МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

VII ВСЕУКРАЇНСЬКА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ

«СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ IOT»

20 квітня 2026 року

Збірник тез

м. Київ

Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку IoT». Збірник тез. – К.: ДУІКТ, 2026

Збірник містить тези доповідей учасників конференції, представлених на Всеукраїнській науково-технічній конференції «Сучасний стан та перспективи розвитку IoT», яка проводилась 20 квітня 2026 р. на кафедрі Інформаційних систем та технологій Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій, м. Київ.

Робочі мови – українська та англійська.

На конференції розглянуті перспективи розробки та застосування IoT технологій в Україні та світі.

Державний університет інформаційно-комунікаційних технологій
e-mail: kafedraist2049@gmail.com

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Державний університет інформаційно-комунікаційних технологій
Навчально-науковий інститут інформаційних технологій
Кафедра Інформаційних систем та технологій

ПРОГРАМНИЙ КОМІТЕТ

СТОРЧАК Каміла Павлівна, д.т.н., проф., завідувач кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна
БОНДАРЧУК Андрій Петрович, д.т.н., проф. завідувач кафедри Комп'ютерних наук Київського столичного університету імені Бориса Грінченка
СРІБНА Ірина Миколаївна, д.т.н., доц., професор кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна
АЛЬ-АММОРІ Алі Нурддинович, д.т.н., проф., завідувач кафедри Інформаційно-аналітичної діяльності та інформаційної безпеки Національного транспортного університету, м. Київ, Україна
МОРОЗОВА Ольга Ігорівна д.т.н., проф., професор кафедри Комп’ютерних систем, мереж і кібербезпеки факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ».
НІКІТЧУК Тетяна Миколаївна, к.т.н., доц., декан факультету інформаційно-комп’ютерних технологій Державного університету «Житомирська політехніка».
ПОПЕРЕШНЯК Світлана Володимирівна, к.ф.-м.н., доцент, доцент кафедри Інформатики та програмної інженерії Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

НАПРЯМ 1. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УКРАЇНІ І СВІТІ

Карпенко Олександр Олексійович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
karpenko5522@gmail.com

Ткаленко Оксана Миколаївна
доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
tkalenko-oksana888@ukr.net

АНАЛІЗ ТИПІВ СПОВІЩЕНЬ У TELEGRAM

У сучасному цифровому середовищі месенджери відіграють ключову роль у комунікації між користувачами. Одним із найпопулярніших сервісів є Telegram, який забезпечує швидкий обмін повідомленнями, підтримку ботів, каналів і груп. Важливою складовою цього сервісу є система сповіщень, яка інформує користувачів про нові події в режимі реального часу.

Основною проблемою є необхідність ефективного управління різними типами сповіщень, оскільки їх надлишок може призводити до інформаційного перевантаження, а недостатня кількість – до втрати важливих повідомлень. Таким чином, виникає потреба у дослідженні класифікації та особливостей функціонування сповіщень у Telegram.

Метою роботи є аналіз основних типів сповіщень у Telegram, визначення їх функціонального призначення, а також оцінка їх впливу на зручність користування додатком. Додатково розглядаються механізми налаштування сповіщень та можливості їх персоналізації.

У процесі дослідження було визначено, що Telegram використовує багаторівневу систему сповіщень, яка дозволяє користувачам отримувати інформацію з різних джерел. Основні типи сповіщень можна класифікувати наступним чином:

1. Особисті повідомлення

Цей тип сповіщень виникає при отриманні повідомлень у приватних чатах. Вони мають найвищий пріоритет і, як правило, супроводжуються звуковими сигналами та візуальними індикаторами. Користувач може налаштовувати індивідуальні параметри для кожного контакту.

2. Групові сповіщення

Групові чати можуть генерувати значну кількість повідомлень, тому Telegram пропонує можливість вимкнення звуку або повного відключення сповіщень. Також доступна функція згадування (mentions), яка дозволяє отримувати повідомлення лише у випадку прямого звернення до користувача.

3. Сповіщення каналів

Канали використовуються для односторонньої передачі інформації. Сповіщення з каналів можна налаштовувати окремо, включаючи можливість отримання лише важливих повідомлень або повного їх ігнорування.

4. Системні сповіщення

До цієї категорії належать повідомлення про зміни в обліковому записі, входи з нових пристроїв, оновлення політики конфіденційності тощо. Вони мають високий рівень важливості, оскільки пов’язані з безпекою користувача.

5. Сповіщення ботів

Telegram активно підтримує використання ботів, які можуть надсилати повідомлення різного характеру – від нагадувань до аналітичних звітів. Користувач може контролювати їх активність через налаштування або блокування.

6. Push-сповіщення

Це повідомлення, які надходять на пристрій навіть тоді, коли додаток неактивний. Вони реалізуються через сервери Telegram та системи мобільних операційних систем (Android, iOS).

Особливістю Telegram є гнучка система налаштувань, яка дозволяє:

- змінювати звуки сповіщень;
- встановлювати винятки для окремих чатів;
- налаштовувати час "тиші" (mute);
- використовувати пріоритети повідомлень.

Порівняльний аналіз показав, що Telegram забезпечує більш розширені можливості керування сповіщеннями порівняно з іншими месенджерами, що позитивно впливає на досвід користувача.

У результаті дослідження встановлено, що система сповіщень у Telegram є багатофункціональною та адаптивною. Вона дозволяє ефективно управляти інформаційними потоками та мінімізувати відволікання користувача.

Подальший розвиток може бути пов’язаний із впровадженням інтелектуальних алгоритмів, які автоматично визначатимуть важливість повідомлень на основі поведінки користувача. Також перспективним є використання штучного інтелекту для персоналізації сповіщень.

Список використаних джерел

1. *Telegram FAQ. [Електронний ресурс]. – Режим доступу: https://telegram.org/faq*
2. *Telegram API Documentation. [Електронний ресурс]. – Режим доступу: https://core.telegram.org*
3. *Коваленко О. В. Мобільні додатки та їх інтерфейси. – Київ: НТУУ, 2022.*
4. *Сидоренко П. І. Інформаційні системи та технології. – Львів: ЛНУ, 2021.*

Сягровський Павло Дмитрович
студент 4 курсу
спеціальності «Технології цифрового розвитку»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
pasha.syagro@gmail.com

Чутулян Вадим Олегович
старший викладач кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
vadymchytulian@gmail.com

ЗАСТОСУВАННЯ WEB3 ТА ГЕОЛОКАЦІЙНИХ СЕРВІСІВ У ПЛАТФОРМІ AUTOASSIST+ ДЛЯ ЦИФРОВІЗАЦІЇ СЕРВІСНИХ ПРОЦЕСІВ

Цифровізація сервісних процесів є одним із ключових напрямів розвитку сучасних інформаційних систем. Для платформ, пов’язаних із технічною допомогою, логістикою, страхуванням та супроводом транспортних засобів, особливо важливими є швидкість обробки звернення, прозорість фінансової взаємодії та можливість просторового визначення місця надання послуги. Традиційні CRM-рішення забезпечують облік звернень і статусів, однак часто не мають вбудованих механізмів відкритої верифікації транзакцій та інтегрованого геолокаційного підбору виконавців [2]. У зв’язку з цим доцільним є поєднання класичної вебплатформи з геолокаційними сервісами та Web3-інструментами.

У межах дослідження розглядається платформа AutoAssist+, призначена для автоматизації сервісних процесів від моменту створення заявки до завершення робіт і формування підтверджуючих документів. Концепція системи передбачає використання єдиного сценарію обробки замовлення, що охоплює реєстрацію звернення, географічне позиціонування, автоматизоване формування оцінки, фіксацію суми перед оплатою, проведення транзакції, генерацію чека та створення цифрового доказу виконання. Така побудова забезпечує безперервний ланцюг подій і підвищує відтворюваність сервісного процесу.

Одним із базових функціональних компонентів платформи є геолокаційний модуль. Під час створення заявки користувач вказує адресу або координати, після чого система визначає найближчі сервісні центри та формує перелік доступних виконавців. Для обчислення відстані між координатами доцільно використовувати формулу Гаверсина, яка забезпечує достатню точність для задач радіусного пошуку [3]. Геолокаційний підхід дозволяє скоротити час реагування, зменшити логістичні витрати та підвищити якість обслуговування за рахунок вибору найближчого центру. Архітектурну схему взаємодії основних модулів наведено на рис. 1.

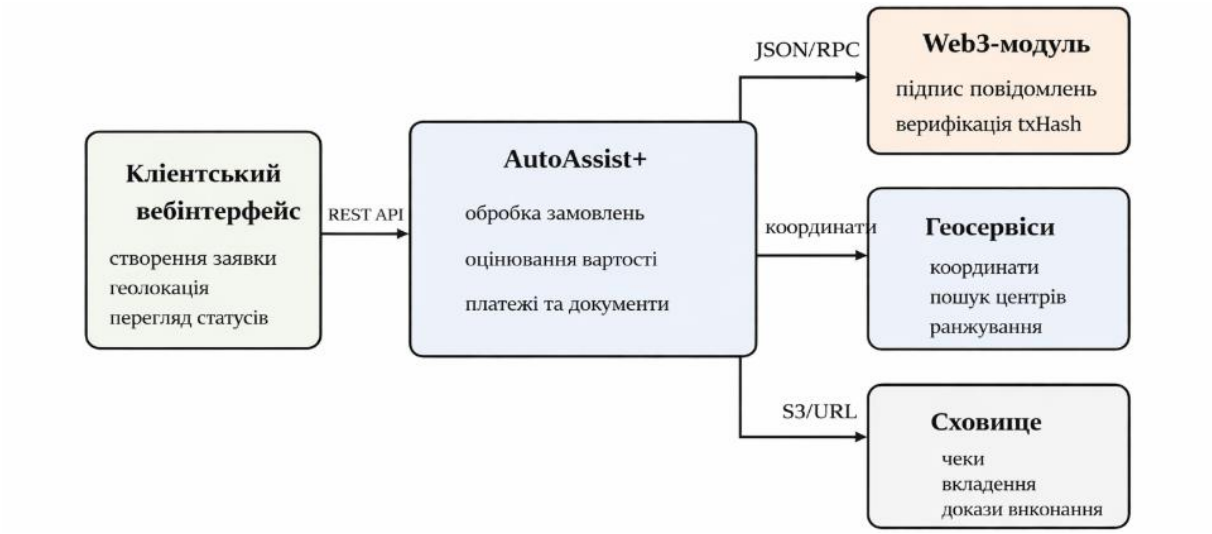

Рис. 1. Архітектурна схема платформи AutoAssist+

Іншим важливим елементом є модуль Web3-платежів, який реалізує авторизацію гаманця, підпис повідомлень та перевірку транзакції на рівні блокчейну. Після підтвердження оцінки вартості сума блокується в межах замовлення, що усуває ризик її зміни під час оплати. Далі користувач ініціює платіж через сумісний гаманець, а система отримує txHash і виконує перевірку основних параметрів транзакції: мережі, адреси одержувача, суми та кількості підтверджень [1], [8]. У разі успішної верифікації платіж набуває підтвердженого статусу, після чого стає доступною генерація квитанції та цифрового доказу виконання робіт.

Запропонований підхід поєднує переваги централізованого керування сервісним процесом і децентралізованої перевірки платіжних даних. Централізована частина платформи відповідає за збереження заявок, оцінок, статусів, вкладень і часових міток подій. Децентралізована складова використовується для перевірки факту транзакції та підвищення довіри між сторонами взаємодії. Унаслідок цього досягається більш прозорий контроль замовлення, оскільки платіжний етап стає перевірним, а цифрові документи можуть бути пов’язані з конкретним фактом фінансової операції.

Функціональні компоненти платформи AutoAssist+ та їх роль у цифровізації сервісного процесу наведено в табл. 1. Узагальнення цих компонентів дає змогу показати, що геолокаційний пошук і Web3-підтвердження не є ізольованими модулями, а виступають частинами єдиної системи прийняття рішень, оплати та документування виконаних дій.

