондор», 2011. – 432 с.

ВЕБЗАСТОСУНОК ДЛЯ АНАЛІЗУ КОЛЬОРОВОЇ ПАЛІТРИ САЙТІВ ДЛЯ ЛЮДЕЙ З ПОРУШЕННЯМ КОЛЬОРОСПРИЙНЯТТЯ

Мельников О.Ю., Канішев В.О.,

Донбаська державна машинобудівна академія

***Анотація.** Перелічені проблеми осіб з особливими проблемами сприйняття кольорів. Сформульовано задачу створення застосунку для аналізу рівня задоволення сайтами людей з такими порушеннями. Описано створений раніше модуль для перевірки сполучень кольорів. Перелічені шляхи реалізації процесу аналізу сайтів. Наведено два приклади роботи застосунку.*

***Abstract.** The problems of people with special problems of color perception are listed. The task of creating an application for analyzing the level of satisfaction with websites of people with such disorders is formulated. The previously created module for checking color combinations is described. The ways of implementing the process of analyzing websites are listed. Two examples of the application's operation are given.*

Дальтонізм – це особливість людського зору, яка проявляється у зниженій або повній нездатності бачити чи розрізняти всі або деякі кольори [1]. Є низка методів та програмних засобів для виявлення аномалій визначення кольорів [2], але окремою проблемою є створення доступного середовища для людей з особливими потребами. На сучасному рівні це означає наявність електронних ресурсів (інтернет-сайтів), що будуть цілком задовольняти потреби людей із порушенням кольоросприйняття [3].

Було поставлено та реалізовано задачу створення застосунку для аналізу рівня задоволення сайтами людей з порушеннями кольоросприйняття. Створений інструмент повинен аналізувати кожне можливе сполучення кольорів на сайті (кольори фону vs кольори символів) і розраховувати спеціальний коефіцієнт задоволеності (коефіцієнт інклюзивності) кожного можливого відвідувача з різними порушеннями кольоросприйняття за кожним з трьох варіантів дальтонізму [4].

На першому етапі було створено модуль для перевірки сполучень кольорів, які саме користувач або вебдизайнер бажає застосувати для свого проєкту [5]. Розділ «Звичайний зір» показує, як виглядають кольори для людей із нормальним зором. Розділи «Протанопія», «Дейтеранопія» та «Тританопія» демонструють, як виглядають ці ж кольори для людей із дальтонізмом. Кожен з прикладів може змінювати кольори в реальному часі, що дає можливість більш прискіпливо налаштовувати палітру кольорів за допомогою RGB повзунків. Приклад наведено на рис. 1.

Калькулятор видимості для дальтонізму

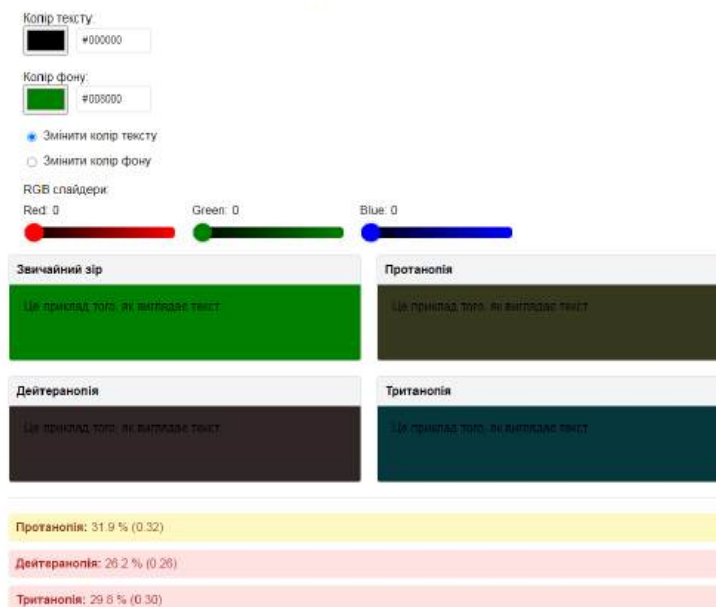
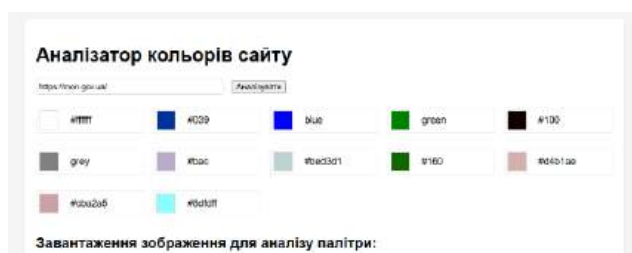


Рис. 1 – Приклад калькулятора

Далі потрібно саме аналізувати сайти. Це можливо зробити двома шляхами.

По-перше, можна вставити адресу сайту, після чого система виконає аналіз доступних кольорів, присутніх на сторінці, та відобразить їх. Завдяки цій функції забезпечується повний огляд кольорової гами аналізованого ресурсу (рис. 2, а).

По-друге, у разі недоступності автоматичного аналізу за адресою сайту, користувач може завантажити зображення – скріншот вебсторінки, для подальшого визначення кольорової палітри. Для цього необхідно попередньо зробити знімок екрана та завантажити його до системи. У результаті буде здійснено аналіз кольорів, присутніх на зображенні, та надано відповідні результати (рис. 2, б).



а



б

Рис.2 – Приклад аналізу сайтів

Список літератури

1. Дальтонізм: відповіді та питання [сайт]. URL: <https://doc.ua/ua/news/articles/daltonizm-voprosy-i-otvety>.
2. Мельников О. Ю., Канішев В. О. Система підтримки прийняття рішень для виявлення аномалій визначення кольорів // Automation of Technological and Business Processes. – Одеса: ОНТУ, 2024. – № 16 (3). – С. 58–68. – ISSN 2312-3125. – DOI: <https://doi.org/10.15673/atbp.v16i3.2921>

3. Горло А. М., Мінтій І. С. Адаптація дизайну сайту для людей із порушенням кольоросприйняття. Новітні комп'ютерні технології. Кривий Ріг: Видавничий центр ДВНЗ «Криворізький національний університет», 2018, Т. XVI. С. 182–187.

4. Канішев В. О., Мельников О. Ю. Постановка задачі створення застосунку для аналізу рівня задоволення сайтами людей із порушенням кольоросприйняття // Сучасні інформаційні системи та технології: матеріали VII Всеукр. наук.-практ. інтернет-конф. за тематикою «Сучасні комп'ютерні системи та мережі в управлінні» (29 листопада 2024 р., м. Херсон, м. Хмельницький) / за ред. А. А. Григорової. – Херсон: Книжкове видавництво ФОП Вишемирський В. С., 2024. – С. 180–181.

5. Канішев В. О., Мельников О. Ю. Вебзастосунок для розрахунку ступеня бачення дизайну сайтів для людей з порушенням кольоросприйняття // Розвиток науки – простір для відновлення регіону: збірник тез наукової конференції молодих вчених 19 грудня 2024 р., – м. Краматорськ: Донецька обласна державна адміністрація, Рада молодих вчених при Донецькій облдержадміністрації, 2024. – С. 76–79.

РОЗВИТОК ШТУЧНОГО ІНТЕЛЕКТУ В СИНТЕЗІ ІНФОРМАЦІЙНИХ СИСТЕМ

DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN THE SYNTHESIS OF INFORMATION SYSTEMS

Касілов Д.В.

*II курс, група KI-23-1phd, спеціальність 123 «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»,*

ORCID: <https://orcid.org/0009-0001-9314-5019>, dimakasilov@gmail.com

*Науковий керівник: Писарчук О.О., доктор технічних наук, професор,
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського», Київ, Україна.*

ORCID: <https://orcid.org/0000-0001-5271-0248>, platinumpa2212@gmail.com

Анотація. У статті проаналізовано етапи еволюції використання технологій штучного інтелекту у процесі синтезу інформаційних систем. Розглянуто розвиток відповідних підходів — від експертних систем та агентно-орієнтованих моделей до нейроморфних архітектур, пояснюваного штучного інтелекту (*explainable AI*) та нейросимволічного синтезу. Особливу увагу приділено впливу концепції «*affordances*» та інформаційно-польової теорії на архітектуру взаємодії користувача з системою. Окреслено актуальні виклики, пов'язані з інтерпретованістю рішень ШІ, забезпеченням кібербезпеки, стійкістю розподілених екосистем та необхідністю міждисциплінарної інтеграції. Виокремлено перспективні напрями досліджень, що включають застосування онтологічного моделювання, когнітивної автоматизації та концепції співеволюції користувача й системи.

Abstract. *The article examines the evolution of artificial intelligence technologies in the context of synthesizing information systems. It reviews the progression of approaches — from expert systems and agent-based models to neuromorphic architectures, explainable artificial intelligence (XAI), and neurosymbolic integration. Particular emphasis is placed on the influence of the affordances concept and information field theory on the architecture of human–system interaction. The study outlines current challenges, including interpretability of AI-driven decisions, cybersecurity, resilience of distributed ecosystems, and the demand for interdisciplinary integration. Promising directions for further research are identified, such as ontology-based modeling, cognitive automation, and the co-evolution of users and systems.*

Синтез інформаційних систем (ІС) охоплює процес проектування, інтеграції та оптимізації компонентів для ефективного управління, обробки, зберігання та поширення інформації. Штучний інтелект (ШІ) із кожним десятиріччям дедалі глибше інтегрується у різні рівні синтезу ІС, стаючи рушієм інновацій: від логіко-правильних експертних систем, через агентні і знання-орієнтовані моделі, до сучасної когнітивної автоматизації та *explainable AI*.

1. Початковий етап: Автоматизація й експертні системи.

У 1970–1980-х роках основну роль у синтезі ІС відігравали експертні й логічні системи, які забезпечували автоматизацію рутинних рішень на основі продукційних правил. Хоч ці підходи обмежувалися фіксованими алгоритмами, вони започаткували концепцію автоматизованого прийняття рішень у проектуванні ІС. Ці досягнення стали підґрунтям для подальшої еволюції систем управління даними та бізнес-процесів [1].

2. Розширення функціональності: Інтелектуальні агенти, об'єктно-орієнтовані підходи.

З 1990-х років відбулося поширення агентно-орієнтованих концепцій та автоматизованих методів моделювання [2]. Інтелектуальні агенти почали виконувати роль автономних модулів, здатних брати участь у синтезі архітектури ІС, координуючи міжгалузеву інтеграцію (наприклад, у виробничих інформаційних системах — CRM, SCM, планування виробництва тощо)[2]. Водночас CASE-засоби та знання-орієнтоване моделювання сприяли логічному узгодженню вимог замовника із системними характеристиками.

3. Ера машинного навчання та розумних інформаційних екосистем

Починаючи з 2000-х, синтез ІС дедалі більше орієнтується на застосування машинного навчання та глибинних нейромереж. У корпоративних ІС (наприклад, у виробництві) ML- і AI-сервіси інтегруються в модулі управління логістикою, плануванням виробництва, обліком ризиків, підтримкою інноваційних рішень через аналіз великих даних [2].

Новою віхою стали "нейроморфні" ІС із архітектурними рішеннями, натхненними особливостями мозку (наприклад, паралельністю, асинхронністю обчислень, імпульсною природою передачі інформації). Нейроморфний підхід дозволяє зменшити енергоспоживання та підвищити адаптивність у реальному часі, що перспективно для edge-комп'ютингу і автономних ІС [3].

4. Концепція affordances: Еволюція впливу ІІ на інформаційну екосистему

Сучасний підхід вивчає не лише технічний синтез, а й концепцію affordances — можливостей, які відкриваються користувачам через інтеграцію ІІ в повсякденних ІС (наприклад, пошукові системи, стрімінгові сервіси) [4]. Це змінює практики інформаційної поведінки, впливаючи як на достовірність, так і на різноманітність інформації.

5. Новітні напрямки: Neurosymbolic AI, Explainable AI та онтології.

Останнє десятиріччя позначено переходом до нейросимволічних та ХАІ-підходів, коли поєднуються переваги нейромереж із інтерпретованістю символічних знань [5][6]. У синтезі ІС це дає змогу рухатись від "чорного ящика" до прозорого AI-design: експертні знання інтегруються прямо в архітектуру системи через онтології [7], а вбудовані моделі explainable AI дають змогу аудитувати, перевіряти та оптимізувати процес автоматизованої генерації компонентів. Особлива увага приділяється безпеці — знання-орієнтовані фреймворки допомагають стандартизувати опис загроз та механізми самозахисту ІС [7].

6. Системний і когнітивний погляд: Інформаційно-польова теорія та co-evolution.

Інформаційно-польова теорія розглядає синтез ІС як задачу реконструкції складних інформаційних полів, у якій ШІ відіграє роль "когнітивного фільтра" чи генератора гіпотез, натомість інтеграція людських і машинних суб'єктів приводить до co-evolution—спільного розвитку інформаційних екосистем [4][8].

7. Виклики та перспективи.

- Пояснюваність і прозорість: Значна частина сучасних AI-систем залишається недостатньо інтерпретованою для людини, що ускладнює аудит складних ІС [5][6].

- Безпека та етика: Актуальні напрями досліджень акцентують на стандартизації опису загроз (онтології) та оцінці ризиків [7][9].

- Стійкість інформаційних екосистем: Використання affordances і освіта користувачів здатні пом'якшити ризики маніпуляцій та інформаційного зниження різноманіття [4].

- Конвергенція дисциплін: Злиття AI з Internet of Things, агентними системами і хмарними рішеннями визначає майбутнє ІС у промисловості та інших секторах [2].

8. Таблиця. Еволюція і ключові висновки щодо ШІ у синтезі інформаційних систем.