Табл. 1

Функціональні компоненти платформи AutoAssist+

Компонент	Призначення	Технологічна основа	Результат
Модуль замовлень	Реєстрація заявки, статуси, таймлайн подій	React, Node.js, PostgreSQL	Керування повним життєвим циклом заявки
Геолокаційний модуль	Пошук найближчих сервісних центрів і визначення координат	Leaflet, формула Гаверсина	Скорочення часу реагування та логістичних витрат
Web3-модуль	Підключення гаманця, підпис повідомлення, перевірка txHash	ethers.js, SIWE, блокчейн-вузол	Підвищення прозорості та перевірності оплати
Документний модуль	Генерація чека та формування доказу виконання	PDF, S3-сумісне сховище	Отримання цифрових підтверджуючих документів

Наведена характеристика свідчить про те, що платформа AutoAssist+ може виступати ефективним засобом цифровізації сервісної взаємодії в середовищах, де важливими є мобільність, оперативність і доказовість виконаних дій. Упровадження геолокаційного підбору виконавців покращує логістичну складову, а Web3-механізми забезпечують перевірність фінансової операції без зміни базової логіки сервісного застосунку. Таке поєднання є перспективним для транспортного обслуговування, технічної допомоги, страхових сценаріїв та інших процесів, де послуга має просторову прив’язку.

Отже, застосування Web3 та геолокаційних сервісів у платформі AutoAssist+ створює основу для побудови сучасного цифрового сервісу, у якому поєднано автоматизоване оброблення замовлень, просторовий аналіз, перевірну оплату та генерацію цифрових підтверджень. Подальший розвиток такого підходу може бути пов’язаний з інтеграцією аналітичних модулів, розширенням картографічних алгоритмів і використанням додаткових каналів взаємодії з користувачем [4], [7].

Список використаних джерел

1. *Ethers.js. (n.d.). Documentation.* https://docs.ethers.org/
2. *Fowler, M. (2002). Patterns of enterprise application architecture. Addison-Wesley.*
3. *Leaflet. (n.d.). Leaflet documentation.* https://leafletjs.com/reference.html
4. *Mozilla Developer Network. (n.d.). Web APIs documentation.* https://u.to/NvdyHA
5. *PostgreSQL Global Development Group. (n.d.). PostgreSQL documentation.* https://www.postgresql.org/docs/
6. *Prisma. (n.d.). Prisma ORM documentation.* https://www.prisma.io/docs/
7. *React. (n.d.). React documentation.* https://react.dev/
8. *SpruceID. (n.d.). Sign-In with Ethereum.* https://siwe.xyz/

Геращенко Вадим Романович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
vadim172002@gmail.com

АНАЛІЗ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ WI-FI 6

Сучасні бездротові мережі є основою для розвитку розумних будинків, мультимедійних сервісів та промислових IoT-застосувань. Поява технології Wi-Fi 6 забезпечує значне покращення швидкості, щільності з'єднань та енергоефективності, що робить її ключовим стандартом наступного покоління.

У цьому дослідженні розглянуто переваги Wi-Fi 6 у різних сценаріях використання, включаючи розумні будинки, відео високої роздільної здатності, онлайн-ігри та промислові мережі [1, 2].

1. Розумний будинок. Wi-Fi 6 значно перевищує можливості Wi-Fi 5 у сценаріях з високою швидкістю, великою щільністю підключень та низькою затримкою. Його переваги включають:

- висока пропускна здатність: стабільно до 500 Мбіт/с у діапазоні 5 ГГц, що забезпечує підтримку VR та HD-відео;
- низька затримка: середня затримка менше 5 мс, що оптимально для VR та онлайн-ігор;
- висока щільність: можливість одночасного підключення до 128 пристроїв, що дозволяє масштабувати домашні IoT-системи.

Ці характеристики роблять Wi-Fi 6 ідеальним рішенням для домашніх мереж, що включають численні смарт-пристрої та системи безпеки [3].

2. Відео високої роздільної здатності (4K/8K/VR). Розвиток відеосервісів від SD до VR підвищує вимоги до пропускної здатності, затримки та втрат пакетів. Wi-Fi 6 підтримує смуги 2,4 ГГц та 5 ГГц, включає технології OFDMA, MU-MIMO, BSS Coloring та динамічну CCA для зменшення перешкод і втрат пакетів. Це забезпечує стабільну передачу відео, високу якість зображення та комфортний досвід користувачів на мобільних терміналах і гарнітурах VR.

3. Послуги з низькою затримкою (Інтернет-ігри). Ігрові сервіси, особливо VR та хмарні ігри, потребують пропускної здатності до 1 Гбіт/с, затримки менше 20 мс і мінімальних втрат пакетів. Wi-Fi 6 використовує виділені канали, OFDMA та MU-MIMO для оптимізації багатокористувацьких сценаріїв, зменшення перешкод та забезпечення стабільного ігрового процесу в домашніх мережах.

4. Промислове застосування. Wi-Fi 6 забезпечує високошвидкісний доступ у багатокористувацьких щільних мережах, включно з офісами, кампусами та громадськими місцями (аеропорти, стадіони). Технології MU-MIMO, OFDMA, 1024-QAM та динамічна CCA покращують ефективність мережі, а WPA3

підвищує безпеку передачі даних. Завдяки високій пропускній здатності, низькій затримці та стабільності Wi-Fi 6 стає перспективним стандартом для промислових та громадських мереж наступного покоління.

Технологія Wi-Fi 6 забезпечує значні переваги в порівнянні з попередніми стандартами: високу пропускну здатність, низьку затримку, здатність підключати велику кількість пристроїв та ефективне енергоспоживання. Це робить її оптимальним рішенням для розумних будинків, мультимедійних сервісів та промислових мереж. Використання Wi-Fi 6 дозволяє інтегрувати IoT-пристрої, покращити користувацький досвід та забезпечити надійну та безпечну бездротову передачу даних у сучасних мережах.

Список використаних джерел

1. Andrews, J., Buzzi, S., Choi, W., et al. (2014). What Will 5G Be? IEEE Journal on Selected Areas in Communications, 32(6), 1065–1082. https://doi.org/10.1109/JSAC.2014.2328098

2. Dang, S., Amin, O., Shihada, B., & Alouini, M. (2020). What Should 6G Be? Nature Electronics, 3, 20–29. https://doi.org/10.1038/s41928-019-0355-6

3. Khorov, A., & Levitsky, I. (2021). Wi-Fi 6: New IEEE 802.11ax Standard. IEEE Communications Standards Magazine, 5(1), 26–32. https://doi.org/10.1109/MCOMSTD.001.2000001

Цайгер Юрій Петрович
студент групи ТЦР-43
спеціальності «Інженерія програмного забезпечення»,
Державного університету
інформаційно-комунікаційних технологій, м. Київ
uastalavista@gmail.com

Чернявський Ждан Анатолійович
старший викладач кафедри Технологій цифрового розвитку
Державного університету
інформаційно-комунікаційних технологій, м. Київ
z.cherniavskyi@duikt.edu.ua

ОГЛЯД ТЕХНОЛОГІЧНОГО СТЕКУ ДЛЯ МОНІТОРИНГУ ФІНАНСОВИХ ВИТРАТ

В умовах зростаючої кількості фінансових операцій актуальність систем автоматизованого обліку доходів і витрат постійно зростає. Більшість наявних рішень - Mint/Credit Karma, YNAB - орієнтовані на іноземні ринки, не підтримують формати виписок українських банків та залежать від хмарних сервісів [1, 2]. Метою дослідження є обґрунтування вибору технологічного стеку та проєктування архітектури веб-застосунку для обліку особистих фінансів. На

цьому етапі виконується аналіз та проєктування - реалізація є предметом подальших досліджень.

У процесі проєктування розглядались альтернативні технології для кожного компонента системи (табл. 1).

Табл. 1

Порівняльний аналіз технологічного стеку

Компонент	Альтернативи	Обрано	Обґрунтування
Серверний фреймворк	Django, Spring MVC	ASP.NET Core MVC	Вбудований захист XSS/CSRF, інтеграція з Identity
СУБД	MongoDB, Cassandra, Redis	SQLite	Фінансові дані мають фіксовану схему та зв'язки – NoSQL не дає переваг; SQLite: реляційна модель, ACID, без окремого сервера
ORM	Dapper, NHibernate	Entity Framework Core 9.0	Міграції, робота з .NET без SQL вручну
Автентифікація	JWT + custom, OAuth	ASP.NET Core Identity	PBKDF2, блокування після 5 спроб
UI / Діаграми	Material UI, Highcharts	Bootstrap 5 + Chart.js	Open-source, сумісний з Razor, без ліцензій

Для серверної частини обрано ASP.NET Core MVC, оскільки він забезпечує вбудований захист від XSS (впровадження шкідливих скриптів) і CSRF (підробка запитів від імені користувача) без підключення сторонніх бібліотек, а також нативно інтегрується з ASP.NET Core Identity. На відміну від Spring MVC, що потребує окремого налаштування Spring Security, ASP.NET Core MVC пропонує безшовну екосистему платформи .NET: захист, автентифікація та ORM є частиною єдиного стеку і не вимагають інтеграції з інструментами інших вендорів [3].

Для зберігання даних розглядались як реляційні, так і нереляційні СУБД. MongoDB орієнтована на гнучкі документи зі змінною структурою; Cassandra – на запис великих обсягів розподілених даних; Redis – на кешування у пам'яті. Фінансові транзакції мають чітко визначену схему з фіксованими полями та зв'язками між сутностями (транзакція, категорія, користувач), тому жодна з NoSQL-альтернатив не дає переваг, натомість ускладнює агрегацію та побудову звітів. Обрано SQLite як реляційну СУБД: вона підтримує повноцінний SQL, забезпечує ACID-транзакції та зберігає базу в одному файлі без окремого серверного процесу, що спрощує розгортання. Entity Framework Core 9.0 використовується як ORM для роботи з базою через об'єкти C# [3].

Для клієнтської частини обрано Bootstrap 5 та Chart.js - open-source бібліотеки, які добре поєднуються з шаблонізатором Razor в ASP.NET Core MVC. На відміну від Highcharts чи Material UI, вони не потребують комерційних ліцензій і мають широку документацію [4].

Спроєктована архітектура побудована за патерном MVC з сервісним рівнем. CategoryService ініціалізує 12 категорій витрат і автоматично визначає категорію транзакції за ключовими словами. BankImportService виконує парсинг CSV-виписок українських банків та пакетне збереження транзакцій. Автентифікація через ASP.NET Core Identity: хешування PBKDF2, блокування після 5 невдалих спроб на 15 хвилин [3].

На основі порівняльного аналізу обґрунтовано вибір технологічного стеку. ASP.NET Core MVC обрано через вбудований захист і інтеграцію з Identity; SQLite - як файлову СУБД без окремого сервера; Bootstrap 5 і Chart.js - завдяки сумісності з Razor та відсутності ліцензійних обмежень. Порівняно з Mint і YNAB, спроєктоване рішення підтримує формати українських банків і не залежить від хмарних сервісів. Подальші дослідження будуть спрямовані на реалізацію застосунку та інтеграцію з банківськими API.

Список використаних джерел

1. Mint. (б. д.). Budget Tracker & Planner | Free Online Money Management | Mint. https://www.engadget.com/intuit-is-closing-down-mint-its-popular-free-budget-tracking-app-054145229.html

2. YNAB. (б. д.). YNAB. https://www.ynab.com/

3. Overview of ASP.NET Core MVC. (б. д.). Microsoft Learn: Build with answers in reach. https://learn.microsoft.com/en-us/aspnet/core/mvc/overview?view=aspnetcore-10.0

4. Chart.js | Chart.js. (б. д.). Chart.js | Open source HTML5 Charts for your website. https://www.chartjs.org/docs/latest/

Саєнко Кирил Олександрович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kirihac@gmail.com

Данильченко Валентина Миколаївна
доцент, доктор філософії (PhD)
кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ВЕБ-САЙТ ІНТЕРНЕТ-МАГАЗИНУ ОДЯГУ НА WORDPRESS З ІНТЕГРАЦІЄЮ ОНЛАЙН-ОПЛАТ І ДОСТАВКИ

В умовах активного розвитку цифрової економіки електронна комерція посідає важливе місце серед основних напрямів використання інформаційних технологій в Україні та глобально. Використання веб-сайтів для продажу товарів дозволяє підприємствам автоматизувати бізнес-процеси, покращити клієнтский досвід та забезпечити безперервний доступ до товарів і послуг. Особливо актуальним це є для сфери продажу одягу, де важливу роль відіграють зручний каталог, швидке оформлення замовлення, онлайн-оплата та організація доставки.

Одним із найпоширеніших рішень для створення інтернет-магазинів є система керування вмістом WordPress. Її популярність пояснюється відкритістю, гнучкістю, великою кількістю готових шаблонів і модулів, а також відносною простотою адміністрування [1]. Для реалізації функцій електронної торгівлі на цій платформі широко застосовується плагін WooCommerce, який забезпечує створення каталогу товарів, керування кошиком, оформлення замовлень, облік клієнтів і базові засоби аналітики [2].

З точки зору програмування, розробка інтернет-магазину на базі WordPress передбачає використання серверної мови програмування PHP, яка забезпечує обробку запитів користувачів, взаємодію з базою даних та генерацію динамічного веб-контенту. Для зберігання інформації про користувачів, замовлення, та товарів обрана система керування базами даних MySQL. На стороні клієнта застосовуються HTML, CSS та JavaScript, які відповідають за структуру, оформлення та інтерактивність веб-інтерфейсу.

Розширення функціональності інтернет-магазину реалізується через розробку або налаштування плагінів, зокрема WooCommerce. Інтеграція платіжних систем і служб доставки здійснюється через API, що дозволяє автоматизувати обмін даними між сайтом і зовнішніми сервісами в режимі реального часу. Використання REST API забезпечує передачу даних у форматі

JSON, що спрощує взаємодію між клієнтською та серверною частинами застосунку [1, 3].

Важливим аспектом сучасного інтернет-магазину є інтеграція платіжних сервісів. Онлайн-оплата значно спрощує процес покупки, скорочує час обслуговування клієнта та підвищує зручність користування сайтом. Для українського ринку актуальним є підключення популярних платіжних систем, які підтримують оплату банківськими картками, електронними сервісами та швидке підтвердження транзакцій [3]. Не менш значущою є інтеграція служб доставки, завдяки якій користувач отримує можливість обрати населений пункт, відділення або адресу доставки безпосередньо під час оформлення замовлення [4].

Розробка веб-сайту інтернет-магазину одягу на WordPress із використанням WooCommerce, платіжних модулів та сервісів доставки є прикладом практичного застосування сучасних інформаційних технологій. Такий підхід дозволяє створити доступне, масштабоване та функціональне рішення для ведення онлайн-бізнесу. Крім того, автоматизація основних етапів продажу сприяє зменшенню навантаження на персонал, підвищенню точності обробки замовлень та покращенню якості обслуговування клієнтів [2].

Отже, створення інтернет-магазину одягу на платформі WordPress з інтеграцією онлайн-оплат і доставки є актуальним напрямом у сфері сучасних інформаційних технологій. Такі системи відповідають потребам цифрового суспільства, сприяють розвитку електронної комерції та демонструють ефективність використання веб-технологій для вирішення прикладних бізнес-завдань [1].

Список використаних джерел

1. *WordPress.org. (2025). WordPress documentation.*
2. *WooCommerce. (2025). WooCommerce documentation.*
3. *LiqPay. (2025). Приймання онлайн-платежів: документація сервісу.*
4. *Нова пошта. (2025). Доставка для e-commerce: можливості інтеграції та API.*

Котух Олексій Олександрович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
akotukh25@gmail.com

Полоневич Ольга Володимирівна
к.т.н., доцент, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ВЕБ-ПЛАТФОРМИ БРОНЮВАННЯ ПРИМІЩЕНЬ У СЕРЕДОВИЩІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Сучасні інформаційні системи, орієнтовані на надання онлайн-сервісів, зокрема у сфері оренди приміщень, повинні відповідати підвищеним вимогам до стабільності функціонування. Безперервний доступ користувачів до сервісу, швидка обробка запитів та здатність системи працювати в умовах зростаючого навантаження визначають її ефективність. У зв’язку з цим особливої уваги потребує питання побудови відмовостійких програмних рішень [1].

Одним із сучасних підходів до створення таких систем є використання мікросервісної архітектури. Її сутність полягає у поділі програмного продукту на окремі незалежні компоненти, кожен із яких реалізує конкретну функцію. Це дозволяє підвищити адаптивність системи та спростити процес її модернізації. Водночас така архітектура супроводжується появою нових викликів, пов’язаних із забезпеченням надійної взаємодії між сервісами та мінімізацією впливу відмов окремих елементів.

Для підвищення стійкості системи до збоїв застосовуються спеціалізовані архітектурні рішення. Одним із таких є механізм обмеження викликів до нестабільних сервісів, відомий як Circuit Breaker. Його використання дозволяє тимчасово блокувати звернення до проблемних компонентів і тим самим запобігати перевантаженню всієї системи. Завдяки цьому досягається ізоляція помилок і підтримується працездатність інших сервісів.

Ще одним важливим інструментом є реалізація повторних запитів із контрольованими інтервалами. Такий підхід дає змогу компенсувати короткочасні збої без значного впливу на загальну продуктивність. При цьому застосування обмеження часу очікування відповіді (тайм-аутів) дозволяє уникнути ситуацій, коли система витрачає ресурси на обробку завислих запитів.

Підвищенню надійності також сприяє використання механізмів розподілу навантаження між декількома екземплярами сервісів. Це забезпечує більш ефективне використання ресурсів та дозволяє системі продовжувати роботу

навіть у випадку відмови окремих вузлів. У поєднанні з автоматичним масштабуванням це створює умови для стабільної роботи при змінному навантаженні.

Важливим аспектом є впровадження асинхронної моделі взаємодії між компонентами системи. Використання черг повідомлень дає можливість зменшити залежність між сервісами та забезпечити їх автономність. У результаті система стає більш стійкою до тимчасових збоїв і здатною обробляти запити навіть у складних умовах експлуатації [2].

Окрему роль відіграють інструменти спостереження за станом системи, зокрема засоби моніторингу та централізованого логування. Вони дозволяють отримувати актуальну інформацію про роботу сервісів, виявляти аномалії та швидко реагувати на виникнення проблем. Це є необхідною умовою підтримки стабільної роботи розподілених систем.

Отже, забезпечення відмовостійкості веб-платформи бронювання приміщень у мікросервісному середовищі потребує комплексного використання сучасних архітектурних підходів і технологічних рішень. Поєднання механізмів ізоляції збоїв, повторних запитів, балансування навантаження та інструментів моніторингу дозволяє створити ефективну систему, здатну стабільно функціонувати в умовах високого навантаження та часткових відмов [3, 4].

Список використаних джерел

1. *Microsoft. Cloud-Native Applications and Microservices Architecture. – 2023. URL: https://learn.microsoft.com/*
2. *Google Cloud. Building Reliable Microservices Systems. – 2024. URL: https://cloud.google.com/*
3. *AWS. Resilience in Distributed Systems. – 2022. URL: https://aws.amazon.com/*
4. *Nginx. Modern Application Architecture Guide. – 2023. URL: https://www.nginx.com/*

Тимошенко Давід Сергійович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st7914445@stud.duikt.edu.ua

Козлов Дмитро Євгенович
PhD, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

МЕТОД ВПРОВАДЖЕННЯ SDN OPENFLOW ДЛЯ ЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ МУЛЬТИВЕНДОРНИМ МЕРЕЖЕВИМ ОБЛАДНАННЯМ

У комп'ютерних мереж спостерігається явний вектор до збільшення складності архітектури, що включає інтеграцію засобів технічного забезпечення від різнорідних постачальників. Цей стан речей створює перешкоди для забезпечення єдиного управління та стандартизації протоколів. Перспективним напрямком для подолання труднощів вважається запровадження парадигми мереж, керованих програмним забезпеченням (SDN), та використання відповідного стандарту, а саме протоколу OpenFlow.

У SDN реалізація поділу між площиною керування та площиною передачі даних, це дає змогу здійснювати програмне управління мережею з програмного контролера. Для забезпечення спілкування між контролером та фізичними елементами мережевої інфраструктури, незалежно від виробника, використовується протокол OpenFlow як універсальний механізм зв'язку. [1] [2]

Процедура впровадження програмно-конфігурованої мережі (SDN) з використанням OpenFlow охоплює низку послідовних етапів. Спочатку треба провести аналіз наявної мережевої інфраструктури, потім вибрати відповідний SDN-контролер. Далі впроваджуються комутаційні пристрої, у яких є підтримка протокола OpenFlow. Після налаштовуються необхідні директиви для контролю потоків даних та аспектів безпеки, а фінальним кроком є тестування та оптимізація.

Винятково важливим є моніторинг взаємодії апаратних компонентів, бо при використанні обладнання від різних постачальників може виникнути проблема з реалізації підтримки стандарту OpenFlow. У Таблиці 1 наведено порівняльний огляд того, яким чином здійснюється управління мережею у традиційному стані та у парадигмі SDN.

Табл. 1.

Порівняння традиційної мережі та SDN

Характеристика	Традиційна мережа	SDN
Управління	Децентралізоване	Централізоване
Гнучкість	Низька	Висока
Масштабованість	Обмежена	Висока
Автоматизація	Часткова	Повна

Використання концепції SDN, яка базується на протоколі OpenFlow, прокладає маршрут до полегшення управління мережевими інфраструктурами, підвищення адаптивності системи та змога швидшого розгортання новітніх послуг. Також, централізований контроль забезпечує підвищення рівня загальної безпеки.

Таким чином, впровадження програмно-визначених мереж із застосуванням OpenFlow є виваженим рішенням для роботи з мережами, які містять компоненти від різноманітних постачальників, що у свою чергу веде до зменшення експлуатаційних витрат та посилення продуктивності базової мережевої архітектури. [3]

Список використаних джерел

1. Kreutz, D., et al. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE. URL: https://ieeexplore.ieee.org/document/6994333

2. McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks. ACM SIGCOMM CCR. URL: https://dl.acm.org/doi/10.1145/1355734.1355746

3. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. URL: https://ieeexplore.ieee.org/document/6739370?utm_source=copilot.com

Мирончук Микола Володимирович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st8923769@stud.duikt.edu.ua

Сагайдак Віктор Анатолійович
PhD, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ВЕБ-ДОДАТОК ДЛЯ АВТОМАТИЗАЦІЇ ДОКУМЕНТООБІГУ З ВИКОРИСТАННЯМ ЧАТ-БОТУ

У сучасних умовах цифровізації організацій значна увага приділяється автоматизації внутрішніх бізнес-процесів, зокрема документообігу. Традиційні методи обробки документів потребують значних витрат часу, супроводжуються ризиком помилок та ускладнюють контроль виконання завдань. У зв'язку з цим актуальним є впровадження веб-додатків, що забезпечують централізоване керування документами та автоматизацію взаємодії між користувачами [1].

Веб-додаток для автоматизації документообігу дозволяє здійснювати створення, редагування, погодження та зберігання документів у цифровому вигляді. Основними функціональними можливостями такої системи є реєстрація користувачів, розподіл ролей, контроль доступу, відстеження статусу документів та формування звітності. Використання сучасних веб-технологій забезпечує доступ до системи з будь-якого пристрою через браузер, що підвищує мобільність і ефективність роботи [2].