Період	Ключові технології	Особливості застосування	Приклади/Висновки	Джерела
1970–1990	Експертні системи, правило-орієнтовані моделі	Обмежена автоматизація, жорсткі алгоритми	Автоматизація рутинних рішень	[1]
1990–2005	Інтелектуальні агенти, CASE-засоби	Автономний аналіз вимог, синтез модулів, інтеграція	Agent-based синтез, knowledge-driven design	[2]
2005–2015	Машинне навчання, ансамблі ML	Сегментація архітектур, прогнозування, оптимізація	ML-планування в логістиці, складних ІС	[2]
2015-сьогодні	Глибинне навчання, нейроморфні ІС, ХAI,	Full-stack automation, explainability,	Explainable AI, онтологічні фреймворки, neurosymbolic AI	[3][5][7][2][6]

Період	Ключові технології	Особливості застосування	Приклади/Висновки	Джерела
	онтології, LLMs	cybersecurity, когнітивність		
Поточні тренди	Affordances, Ontology-driven architectures, neurosymbolic AI, інформаційно-польова теорія	Вплив ШІ на інформаційну екосистему, співеволуція користувача й системи	Стандарт. опис загроз, підвищена стійкість ІС	[4][7][5][8]

Список використаних джерел:

1. Benbya, H., Pachidi, S., & Jarvenpaa, S. (2021). Special Issue Editorial: Artificial Intelligence in Organizations: Implications for Information Systems Research. *J. Assoc. Inf. Syst.*, 22, 10 с.
2. Zdravković, M., Panetto, H., & Weichhart, G. (2021). AI-enabled Enterprise Information Systems for Manufacturing. *Enterprise Information Systems*, 16, 668-720.
3. Anand Ramachandran. Neuromorphic Computing The Next Frontier in Brain-Inspired AI, Scalable Architectures, and Intelligent Systems. ResearchGate, 2025, 91с.
4. Hirvonen, N., Jylhä, V., Lao, Y., & Larsson, S. (2023). Artificial intelligence in the information ecosystem: Affordances for everyday information seeking. *J. Assoc. Inf. Sci. Technol.*, 75, 1152-1165 с.
5. Piplai, A., Kotal, A., Mohseni, S., Gaur, M., Mittal, S., Joshi, A., & Sheth, A. (2023). Knowledge-Enhanced Neurosymbolic Artificial Intelligence for Cybersecurity and Privacy. *IEEE Internet Computing*, 27, 43-48 с.
6. Rjoub, G., Bentahar, J., Wahab, O. A., Mizouni, R., Song, A., Cohen, R., Otrok, H., & Mourad, A. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. *IEEE Transactions on Network and Service Management*, 20, 5115-5140.
7. Preuveneers, D., & Joosen, W. (2024). An Ontology-Based Cybersecurity Framework for AI-Enabled Systems and Applications. *Future Internet*, 16, 69 с.
8. Ensslin, T. (2021). Information Field Theory and Artificial Intelligence. *Entropy*, 24 с.
9. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, 10 с.

ІНТЕГРАЦІЯ ПЛАТФОРМ THREAT INTELLIGENCE У SIEM-СИСТЕМИ ДЛЯ ПОКРАЩЕННЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ INTEGRATING THREAT INTELLIGENCE PLATFORMS INTO SIEM SYSTEMS TO IMPROVE CYBER THREAT DETECTION

Кошара Артем Васильович

II курс, група KI-23-2, спеціальність 123 «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «УКРАЇНА»,
ORCID: <https://orcid.org/0009-0000-8468-2704>, artemkosharaa@gmail.com

Науковий керівник: **Писарчук О.О.**, доктор технічних наук, професор,
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: <https://orcid.org/0000-0001-5271-0248>, platinumpa2212@gmail.com

Анотація. Розглядається питання підвищення ефективності виявлення кіберзагроз шляхом інтеграції систем аналізу безпекових подій (SIEM) із зовнішніми платформами threat intelligence, зокрема VirusTotal, IBM X-Force Exchange тощо. Проаналізовано механізми інтеграції через API та їхню роль у збагаченні подій безпеки контекстними індикаторами. Наведено приклади практичного застосування для автоматичної перевірки IP-адрес, доменів та хешів файлів, що дозволяє суттєво скоротити кількість хибнопозитивних спрацювань та пришвидшити реагування на інциденти. Визначено основні переваги та виклики впровадження таких рішень у державному секторі та корпоративному середовищі. Перспективи дослідження пов'язані зі створенням адаптивних скорингових моделей та використанням локальних баз загроз.

Abstract. The article addresses the enhancement of cyber threat detection efficiency through the integration of Security Information and Event Management (SIEM) systems with external threat intelligence platforms, such as VirusTotal and IBM X-Force Exchange. Integration mechanisms via APIs are analyzed, along with their role in enriching security events with contextual indicators. Practical examples are provided, including automated checks of IP addresses, domains, and file hashes, which significantly reduce false positives and accelerate incident response. The study outlines the key advantages and challenges of implementing such solutions in the public and enterprise sectors. Future research directions include the development of adaptive scoring models and the use of locally cached threat data.

Враховуючи постійне безупинне зростання кількості цілеспрямованих та складних кібератак, традиційних можливостей SIEM-систем часто виявляється недостатньо для своєчасного виявлення та реагування на загрози. Це, особливо, стосується нових або маловідомих загроз, що не мають чітких визначених, відомих сигнатур. У цьому контексті інтеграція з зовнішніми сервісами threat intelligence, такими як VirusTotal, IBM X-Force Exchange та ін., дозволяє суттєво підвищити ефективність виявлення та аналізу інцидентів. Вона забезпечує доступ до актуальних баз індикаторів компрометації (IOC): шкідливих або підозрілих IP-

адрес, доменів, хешів файлів та поведінкових шаблонів, що розширює аналітичні можливості SIEM-систем.

Інтеграція SIEM з threat intelligence сервісами реалізується найчастіше через API, конекторні модулі або плагіни, що дозволяють збагачувати події безпеки додатковими контекстними даними автоматично у фоновому режимі. Наприклад, під час надходження події (івенту) з підозрою IP-адресою джерела, SIEM автоматично звертається до VirusTotal або IBM X-Force для перевірки наявності цієї адреси у відомих репутаційних списках. У випадку збігу, подія позначається, як високоризикова, що дає змогу пріоритизувати її обробку. Такий підхід дозволяє скоротити час на ручний аналіз, підвищити точність класифікації інцидентів та зменшити кількість хибнопозитивних спрацювань (false positive).

У практиці кібербезпеки інтеграція threat intelligence у SIEM дає змогу не лише виявляти загрози, а й оперативно верифікувати їх без участі аналітика. Наприклад, при виявленні нових виконуваних файлів на кінцевих точках (комп'ютери, сервери, тощо), SIEM може автоматично надсилати їх хеші до VirusTotal для перевірки. Якщо файл класифіковано, як шкідливий кількома антивірусними рушіями, подія миттєво отримує підвищений рівень критичності. У випадку підозрілих доменів або URL-адрес SIEM може звернутися до IBM X-Force, щоб оцінити історію репутації домену. Такі сценарії дозволяють підвищити ефективність обробки подій, зменшити навантаження на аналітиків та покращити швидкість реагування на інциденти.

Попри очевидні переваги, інтеграція з threat intelligence сервісами має низку викликів. Насамперед – потреба у постійній актуалізації індикаторів, адже застарілі дані можуть спричинити як пропущення реальної загрози, так і зростання хибнопозитивних спрацювань. Також можливі обмеження на кількість запитів до зовнішніх API, що ускладнює масштабованість рішення. Додаткову складність становить потреба в узгодженні форматів даних (наприклад, STIX/TAXII) та забезпеченні їхньої безпечної передачі. Окремим викликом є забезпечення довіри до джерел threat intelligence, оскільки різні платформи можуть надавати суперечливу інформацію про один і той самий об'єкт.

Інтеграція зовнішніх платформ threat intelligence з SIEM-системами значно підвищує якість виявлення кіберзагроз завдяки додатковому контексту та оперативній валідації індикаторів. Такий підхід дозволяє не лише автоматизувати процес прийняття рішень, а й зменшити навантаження на аналітичні групи. Водночас існують технічні та методологічні обмеження, які потребують подальшого опрацювання. Перспективними напрямками досліджень є створення адаптивних моделей зважування індикаторів на основі їхньої достовірності та релевантності, впровадження локальних кешованих баз для зменшення кількості зовнішніх запитів, а також розробка гібридних рішень із використанням власного threat intelligence.

Список використаних джерел:

1. О.О. Писарчук, А.В. Кошара, Аналіз індикаторів загроз інформаційній безпеці в інформаційно-телекомунікаційних системах за результатами застосування siem-систем / Інфокомунікаційні та комп'ютерні технології, 2024. № 1(07). С. 79-

2. Писарчук О. О. Оцінювання ефективності інформаційних систем за вектором критеріїв // Збірник наукових праць ЖВІ НАУ. Випуск 3. – 2010. – С. 117–

Exchange. [Електронний ресурс]. – Режим доступу:

5. VirusTotal. [Електронний ресурс]. – Режим доступу:

6. STIX/TAXII Specifications. [Електронний ресурс]. – Режим доступу:

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Левченко Лариса Іванівна, к. мед. н., доц.

Інститут соціальних технологій

кафедра фізичної терапії, Ерготерапії та фізичного виховання
Відкритий міжнародний університет розвитку людини “Україна”

Анотація. Проаналізовано проблему використання систем штучного інтелекту (ШІ) як інструменту цифровізації освіти, зв'язок з розвитком критичного мислення у студентів – майбутніх фізичних терапевтів. Виокремлено загальні тенденції та описано напрями та перспективи використання систем штучного інтелекту для підтримки освіти. До сучасних технологій ШІ належать: експертні системи, чат-боти, інтелектуальні репетитори, персоналізовані системи навчання, візуалізації та віртуальні навчальні середовища, технології машинного навчання. Основним напрямом використання ШІ в освіті, розвиток яких сприяє підтримці освітньої галузі є: персоналізація навчання, використання інтелектуальних систем-помічників, аналітика навчання, автоматизація рутинних завдань, інноваційні методи навчання з використанням систем штучного інтелекту. Акцентовано увагу на викликах щодо використання систем штучного інтелекту, з якими стикаються сучасні заклади освіти: проблема етики, забезпечення конфіденційності та безпеки, недостатній рівень сформованості цифрової компетентності в аспекті штучного інтелекту.

Abstract. The problem of using artificial intelligence (AI) systems as a tool for digitalizing education is analyzed, as well as the connection with the development of critical thinking in students - future physical therapists. General trends are identified and the directions and prospects for using artificial intelligence systems to support education are described. Modern AI technologies include: expert systems, chatbots, intelligent tutors, personalized learning systems, visualizations and virtual learning environments, machine learning technologies. The main areas of use of AI in education, the development of which contributes to the support of the educational industry are: personalization of learning, the use of intelligent assistant systems, learning analytics, automation of routine tasks, innovative teaching methods using artificial intelligence systems. The focus is on the challenges of using artificial intelligence systems that modern educational institutions face: the problem of ethics, ensuring confidentiality and security, and the insufficient level of formation of digital competence in the aspect of artificial intelligence.

Сьогодні інформаційно-комунікаційні технології активно інтегруються в освітній процес на всіх рівнях навчання. Це питання стає особливо важливим у контексті диференційованого навчання, запровадження модульних систем оцінювання та функціонування системи вищої освіти в умовах кредитно-модульного підходу. Освіта зосереджується не тільки на набутті випускниками hard skills (знання, вміння, навички у певній предметній галузі), а й soft skills, якості, які повинен мати майбутній конкурентно спроможний фахівець: Collaboration, Communication, Creativity, Critical thinking – «Систему 4К» (Колаборація,

Комунікація, Креативність, Критичне мислення) (10 Top Soft Skills for 2020: What They Are and How To Train Them, 2016).

Розвиток критичного мислення є ключовим для майбутніх фізичних терапевтів, дозволяє ефективно аналізувати інформацію, виявляти та вирішувати проблеми, приймати обґрунтовані клінічні рішення. Критичне мислення допомагає студентам не лише у навчанні, а й майбутній професійній діяльності, підвищуючи якість їх роботи, правильно оцінювати стан пацієнта та виявляти проблеми.

Розвиток штучного інтелекту в освіті є ключовим елементом сучасних технологій. Його застосування відкриває значні можливості для покращення якості навчання та індивідуалізації освітнього процесу. Недостатньо комплексних стратегій його розвитку в багатьох країнах, нечіткі етичні та нормативні вимоги до створення та використання ШІ в університетах у сфері вищої освіти. Штучний інтелект здатний вирішити багато актуальних проблем сучасної системи освіти, проте його розробка та впровадження стикаються з низкою етичних і технічних викликів, пов'язаних із гарантуванням безпеки та збереженням конфіденційності.

Міністерство освіти і науки та Міністерство цифрової трансформації України спільно з експертами розробили рекомендації щодо відповідального використання штучного інтелекту в закладах вищої освіти. Документ містить поради для викладачів, студентів, адміністрацій ЗВО та дослідників, що допоможуть ефективно інтегрувати ШІ в освітній і науковий процес.

В загальному розумінні штучний інтелект – це здатність інтелектуальної системи виконувати творчі завдання, які зазвичай вважаються характерними для людського інтелекту. Сюди входить розроблення інтелектуальних машин, що працюють на основі комп'ютерних програм; ШІ дає змогу комп'ютерним технологіям навчатися на основі наявних матеріалів і виконувати аналітичні, а інколи й творчі завдання. Штучний інтелект може стати корисним інструментом як для викладачів, так і для студентів вищих навчальних закладів для оцінювання наукових робіт і моніторингу навчального процесу.

ШІ здатний допомогти в розробці індивідуальних навчальних планів, які враховують особливості, потреби й здібності кожного студента. Такі підходи сприяють ефективнішому засвоєнню матеріалу, дозволяючи студентам навчатися у зручному для них темпі [1].

Серед освітніх послуг, які можна реалізувати за допомогою штучного інтелекту у вищих навчальних закладах, виділяють: організацію та проведення лекцій, семінарів і практичних занять; надання викладацьких консультацій; створення навчальних програм і електронних курсів; розробку завдань і моделювання їх розв'язання; організацію різноманітних освітніх заходів; оцінювання студентських робіт тощо [2, 4].

Штучний інтелект дозволяє автоматизувати процеси, які раніше вимагали безпосередньої участі викладачів чи науково-педагогічних працівників, роблячи навчання більш індивідуалізованим і гнучким. Адаптивне навчання забезпечує підбір матеріалів відповідно до потреб студентів на різних рівнях освіти, моніторинг їхнього прогресу та корекцію навчальної траєкторії на основі досягнутих результатів.

Такий підхід враховує стиль навчання, швидкість засвоєння матеріалу, особисті інтереси й уподобання студентів, а також пропонує завдання відповідного рівня складності, що підвищує ефективність освітнього процесу.

Незважаючи на значні можливості та перспективи, впровадження технологій штучного інтелекту в освіту супроводжується низкою викликів і проблем [3]. Якщо студенти будуть лише пасивно споживати інформацію, надану системами ШІ, це може призвести до зниження якості навчання та ослаблення їх критичного мислення. Тому важливо знаходити баланс між використанням технологій ШІ та збереженням навичок і цінностей, які сприяють розвитку критичного мислення.

Крім того, впровадження ШІ впливає на поняття академічної доброчесності, викликаючи нові виклики для збереження високих стандартів у науковій сфері. Забезпечення якісної освіти в Україні, яка прагне інтеграції в європейський науковий простір, вимагає врахування цих інновацій у дотриманні стандартів доброчесності при створенні наукових робіт.

На мою думку, повинні бути такі основні принципи етичного кодексу в університеті: принцип прозорості, згідно з яким учасники освітньо-наукового процесу зобов'язані чітко вказувати на використання інструментів ШІ у своїх роботах, зазначаючи конкретні платформи, неймережі та обсяг їх застосування; принцип етичності та відповідальності, за яким учасники несуть повну відповідальність за зміст своїх робіт, включаючи частини, створені за допомогою ШІ, та повинні ретельно перевіряти й редагувати отримані результати. Етичне використання ШІ передбачає уникнення створення або поширення шкідливого, дискримінаційного чи неправдивого вмісту; принцип академічної доброчесності. Плагіат, фальсифікація даних та інші форми порушень академічної доброчесності суворо забороняються. Учасники освітньо-наукового процесу повинні застосовувати критичне мислення під час використання ШІ, оцінюючи доречність, точність та надійність отриманої інформації; принцип дотримання балансу між застосуванням ШІ та розвитком власних компетенцій здобувачів. Використання ШІ має доповнювати, а не замінити власні знання та навички; принцип законності та прозорості передбачає наявність необхідних прав для застосування інструментів генеративного штучного інтелекту та розуміння джерел інформації на основі штучного інтелекту; принцип конфіденційності, безпеки та захисту даних передбачає недопущення витоку персональних, корпоративних даних і конфіденційної інформації через використання інструментів генеративного штучного інтелекту, а також захист від шкідливого вмісту та небажаного контенту; принцип доступності та інклюзивності, що передбачає доступність для всіх учасників освітньо-наукового процесу незалежно від їхніх індивідуальних можливостей. Університет заохочує до творчого та інноваційного використання ШІ для покращення якості та результативності навчання. Водночас заклад залишає за собою право встановлювати обмеження на використання ШІ в певних видах академічних робіт або навчальних дисциплінах.

Широке впровадження штучного інтелекту поступово трансформує освітній процес. Водночас ШІ може слугувати ефективним інструментом підтримки викладачів у навчанні або створення індивідуалізованого освітнього середовища.

У таких випадках використання ШІ сприяє позитивним результатам, не порушуючи фундаментальних принципів академічної доброчесності в закладах освіти. Впроваджуючи штучний інтелект у систему вищої освіти, важливо забезпечити, щоб цей процес сприяв розвитку людського потенціалу та не створював нерівності чи виключення. Українські заклади освіти активно працюють над формуванням етичних стандартів і принципів застосування ШІ в наукових дослідженнях, враховуючи як національні, так і міжнародні норми. Такий підхід забезпечує безпечне й ефективне використання ШІ, мінімізуючи потенційні ризики, пов'язані з етичними аспектами дослідницької діяльності.

Список використаної літератури

1. Бедро Р. С., Расюн В. Л., Величко В. А. Штучний інтелект та його вплив на етичні аспекти наукових досліджень в українських закладах освіти. Академічні візії. 2023. № 22. DOI: <http://dx.doi.org/10.5281/zenodo.8174388> (дата звернення: 05.01.2025).

2. Мар'єнко М., Коваленко В. Штучний інтелект та відкрита наука в освіті. Фізико-математична освіта. 2023. №. 38(1). С. 48–53. DOI: <https://doi.org/10.31110/2413-1571-2023-038-1-007> (дата звернення: 29.09.2023).

3. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. Науковий вісник Ужгородського національного університету. 2022. № 71. С. 49–54. DOI: <https://doi.org/10.24144/2307-3322.2022.71.7> (дата звернення: 05.01.2025).

4. Філіпенко Л. В., Думанський О. В., Козак О. В. Академічна доброчесність в науковому та освітньому середовищі закладів освіти України: погляд крізь призму наявності штучного інтелекту. Академічні візії. 2023. № 19. DOI: <http://dx.doi.org/10.5281/zenodo.7966703> (дата звернення: 05.01.2025)

АРХІТЕКТУРА СТІЙКИХ МІКРОСЕРВІСІВ: ЯК ПРОЕКТУВАТИ НА ВІДМОВУ

Михайленко О. О.

III курс, група КІ-22-1phd, спеціальність «Комп'ютерна інженерія»,
Інститут комп'ютерних технологій Університету «Україна».

Анотація. У цій статті розглянуто ключові принципи створення стійкої мікросервісної архітектури, яка здатна витримувати часткові збої системи без впливу на користувача. Акцент зроблено на практичних паттернах, таких як *Circuit Breaker*, *Timeout*, *Retry*, *Bulkhead* і *Fallback*, які допомагають забезпечити надійність у розподілених системах. Окрема увага приділена ролі хмарної інфраструктури, *autoscaling*, *self-healing* і засобам спостереження (*observability*). Через приклади демонструється, як заздалегідь спроектовані механізми стійкості дозволяють уникнути каскадних відмов. Доповідь буде корисною для архітекторів, *DevOps*-фахівців та розробників, які проектують системи з високими вимогами до доступності.

Abstract. This article explores the core principles of designing resilient microservice architectures that remain functional despite partial system failures. It focuses on practical patterns like *Circuit Breaker*, *Timeout*, *Retry*, *Bulkhead*, and *Fallback* that help ensure reliability in distributed systems. Special attention is given to the role of cloud infrastructure, *autoscaling*, *self-healing*, and *observability* tools. Real-world examples show how resilience mechanisms prevent cascading failures. The session is valuable for architects, *DevOps* engineers, and developers building highly available and fault-tolerant systems.

Вступ. У світі розподілених систем і хмарних рішень мікросервісна архітектура стала стандартом. Вона дозволяє масштабувати команди, швидше релізити нові функції та зменшувати зв'язаність компонентів. Але з переходом до мікросервісів зростає складність: кожна окрема точка системи може відмовити, а відмова одного сервісу — спричинити каскад проблем в інших. Саме тому проектування стійких до відмов архітектур — не розкіш, а необхідність. Ця стаття присвячена практичному підходу до проектування resilient-мікросервісів — сервісів, які "ламаються правильно" та вміють самі відновлюватися.

Принципи стійкості. Перший крок до побудови відмовостійких сервісів — це усвідомлення, що відмова — неминуча. Мета — зробити її локальною, контрольованою і безболісною.

Основні принципи:

- Fail fast & recover gracefully — швидко виявляємо проблему і дозволяємо системі продовжити роботу.
- Ізоляція — жоден сервіс не повинен тягнути за собою інші.
- Автоматичне відновлення — *self-healing* за рахунок *Kubernetes*, *health checks* тощо.
- Спостережуваність (*observability*) — без логів, метрик і трасування resilient неможливий.

Ключові патерни

- **Circuit Breaker:** Захищає систему від повторюваних помилок. Якщо зовнішній сервіс "лежить", ми не шлемо запити далі, а відкриваємо "ланцюг".
- **Timeout + Retry:** Кожен запит повинен мати чіткий timeout. Якщо щось не відповідає — не чекай вічність. Retry з exponential backoff дозволяє дати сервісу шанс відновитися.
- **Bulkhead:** Розділяємо ресурси. Якщо один модуль перевантажений — інші працюють без збоїв.
- **Fallback:** У випадку недоступності — надаємо альтернативну відповідь. Наприклад, рекомендації з кешу замість запиту до сервісу ML.
- **Queue-based communication:** Асинхронна взаємодія через черги (SQS, Kafka) дозволяє сервісам працювати незалежно навіть у випадку тимчасових збоїв.

Хмарна інфраструктура: вбудована стійкість

У хмарі стійкість можна досягти простіше завдяки готовим механізмам:

- **Kubernetes:** liveness та readiness probes для самовідновлення.
- **Autoscaling:** динамічна реакція на навантаження.
- **Multi-AZ / Multi-Region:** географічна відмовостійкість.
- **Load balancing + health checks:** автоматичне вилучення

проблемних інстансів.

Комбінуючи це з архітектурними патернами, ми отримуємо "живу" систему, яка адаптується до змін.

Observability: основа реакції на збої

Важливо не лише проектувати стійкість, а й бачити, як вона працює.

Нам потрібні:

- Метрики (Prometheus, CloudWatch)
- Логи (Loki, ELK)
- Трасування (Jaeger, OpenTelemetry)

Ці інструменти дозволяють зрозуміти, що саме відмовило, коли і чому — і вчасно зреагувати.

Реальний приклад. Сервіс обробки платежів у нас раніше мав пряме підключення до стороннього API. Коли API падав — ми втрачали замовлення.

Рішення:

- Додали чергу перед обробкою.
- Обгорнули запит у Circuit Breaker.
- Додали fallback на кешовані відповіді.
- Налаштували сповіщення через Grafana Alerting.

У результаті — навіть при падінні шлюзу ми продовжували приймати замовлення, а обробка виконувалась пізніше.

Resilience — це не разове рішення, а філософія проектування. Вона вимагає думати не лише про "щасливий шлях", а й про те, що відбувається, коли щось йде не так. Мікросервісна архітектура і хмара дають нам всі інструменти — залишилось правильно ними скористатись.

ОСОБЛИВОСТІ ZERO-CODE ПІДХОДУ ДЛЯ СТВОРЕННЯ ВЕБ-РЕСУРСІВ

Юрій Міронов

викладач, Інститут комп'ютерних технологій

Кафедра інформаційних технологій та програмування

Відкритий міжнародний університет розвитку людини «Україна»

ORCID: 0000-0002-2291-5864

yurymironov96@gmail.com

Анотація – дана робота розглядає zero-code підхід до створення веб-застосунків презентаційного характеру. Прикладами таких веб-застосунків є персональні сайти-візитівки чи онлайн-звіти для грантових проєктів. Основними вимогами до подібних ресурсів є можливість швидкої стилізації, здатність оновлювати вміст сайту та висока доступність з мінімальним ручним втручанням. Освітлені критерії вибору zero-code платформ. Також розглянуті особливості платформ, що є доступними на ринку.

Вступ. Цифровізація є невід'ємною частиною сучасності, будь то особисте життя чи професійна діяльність людини. Окрім іншого, для представників певних професій (здебільшого пов'язаних з інформаційними технологіями) це виражається в необхідності мати персональні сайти-візитівки. Також, певні види проєктної діяльності також спонукають учасників до створення персоналізованих веб-ресурсів для представлення унікальних результатів власної роботи.

З іншого боку, послуги сучасних веб-розробників є доволі дорогими – згідно з актуальною аналітикою майданчику для пошуку IT-спеціалістів Upwork, вартість розробки сайту може варіюватись від \$300 до \$5000 тільки за перший рік діяльності, з вартістю подальшої підтримки від \$50 до \$2000 на місяць [1].

Окрім цього, проєкт з розробки веб-ресурса нерозривно пов'язаний з ризиками людського фактору, та покладає на замовника необхідність формулювати технічне завдання та слідкувати за належним виконанням та кінцевим виглядом продукту. В протилежному випадку може виникнути необхідність виконувати додаткові роботи, що в свою чергу потягне за собою додаткові витрати.

Іншим викликом є підтримка вже створених веб-ресурсів, оскільки через технічні збої можливо втратити доступ до них, через що необхідна постійна залученість спеціалістів з технічної підтримки.

Альтернативою даним підходам є zero-code розробка, що дозволяє створювати веб-ресурси довільного рівню складності за допомогою графічних інтерфейсів.

Основна частина. Протягом останнього десятиліття визначного поширення набули zero-code платформи. До їхнього функціоналу входить можливість розробки застосунків через середовища графічного програмування, багата бібліотека готових шаблонів та вбудована можливість до хостингу готових застосунків. Популярними представниками подібних платформ є Airtable, Notion та Smartsuite [2-4], але можливість створювати веб-ресурси без програмування пропонує значно більша кількість сервісів.