Реалізація веб-додатку передбачає використання клієнт-серверної архітектури. Серверна частина може бути реалізована із застосуванням мови Python або PHP та фреймворків, що забезпечують обробку бізнес-логіки і взаємодію з базою даних. Для зберігання даних використовується PostgreSQL або MySQL. Клієнтська частина створюється за допомогою JavaScript із використанням сучасних бібліотек або фреймворків для побудови інтерактивного інтерфейсу користувача [3].

Додатково важливим етапом розробки веб-додатку є проєктування структури бази даних, яка забезпечує ефективне зберігання та обробку інформації. Основними сутностями системи є користувачі, документи, статуси обробки та історія змін. Для кожного документа зберігаються метадані, такі як дата створення, автор, тип документа та поточний стан. Нормалізація бази даних дозволяє уникнути дублювання інформації та підвищує продуктивність системи при виконанні запитів [3].

Крім того, доцільним є використання принципів модульної розробки та шаблонів проєктування, що забезпечують масштабованість і гнучкість системи. Зокрема, застосування архітектурного підходу MVC (Model–View–Controller) дозволяє розділити бізнес-логіку, інтерфейс користувача та обробку даних. Це спрощує підтримку програмного коду, його тестування та подальше розширення функціональності веб-додатку, що є важливим для довготривалих програмних проєктів [3], [5].

Важливим компонентом системи є інтеграція чат-боту, який забезпечує автоматизацію взаємодії з користувачами. Чат-бот може бути реалізований на базі платформ обміну повідомленнями, таких як Telegram, та використовувати API для обробки запитів. За допомогою чат-боту користувачі можуть отримувати сповіщення про нові документи, зміну їх статусу, а також здійснювати базові операції, наприклад погодження або відхилення документів без необхідності входу до веб-додатку [4].

Інтеграція чат-боту з веб-додатком здійснюється через REST API, що дозволяє організувати обмін даними у форматі JSON та забезпечити синхронізацію між системами в реальному часі. Це підвищує швидкість обробки інформації та зручність використання системи. Додатково важливим аспектом є забезпечення безпеки, що включає аутентифікацію користувачів, шифрування даних та контроль доступу до ресурсів [5].

Отже, розробка веб-додатку для автоматизації документообігу з використанням чат-боту є перспективним напрямом застосування сучасних інформаційних технологій. Такий підхід дозволяє підвищити ефективність управління документами, зменшити кількість помилок та забезпечити швидкий доступ до інформації, що є важливим фактором у діяльності сучасних організацій [1], [2].

Список використаних джерел

1. *Thomas H. Davenport Process Innovation: Reengineering Work Through Information Technology.*

2. *Laudon, K. C., & Laudon, J. P. Management information systems (16th ed.). Pearson.*

3. *Fielding, R. T. Architectural styles and the design of network-based software architectures.*

4. *Telegram. Telegram Bot API documentation.*

5. *OWASP Foundation. OWASP Top 10 Web Application Security Risks.*

Перевозник Валерій Олександрович
слухач 1 курсу
другого (магістерського) рівня вищої освіти
спеціальності «Національна безпека»
Національної академії служби безпеки України
perevoznikvalera@gmail.com

МОДЕЛІ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ У ЦИФРОВОМУ СЕРЕДОВИЩІ ДЕРЖАВИ

У сучасних умовах повномасштабної війни та цифровізації суспільства інформаційний простір держави стає складною багаторівневою системою. У такому середовищі інформаційно-психологічні впливи перетворюються на системну загрозу національній безпеці. Вони реалізуються через використання сучасних технологій обробки даних, штучного інтелекту та цифрових комунікацій. Такі впливи спрямовані на масову свідомість, поведінку та прийняття рішень громадянами. Це зумовлює необхідність розроблення нових підходів до їх виявлення та нейтралізації, зокрема на основі інтеграції технологічних і когнітивних компонентів [1, с. 1-2]. Зокрема, Правдюк досліджує інформаційні війни та механізми психологічного впливу. Автор доводить маніпулятивний характер інформаційних впливів і підкреслює необхідність системного моделювання процесів протидії.

Подальший розвиток цифрового середовища посилює роль штучного інтелекту. Він використовується як для здійснення впливу, так і для аналізу інформаційних процесів. Особливо це проявляється у політичних комунікаціях і соціальних мережах. Автоматизовані алгоритми здатні формувати персоналізовані повідомлення, аналізувати емоційний стан аудиторії та виконувати мікротаргетинг. Це значно підвищує ефективність маніпулятивних впливів [2, с. 2]. Старовойтенко та співавтори досліджують використання AI, NLP і big data у політичних процесах. Вони показують, що алгоритми можуть генерувати дезінформацію та впливати на емоційний стан аудиторії. Це підтверджує необхідність врахування когнітивних індикаторів у системах оцінювання загроз.

Важливим напрямом досліджень є аналіз змісту інформаційних повідомлень. Саме мовні конструкції виступають носіями психологічного впливу та формують когнітивні установки. Це обумовлює застосування психолінгвістичних методів у системах інформаційної безпеки [3, с. 3]. Крилова-Грек та колеги досліджують психолінгвістичний аналіз медіатекстів. Вони доводять можливість виявлення маніпулятивних стратегій через мовні маркери. Це створює основу для використання семантичного аналізу у моделях виявлення впливів.

Сучасні міжнародні дослідження розширюють можливості аналізу інформаційних потоків за рахунок використання методів штучного інтелекту. Зокрема застосовуються моделі обробки природної мови та тематичного моделювання [4, с. 6; 5, с. 8].

Domingues Aparecido та ін. використовують LLM і лексиконні підходи для визначення емоцій у текстах. Вони вводять метод «emotional fingerprinting», який дозволяє інтерпретувати когнітивні характеристики контенту. Couto та ін. застосовують тематичне моделювання (LDA, BERTopic) для виявлення психологічних патернів у соціальних мережах. Це підтверджує ефективність поєднання автоматичного аналізу та експертної оцінки.

У межах дослідження запропоновано авторське методичне забезпечення багаторівневої моделі виявлення та протидії інформаційно-психологічним впливам у цифровому середовищі держави. Підхід базується на поєднанні структурно-функціонального представлення інформаційних процесів і системи оцінювання рівня загроз. Це дозволяє об'єднати семантичні, поведінкові та когнітивні характеристики інформаційних потоків в одну систему аналізу. Структура моделі має ієрархічну будову та складається з взаємопов'язаних рівнів аналізу. Кожен рівень виконує окрему функцію обробки інформації та формує часткові індикатори. У сукупності вони визначають загальну оцінку інформаційно-психологічного впливу.

На першому рівні моделі реалізується семантичний аналіз інформаційного контенту, що передбачає ідентифікацію ключових тематичних ознак, емоційного забарвлення та маніпулятивних мовних конструкцій, які формалізуються у вигляді векторів ознак $S = \{s_1, s_2, \dots, s_n\}$, де кожен компонент відображає інтенсивність відповідної семантичної характеристики повідомлення. Другий рівень орієнтований на аналіз поведінкових патернів поширення інформації, що включає оцінювання динаміки інформаційних потоків, мережевої взаємодії та аномальних змін активності, які описуються множиною показників $B = \{b_1, b_2, \dots, b_m\}$, зокрема частотою репостів, швидкістю дифузії та кластеризацією джерел. Третій рівень забезпечує оцінювання когнітивного впливу на аудиторію шляхом визначення індикаторів емоційної поляризації, рівня довіри, схильності до сприйняття дезінформації та потенційної зміни поведінкових реакцій, що узагальнюються у множині $C = \{c_1, c_2, \dots, c_k\}$.

Інтеграція зазначених компонентів здійснюється через формування узагальненого індикатора рівня інформаційно-психологічної загрози, який визначається як зважена функція:

$$R = \alpha \cdot f(S) + \beta \cdot g(B) + \gamma \cdot h(C), \quad (1)$$

де α, β, γ – вагові коефіцієнти, що відображають значущість відповідних рівнів аналізу, а $f(\cdot), g(\cdot), h(\cdot)$ – функції нормалізації та агрегування показників. Запропонований підхід дозволяє враховувати як змістовні характеристики інформації, так і її поширення та сприйняття, що забезпечує комплексність

оцінювання. При цьому адаптивність моделі досягається за рахунок динамічного коригування вагових коефіцієнтів залежно від типу інформаційного середовища, рівня конфліктності та специфіки інформаційної кампанії.

У результаті дослідження сформовано основи багаторівневої моделі виявлення та протидії інформаційно-психологічним впливам у цифровому середовищі держави. Модель поєднує семантичний аналіз контенту, поведінкові характеристики інформаційних потоків і когнітивні індикатори впливу на аудиторію в межах єдиного підходу до оцінювання загроз.

Запропонована модель дозволяє перейти від фрагментарного аналізу до системного опису інформаційних процесів. Це підвищує обґрунтованість оцінювання рівня інформаційно-психологічної небезпеки та створює основу для прийняття рішень у сфері національної інформаційної безпеки.

Подальші дослідження мають бути спрямовані на вдосконалення окремих компонентів моделі. Зокрема, це стосується уточнення методів визначення когнітивних індикаторів, розширення параметрів поведінкового аналізу та розроблення підходів до емпіричної перевірки моделі на реальних даних. Також важливим напрямом є інтеграція моделі з сучасними інтелектуальними системами моніторингу та прогнозування загроз. Це дозволить підвищити адаптивність реагування та ефективність державної політики у сфері інформаційної безпеки.

Список використаних джерел

1. *Pravdiuk, A. (2023). INFORMATION SECURITY OF UKRAINE: INFORMATION INFLUENCE AND INFORMATION WARS. European Political and Law Discourse, 10(1), 111–121. https://doi.org/10.46340/eppd.2023.10.1.6*

2. *Старовойтенко, О. (2025). Штучний інтелект у виборчому процесі: нові виміри кіберзагроз і кібербезпеки. Проблеми Політичної Психології, 17. https://doi.org/10.33120/popp-vol17-year2025-194*

3. *Krylova-Grek, Y., & Korniyaka, O. (2023). Information and Psychological Security of the Media Space. Ukrainian Experience of Implementation of Psycholinguistic Component Into Media Education. PSYCHOLINGUISTICS, 34(1), 111–128. https://doi.org/10.31470/2309-1797-2023-34-1-111-128*

4. *Domingues Aparecido, T. D., Carrillo, A., Camargo, C. Q., & Stella, M. (2025). Benchmarking Psychological Lexicons and Large Language Models for Emotion Detection in Brazilian Portuguese. AI, 6(10), 249. https://doi.org/10.3390/ai6100249*

5. *Couto, M., Parapar, J., & Losada, D. E. (2026). Exploiting topic analysis models to explore psychological dimensions in social media data. Scientific Reports, 16(1). https://doi.org/10.1038/s41598-026-36339-y*

Денисов Дмитро Вячеславович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
denisov1985@gmail.com

ІНТЕЛЕКТУАЛЬНА ХМАРНА ПЛАТФОРМА МЕДИЧНОГО СТРАХУВАННЯ ДОМАШНІХ ТВАРИН НА ОСНОВІ ВЗАЄМОДІЇ СПЕЦІАЛІЗОВАНИХ AI-АГЕНТІВ

Мультиагентні системи на основі великих мовних моделей (LLM) є одним із найперспективніших напрямів автоматизації складних бізнес-процесів [4]. Їхня ключова перевага - можливість розподілити задачу між кількома спеціалізованими агентами, кожен з яких оперує власною базою знань та набором інструментів. Однак на практиці залишається відкритим питання архітектурної організації таких систем: як забезпечити маршрутизацію запитів, передачу контексту між агентами та масштабування без виділених серверів. За даними McKinsey, у 2024 р. 72% організацій уже використовують ту чи іншу AI-функцію у своїх процесах [1], проте більшість рішень обмежуються одноагентними сценаріями. Як предметну область для апробації мультиагентного підходу обрано ветеринарне страхування - ринок обсягом 21,84 млрд дол. США із темпами зростання 17,53% на рік [2], де один запит клієнта охоплює і страхові, і медичні питання, а ручне обслуговування займає 45–60 хвилин із втратою контексту між фахівцями.