Широкий вибір сервісів для zero-code розробки спонукає до обережного вибору технологій. Нижче запропонований перелік критеріїв, які на які необхідно зважати при виборі сервісу:

- **Гнучкість функціоналу** – можливість використовувати готовий функціонал засобами графічного програмування обумовлюється тим, що розробник платформи попередньо реалізував даний функціонал. Тому перед вибором платформи необхідно мати чіткі очікування;
- **Стилізація** – zero-code платформи пропонують певну стилізацію застосунків, але в більшості випадків стилізація обмежується вибором кольорової схеми. Можливість більш гнучкої стилізації зазвичай компенсується «статичністю» застосунка та неможливістю використання динамічних даних;
- **Простота міграції** – даний пункт є важливим для уникнення так званого «vendor lock», тобто неможливості змінити провайдера послуг. Для уникнення цього треба проаналізувати, чи є у провайдера функція експорту даних;
- **Здатність до обробки динамічних даних** – деякі провайдери послуг (наприклад, Google Sites [5]) мають обмежену можливість обробки та відображення динамічних даних. Це не є перешкодою для статичних сайтів-візитівок, але може дати незадовільний результат для застосунків, де більшу роль відіграють динамічні дані;
- **Цінова політика** – перед початком використання того чи іншого провайдера необхідне чітке усвідомлення його функціоналу та цінової політики відносно власних потреб. Деякі провайдери є безкоштовними (наприклад, Google Sites), тоді як інші мають випробувальний період. Також варто провести аналіз лінійного збільшення вартості послуг – деякі провайдери (наприклад, Airtable, Smartsuite) збільшують ціну за послуги в залежності від кількості завантажених файлів та внесених даних;
- **White-labeling** – дана функція дозволяє таку публікацію застосунку, з якою кінцевий споживач не бачитиме ознак того, що даний сервіс був зроблений за допомогою zero-code платформи. Це може позитивно вплинути на користувацький досвід, але є рідкісною функцією.

В даній доповіді були розглянуті особливості вибору провайдерів zero-code послуг для розробки веб-ресурсів. Вищезазначений перелік критеріїв дозволить зробити проінформований вибір та уникнути зайвих ризиків, запобігши труднощі на більш пізніх етапах розробки та впровадження цифрового рішення.

Список використаних джерел

ГЕНЕРАТИВНІ ШІ-АСИСТЕНТИ ДЛЯ АДАПТИВНИХ САД-ІНТЕРФЕЙСІВ

Павлик Віталій Юрійович

III курс, група KI-22-1phd, спеціальність 123 «Комп'ютерна інженерія»
Відкритий міжнародний університет розвитку людини «Україна», м. Київ
ORCID: <https://orcid.org/0000-0002-3473-6812>

vitalik2698@gmail.com

Науковий керівник: Самарай В.П., к.т.н, с.н.с., професор

Відкритий міжнародний університет розвитку людини «Україна», м. Київ
samaraj@ukr.net

Анотація. Тези доповіді присвячені дослідженню можливостей генеративних ШІ-асистентів, що інтегруються у сучасні САД-платформи (Fusion 360, NX, SOLIDWORKS), для автоматичного перетворення запитів природною мовою на параметричні команди й адаптивні елементи інтерфейсу. Показано, що поєднання підходу «vibe-coding» і принципів універсального дизайну здатне знизити когнітивне навантаження користувачів з інвалідністю, скоротити час виконання типових операцій на 27–41 % та підвищити доступність інженерного ПЗ.

Abstract. These thesis statements investigates the potential of generative AI assistants embedded in modern CAD platforms (Fusion 360, NX, SOLIDWORKS) to translate natural-language queries into parametric commands and adaptive UI elements. Combining the “vibe-coding” approach with universal-design principles reduces cognitive load for users with disabilities, shortens common task execution time by 27–41 %, and enhances the overall accessibility of engineering software.

Вступ

Ідея «vibe-coding» — використання великих мовних моделей (LLM) для генерації коду чи креслень за короткими описами отримала широкий резонанс у 2024-2025 рр. [1]. Зі зростанням ринку генеративного дизайну (USD 398,3 млн у 2024 р., прогноз USD 949,9 млн у 2032 р.) [2], виробники САД активно інтегрують ШІ-асистенти, надаючи нові можливості для інклюзивного інтерфейсу.

Огляд сучасних ШІ-асистентів у САД

У січневому оновленні 2025 р. Autodesk представила «Text-to-CAD» і AutoConstrain, що автоматично накладає обмеження на ескізи, зменшуючи ручну працю до ± 20 % [3]. Перші бета-тести показали 1,4-разове прискорення створення повністю параметризованого ескізу корпусу редуктора.

2) CursorAI та Codeium (плагіни - «копайлоти» для редакторів макросів/скриптів)

Підхід Cursor AI, який розуміє контекст усього проєкту та генерує багатофайлові зміни, став прототипом «внутрішнього Copilot» для САД-середовищ [4],[5]. Codeium демонструє аналогічну ідею, дозволяючи науковцям без досвіду програмування створювати симуляції Сонячної системи за 10-15 хв [6].

3) Приклади голосових і жестових інтерфейсів

Відеодемонстрація NX Voice Command Assistant уже містить ≈ 300 команд; одна фраза «Create symmetric slot 30 \times 8» замінює 5-7 кліків мишею [6]. VPAT 2024

для SOLIDWORKS підтверджує підтримку альтернативних методів введення й масштабування UI [7].

Головна новинка World 2025; вчиться на ваших діях і автоматично виправляє ескізи, скорочуючи рутинні операції на $\approx 35\%$ за даними бета-тесту. Публічний реліз — липень 2025, з інтеграцією в локальній SOLIDWORKS.

Методологія експерименту

Учасники: 12 користувачів віком 21–55 років: 5 з моторними порушеннями верхніх кінцівок, 4 з легкими когнітивними порушеннями, 3 контрольної групи.

Процедура:

- Базові завдання (побудова корпусу, додавання філе, експорт STEP) виконувались у Fusion 360.

- Порівнювались три режими: класичний GUI, «Text-to-CAD» (генеративний запит) та голосові команди.

- Метрики: час виконання, кількість помилкових дій, суб'єктивне навантаження (NASA-TLX).

Результати:

Метрика	GUI	Text-to-CAD	Голосові команди
Час, с ($M \pm SD$)	412 \pm 38	301 \pm 27	242 \pm 19
Помилкові дії	7,2	3,4	2,9
NASA-TLX	63/100	48/100	45/100

Text-to-CAD скоротив час на 27 %, а голосові команди — на 41 % порівняно з класичним GUI, що узгоджується зі звітом W3C про переваги мовного управління [8]. 54 % компаній уже впровадили генеративні ШІ-інструменти у R&D, хоча 74 % відчують труднощі зі масштабуванням цінності. Ахе DevTools AI у травні 2025 р. представив модуль автоматичної пріоритизації дефектів, що покриває 78 % критеріїв WCAG 3 для мобільних UI.

Генеративні ШІ-асистенти значно знижують когнітивні та моторні бар'єри в CAD. Вони сприйнятливі до помилок мовного вводу; тому потрібна адаптивна підтверджувальна взаємодія. Подальші дослідження зосередяться на комплексній інтеграції WCAG 3 outcome-метрик та AI-підсиленому тестуванні в єдиному CI-pipeline.

AI-INFLUENCED TRANSFORMATION OF HIGHER EDUCATION

Podlesny Serhii

Dean of the Faculty of Automation, Mechanical Engineering and Information Technology

<https://orcid.org/0000-0001-8271-4004>

Donbass State Engineering Academy, Ternopil, Ukraine.

Abstract. *Key changes in higher education brought about by the integration of artificial intelligence (AI), including personalization of learning, automation of administration, and new teaching methodologies, are examined. The benefits of AI, such as adaptive learning platforms, virtual assistants, and predictive analytics, as well as challenges related to ethics, technical limitations, and social consequences, are analyzed. AI should become a tool for enhancing the quality of education, not its full automation.*

Keywords: *artificial intelligence, higher education, personalization of learning, ethics, adaptive technologies.*

In the modern world, artificial intelligence (AI) is becoming a key factor in the transformation of various fields of activity, including higher education. The integration of AI into the educational process, administration, and research opens up new opportunities, but also poses serious challenges to the academic community. According to recent research, the introduction of adaptive learning systems, automated assessments, and intelligent assistants is significantly changing traditional education models, making them more flexible and personalized.

The relevance of this topic is confirmed by a number of scientific publications in high-ranking journals. Thus, a study [1] proves that AI can increase the effectiveness of learning through big data analysis and content individualization. analyzes the impact of generative AI (e.g. ChatGPT) on academic integrity. These publications indicate that the transformation of education under the influence of AI is not only a technological, but also a socio-cultural phenomenon that requires a comprehensive scientific understanding.

The current stage of development of higher education is characterized by qualitative changes caused by the integration of artificial intelligence into the educational process. One of the most important areas of this transformation is the personalization of learning, which radically changes traditional approaches to the organization of the educational process. An important aspect of this transformation has been the proliferation of AI-powered adaptive learning platforms such as Coursera, Duolingo, and Khan Academy. These systems use sophisticated machine learning algorithms to analyze students' learning behavior, which allows you to dynamically adapt educational content to the individual needs of each user. For example, recommendation systems similar to those used in Netflix or Spotify offer students courses and learning modules that are optimally tailored to their previous learning activity. Adaptive testing, implemented on ALEKS-type platforms, automatically adjusts the complexity of tasks according to the student's level of training. Predictive models allow you to identify students who are at risk of not completing the course and prevent this through timely individual support. Studies show that such approaches can increase the efficiency of the educational process by 20-30%, as they allow you to minimize the time spent on already learned material and focus on problem aspects.

Particular attention within the framework of personalized learning is paid to the formation of individual trajectories, taking into account the cognitive styles of students. Modern AI-based systems are able to identify individual characteristics of information perception - whether it is a visual, auditory or kinesthetic type of cognition - and adapt educational content according to these preferences. Infographics and videos are generated for visuals, lectures and podcasts are generated for audio, while kinesthetics get the opportunity to work with interactive simulations. Virtual labs like Labster offer immersive simulations of scientific experiments, AI tutors like ChatGPT act as personal mentors who can explain material in a variety of ways, and gamification elements implemented in Duolingo provide motivation through a system of individual goals and achievements. This transformation of education goes beyond simple technological improvement, representing a fundamental change in the educational paradigm – a shift from massive, unified learning to a model focused on the individual needs and capabilities of each student. However, along with the obvious benefits, this process requires attention to ethical aspects, such as the protection of personal data and the prevention of algorithmic bias, as well as maintaining a balance between technological innovation and the humanitarian component of education, where the role of the educator remains indispensable.

AI is establishing itself as a powerful transformational tool in higher education, leading to radical changes in all aspects of the educational process - from teaching methods to administrative procedures. However, this technological revolution requires a careful balance between the innovative potential of new tools and the preservation of fundamental academic values that have formed the basis of university education for centuries. The prospects for the further introduction of AI in higher education are directly related to the need to conduct large-scale interdisciplinary research aimed at a comprehensive assessment of the effectiveness of these technologies and their long-term impact on the quality of training of specialists. Particular attention should be paid to the formation of new models of academic integrity in the context of the mass use of generative AI, the impact of automation on the development of students' cognitive abilities, as well as the socio-psychological consequences of the partial replacement of human interaction with algorithmic systems. The scientific community is faced with the task of developing methodological approaches to assess the quality of AI tools in education, which will take into account not only their technical parameters, but also compliance with pedagogical principles and learning goals.

References:

1. Luckin, R. (2022). *AI for School Teachers*. *Nature Human Behaviour*, 6(4), 123-135.
2. Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2023). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *Computers & Education*, 179, 104-120.
3. Holmes, W., Persson, J., Chounta, I.-A., Wasson, B., & Dimitrova, V. (2023). Artificial Intelligence and Education: A Critical View through the Lens of Human Rights, Democracy and the Rule of Law. *International Journal of Educational Technology in Higher Education*, 20(1), 1-18.

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ГЕНЕРАЦІЇ ТЕСТОВИХ ЗАВДАНЬ З ВИЩОЇ МАТЕМАТИКИ

Одрібець Наталія Василівна

доцент кафедри інформаційних технологій та програмування
Інститут комп'ютерних технологій Університету "Україна", м Київ,
Україна
<https://orcid.org/0009-0008-0176-1211>
sosn@ukr.net

Анотація. У роботі представлено підхід до автоматизованого формування тестових завдань з вищої математики з використанням великих мовних моделей (LLM), шаблонів запитів та візуального інтерфейсу для викладача. Система враховує рівні таксономії Блума та забезпечує створення завдань різної складності з математичними формулами. Особливу увагу приділено відображенню формул у форматах LaTeX та їх перевірці на математичну еквівалентність. Інтерфейс реалізовано на базі Streamlit, а генерація запитань — з використанням бібліотеки LangChain. Підтримується експорт тестів у форматах, сумісних із Moodle. Запропонований підхід забезпечує адаптивність, повторне використання та ефективну інтеграцію в навчальний процес.

Ключові слова: інтелектуальна система, генерація тестів, вища математика, великі мовні моделі, таксономія Блума, LaTeX, LangChain, Streamlit, Moodle, математична еквівалентність.

Abstract. The paper presents an approach to automated generation of higher mathematics test tasks using large language models (LLMs), prompt templates, and a user-friendly interface for instructors. The system incorporates Bloom's Taxonomy levels and provides question generation of varying complexity, including mathematical formulas. Special attention is paid to formula rendering using LaTeX and validation of mathematical equivalence. The interface is built with Streamlit, while the question generation logic is powered by LangChain. Export to Moodle-compatible formats is supported. The proposed solution enables adaptability, reusability, and efficient integration into the educational process.

Keywords: intelligent system, test generation, higher mathematics, large language models, Bloom's taxonomy, LaTeX, LangChain, Streamlit, Moodle, mathematical equivalence

Із розвитком цифрових освітніх технологій зростає потреба в автоматизованих інструментах для формування контрольних завдань, зокрема у галузі математичних дисциплін. Вищу математику вирізняє наявність складної термінології та виразів, які потребують коректного синтаксичного оформлення та

об'єктивної перевірки. Традиційні засоби створення тестів є трудомісткими та обмеженими за варіативністю.