Мета дослідження - розробити архітектуру та програмну реалізацію хмарної мультиагентної платформи на базі безсерверної інфраструктури та LLM, здатної автоматизувати міждоменні діалогові сценарії. Апробацію проведено на платформі «ВетЕксперт», що в межах одного діалогу дозволяє уточнити умови страхового полісу, отримати попередню ветеринарну оцінку та записатися на прийом до клініки. (рис. 1).

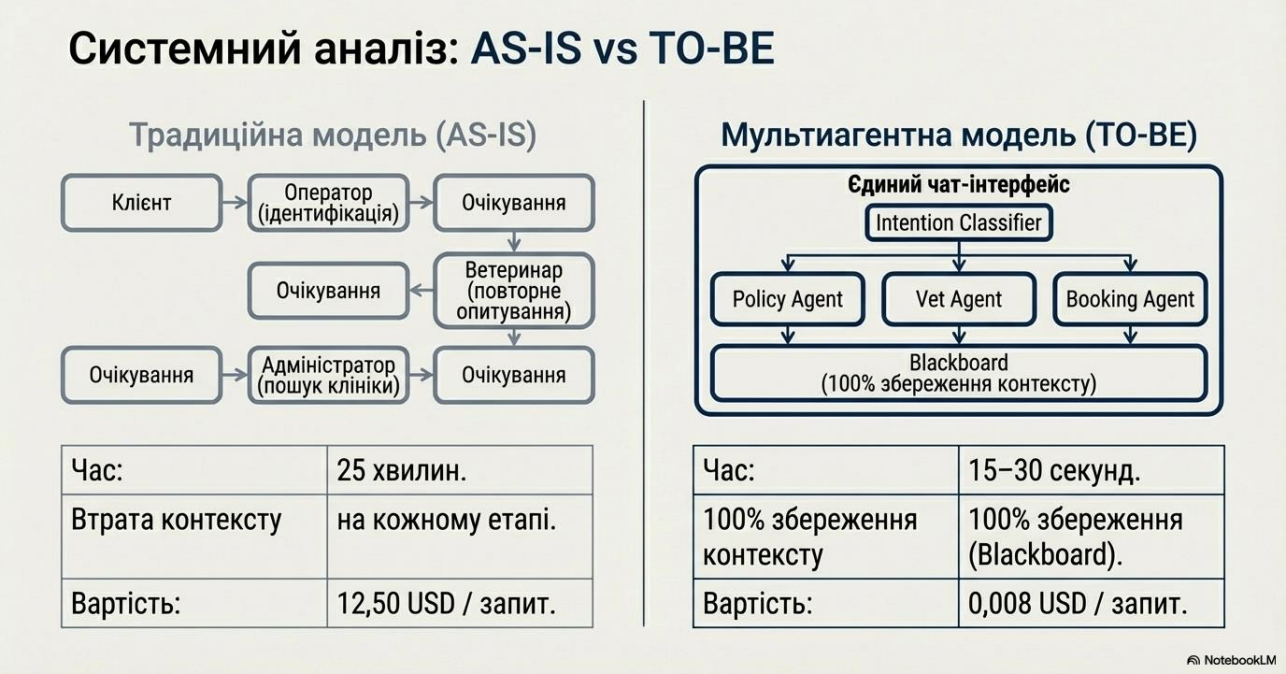

Рис. 1. Системний аналіз AS-IS vs TO-BE

Серверну частину побудовано на повністю безсерверній інфраструктурі AWS [3]: обчислення виконуються у Lambda-функціях, дані зберігаються у DynamoDB, а агенти працюють у середовищі Amazon Bedrock Agents із моделлю Claude 3.5 Haiku. Такий підхід забезпечує автоматичне масштабування та оплату лише за фактичне використання ресурсів. Міжкомпонентну взаємодію організовано через гібридний протокол: синхронна маршрутизація запитів між агентами через SNS поєднується з асинхронною доставкою подій клієнту через Server-Sent Events (SSE). Архітектурно систему побудовано за моделлю централізованої оркестрації - сервіс-оркестратор за допомогою few-shot prompting класифікує намір користувача і делегує запит одному з чотирьох спеціалізованих агентів: класифікатору намірів, агенту полісів, ветеринарному агенту або агенту бронювання.

Для агентів, що працюють із доменними знаннями, застосовано підхід Retrieval-Augmented Generation (RAG): перед формуванням відповіді модель відбирає релевантні фрагменти з верифікованої бази знань і спирається на них. Без такого механізму мовні моделі допускають 15–25% фактичних помилок; RAG знижує цей показник до 3–5% [5]. Окрему технічну задачу становить передача контексту між агентами в рамках однієї сесії - дані, зібрані одним агентом, мають бути доступні іншим без повторного запиту до користувача. Для цього реалізовано спільне сховище сесії за патерном «спільної дошки» (blackboard) [6]: кожен агент фіксує результати своєї роботи (класифікація наміру, дані полісу, діагностична оцінка, рівень терміновості), а наступний агент у ланцюжку одразу має до них доступ.

Для валідації запропонованого підходу проведено порівняння бізнес-процесів до впровадження (AS-IS) та після (TO-BE). Результати зведено у табл. 1. Слід уточнити, що колонка TO-BE фіксує час первинної відповіді системи, тоді як AS-IS - повний цикл роботи спеціаліста, тому пряме зіставлення потребує врахування різниці у глибині відповіді.

Табл. 1

Порівняльний аналіз бізнес-процесів AS-IS та TO-BE

Параметр	AS-IS	TO-BE	Покращення
Час консультації щодо полісу	10-20 хв	3-8 с	у 75-150 разів
Час ветеринарної консультації	15-30 хв	5-15 с	у 60-120 разів
Час запису на прийом	10-15 хв	15-30 с	у 20-30 разів
Сумарний час обслуговування	45-60 хв	2-5 хв	у 9-30 разів
Доступність	8-10 год	24/7	постійна
Передачі контексту між фахівцями	3-4 хв	0	усунено

Клієнтську частину реалізовано на Nuxt 4 із Tailwind CSS та Pinia для управління станом. Інтеграцію з серверною частиною побудовано на SSE-з'єднанні, що дозволяє відображати відповіді агентів у реальному часі - в міру їх формування моделлю. Повний цикл обробки запиту через ланцюжок агентів не перевищує 15 секунд. Безсерверна архітектура забезпечує ефективне використання ресурсів: за розрахункового навантаження 10 000 сесій на місяць вартість інфраструктури складає близько 79 USD, оскільки компоненти працюють за моделлю pay-per-use і не споживають ресурси у стані простою.

У роботі запропоновано архітектуру безсерверної мультиагентної системи з централізованою оркестрацією на базі LLM, яка забезпечує автоматичну маршрутизацію міждоменних запитів між спеціалізованими AI-агентами. Розроблено механізм збереження та передачі контексту сесії між агентами на основі патерну «спільної дошки», що усуває дублювання запитів до користувача при послідовній обробці різними агентами. Реалізовано гібридний протокол міжагентної комунікації, в якому синхронна маршрутизація через оркестратор поєднана з асинхронною доставкою подій через SSE, що забезпечує детермінованість обробки запитів при збереженні швидкості відгуку інтерфейсу.

Результати апробації підтверджують, що запропонована безсерверна мультиагентна архітектура дозволяє кратно скоротити час обробки міждоменних запитів і забезпечити цілодобову доступність сервісу без виділеної

інфраструктури. Обмеженнями поточної реалізації є залежність якості відповідей від повноти бази знань та коректності промптів, а також текстовий формат взаємодії. Перспективи подальшого розвитку пов'язані з додаванням мультимодального введення (зображення), розширенням бази знань та інтеграцією із зовнішніми API страхових провайдерів.

Список використаних джерел

1. *McKinsey & Company. The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. McKinsey Global Survey, May 2024. URL: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai*

2. *Grand View Research. Pet Insurance Market Size, Share & Trends Analysis Report By Animal Type, By Coverage Type, By Provider, By Region, And Segment Forecasts, 2025–2030. Grand View Research, 2025. URL: https://www.grandviewresearch.com/industry-analysis/pet-insurance-market*

3. *Newman S. Building Microservices: Designing Fine-Grained Systems. 2nd ed. Sebastopol: O'Reilly Media, 2021. 616 p.*

4. *Wang L., Ma C., Feng X. et al. A Survey on Large Language Model based Autonomous Agents. Frontiers of Computer Science. 2024. Vol. 18, No. 6. Article 186345. DOI: 10.1007/s11704-024-40231-1.*

5. *Lewis P., Perez E., Piktus A. et al. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. Advances in Neural Information Processing Systems (NeurIPS 2020). 2020. Vol. 33. P. 9459–9474.*

6. *Corkill D. D. Blackboard Systems. AI Expert. 1991. Vol. 6, No. 9. P. 40–47.*

Григор’єв Роман Віталійович
студент 4 курсу
спеціальності «Інформаційні системи і технології»
Державного університету
інформаційно-комунікаційних технологій
(067)-459-13-99
romagrom1102@gmail.com

Бондарчук Олександр Павлович
викладач кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.bondarchuk@duikt.edu.ua

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УКРАЇНІ ТА СВІТІ: ГЛОБАЛЬНІ ТРЕНДИ ТА МАКРОЕКОНОМІЧНИЙ ВПЛИВ

Сучасний етап еволюції глобальної економіки визначається інтенсивним розвитком інформаційних технологій, що формують ядро нового «інтелектуального суперциклу». Трансформація цифрового середовища перейшла до створення автономних систем штучного інтелекту (ШІ), просторових обчислень та адаптивних інфраструктурних мереж. Для України цей глобальний технологічний перехід відбувається в екстремальних умовах повномасштабної війни, що стимулювало формування унікальної екосистеми безпрецедентної цифрової стійкості. Традиційні парадигми інформаційної взаємодії потребують переосмислення у зв'язку зі швидкістю розгортання інновацій на рівні електронного урядування (GovTech), оборонних технологій (DefenseTech) та корпоративного сектору. Метою даної роботи є аналіз ключових глобальних технологічних інновацій (зокрема агентного ШІ, гібридних обчислень та превентивної кібербезпеки), а також оцінка їхнього впливу на макроекономічні показники, стійкість та експортний потенціал ІТ-галузі України у період 2024–2026 років.

Встановлено, що глобальний ринок демонструє стійке гіперзростання: за прогнозами аналітичного агентства Gartner, світові витрати на ІТ досягнуть 6,15 трильйона доларів США у 2026 році, зростаючи на 10,8% [1].Це зростання зумовлене масштабною і капіталомісткою розбудовою хмарної інфраструктури для потреб машинного навчання. Визначальними стратегічними трендами стають багатоагентні системи (Multiagent Systems) та Агентний ШІ (Agentic AI), які здатні автономно планувати та виконувати багатокрокові завдання у зовнішньому цифровому середовищі. Прогнозується, що вже до 2028 року щонайменше 15% щоденних рутинних бізнес-рішень у світі прийматимуться повністю автономно за допомогою ШІ-агентів [2]. Водночас критичного значення набувають технології конфіденційних обчислень (Confidential

Computing) та превентивної кібербезпеки. Вони переходять від реактивної моделі захисту інформації до проактивного виявлення загроз, і до 2030 року превентивні рішення складатимуть половину всіх світових витрат на безпеку [3].