У межах дослідження розроблено інтелектуальну систему генерації тестових завдань з вищої математики, яка поєднує можливості великих мовних моделей (GPT-4), бібліотеки LangChain для управління шаблонами запитів і логіки, а також Streamlit як основу для візуального інтерфейсу.

Основу системи становить модуль генерації, що формує тестові завдання із зазначеними параметрами: предмет, тема, тип завдання, рівень складності відповідно до таксономії Блума. Для відображення математичних формул використано синтаксис LaTeX та підтримку MathJax. Для валідації відповідей у відкритих завданнях реалізовано механізм перевірки математичної еквівалентності виразів на базі бібліотеки SymPy.

Інтерфейс викладача дозволяє обрати необхідні параметри, згенерувати кілька варіантів запитань, переглянути результати та експортувати їх у формат GIFT/XML для подальшого імпорту до Moodle. Передбачено підтримку адаптивного дизайну, кешування та збереження шаблонів генерації.

Система створена з урахуванням перспектив масштабування, інтеграції з іншими освітніми платформами та можливості персоналізованого тестування. Результати апробації свідчать про значне скорочення часу на підготовку контрольних заходів та підвищення якості навчального матеріалу.

Список використаних джерел:

1. Блум Б. С. Таксономія освітніх цілей. Книга 1: Пізнавальна сфера / Пер. з англ. — Київ: Педагогіка, 2007. — 336 с.
2. GPT-4 Technical Report // *arXiv preprint*. — 2023. — Режим доступу: <https://arxiv.org/abs/2303.08774>
3. LangChain Documentation. — 2024. — Режим доступу: <https://docs.langchain.com/>
4. Streamlit. A faster way to build and share data apps. — Режим доступу: <https://streamlit.io/>
5. Meurer A., Smith C. P., Paprocki M. та ін. SymPy: symbolic computing in Python // *PeerJ Computer Science*. — 2017. — Vol. 3. — e103. — DOI: 10.7717/peerj-cs.103
6. Moodle XML format. — Режим доступу: https://docs.moodle.org/dev/Moodle_XML_format
7. Божко Н. С. Інформаційні технології в освіті: автоматизація контролю знань // *Інформаційні технології і засоби навчання*. — 2021. — №1(81). — С. 15–27. — DOI: 10.33407/itlt.v8i1.4023

МЕТОДОЛОГІЯ ПОБУДОВИ НАВЧАЛЬНОГО РОЗКЛАДУ З ВИКОРИСТАННЯМ ЦІЛОЧИСЕЛЬНОГО ПРОГРАМУВАННЯ

Одрібець Сергій Петрович

*доцент кафедри інформаційних технологій та програмування
Інститут комп'ютерних технологій Університету "Україна", м Київ,
Україна*

<https://orcid.org/0009-0002-2522-5794>

onspo@ukr.net

Анотація. У роботі розглядається методологія автоматизованого формування навчального розкладу на основі змішаного цілочисельного програмування (MIP). Запропонована модель враховує широкий спектр обмежень, які відповідають реальним умовам функціонування навчального закладу: часові вікна, доступність аудиторій, викладачів, груп студентів, а також пріоритети щодо рівномірного навантаження. Експериментальна перевірка показала високу якість отриманих розкладів. Результати дослідження свідчать про ефективність використання сучасних бібліотек математичного програмування у сфері освітнього планування.

Ключові слова: розклад занять, змішане цілочисельне програмування, математична модель, освітнє планування, оптимізація.

Keywords: *timetable, mixed integer programming, mathematical model, educational planning, optimization.*

У роботі запропоновано підхід до автоматизованого формування навчального розкладу, який базується на методах цілочисельного програмування (Mixed Integer Programming, MIP). Задача побудови розкладу формалізується як задача математичної оптимізації, що передбачає облік широкого спектра обмежень. Серед них — вимоги до призначення занять у доступні аудиторії, врахування графіків викладачів, заплановане навантаження студентських груп та доступні часові слоти. Такий підхід забезпечує системність та гнучкість при врахуванні численних реальних факторів.

Побудована модель включає як жорсткі обмеження, які мають бути дотримані обов'язково, так і м'які обмеження, які бажано виконати для поліпшення якості розкладу. Жорсткі обмеження охоплюють унеможливлення конфліктів, перевищення доступного часу чи ресурсів, недопустимі перекриття занять тощо. М'які обмеження включають побажання викладачів щодо днів викладання, рівномірність розподілу навантаження протягом тижня та інші фактори, що підвищують зручність користування розкладом. Для реалізації цієї моделі було застосовано бібліотеки Puomo та OR-Tools, які надали інструменти для побудови математичної моделі у вигляді системи обмежень і об'єктивної функції. Розв'язання задачі здійснюється за допомогою сучасних солверів, таких як Gurobi та CVC, які ефективно опрацьовують моделі з великою кількістю змінних і обмежень.

Особливу увагу в дослідженні приділено формуванню об'єктивної функції, яка визначає пріоритети при складанні розкладу. До неї включено мінімізацію кількості конфліктів, перевантажень, занять у небажані дні або час, а також забезпечення балансованого навантаження. Така постановка задачі дає змогу автоматизовано створювати якісний розклад, що відповідає практичним потребам освітнього процесу.

В межах експериментального дослідження було здійснено апробацію запропонованої системи на прикладі навчального тижня одного з інститутів. Експеримент показав, що модель здатна генерувати розклади, які відповідають усім заданим вимогам та можуть бути безпосередньо використані в навчальному процесі без значної ручної корекції. Гнучкість підходу дозволяє адаптувати модель до різних навчальних закладів, змінюючи параметри обмежень та ваги в об'єктивній функції.

Таким чином, результати роботи підтверджують ефективність використання методів змішаного цілочисельного програмування у сфері освітнього планування. Отримані результати відкривають нові перспективи для подальших досліджень, зокрема у напрямку створення гібридних моделей, які поєднують точні методи оптимізації з евристичними алгоритмами для підвищення швидкодії та адаптивності.

Список використаної літератури:

1. Lu, Y., Liu, F., & Liu, C. (2023). Optimizing University Course Timetabling using Mixed Integer Programming and Constraint Relaxation. *Journal of Scheduling*, 26(2), 145–162.
2. Xu, J., & Zhang, Y. (2022). A Hybrid Optimization Model for Timetable Generation in Higher Education Institutions. *Computers & Industrial Engineering*, 173, 108729.
3. Li, Z., Wang, P., & Zhao, Y. (2022). Enhancing Educational Scheduling through MIP and Graph-based Approaches. *Applied Soft Computing*, 122, 108324.
4. Silva, M. R., & Gomes, R. (2021). Timetable optimization using modern solver architectures: a Pyomo and Gurobi approach. *Procedia Computer Science*, 198, 488–494.
5. Google OR-Tools Documentation. Retrieved from <https://developers.google.com/optimization>
6. Gurobi Optimization Documentation. Retrieved from <https://www.gurobi.com/documentation/>
7. Pyomo Documentation. Retrieved from <https://pyomo.org/documentation>

ОПТИМІЗАЦІЯ ПАРТИЦІЮВАННЯ ТА ІНДЕКСАЦІЇ У ВИСОКОНАВАНТАЖЕНИХ БАЗАХ ДАНИХ У ХМАРНИХ СЕРВІСАХ OPTIMIZATION OF PARTITIONING AND INDEXING IN HIGH-LOAD DATABASES IN CLOUD SERVICES

Рожков С.М.

III курс, група КІ-22-1а, спеціальність «Комп'ютерна інженерія»

Інститут комп'ютерних технологій університету «Україна»

ORCID: <https://orcid.org/0009-0004-2972-7163>

serj.rozhkov@gmail.com

Науковий керівник: Павленко В. І., к.ф.-м.н, доцент

Інститут комп'ютерних технологій університету «Україна»

ORCID: <https://orcid.org/0000-0002-3958-0415>

pavlenko.v@i.ua

***Анотація.** У тезах досліджено підходи до оптимізації продуктивності високонавантажених таблиць у базах даних, розгорнутих у хмарному середовищі. Особливу увагу приділено партиціюванню та індексації як ключовим інструментам підвищення швидкодії при роботі з великими обсягами даних. Розглянуто порівняння реалізації даних механізмів у керованому сервісі Amazon RDS (PostgreSQL) та на самоінстальованому інстансі бази даних. Проведено аналіз продуктивності на основі тестових навантажень, визначено переваги та обмеження кожного з підходів у контексті затримок, витрат на обслуговування та масштабованості. Запропоновано використання скриптів для перенесення старих даних у окремі таблиці з подальшим очищенням від bloat для зменшення розміру основної таблиці та підвищення продуктивності.*

***Abstract.** The paper investigates approaches to optimizing the performance of high-load tables in databases deployed in a cloud environment. Particular attention is paid to partitioning and indexing as key tools for improving query performance with large data volumes. The implementation of these mechanisms in the managed Amazon RDS (PostgreSQL) service and a self-installed database instance is compared. Performance analysis based on test workloads is conducted, identifying the advantages and limitations of each approach in terms of latency, maintenance costs, and scalability. The use of scripts for transferring old data to separate tables with subsequent bloat cleanup is proposed to reduce the size of the main table and enhance performance.*

Вступ

У фінансовому секторі бази даних часто містять десятки мільйонів записів, таких як транзакції, логи чи історія змін. Навіть оптимізовані запити можуть бути неефективними через повне сканування таблиць або неправильну стратегію планування запитів. Оптимізація партиціювання та індексації є ключовими для забезпечення швидкодії та масштабованості високонавантажених систем у хмарних сервісах.

Партиціювання у PostgreSQL

У роботі розглянуто використання декларативного партиціювання в PostgreSQL 11+, яке дозволяє розділити великі таблиці за часовими або категоріальними критеріями. Наприклад, таблиця транзакцій може бути розділена за датами (наприклад, щомісячно). У Amazon RDS автоматичне створення індексів на партиціях потребує додаткових скриптів, що ускладнює адміністрування. Натомість самоінстальовані рішення надають повну гнучкість, але вимагають вищих витрат на обслуговування.

Для зменшення розміру основної таблиці пропонується створення скриптів, які переносять старі дані (наприклад, записи старше одного року) в архівні таблиці. Це дозволяє значно зменшити обсяг основної таблиці, що покращує продуктивність запитів. Однак перенесення даних може спричинити bloat (надлишкове використання дискового простору через фрагментацію) у PostgreSQL. Для боротьби з цією проблемою необхідно регулярно виконувати очищення за допомогою команди VACUUM FULL або pg_repack. Це особливо корисно для застосунків, які не підтримують роботу з партиціонованими таблицями, оскільки дозволяє зменшити розмір таблиці без зміни логіки програми.

Індексація

Індексація в високонавантажених системах передбачає використання спеціалізованих індексів, таких як часткові індекси (partial indexes), BRIN для часових рядів та GIN для JSONB даних. У Amazon RDS існують обмеження, пов'язані з тривалістю створення індексів (таймаути, обмеження на дисковий простір), що може ускладнити оптимізацію. Наприклад, для запиту типу *SELECT * FROM transactions WHERE date > now() - interval '7 days'* отримано такі результати: без індексу – 4.2 с, з частковим індексом та партицією – 0.37 с.

Проблеми bloat у Amazon RDS

У Amazon RDS проблема bloat може бути особливо критичною через обмеження на виконання операцій VACUUM FULL, які потребують значних ресурсів і можуть викликати таймаути. Автоматичне очищення bloat у RDS є обмеженим, що призводить до накопичення «мертвих» кортежів і погіршення продуктивності. Для вирішення цієї проблеми рекомендується використовувати сторонні інструменти, такі як pg_repack, або періодично створювати нові таблиці з перенесенням даних і видаленням старих.

Порівняння підходів

У порівняльній таблиці наведено ключові особливості двох підходів:

Характеристика	AWS RDS	Самоінстальована БД
Автоматизація партицій	часткова	повна свобода
BRIN/GiST підтримка	обмежена	повна
Витрати на обслуговування	нижчі	вищі
Гнучкість	обмежена параметрами сервісу	максимальна
Пікова продуктивність	стабільна	залежить від конфігурації

Оптимізація партиціювання та індексації є критично важливою для високонавантажених баз даних у хмарних сервісах. Використання декларативного партиціювання та спеціалізованих індексів у PostgreSQL дозволяє значно підвищити швидкодію. Перенесення старих даних у архівні таблиці з подальшим очищенням bloat є ефективним рішенням для зменшення розміру таблиць і підвищення продуктивності, особливо для застосунків, які не підтримують партиціювання. Однак у Amazon RDS необхідно враховувати обмеження, пов'язані з bloat і тривалістю створення індексів, що вимагає додаткових інструментів і скриптів для оптимізації.

Список використаних джерел:

1. Amazon Web Services. Amazon RDS for PostgreSQL.
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_PostgreSQL.html
4. Семенов І.В. Високонавантажені системи обробки даних. – Київ: НТУУ «КПІ», 2022

УДОСКОНАЛЕННЯ СИСТЕМ УПРАВЛІННЯ СКЛАДСЬКОЮ ЛОГІСТИКОЮ

Рубаняк Т. М.