В Україні, незважаючи на об'єктивні складнощі та повномасштабну війну, IT-сектор залишається однією з головних опор національної економіки. Галузь забезпечує від 3,4% до 4,4% ВВП країни, а за підсумками 2024 року обсяг експорту комп'ютерних послуг склав 6,4 млрд доларів США, що становить 37,4% від усього експорту послуг України [4]. Ринок продовжують очолювати такі сервісні гіганти як EPAM Systems (10,22 млрд грн виторгу) та GlobalLogic Україна (10,88 млрд грн) [5], проте індустрія активно трансформується у бік створення власних високомаржинальних продуктів. Цьому процесу сприяє функціонування унікального податкового та правового режиму Дія.City, який на початку 2026 року об'єднував понад 3700 компаній-резидентів. Ці компанії генерують стабільні надходження до бюджету, сплативши 65 мільярдів гривень податків за 2025 рік [6].

Феноменальний прогрес спостерігається у сфері електронного урядування (GovTech). Запуск наприкінці 2025 року Дія.AI – першого у світі національного урядового штучного інтелекту-помічника – докорінно змінив архітектуру взаємодії громадян з державою. Ця система здатна не просто надавати довідкову інформацію, але й самостійно ініціювати замовлення необхідних послуг від імені користувача [7]. Цифрова інфраструктура продовжує розвиватися: у 2026 році в Україні було розпочато пілотне впровадження мобільного зв'язку п'ятого покоління (5G) у трьох містах, що є критично важливим для забезпечення роботи просторових обчислень [8]. Окремим, надзвичайно динамічним вектором розвитку став сегмент оборонних технологій (DefenseTech). Координаційна платформа Brave1 консолідувала понад 3400 військово-технічних розробок від вітчизняних інженерів. Впровадження ШІ в системи наведення БПЛА (машинний зір) та розробка наземних роботизованих комплексів перетворили Україну на передовий глобальний майданчик для випробування військових інновацій у реальних бойових умовах, привертаючи десятки мільйонів доларів міжнародного венчурного капіталу [9].

Таким чином, інтеграція багатоагентного штучного інтелекту, гібридних обчислень та превентивних безпекових платформ є ключовим етапом сучасного розвитку глобального IT-сектору. Україна надзвичайно успішно адаптувалася до цих макротрендів, перетворивши IT-галузь на інструмент національної стійкості. Перспективи подальшого розвитку полягають у масштабуванні українських продуктових рішень на міжнародних ринках, поглибленні інтеграції ШІ у державні цифрові сервіси та остаточному закріпленні за державою статусу світового лідера у сфері GovTech та DefenseTech. Ключовими викликами залишаються необхідність утримання висококваліфікованого людського

капіталу та подальша розбудова енергонезалежної телекомунікаційної інфраструктури.

Список використаних джерел

1. *Gartner. (2026). Gartner forecasts worldwide IT spending to grow 10.8% in 2026, totaling $6.15 trillion. URL: https://shorturl.at/M6zEP*
2. *Gartner. (2024). Gartner identifies the top 10 strategic technology trends for 2025. URL: https://shorturl.at/DFT9l*
3. *Gartner. (2025). Gartner identifies the top strategic technology trends for 2026. URL: https://shorturl.at/QqWgZ*
4. *IT Ukraine Association. (2024). Digital Tiger: The Market Power of Ukrainian IT 2024. URL: https://itukraine.org.ua/files/DigitalTiger2024.pdf*
5. *DOU. (2026). Сукупний виторг найбільших IT-компаній України за 2025 рік становив 55,54 млрд грн. URL: https://shorturl.at/6qusI*
6. *Diia.City United. (2026). Diia.City turned four: Results and strategic priorities. URL: https://diiacityunited.org/en/diia-city-turned-four-results-and-strategic-priorities/*
7. *Міністерство цифрової трансформації України. (2026). Diia.AI: Building the architecture of an AI-native state. The Digital. URL: https://digitalstate.gov.ua/news/govtech/diiaai-building-the-architecture-of-an-ai-native-state*
8. *Укр.нет. (2026). Міністерство цифрової трансформації України: Підсумки 2026 року. URL: https://www.ukr.net/news/details/technologies/116267504.html*
9. *Міністерство цифрової трансформації України. (2025). Три роки незламності, боротьби та єдності – як Мінцифра працює в умовах повномасштабної війни. The Digital. URL: https://thedigital.gov.ua/news/progress/tri-roki-nezlamnosti-borotbi-ta-ednosti-yak-mintsifra-pratsyue-v-umovakh-povnomasshtabnoi-viyni*

Палагній Станіслав Олегович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
palagniystas@gmail.com

Бондарчук Олександр Павлович
викладач кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

UX/UI-ДИЗАЙН ЯК КЛЮЧОВИЙ ЧИННИК ЕФЕКТИВНОСТІ IoT-СИСТЕМ: ПРИНЦИПИ ПРОЄКТУВАННЯ ІНТЕРАКТИВНИХ ВЕБ-ІНТЕРФЕЙСІВ

Стрімке поширення Інтернету речей (IoT) трансформує не лише технологічну інфраструктуру, а й підходи до проєктування цифрових

інтерфейсів. За прогнозами аналітиків, глобальний ринок IoT-програмного забезпечення зростатиме зі щорічним темпом 24,7% і до 2029 року досягне понад 1,6 трлн доларів [1]. При цьому ефективність IoT-системи залежить не лише від якості апаратного чи програмного забезпечення, а й від того, наскільки зрозумілим і зручним є інтерфейс взаємодії з нею для кінцевого користувача.

Метою роботи є дослідження принципів UX/UI-дизайну, що визначають ефективність веб-інтерфейсів для IoT-систем, та визначення підходів до їх практичного застосування. Актуальність дослідження зумовлена тим, що IoT-інтерфейси принципово відрізняються від традиційних веб-додатків: вони мають взаємодіяти одночасно з множиною фізичних пристроїв, відображати потоки даних у реальному часі та забезпечувати стабільну роботу в умовах нестабільного з'єднання [2].

На відміну від класичного веб-дизайну, UX/UI для IoT-систем стикається з унікальними викликами. По-перше, користувач взаємодіє не з одним пристроєм, а з цілою екосистемою – смартфон, планшет, настінний дисплей, голосовий інтерфейс мають надавати когерентний досвід із єдиною візуальною мовою [3]. По-друге, IoT-інтерфейс має трансформувати складні технічні стани пристроїв у зрозумілу для нетехнічного користувача форму – наприклад, замість показника «напруга 220В» відображати просто «мережа стабільна» [4]. По-третє, реальний час накладає особливі вимоги до анімації та візуального зворотного зв'язку: користувач має миттєво розуміти, чи спрацювала його команда.

На основі аналізу сучасних підходів до проєктування IoT-інтерфейсів виокремлено п'ять ключових UX/UI-принципів, що безпосередньо впливають на ефективність таких систем (табл. 1).

Табл. 1

Ключові UX/UI-принципи для IoT-інтерфейсів та їх застосування

Принцип UX/UI	Зміст принципу	Застосування в IoT
Простота	Мінімалістичний інтерфейс без зайвих елементів	Одним натисканням керувати групою пристроїв
Консистентність	Єдина візуальна мова на всіх платформах	Однаковий вигляд дашборду на смартфоні та ПК
Зворотний зв'язок	Миттєве підтвердження дій користувача	Анімація підтвердження при вмиканні пристрою
Контекстність	Інтерфейс адаптується до поведінки користувача	Автоматичне відображення пріоритетних даних
Безпека	Прозорість у питаннях доступу та захисту даних	Чіткі індикатори стану підключення та шифрування

Особливу роль у проєктуванні IoT-інтерфейсів відіграють анімація та motion design. На відміну від суто декоративного застосування у маркетингових матеріалах, в IoT-контексті анімація виконує функціональну роль: підтверджує зміну стану пристрою, сигналізує про критичні події, візуалізує потоки даних між вузлами мережі. Дослідники UX-спільноти зазначають, що правильно реалізований motion design знижує когнітивне навантаження на користувача і прискорює прийняття рішень [5].

Практичне проєктування IoT-інтерфейсу передбачає дотримання системного підходу: спочатку визначається повний перелік користувацьких сценаріїв – від первинного налаштування пристрою до реагування на аварійний сигнал; потім для кожного сценарію проєктуються мікроінтеракції та анімаційні переходи відповідно до пріоритету дії. Наприклад, для сценарію «критична тривога» анімація має бути різкою та контрастною, тоді як для «штатне оновлення даних» – ненав'язливою та плавною [2].

Таким чином, UX/UI-дизайн є не допоміжним, а системоутворюючим елементом сучасних IoT-рішень. Ефективний інтерфейс визначає, чи буде технологічно досконала система прийнята користувачем, або залишиться незатребуваною через складність взаємодії. Виявлені принципи – простота, консистентність, зворотний зв'язок, контекстність і безпека – становлять методологічну основу для проєктування веб-інтерфейсів IoT-систем. Перспективою подальших досліджень є розробка типових UX-патернів для конкретних IoT-сценаріїв та їх верифікація шляхом юзабіліті-тестування.

Список використаних джерел

1. *A3Logics. (2025). Best Practices for UI/UX Design for IoT Apps.* https://www.a3logics.com/blog/ui-ux-for-iot-apps/

2. *Leverege. (2024). Design in IoT: UI and UX Considerations.* https://www.leverege.com/iot-ebook/ui-and-ux-design-iot

3. *Loop11. (2024). Enhancing IoT Impact Through Superior UX Design: A Comprehensive Guide.* https://www.loop11.com/enhancing-iot-impact-through-superior-ux-design-a-comprehensive-guide/

5. *Ramotion. (2025). IoT UX Design Best Practices.* https://www.ramotion.com/blog/iot-ux-design/

6. *UXmatters. (2024). Designing User Experiences for the Internet of Things.* https://www.uxmatters.com/mt/archives/2024/10/designing-user-experiences-for-the-internet-of-things.php

Khairulin Dmytrii Yuriiovych
5th-year student majoring in "Management of Information and Communication Activities"
State University of Information and Communication Technologies, Kyiv
st01239658@stud.duikt.edu.ua

Karpenko Olena Oleksiivna
PhD in Pedagogical Sciences, Associate Professor,
Associate Professor of the Department of Journalism and Information Activities
State University of Information and Communication Technologies, Kyiv
o.karpenko@duikt.edu.ua

ANALYSIS OF THE EFFECTIVENESS OF DIGITAL COMMUNICATION STRATEGIES FOR EDUCATIONAL SPECIALTIES IN THE GLOBAL INFORMATION SPACE

In the era of rapid digitalization, conventional methods of sharing information about educational opportunities are experiencing a radical transformation. Traditional university websites, long regarded as the exclusive hubs for verified data, are seeing their dominance decline. Today's applicants increasingly turn to social networking sites as their primary data sources. This shift is driven by the desire for instantaneous access to details regarding specific majors and the opportunity for direct, real-time interaction [8]. Consequently, evaluating how effectively particular educational programs are represented in the digital landscape is vital for maintaining their market relevance.

The core challenge lies in the fact that data provided on general university portals is frequently too bureaucratic and fails to resonate with the expectations of the modern youth. By leveraging SMM instruments, producing multifaceted digital content, and adopting a more relatable "humanized" communication style, institutions can go beyond mere information sharing to foster a genuine emotional connection with their audience [11, p. 2]. However, the absence of a synchronized strategy and a standardized aesthetic across various departments often results in a disjointed online presence. This fragmentation weakens the institution's brand identity and diminishes the public's confidence in the professional information provided.

The academic and practical value of this research stems from the necessity to create structured frameworks for promoting educational specialties as distinct brands within a coordinated communicative system. Moving from a basic "web presence" to a sophisticated digital engagement strategy allows academic institutions to adapt more fluidly to market shifts. Developing a cohesive visual and thematic identity in the global media arena is a fundamental component for both successful recruitment drives and the sustainable growth of academic programs.

This research aims to demonstrate the importance of an integrated strategy for marketing educational programs globally and to assess how modern digital platforms can be utilized to strengthen their market position. To reach this goal, several key objectives must be met: evaluating the current digital footprint of academic majors on

university sites to understand why they are becoming less effective than social media; exploring the analytical features of platforms like Facebook, Instagram, and Telegram for brand building; identifying how a standardized visual identity and content plan foster student engagement and trust; weighing the benefits of interactive communication against potential risks like loss of formal prestige; and outlining actionable steps for tracking digital performance to ensure long-term competitiveness.

An examination of how prominent Ukrainian universities – including Taras Shevchenko National University of Kyiv [10], Kyiv-Mohyla Academy [7], KNEU [6], Igor Sikorsky KPI [4], SUICT [9], and the Kyiv Aviation Institute [5] – interact with audiences on Facebook and Instagram reveals a wide spectrum of communication styles. These schools generally mix graphic design elements with actual photography of campus life and facilities. Notably, KAI and Kyiv-Mohyla Academy demonstrate the most disciplined application of brand identity guidelines [5], [7]. In contrast, institutions like KPI and KNEU often use a more varied and less consistent design approach, even when the university logo is present [4], [6]. The SUICT strategy stands out for its heavy reliance on a mixture of authentic photography and AI-generated imagery [9].

A particularly effective example of visual consistency can be found in the Faculty of PR, Journalism, and Information Policy at KNUKIM, which utilizes a distinctive red-themed grid, uniform typography, and a stable color palette [2]. Similarly, the "Economic Journalism" program at KNEU has experimented with a unique Instagram concept featuring specific green and yellow motifs, though this consistency sometimes wavered when student-led content was introduced [1]. These variations highlight the general lack of a universal standard for positioning academic programs and underscore the critical need for more robust, unified communication blueprints.

Modern social platforms offer sophisticated feedback loops and targeting capabilities that help build a compelling narrative around an educational specialty. Unlike traditional, non-interactive web pages, these platforms allow for dynamic content adjustments and precise audience segmentation. Utilizing built-in analytics helps administrators monitor public engagement instantly, making it possible to refine communication strategies based on what prospective students actually want.

Establishing a recognizable visual language and a strategic content plan is essential for connecting with the younger generation. A stable aesthetic–encompassing color schemes and post layouts–helps an educational brand stand out in a crowded digital feed and reinforces its credibility. By blending formal academic requirements with "live" elements like video testimonials and infographics, an educational program ceases to be merely a listing in a catalog and starts being perceived as a vibrant professional community.

Nevertheless, moving from formal web-based announcements to a "live" social media model introduces both opportunities and vulnerabilities. While the main benefit is the speed of engagement and immediate feedback, institutions must also navigate the

risks of losing academic decorum or facing public criticism [3, p. 2]. To mitigate these issues, a rigorous system of digital oversight is required. Such monitoring ensures high-quality interactions and provides the data necessary to evolve the educational brand's strategy over time.

In conclusion, this analysis confirms that in a digital-first world, the success of an educational program's positioning depends on active social media engagement rather than just static website listings. Implementing a synchronized visual style and a responsive communication model on platforms like Instagram and Telegram significantly boosts brand awareness and builds lasting trust with future students. Therefore, designing comprehensive communication strategies and maintaining consistent digital oversight are indispensable tools for any educational program aiming to thrive in today's competitive market.

References

1. *Economic Journalism KNEU (@economicjournalismkneu). (2025). Instagram. https://www.instagram.com/economicjournalismkneu/.*
2. *Faculty of PR, Journalism and Information Policy of KNUKIM. (2026). Instagram. https://www.instagram.com/fprjip_knukim.*
3. *Galioto, M., Pedone, F., Vantarakis, A., La Marca, A., & Bianco, A. (2025). University, social media, and student engagement: the challenge of "trust" in organizational communication. A voice from European university researchers to foster inclusion in higher education. Frontiers in Communication, 10. https://doi.org/10.3389/fcomm.2025.1546333.*
4. *Igor Sikorsky Kyiv Polytechnic Institute. (2026). Facebook. https://www.facebook.com/kpiua1898.*
5. *KAI University. (2026). Instagram. https://www.instagram.com/kai_university/.*
7. *Kyiv National Economic University named after Vadym Hetman. (2026). Instagram. https://www.instagram.com/kneu.edu.ua/.*
8. *National University of Kyiv-Mohyla Academy. (2026). Facebook. https://www.facebook.com/naukma.*
9. *Semerak, B. (2025, August 1). Can students depend on information gathered through social media platforms? Versii. https://versii.if.ua/novunu/chy-mozhut-studenty-pokladatysya-na-dani-otrymani-v-soczmerezhah/.*
10. *State University of Information and Communication Technologies. (2026). Facebook. https://www.facebook.com/duikt.edu.ua/.*
11. *Taras Shevchenko National University of Kyiv. (2026). Facebook. https://www.facebook.com/kyiv.university/.*
12. *Zintso, Y., & Fedoruk, M. (2025). Main types and formats of content for SMM. Economy and Society, 71. https://doi.org/10.32782/2524-0072/2025-71-86.*

Руденко Олександр Олександрович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
rudenkosasha40@gmail.com

Полоневич Ольга Володимирівна
кандидат технічних наук, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.polonevych@duikt.edu.ua

ІНФОРМАЦІЙНА СИСТЕМА ОНЛАЙН-БРОНЮВАННЯ ПОСЛУГ ТА КООРДИНАЦІЇ ВИКОНАВЦІВ ЧЕРЕЗ TELEGRAM-БОТ

Актуальність теми. У цифрову епоху ефективність сервісних служб безпосередньо залежить від швидкості передачі інформації між клієнтом та виконавцем. Традиційні методи фіксації замовлень (телефон, паперові журнали) часто призводять до втрати даних, помилок у розкладі та зниження якості обслуговування. Використання єдиної екосистеми JavaScript (Node.js) у поєднанні з нереляційними базами даних (MongoDB) дозволяє створити масштабовану систему, яка миттєво доставляє деталі замовлення з веб-сайту безпосередньо в Telegram-бот виконавця, забезпечуючи мобільність та високу швидкість координації польового персоналу.

Об'єкт та предмет дослідження. Об'єктом дослідження є процеси автоматизації збору клієнтських даних та управління виїзним персоналом. Предметом дослідження є архітектура взаємодії веб-інтерфейсу та месенджера Telegram на базі єдиного середовища виконання Node.js та документоорієнтованої бази даних MongoDB.

Система базується на єдиній мові програмування – JavaScript, що суттєво спрощує підтримку та інтеграцію компонентів. Client-side реалізовано у вигляді адаптивного веб-сайту на чистих HTML5/CSS3/JS із використанням fetch API для передачі даних на сервер. Server-side побудовано на платформі Node.js: сервер одночасно обробляє HTTP-запити від сайту та керує логікою Telegram-бота. Як сховище даних обрано MongoDB – NoSQL СУБД, що зберігає замовлення у форматі JSON-подібних документів. Інтерфейс бота реалізовано через бібліотеку telegraf .

Алгоритм функціонування системи. Процес взаємодії реалізовано у вигляді чотирьох послідовних етапів: (1) реєстрація замовлення – клієнт вводить ПІБ, номер телефону, адресу, тип послуги та обирає зручний час, після чого дані у форматі JSON надходять на API-ендпоінт сервера; (2) збереження – Node.js-

сервер за допомогою Mongoose валідує дані та записує їх у колекцію orders бази MongoDB із присвоєнням унікального _id та статусу "new"; (3) координація через бот – авторизований виконавець переглядає актуальні завдання через кнопку «Сьогоднішні записи»; (4) видача даних – бот формує картку замовлення з клікабельними посиланнями на навігатор та номером телефону клієнта.

Асинхронна природа Node.js забезпечує обробку великої кількості паралельних запитів без затримок. Гнучкість схем MongoDB дозволяє без міграцій додавати нові поля (наприклад, геолокацію або фото). Уніфікований формат JSON на всіх рівнях системи мінімізує витрати на конвертацію та парсинг.

Функціональні можливості Telegram-бота. Інтерфейс реалізовано за допомогою Reply Keyboards та Inline Buttons. Кнопка «Сьогоднішні записи» відображає список завдань поточної доби, відсортований за часом; кнопка «Всі записи» надає доступ до повної історії та майбутніх замовлень. При виборі конкретного запису виконавець отримує повний набір даних: ПІБ клієнта, точну адресу та опис проблеми.

Захист даних забезпечується валідацією вхідних даних на рівні Express-сервера, обмеженням доступу до бота за ідентифікатором чату (chatId) – виключно для зареєстрованих виконавців – та транзакційними гарантіями MongoDB щодо цілісності документів при пікових навантаженнях.

Висновки. Результатом роботи є повноцінна інформаційна система, яка автоматизує шлях замовлення від форми на сайті до мобільного пристрою майстра. Стек Node.js + MongoDB забезпечує легкість розгортання, високу продуктивність і готовність до подальшого розширення – додавання модулів онлайн-оплати, системи відгуків або push-сповіщень.

Список використаних джерел

1. *telegraf* - *telegraf.js - v4.16.3*
2. *Node.js* - *Index | Node.js v25.9.0 Documentation*
3. *MongoDB Compass* - *What is MongoDB Compass? - Compass - MongoDB Docs*
4. *JavaScript* - *JavaScript | MDN*

Грицанюк Дмитро Сергійович
студент 4 курсу
Державного університету інформаційно-комунікаційних технологій
(098) 484-86-44
dhrutsaniuk@gmail.com

Чутулян Вадим Олегович
старший викладач кафедри
технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м. Київ
vadymchytulian@gmail.com

РОЗРОБКА ТА ТЕСТУВАННЯ ВЕБ-ДОДАТКУ УПРАВЛІННЯ АВТОПАРКОМ НА ОСНОВІ DJANGO REST FRAMEWORK ТА REACT З TYPESCRIPT

Постановка задачі. Автоматизація управління автопарком приватного підприємства потребує програмного рішення, яке забезпечує оперативний облік транспортних засобів і водіїв, контроль витрат пального, реєстрацію ремонтів та формування аналітичних звітів. На відміну від комерційних систем класу Enterprise Fleet Management, що є економічно недоцільними для малих і середніх підприємств, спеціалізований веб-додаток на основі відкритих технологій дозволяє реалізувати необхідний функціонал без ліцензійних витрат та адаптувати його до специфічних вимог конкретного підприємства. Завданням даної роботи є практична реалізація та тестування веб-додатку для управління автопарком з підтвердженням відповідності реалізованого функціоналу визначеним функціональним і нефункціональним вимогам.

Мета дослідження. Реалізувати повнофункціональний веб-додаток для управління автопарком приватного підприємства з використанням Python (Django, Django REST Framework) на серверній стороні та TypeScript (React) на клієнтській стороні, налаштувати відтворюване середовище розгортання на основі Docker Compose та підтвердити відповідність реалізованої системи нефункціональним вимогам через тестування.

Результати.

Реалізація серверної частини. Серверну частину реалізовано на Django 5 з розширенням Django REST Framework. Бізнес-логіку виділено у Service Layer – окремий шар класів, що не залежить від HTTP-рівня. Зокрема, FuelService реалізує алгоритм автоматичного виявлення аномального споживання пального: для кожного запису заправки обчислюється фактична витрата (л/100 км) та порівнюється з нормативним значенням, визначеним для конкретного транспортного засобу; відхилення понад 15 % позначається як аномалія і відображається на дашборді. VehicleService керує станами транспортного засобу

(активний, у ремонті, списаний) та валідує переходи між станами. REST API реалізовано через DRF ViewSets і охоплює 27 ендпоінтів, згрупованих у п'ять ресурсних колекцій з версіонуванням через HTTP-заголовок Accept.

Реалізація клієнтської частини. Frontend реалізовано як SPA на React 18 з TypeScript. Маршрутизацію забезпечує React Router v6, управління серверним станом – React Query. Весь HTTP-трафік проходить через централізований Axios-клієнт, що автоматично додає JWT-заголовок та обробляє оновлення access-токена через refresh-токен без втручання користувача. Дашборд відображає зведену статистику по автопарку: кількість активних ТЗ, записи аномальних витрат пального та найближчі планові ТО. Модуль звітності формує аналітику у розрізі транспортних засобів, водіїв та часових періодів. Multi-stage Docker build скоротив розмір виробничого образу серверної частини з приблизно 800 до 180 МБ. У табл. 1 наведено результати перевірки нефункціональних вимог.