*III курс, група KI-22-1phd, спеціальність «Комп'ютерна інженерія»,
Відкритий міжнародний університет розвитку людини «Україна», ,
taras.rubaniak@gmail.com*

Тимошенко О. М., к. ф.-м. наук, Відкритий міжнародний університет
розвитку людини «Україна», <https://orcid.org/0009-0003-4331-1706>,
ontimoshenko@gmail.com

***Анотація.** Розглянуто удосконалення автоматизованих систем управління складською логістикою, що базується на інтегрованому використанні IoT, аналітики великих даних і штучного інтелекту, впровадженні гібридних WMS-архітектур, автоматизації обладнання, підвищенні кібербезпеки, а також системному розвитку людських ресурсів. Розширення можливостей цифрових двійників і сценарне моделювання, посилення захищеності даних та energy management.*

IMPROVEMENT OF WAREHOUSE LOGISTICS MANAGEMENT SYSTEMS

Taras Rubaniak, group KI-22-1phd, specialty «Computer Engineering», Open International University for Human Development «Ukraine», taras.rubaniak@gmail.com
Oksana Tymoshenko, Ph.D. in Physics and Mathematics, Open International University for Human Development «Ukraine», <https://orcid.org/0009-0003-4331-1706>,
ontimoshenko@gmail.com

***Abstract.** The paper considers the improvement of automated warehouse logistics management systems based on the integrated use of IoT, big data analytics and artificial intelligence, the implementation of hybrid WMS architectures, equipment automation, increased cybersecurity, and the systemic development of human resources. Expanding the capabilities of digital twins and scenario modeling, strengthening data security and energy management*

Удосконалення автоматизованих систем управління складською логістикою (АСУ СЛ) є стратегічним чинником підвищення конкурентоспроможності та ефективності логістичних ланцюгів, особливо в умовах цифрової трансформації та Індустрії 4.0. Ключові напрями цього удосконалення охоплюють не лише технологічні інновації, а й організаційні, аналітичні та управлінські аспекти.

Інтеграція Індустрії 4.0 та IoT у складські системи:

Впровадження Інтернету речей (IoT) дозволяє створювати системи реального часу збору, обробки та аналізу даних про переміщення, статус та розміщення товарів і обладнання, мінімізуючи затримки, неточності та людський фактор [1-4]. Сенсори, RFID-мітки та Wi-Fi RTLS (системи точного позиціонування у режимі реального часу) забезпечують автоматичну ідентифікацію та відстеження матеріальних потоків [1,3,5].

Особливого значення набуває застосування IoT для оптимізації order picking та крос-докінгу, що істотно впливає на рівень обслуговування клієнтів і гнучкість складської логістики [1,3].

Використання штучного інтелекту та аналітики великих даних:

Застосування алгоритмів штучного інтелекту (ШІ), машинного навчання (ML) та гібридних аналітичних моделей у поєднанні із IoT дозволяє прогнозувати попит, оптимізувати розташування товарів, управляти запасами та автоматизувати прийняття рішень щодо внутрішніх логістичних операцій [1,6]. У сучасних WMS (Warehouse Management Systems) все частіше імплементуються алгоритми оптимізації, що дає змогу покращити показники швидкості, точності та надійності обробки логістичних запитів [7-9].

Архітектурна і функціональна модернізація WMS:

Провідний тренд – перехід від жорстко-централізованої до гібридної або децентралізованої архітектури, що поєднує централізований контроль із автономією підсистем, наприклад на рівні функціональних зон складу або окремих транспортних засобів [2][10]. Це підвищує стійкість і гнучкість системи, особливо у великих і багаторівневих логістичних центрах.

Впровадження автоматизованих транспортно-складських рішень:

Автоматизовані транспортні системи (наприклад, AGV та AMR), роботизовані комплекси для переміщення, штабелювання та пакування вагомо підвищують продуктивність і знижують ймовірність помилок [2,9].

Сучасне обладнання має бути інтегроване у WMS і IoT-архітектуру для забезпечення безперервності інформаційних та фізичних потоків [2,4].

Аналітика ефективності та digital twin:

Використання цифрових двійників (digital twins) складу дозволяє моделювати логістичні сценарії, аналізувати вузькі місця, прогнозувати наслідки змін і оптимізувати операції на основі даних [9]. Також сучасна WMS повинна бути здатна формувати, моніторити й автоматично аналізувати ключові показники ефективності (KPI), що стосуються часу виконання замовлень, точності обліку, обігу та використання ресурсів [8,9].

Фокус на підвищенні кібербезпеки та енергозбереження:

З посиленням цифровізації складських процесів, захист від кіберзагроз, забезпечення цілісності та конфіденційності даних стають пріоритетними завданнями [9]. До того ж, слід враховувати енергоефективність рішень, оскільки автоматизація може привести до збільшення енергоспоживання [9].

Виклики і бар'єри впровадження:

Головними бар'єрами залишаються значні капітальні інвестиції, підвищені вимоги до кваліфікації персоналу та складність інтеграції нових технологій у вже існуючі системи [3,9]. Успішне впровадження можливе лише за умов системного навчання персоналу, адаптації підходів до обслуговування обладнання та оновлення IT-інфраструктури [3,9].

Роль людино-орієнтованих інтерфейсів та адаптації персоналу:

Важливим чинником залишається розроблення інтуїтивних інтерфейсів для операторів, що дозволяє зменшити час навчання, мінімізувати помилки та забезпечити швидку адаптацію до нових цифрових рішень [2,8]. Підвищення

цифрової грамотності персоналу є критичним для забезпечення повної віддачі від інвестицій у автоматизацію [3,9].

Удосконалення автоматизованих систем управління складською логістикою базується на інтегрованому використанні IoT, аналітики великих даних і штучного інтелекту, впровадженні гібридних WMS-архітектур, автоматизації обладнання, підвищенні кібербезпеки, а також системному розвитку людських ресурсів. Розширення можливостей цифрових двійників і сценарне моделювання, посилення захищеності даних та energy management, а також гнучкість управління у відповідь на динаміку ринку — основні вектори подальшого розвитку складської автоматизації [1-10].

Список літератури.

- 1.Lee, C., Lv, Y., Ng, K., Ho, W., & Choy, K. (2018). Design and application of Internet of things-based warehouse management system for smart logistics. *International Journal of Production Research*, 56, 2753-2768.
- 2.Khan, M. G., Huda, N. U., & Zaman, U. (2022). Smart Warehouse Management System: Architecture, Real-Time Implementation and Prototype Design. *Machines*.
- 3.Jarašūnienė, A., Čižiūnienė, K., & Cereska, A. (2023). Research on Impact of IoT on Warehouse Management. *Sensors (Basel, Switzerland)*, 23.
- 4.Hasan, M. Z., Junjie, M., Habib, A. A., Mamun, A. A., Ghazal, T. M., & Saeed, R. (2022). IoT-Based Warehouse Management System. *2022 International Conference on Cyber Resilience (ICCR)*, 1-6.
- 5.Ma, X., & Liu, T. (2011). The application of Wi-Fi RTLS in automatic warehouse management system. *2011 IEEE International Conference on Automation and Logistics (ICAL)*, 64-69.
- 6.Wang, L., Hamad, A. A., & Sakthivel, V. (2021). IoT Assisted Machine Learning Model for Warehouse Management. *J. Interconnect. Networks*, 22, 2143005:1-2143005:18.
- 7.Autry, C. W., Griffis, S. E., Goldsby, T. J., & Bobbitt, L. M. (2005). Warehouse management systems : resource commitment, capabilities, and organizational performance. *Journal of Business Logistics*, 26, 165-183.
- 8.Min, H. (2006). The applications of warehouse management systems: an exploratory study. *International Journal of Logistics Research and Applications*, 9, 111-126.
- 9.Tikwayo, L. N., & Mathaba, T. (2023). Applications of Industry 4.0 Technologies in Warehouse Management: A Systematic Literature Review. *Logistics*.
- 10.Basile, F., Chiacchio, P., & Coppola, J. (2016). A cyber-physical view of automated warehouse systems. *2016 IEEE International Conference on Automation Science and Engineering (CASE)*, 407-412.

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНА СИСТЕМА ЕКОЛОГІЧНОГО МОНІТОРИНГУ ВОДНОГО СЕРЕДОВИЩА НА ОСНОВІ ТЕХНОЛОГІЙ ІІІ ТА ІР

Топалов А.М., к.т.н.,

Національний університет кораблебудування імені адмірала Макарова

Моніторинг якості водного середовища представляє собою комплексний процес, спрямований на проведення систематичних спостережень за станом та рівнем забруднень у воді певної акваторії. Його основною метою є виявлення змін у природному складі води та оцінка впливу антропогенних і природних факторів на водне середовище. Для цього організовується стаціонарна мережа пунктів спостережень, де здійснюється контроль як природного хімічного складу води, так і вмісту забруднювальних речовин, включно з біологічними та фізико-хімічними параметрами [1].

Сучасні тенденції розвитку моніторингу тісно пов'язані з упровадженням автоматизованих технологій, які базуються на використанні інноваційних мікропроцесорних систем, сенсорних комплексів та спеціалізованого програмного забезпечення, зокрема IoT-систем [2, 3]. Такі рішення дають змогу здійснювати безперервний збір даних, їх оперативну обробку та передачу на центральні сервери для подальшого аналізу. Завдяки IoT з'являється можливість організувати інтегровані мережі моніторингу, де кожен пристрій автоматично передає актуальні дані про стан водного середовища, що забезпечує високу точність і своєчасність отримання інформації.

Головні принципи і рівні Інтернету речей сформовані в загальній схемі поєднання фізичних і віртуальних речей, яка представлена на рис. 1. В свою чергу, з рис. 1 видно, що віртуальні речі можуть існувати без їх фізичного втілення, в той час як фізичні об'єкти/речі обов'язково відповідають як мінімум одному віртуальному об'єкту. При цьому провідну роль грають ті самі пристрої, які можуть вибирати різну інформацію та розширювати комунікаційні мережі різними способами: через шлюзи та через мережу; без шлюзів, але через мережу; між собою. Рекомендація Y.2060 описує різне поєднання перерахованих способів з'єднання. Це вказує на те, що M2M використовує для IoT безліч мережевих технологій – глобальних мереж, локальних мереж, бездротових систем, що самоорганізуються (ad-hoc) і пористих (mesh) мереж.

Принцип роботи системи моніторингу параметрів води на основі IoT є доволі послідовним. Він складається з низки малопотужних інтелектуальних датчиків, підключених до промислового комп'ютера для визначення параметрів якості води, і шлюза IoT для спрямування отриманих даних у хмару для віддаленого моніторингу і виконання класифікації даних.

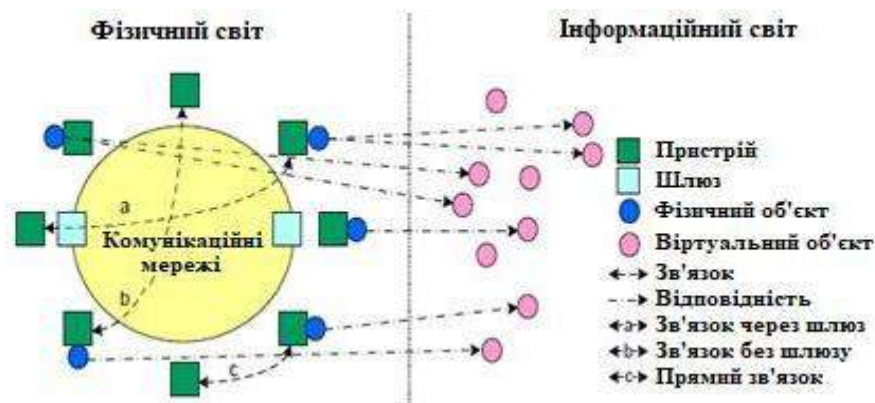


Рисунок 1. Схема відображення фізичних і віртуальних речей

Щоб зібрати інформацію з численних параметрів, датчики спочатку занурюють у воду. Датчики перетворюють фізичний параметр на електричний, який можна виміряти. Дані з датчиків зчитуються контролером шлюзу IoT, який потім використовує відповідну комунікаційну технологію для передачі даних та, якщо необхідно, їх обробки. Це дозволяє здійснювати віддалений моніторинг в реальному часі за допомогою смартфонів або ПК. Датчики є основними апаратними компонентами систем моніторингу якості води на основі Інтернету речей. Вони часто розгортаються в джерелах води, що контролюються (таких як озера, річки тощо), і використовуються для вимірювання параметрів таких як: температури, рН, каламутності, електропровідності тощо.

Шлюзи є ключовими зв'язками між мережею датчиків і хмарними серверами, особливо коли ці датчики не можуть використовувати IP-адресу. Дані з системи моніторингу якості води неможливо завантажити в хмару без шлюзу IoT, який виступає як міст до Інтернету. Глобальні мережі малої потужності (LPWAN) або інші протоколи бездротового зв'язку, такі як WiFi, Bluetooth або Zigbee, можна використовувати для підключення датчиків у системах моніторингу якості води.

Центральний сервер або хмарна служба може зберігати та обробляти дані датчиків за допомогою програмного забезпечення. Якщо виникне занепокоєння щодо якості води, відповідним органам буде подано сигнал тривоги для вжиття заходів.

Основними завданнями моніторингу поверхневих вод є спостереження, оцінювання та прогнозування змін якості води у відкритих водних об'єктах. Система моніторингу поверхневих вод є інформаційною і не містить в собі елементів управління. При цьому, вона є необхідною складовою частиною державної системи управління навколишнім середовищем і регулювання його якості води зокрема. Ці завдання формують системи моніторингу, блок-схема якої наведена на рисунку 2. На схемі зображені прямі та зворотні зв'язки між основними системоутворювальними блоками.

Блоки «Спостереження» і «Прогноз стану» тісно пов'язані між собою, оскільки прогноз стану докільля можливий лише за наявності досить репрезентативної інформації фактичний стан (прямий зв'язок). Побудова прогнозу, з одного боку, має на увазі знання закономірностей змін стану природного середовища, наявність можливостей чисельного розрахунку, з іншого -

спрямованість прогнозу значною мірою має визначати структуру та склад спостережної мережі (зворотний зв'язок). Результати оцінки існуючого та прогнозованого стану водного середовища у свою чергу дають можливість уточнити вимоги до системи спостережень. Процес прогнозування в свою чергу може бути здійснений засобами машинного навчання з логістичною регресією та методами випадкового лісу [4].

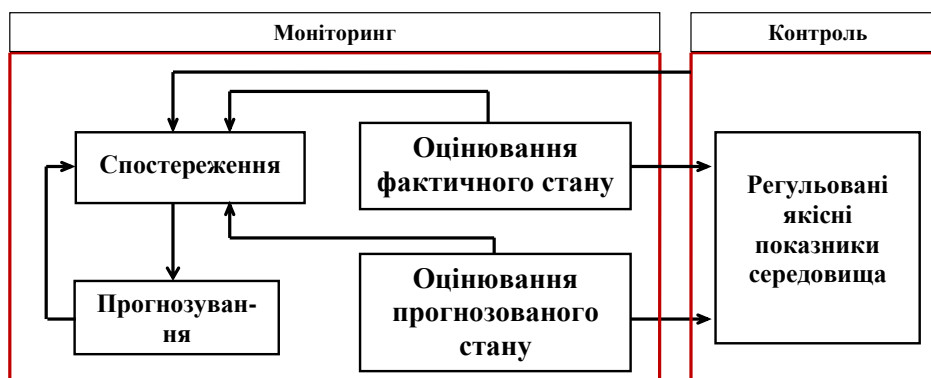


Рисунок 2. Структурна схема системи моніторингу

Розроблена Інформаційно-вимірювальна система моніторингу параметрів водного середовища забезпечує значне розширення діапазону вимірювань та збільшення кількості контрольованих показників якості води, що підвищує її універсальність та адаптивність до використання з різнотипними сенсорними модулями. Застосування IoT технологій зв'язку дає змогу здійснювати безперервний моніторинг у режимі реального часу, оперативно передаючи дані до центральних обчислювальних вузлів. Інтеграція технологій штучного інтелекту та машинного навчання відкриває нові можливості для глибокого аналізу зібраної інформації: автоматичне виявлення аномалій у параметрах водного середовища, прогнозування змін його стану на основі історичних даних. Завдяки цьому система не лише фіксує поточні показники, але й формує аналітичні моделі, що допомагають своєчасно виявляти загрози та приймати ефективні управлінські рішення для збереження та покращення якості водних ресурсів.

Література:

1. В. М. Боголюбов Моніторинг довкілля: підручник /[Боголюбов В. М., Клименко М. О., Мокін В. Б. та ін.]; під ред. В. М. Боголюбова. [2-е вид., перероб. і доп.]. – Вінниця: ВНТУ, 2010. – 232 с.
2. Mukta M., S. Islam, S.D. Barman, A.W. Reza (2019) IoT based Smart Water Quality Monitoring System, 2019 IEEE 4th International Conference on Computer and Communication Systems, doi:10.1109/CCOMS.2019.8821656.
4. Huyen C. (2022) Designing Machine Learning Systems: An Iterative Process for Production-Ready Applications, O'Reilly Media, 1st edition, 386 p.

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВИХ ТЕХНОЛОГІЙ

²Фесенко А.О.

Декан факультету комп'ютерних наук та технологій, к.т.н., доцент

^{1,2}Дуднік А.С.

Професор кафедри мережесих та інтернет технологій, д.т.н., доцент;

¹Київський національний університет імені тараса Шевченка,

²Київський авіаційний інститут

Анотація. У статті розглядається сучасний стан квантових технологій, основні досягнення у галузі квантових обчислень, зв'язку та сенсорики, а також окреслюються ключові проблеми, що стримують масштабне впровадження цих технологій. Окрема увага приділена перспективам подальшого розвитку галузі, зокрема створенню квантового інтернету, переходу до топологічних кубітів та формуванню глобальної квантової інфраструктури. У роботі також акцентується необхідність міждисциплінарної підготовки фахівців та міжнародної кооперації задля забезпечення сталого розвитку квантових систем.

Abstract. The article explores the current state of quantum technologies, key achievements in the fields of quantum computing, communication, and sensing, as well as the main challenges that hinder their large-scale implementation. Special attention is given to the prospects for further development of the sector, including the creation of a quantum internet, the transition to topological qubits, and the formation of a global quantum infrastructure. The study also emphasizes the need for interdisciplinary training of specialists and international cooperation to ensure the sustainable development of quantum systems.

Сучасний стан квантових технологій. Квантові технології є одним із найперспективніших напрямів розвитку науки й техніки в ХХІ столітті. Вони базуються на фундаментальних принципах квантової механіки: суперпозиції, квантовій заплутаності та квантовому тунелюванні. Завдяки цим ефектам квантові системи мають здатність обробляти інформацію в абсолютно новий спосіб, недосяжний для класичних пристроїв. На даний момент ця галузь включає кілька ключових напрямів: квантові обчислення, квантовий зв'язок, квантову криптографію та квантову сенсоріку. У сфері квантових обчислень досягнуто значного прогресу. Такі компанії, як IBM, Google, Rigetti, D-Wave та інші, демонструють функціональні квантові процесори, що містять десятки, а подекуди й сотні кубітів. Google у 2019 році заявила про досягнення так званої «квантової переваги», продемонструвавши, що їхній квантовий процесор здатен вирішити задачу, яка є практично неможливою для класичного суперкомп'ютера. Хоча ця перевага поки не має практичного значення, вона символізує перехід до нової ери обчислень. Не менш вражаючі результати досягнуто в галузі квантового зв'язку. У Китаї реалізовано проєкт «Micius» — перший квантовий супутник, який забезпечує квантово-захищену передачу інформації між наземними станціями. Також активно досліджується використання квантових каналів для телепортації квантового стану, що може стати основою для майбутнього квантового інтернету. Квантові сенсори демонструють надзвичайну чутливість до зовнішніх впливів. Зокрема, квантові гравіметри, акселерометри та магнітометри здатні фіксувати зміни гравітаційного

поля, магнітного середовища та положення з точністю, в рази вищою за можливості класичних аналогів.

Проблеми та виклики галузі Попри значний прогрес, квантові технології стикаються з низкою серйозних викликів. Перш за все, це проблема декогеренції — квантові стани надзвичайно нестійкі до взаємодії із зовнішнім середовищем. Найменше збурення здатне зруйнувати квантовий стан, що вимагає створення ізольованих середовищ та наднизьких температур, часто у діапазоні кількох мілікельвінів. Це значно ускладнює практичне впровадження квантових комп'ютерів. Ще одна серйозна перешкода — необхідність квантової корекції помилок. Для збереження інформації у стійкому квантовому стані потрібно використовувати велику кількість фізичних кубітів для одного логічного кубіта. Наприклад, для реалізації одного логічного кубіта з повноцінною корекцією помилок необхідно до тисячі фізичних кубітів. Це ставить під сумнів швидку появу універсальних квантових комп'ютерів. Крім того, квантові технології потребують надзвичайно точного контролю над квантовими системами, включно з лазерною стабілізацією, мікрохвильовим керуванням та точним калібруванням параметрів.

Перспективи розвитку. Незважаючи на вказані труднощі, перспективи розвитку квантових технологій залишаються надзвичайно привабливими. Одним із головних напрямів є створення глобального квантового інтернету — мережі, у якій обмін інформацією здійснюватиметься за допомогою квантових станів, що гарантує абсолютну захищеність зв'язку. Перші прототипи квантових мереж уже випробовуються в Європі, США, Китаї та Японії. Іншим важливим напрямом є гібридні обчислювальні архітектури, в яких класичні комп'ютери працюють у парі з квантовими прискорювачами. Такі системи вже застосовуються для моделювання молекул у квантовій хімії, розв'язання задач оптимізації, машинного навчання та фінансового моделювання. Перехід до нових типів кубітів, зокрема топологічних та фотонних, дозволяє зменшити вплив шумів і підвищити стабільність квантових систем. Дослідницькі лабораторії Microsoft та Delft University of Technology активно працюють над створенням таких кубітів, які можуть стати основою для масштабованих і надійних квантових обчислювальних платформ. Крім того, розвивається напрям квантового програмного забезпечення: з'являються нові мови програмування (Q#, Quipper, Silq), фреймворки (Qiskit, Cirq, PennyLane), а також симулятори, що дозволяють вивчати квантові алгоритми на класичних комп'ютерах.

Квантові технології наразі перебувають на перетині фундаментальної науки та інженерного прориву. Їхній потенціал у багато разів перевищує можливості класичних систем, особливо в галузі обчислень, комунікацій і точного вимірювання. Успішний розвиток квантових технологій потребує комплексного підходу, що включає: розвиток теоретичної бази, вдосконалення апаратних засобів, створення спеціалізованого програмного забезпечення та, найголовніше, — підготовку фахівців нового покоління. У найближчі десятиліття квантові технології матимуть вирішальний вплив на трансформацію світової науково-технічної парадигми.

ВИКОРИСТАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ СТВОРЕННЯ ДИСТРИБУТИВНИХ ДОДАТКІВ

Хрипко С.Л.

Анотація. Ця стаття досліджує інтеграцію Децентралізованих Ідентифікаторів (DID) та Доказу з Нульовим Розголошенням (ZKP) у архітектуру розподілених додатків (dApps) на базі блокчейну з метою подолання ключових викликів масштабованості, конфіденційності та безпеки користувацьких даних. Поточні dApps, незважаючи на їхній трансформаційний потенціал, стикаються з обмеженнями у пропускній здатності блокчейну та відсутністю надійних механізмів конфіденційності, що перешкоджає їхньому масовому прийняттю, особливо у таких чутливих до даних галузях, як децентралізовані фінанси (DeFi) та управління ланцюгами поставок. Методологія включає кількісний аналіз показників продуктивності, таких як швидкість транзакцій (TPS), вартість газу та затримка мережі, а також якісну оцінку покращення конфіденційності та архітектурної безпеки. Ключові висновки показують, що інтеграція DID та ZKP значно покращує ефективність використання ресурсів блокчейну та забезпечує надійний захист даних, пропонуючи масштабовані та приватно-орієнтовані рішення для майбутніх децентралізованих екосистем. Результати дослідження надають практичні рекомендації для розробників dApps та вказують на важливість цих технологій для розвитку Web3.

Abstract. This paper investigates the strategic integration of Decentralized Identifiers (DIDs) and Zero-Knowledge Proofs (ZKPs) into blockchain-based decentralized applications (dApps) to address critical challenges in scalability, privacy, and user data security. Current dApps, despite their transformative potential, face limitations in blockchain throughput and the absence of robust privacy mechanisms, hindering their widespread adoption, particularly in data-sensitive sectors like Decentralized Finance (DeFi) and supply chain management. The methodology involves a quantitative analysis of performance metrics such as transactions per second (TPS), gas costs, and network latency, alongside a qualitative assessment of privacy enhancements and architectural security. Key findings indicate that the integration of DIDs and ZKPs significantly improves blockchain resource efficiency and provides robust data protection, offering scalable and privacy-preserving solutions for future decentralized ecosystems. The research outcomes provide practical recommendations for dApp developers and underscore the importance of these technologies for the evolution of Web3.

Блокчейн-технологія вже довела свою спроможність трансформувати різні галузі, пропонуючи децентралізацію, прозорість та незмінність даних. Однак, її широке впровадження у dApps стикається зі значними викликами.

Існуючі блокчейн-мережі, часто страждають від низької пропускну здатності та високих транзакційних витрат, що обмежує їхню здатність обробляти великий обсяг операцій, необхідних для масового впровадження dApps.

Принцип прозорості блокчейну, хоча й є перевагою, може становити загрозу конфіденційності користувачів, оскільки всі транзакції та дані є публічними. Це

особливо критично для dApps, що працюють з чутливою інформацією, наприклад, у фінансовій або медичній сфері. ZKP є однією з найбільш перспективних криптографічних примітивів для забезпечення конфіденційності, дозволяючи перевіряти достовірність інформації без розкриття самої інформації. Інтеграція ZKP у dApps є актуальною темою досліджень, так як інтеграція DID та ZKP може впливати на масштабованість не лише прямо (через зменшення обсягу даних, що зберігаються в ланцюзі), а й опосередковано (шляхом оптимізації процесів ідентифікації та верифікації)..

Традиційні централізовані системи ідентифікації є вразливими до зламу та зловживання даними. DID пропонують новий підхід до управління ідентифікацією, надаючи користувачам повний контроль над їхніми цифровими ідентичностями та даними. Дослідження того, як DID можуть бути ефективно інтегровані в dApps, є ключовим для створення надійних, безпечних та орієнтованих на користувача додатків.

У світі, де дані є новою "нафтою", захист персональних даних та конфіденційність стали першочерговими завданнями. Розробка dApps, які ефективно використовують ZKP, може забезпечити високий рівень конфіденційності, що є критично важливим для прийняття цих технологій широким загалом та у відповідності до таких регуляторних норм, як GDPR.

Було проведено дослідження показників швидкості, вартості транзакцій та затримки мережі у прототипах dApps з інтегрованими DID та ZKP. Дані були отримані в тестових середовищах. Для розробки прототипів були використані блокчейн-платформи (Ethereum L2, Polygon (PoS), zkSync Era).

Наведені значення є середніми і можуть коливатися залежно від завантаженості мережі, складності смарт-контракту, типу ZKP-доказу та ін.

В результаті дослідження в сценарії dApp з DID/ZKP вартість ZKP-верифікації (додаткові комісії) найменша для DID-аутентифікації (з ZKP-доказом) і складає

~\$0.10 - \$1.00 (залежить від складності ZKP) на рівні L1 та < \$0.01 на рівні L2. Так

для сценарію конфіденційного голосування (на L2) вона склала \$0.50 - \$5.00+

(більш складні ZKP), а для сценарію приватної верифікації кваліфікації/активу (в DeFi) склала \$0.20 - \$2.00 (середня складність ZKP).

Що стосується сценарію DID-аутентифікації (з ZKP-доказом) вплив на TPS показав незначне збільшення ефективного TPS (менше даних в ланцюзі). Однак для сценарію конфіденційного голосування (на L2) і приватної верифікації кваліфікації/активу (в DeFi) вплив на TPS мережі показав зниження через обчислення ZKP та залежно від складності ZKP-доказу.

Що стосується затримки генерації ZKP (клієнтська сторона) то вона виявилась

більшою для конфіденційного голосування на L2) і склала 1 сек - 10+ сек (для

складного доказу, що залежить від пристрою). Для приватної верифікації кваліфікації/активу (в DeFi) склала 500 мс - 5 сек та 100 мс

- 1 сек (для простого доказу на сучасному пристрої) для сценарію DID-аутентифікація (з ZKP-доказом). Таким чином, хоча інтеграція DID та ZKP у dApps може додавати певну обчислювальну складність та затримку на стороні клієнта, стратегічне їх використання та за допомогою оптимізованих ZKP-схем, призводить до значних покращень у конфіденційності та безпеці без критичного зниження загальної продуктивності.

СИСТЕМНО-ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ТИПОВИХ АЛГОРИТМІВ В ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ

Шкітов Андрій Анатолійович

III курс, група КІ-22-1а, спеціальність “Комп’ютерна інженерія” Інститут комп’ютерних технологій Університету “Україна”, м Київ, Україна.

<https://orcid.org/0009-0005-4600-8467>, opncore@gmail.com

Науковий керівник: Тимошенко А.Г., к.т.н., професор, Інститут комп’ютерних технологій Університету “Україна”, м Київ, Україна.

<https://orcid.org/0000-0003-0954-3186>, timoshag@i.ua

Анотація. В роботі системно-порівняльним аналізом досліджено актуальність типових алгоритмів процесу оптимізації бізнес-рішень. Розглянуто найпоширеніші алгоритми, а саме: «Динамічне програмування»; «Жадібні алгоритми»; «Генетичні алгоритми»; «Лінійне програмування», «Алгоритм найшвидшого спуску».

Запропоновано на тлі війни ефективно діючий механізм реалізації системно-порівняльного аналізу щодо типових алгоритмів оптимізації бізнес-рішень.

Ключові слова: генетичний алгоритм, жадібні алгоритми, динамічне програмування, алгоритм найвищого спуску, бізнес-процеси.

Abstract. This study presents a system-comparative analysis to assess the relevance and applicability of typical algorithms used in the optimization of business decision-making processes. The analysis focuses on five widely recognized algorithmic approaches: Dynamic Programming, Greedy Algorithms, Genetic Algorithms, Linear Programming, and the Steepest Descent Algorithm. In light of the ongoing wartime context, the paper proposes an effective implementation mechanism for applying system-comparative analysis to these algorithms, aiming to enhance the robustness and efficiency of business decision-making under conditions of uncertainty and instability.

Keywords: genetic algorithm, greedy algorithms, dynamic programming, highest descent algorithm, business processes.

У сучасному бізнес-середовищі оптимізація процесів є актуальним фактором підвищення продуктивності та конкурентоспроможності. Використання алгоритмів оптимізації дозволяє “автоматизувати рутинні завдання, зменшити витрати та підвищити ефективність операцій” [1].

З огляду на це, оптимізація бізнес-процесів – це лейтмотивно затребуваний процес в напрямку стратегічно-програмної побудови ефективного та стабільного бізнесу. Адже від того, наскільки вдало буде проведено оптимізацію, залежить розподіл обов’язків та інтелектуального ресурсу між усіма учасниками процесу, оскільки в суб’єктах комп’ютерної інженерії фундаментальною матрицею цифрової криптографії програмування є мікропроцесорна система. Саме в такій системі програмування має нагальне місце динамічна не лінійність цифрової пам’яті. Вдала оптимізація дозволяє підвищити рівень контролю за процесами та виявити ланцюжок цінності для клієнта в послугах. Крім того, відбувається

“спрощення внутрішньої комунікації й створюються фіксовані “правила гри” для кожного працівника компанії” [3].

Таким чином, для оптимізації бізнес-процесів використовуються різні типові алгоритми, які допомагають аналізувати та покращувати ефективність таких процесів.

Пропонуємо розглянути різні типи алгоритмів представлені в таблиці 1, що використовуються для оптимізації процесів, порівняння їх, а також їхні переваги та недоліки.

Таблиця 1. Порівняльний аналіз типових алгоритмів в оптимізації бізнес-процесів

Назва алгоритму	Принцип роботи алгоритму	Складність реалізації	Застосування в бізнесі	Переваги	Недоліки
Динамічне програмування	Застосовуються для вирішення складних проблем, розбиваючи їх на більш дрібні.	Висока	Розподіл ресурсів; фінанси; виробництво	Ефективність; гнучкість; точність	Складність; потреба у великих об'ємах пам'яті; певний формат задачі
Жадібні алгоритми	Приймає найкраще рішення, виходячи з наявних на кожному етапі даних, не зважаючи на можливі наслідки, сподіваючись урешті-решт отримати оптимальний розв'язок.	Низька	Управління завданнями; планування; оптимізація процесів	Висока швидкість	Може працювати некоректно; неможна відмінити вже зроблений вибір.

Генетичні алгоритми	Використовується для вирішення задач оптимізації і моделювання шляхом послідовного підбору, комбінування і варіації шуканих параметрів з використанням механізмів, що нагадують <u>біологічну еволюцію</u>	Середня	Логістика	Точність	Низька швидкість
Лінійне програмування	Математичний метод, що використовується для оптимізації лінійних функцій з лінійними обмеженнями	Середня	Фінансові процеси; оптимальний маршрут доставки;	Точність Висока швидкість	Масове обмеження при вирішенні і нелінійних завдань
Алгоритм найшвидшого спуску (градієнт)	Алгоритм шукає локальні мінімуми або максимуми шляхом повторного оновлення параметрів і переміщення у напрямку найшвидшого спуску (або підйому)	Висока	Оптимізація процесів; Інжиніринг	Ефективність; Загал. застосування	Високий обчислювальний час; Низька швидкість

У результаті цього, вибір алгоритму залежить від специфіки бізнес-процесу, вимог до точності та швидкості виконання. При цьому, жадібні алгоритми підходять для швидких рішень, а генетичні алгоритми ефективні для складних процесів, але мають низьку швидкість. Іншими словами, динамічне програмування – це гнучке, ефективне та точний процес, але складне у використанні. Розуміння сильних і слабких сторін кожного методу допомагає вибрати оптимальний підхід щодо автоматизації як програмного забезпечення бізнес-процесу.

Отже, завдяки автоматизації, покращеному прийняттю рішень та скороченню неефективних рішень компанії можуть досягти значних покращень в ефективності та конкурентоспроможності. Ретельний вибір та впровадження алгоритмів є важливим кроком до досягнення операційної досконалості та зростання бізнесу. За допомогою правильного застосування алгоритмів компанії можуть досягти значних успіхів у конкурентній боротьбі.

Список використаних джерел.

1. Годлюк В. Еволюційні обчислення в економіці та їх застосування URL:
2. Гулаєва, Н. М., Шило, В. П., Глибовець М.М. (2021). Генетичні алгоритми як обчислювальні методи скінченновимірної оптимізації. Кібернетика та комп'ютерні технології: Зб. наук. пр. — 2021. — № 3. — С. 5-14.
3. Оптимізація бізнес процесів. URL: <https://manageable.com.ua/optymizatsiya-biznes-protsesiv/> оптимізація бізнес процесів
4. Генетичний алгоритм. URL: <https://uk.wikipedia.org/wiki/>
5. Лісовський П.М., Лісовська Ю.П., Шкітов А.А. Цифрова криптографія програмування: навч. посібник. Київ : Видавництво Ліра-К, 2025. 1110 с.
6. Лісовський П.М., Лісовська Ю.П., Шкітов А.А. Феноменологія кібербезпеки: венно-правовий стан захищеності інформаційного капіталу в обороноздатній інфраструктурі України : монографія. Київ : Видавництво Ліра-К, 2025. 1050с.

МЕТОДИ ПЕРЕТВОРЕННЯ СУПУТНИКОВИХ RGB ЗОБРАЖЕНЬ В IR У РОЗРІЗІ ВІЗУАЛЬНОЇ НАВІГАЦІЇ БПЛА

Юшко О.В.

аспірант, Відкритий Міжнародний Університет Розвитку Людини «Україна», Київ, Україна. <https://orcid.org/0009-0008-7686-3503>, olegushko94@gmail.com.

Самарай В.П.

к.т.н., доц., Відкритий міжнародний університет розвитку людини «Україна», Київ, Україна. <https://orcid.org/0000-0003-4419-1366>, samaraj@ukr.net

Анотація: У даній роботі розглянуто сучасні методи перетворення зображень з видимого спектру (RGB) у інфрачервоний (IR), зокрема в контексті військового застосування. Основну увагу приділено використанню супутникових RGB зображень, які перетворюються на IR-зображення для подальшого порівняння з даними від інфрачервоних камер безпілотних літальних апаратів (БПЛА). Цей підхід є ключовим для задач візуальної навігації у складних метеоумовах або за відсутності GPS-сигналу. Проаналізовано сучасні глибокі моделі, такі як GAN, автоенкодеру та трансформери. Розглянуто точність відновлення та відповідність реконструйованих IR-зображень реальним даним. Окреслено перспективи використання додаткових модальностей (моделей і модулів) для покращення відповідності зображень.

Abstract: This report reviews current methods of converting visible spectrum (RGB) images to infrared (IR), with a focus on military applications. Special attention is paid to satellite-acquired RGB images, which are converted to synthetic IR for comparison with UAV infrared camera outputs. This technique is critical for visual navigation in GPS-denied environments or adverse weather conditions. Modern deep learning models such as GANs, autoencoders, and transformers are analyzed. The fidelity of the reconstructed IR imagery and its usability for matching real IR UAV imagery is discussed. The use of additional modalities to enhance alignment accuracy is also explored.

У сучасних військових операціях важливим є використання різних каналів спостереження для підвищення точності виявлення та навігації. В умовах відсутності сигналу GPS або дії засобів РЕБ, перетворення RGB-супутникових зображень в інфрачервоний діапазон (IR), дозволяє значно підвищити надійність візуальної навігації, зокрема в темно пору доби, що особливо актуально для ударних БПЛА які летять на малих висотах.

Основна задача — синтезувати IR-зображення з RGB-супутникових кадрів таким чином, щоб вони максимально відповідали даним з IR-камер БПЛА. Це дозволяє виконувати візуальну локалізацію за допомогою технік шаблонного співставлення або глибоких моделей співвіднесення. Серед основних підходів — генеративні змагальні мережі (GAN) [6], трансформери та гібридні архітектури [4]. GAN, зокрема модифікації Pix2Pix та CycleGAN, дозволяють навчатись перетворенню RGB->IR з використанням парних або непарних зображень [1-2].

Трансформерні моделі, як-от TransU-Net, забезпечують глобальне охоплення контексту, що особливо важливо для супутникових зображень [3]. Autoencoder-архітектури(U-Net) забезпечують швидке навчання та узагальнення, хоча поступаються за якістю текстурної реконструкції.

В рамках роботи було проведено порівняльний аналіз даних методів, результати якого показали, що найвищі показники якості продемонструвала трансформерна модель (TransU-Net), Pix2Pix посів друге місце, а CycleGAN третє, автоенкодер (U-Net) посів четверте місце. Ці спостереження узгоджуються з якісними висновками інших дослідників [7].

Синтезовані IR-зображення застосовуються для вирішення задачі співставлення зображень між супутниковим RGB та даними з БПЛА. Для цього можна використовувати такі методи як Mutual Information Matching, Learned Feature Descriptors, або моделі типу SuperGlue [5]. Точність навігації напряму залежить від якості реконструкції та інваріантності синтезованих IR-зображень, що у власну чергу вимагає покращення точності та вдосконалення методів перетворення.

Застосування глибоких моделей для перетворення RGB->IR у військовому контексті відкриває нові можливості для автономної навігації. Подальші дослідження мають бути спрямовані на покращення точності співставлення та реалістичності реконструкції в складних умовах, адже такі умови здебільшого і трапляються на практиці. Одним із можливих методів покращення, може слугувати використання метаданих супутникових знімків (таких як час доби, погодні умови і такі інше), для більш тонкого налаштування параметрів моделей, що у власну чергу може дати кращі результати.

Список використаних джерел

1. Isola P., Zhu J.Y., Zhou T., Efros A.A. Image-to-image translation with conditional adversarial networks // CVPR, 2017.
2. Zhu J.Y., Park T., Isola P., Efros A.A. Unpaired image-to-image translation using Cycle-Consistent Adversarial Networks // ICCV, 2017.
3. Chen J., et al. TransUNet: Transformers Make Strong Encoders for Medical Image Segmentation // arXiv:2102.04306, 2021.
4. Zhou W., et al. Learning Cross-Modality Correspondence for Infrared and RGB Image Registration // IEEE TCSVT, 2021.
5. Sarlin P.-E., et al. SuperGlue: Learning Feature Matching with Graph Neural Networks // CVPR, 2020.
6. Ma W., et al. Deep Infrared Image Synthesis via Coupled GANs with Dual-Discriminator // Sensors, 2020.
7. Liik H. Thermal image generation from RGB // Medium. – 2020. – URL: <https://medium.com/@hannesliik/thermal-image-generation-from-rgb-b152efa66cc2>

Навчальне видання

Відповідальна за випуск

Наталія ОДРІБЕЦЬ

МАРКЕТИНГОВА ТОВАРНА ПОЛІТИКА

Тези доповідей

Електронне видання

Підписано до друку 17.06.2025 р.
Формат 60×84/16. Ум. друк. арк. 6,1.
Наклад 100 прим. Зам. № ...

*Видавець і виготовлювач: Університет «Україна».
03115, м. Київ, вул. Львівська, 23,
тел./факс (044) 424-40-69, 424-56-26
E-mail: ukraina.vdk@email.ua
Свідоцтво суб'єкта видавничої справи ДК № 405 від 06.04.2001.*