Табл. 1

Відповідність реалізованої системи нефункціональним вимогам

ID	Вимога	Порогове значення	Статус
NFR-01	Час відгуку API (p95)	≤ 300 мс	Виконано (індекси PostgreSQL)
NFR-04	Відповідність OWASP Top 10	Повна	Виконано (DRF + PBKDF2 + RBAC)
NFR-06	Кількість команд розгортання	≤ 3 команди	Виконано (Docker Compose)
NFR-07	Тестове покриття бізнес-логіки	≥ 70 %	Виконано (87 %)

Тестування системи. Набір із 41 тесту (23 модульних + 18 інтеграційних) охоплює сервісний шар та REST API-ендпоінти. Модульні тести написано з використанням pytest та factory-boy для генерації тестових даних; кожен тест ізольовано від бази даних через DRF APIClient. Інтеграційні тести перевіряють коректність RBAC-матриці: зокрема, підтверджено, що водій отримує лише власні записи заправок незалежно від параметрів HTTP-запиту. Загальне покриття бізнес-логіки за результатами pytest-cov становить 87 %, що перевищує встановлений поріг NFR-07 (70 %). Усі дев'ять функціональних вимог групи «Першочергово» реалізовано в повному обсязі.

Висновки. Розроблено повнофункціональний веб-додаток для управління автопарком приватного підприємства на основі Django REST Framework та React з TypeScript. Застосування Service Layer дозволило ізолювати бізнес-логіку розрахунку витрат пального та управління станами транспортних засобів від HTTP-шару, що безпосередньо забезпечило досягнення тестового покриття 87 %. Multi-stage Docker build скоротив розмір виробничого образу більш ніж у чотири

рази. Реалізований алгоритм автоматичного виявлення аномального споживання пального дозволяє підприємству оперативно ідентифікувати відхилення витрат від норми без ручного аналізу даних. Система повністю відповідає всім семи нефункціональним вимогам, включно з часом відгуку API на рівні 95-го перцентиля не більше 300 мс та відповідністю стандарту OWASP Top 10.

Список використаних джерел

1. Django Software Foundation. Django documentation. URL: https://docs.djangoproject.com/en/6.0/

2. Django REST Framework. URL: https://www.django-rest-framework.org/

3. Meta Open Source. React documentation. URL: https://react.dev/

4. pytest Development Team. pytest documentation. URL: https://docs.pytest.org/

5. Docker Inc. Docker Compose documentation. URL: https://docs.docker.com/compose/

Гришко Карина Віталіївна
студентка 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st8089870@stud.duikt.edu.ua

Шахматов Іван Олександрович
викладач кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

СИСТЕМА КЕРУВАННЯ ОНЛАЙН-ЗАМОВЛЕННЯМИ ТА ЛОГІСТИКОЮ МОВОЮ PYTHON

Сучасна електронна торгівля набирає обертів, зараз постає завдання розробки дієвих механізмів для управління замовленнями у мережі та налагодження логістичних операцій. Платформи дають змогу автоматизувати процес опрацювання запитів, вдосконалити транспортування вантажів та покращити рівень сервісу для споживачів [1].

Софт для управління замовленнями в мережі містить ключові частини: блок опрацювання запитів, складова управління запасами, частина для організації перевезень та лицьова панель для споживача. Спільна робота елементів гарантує проходження повного ланцюжка обробки запиту, а саме з моменту його оформлення і до вручення покупцеві.

Для втілення цієї системи найліпше використовувати Python, адже вона пропонує багатий арсенал бібліотек для взаємодії з базами даних, веброзробки та

аналізу даних. Конкретно, застосування таких фреймворків як Django чи Flask дає змогу миттєво збудувати бекенд проєкту [2]. На рис.1 представлено узагальнену архітектуру системи керування онлайн-замовленнями та логістикою.

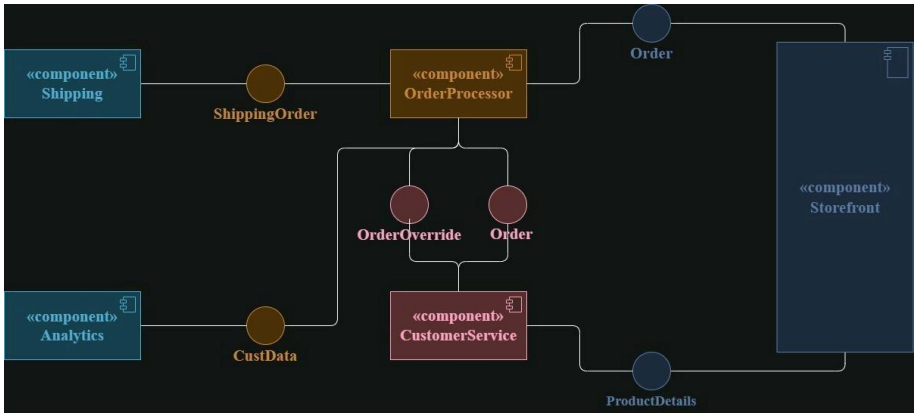

Рис. 1. Архітектура системи керування онлайн-замовленнями [2]

Принцип функціонування системи такий: клієнт розміщує своє замовлення через інтернет-інтерфейс, інформація надсилається на сервер, де її обробляють та фіксують у сховищі даних. Після цього логістичний компонент розраховує найкращий шлях для транспортування, беручи до уваги територіальні, і часові обмеження.

Аби вдосконалити процеси логістики, цілком можливо використовувати методики знаходження найкращого маршруту, зокрема, алгоритм Дейкстри чи A* [3]. Це дає змогу звести до мінімуму затрати часу та матеріальних засобів під час перевезення продукції. У табл. 1 представлені ключові функції, які під силу цій системі.

Табл. 1

Функціональні можливості системи

Модуль	Опис
Обробка замовлень	Прийом, редагування та збереження замовлень
Склад	Облік товарів та залишків
Логістика	Планування маршрутів доставки
Аналітика	Аналіз ефективності роботи системи

Впровадження подібної архітектури надає змогу суттєво наростити продуктивність бізнес-операцій, мінімізувати рівень хибних дій, та удосконалити рівень сервісу для споживачів. Також Python гарантує адаптивність та можливість розширення розробленого продукту [4].

Таким чином, інкорпорація систем для управління прийманням замовлень через інтернет та логістичними потоками є важливим етапом для прогресу нинішніх підприємств, особливо у контексті переходу до цифрових технологій.

Список використаних джерел

1. Laudon, K. C., Laudon, J. P., Pearson Higher Ed,, Management Information Systems: Managing the Digital Firm, 2021. С. 78–85, 392–400 https://books.google.com.ua/books/about/Management_Information_Systems_Managing.html?id=4b4zEAAAQBAJ&redir_esc=y

2. Holovaty, A., Kaplan-Moss, J., Apress Berkeley, The Definitive Guide to Django, 2009. С. 3–15, 95–110 https://link.springer.com/book/10.1007/978-1-4302-1937-8

3. Cormen, T. H., Leiserson, C. E., Rivest, R. L., Stein, C., The MIT Press, Introduction to Algorithms, 2009, С. 657–673 https://www.cs.mcgill.ca/~akroit/math/compsci/Cormen%20Introduction%20to%20Algorithms.pdf

4. Matthes, E., No Starch Press, Python Crash Course, 2022, С. 241–260 https://nostarch.com/python-crash-course-3rd-edition#reviews

Ніколін Кирило Андрійович
студент 4 курсу
спеціальності «Інженерія програмного забезпечення»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kirillnikolin@gmail.com

Жебка Вікторія Вікторівна
доктор технічних наук, професор, завідувач кафедри
Технології цифрового розвитку
Державного університету
інформаційно-комунікаційних технологій, м. Київ
v.zhebka@duikt.edu.ua

РОЗРОБКА КРОСПЛАТФОРМНОЇ СИСТЕМИ УПРАВЛІННЯ ЛАБОРАТОРНИМИ ДОСЛІДЖЕННЯМИ «MONOLAB»

Цифрова трансформація охорони здоров'я – HELSI, eHealth, електронні рецепти - за останні роки в медицині дійсно багато змінилось. Але це якщо говорити про великі заклади. Маленька приватна лабораторія живе у зовсім іншій реальності: запис по телефону, результати скидають у Viber, дані ніде не зберігаються централізовано. Пацієнт просто чекає – коли подзвонять. Персонал витрачає купу часу на ручну комунікацію замість роботи [1].

Постановка проблеми

У рамках дипломної роботи було розроблено проект «Monolab» - цифрову платформу для умовної приватної медичної лабораторії. Вихідна проблема, яку я моделював: персонал витрачає багато часу на ручну комунікацію з пацієнтами, результати можуть затриматись або не дійти взагалі, а самі пацієнти не мають жодного способу відстежити статус своїх аналізів – тільки чекати дзвінка.

Якщо подивитись на те що вже є – Synevo і ДІЛА мають мобільні рішення, однак із суттєвими обмеженнями. Додаток Synevo недоступний для українського ринку. ДІЛА перезапустила свій додаток у березні 2026 року – там є онлайн-запис, перегляд результатів і push-сповіщення, але відсутня динаміка медичних показників у часі. Повного циклу з аналітикою динаміки та верифікованим PDF я не знайшов у жодному публічному рішенні для невеликої лабораторії [2, 3].

Табл. 1

Порівняння з конкурентами

Критерій	Synevo	ДІЛА	Monolab
Онлайн-запис	Так	Так	Так
Результати онлайн	Так	Так	Так
Push-сповіщення	Частково	Так	Так (FCM)
Динаміка показників	Ні	Ні	Так (графіки)
Повний мобільний цикл	Ні (недоступний в Україні)	Частково	Так
Self-hosted / відкритий код	Ні	Ні	Так
Аудит-лог дій	Ні	Ні	Так

Мета та завдання дослідження

Мета роботи – розробити цифрову екосистему для медичної лабораторії, яка охоплює повний операційний цикл: від запису пацієнта до доставки верифікованих результатів на смартфон, при цьому забезпечуючи зручні інструменти для персоналу лабораторії.

Конкретно я мав реалізувати: монорепозиторій з єдиною TypeScript-кодовою базою для трьох застосунків; REST API з рольовим доступом; веб-панель для персоналу де все оновлюється в реальному часі; і мобільний застосунок де пацієнт отримує push і може відкрити PDF із результатом.

Результати розробки

Я організував проект як монорепозиторій на pnpm workspaces – три застосунки в одному репозиторії: API на Node.js + Express, веб-кабінет на React і мобільний на React Native + React Native CLI [7]. Спільна TypeScript-кодова база дала одну просту річ: коли міняєш структуру API – одразу бачиш де у веб і mobile щось поламалось, ще до запуску. Купа помилок відловлюється на етапі компіляції, а не в рантаймі.

Табл. 2

Стек технологій

Шар	Технологія	Обґрунтування
Мова	TypeScript	Єдина екосистема для API, web і mobile; типобезпека
Backend	Node.js + Express	Легковісний, JSON-нативний, великий npm-екосистем
База даних	PostgreSQL 16 + Prisma	Реляційна структура, транзакції, типізовані запити
Web	React 19 + Ant Design	Компонентний підхід, готові UI-компоненти
Mobile	React Native + React Native CLI	Кросплатформно iOS + Android, спільна JS-логіка
Авторизація	JWT access + refresh	Stateless, підходить для web і mobile одночасно
Файли (PDF)	MinIO (S3)	Self-hosted сховище, не навантажує основну БД
Push	Firebase FCM	Стандарт для iOS/Android push-сповіщень

Для зберігання даних обрано PostgreSQL 16 у зв'язці з Prisma ORM. PostgreSQL тут очевидний вибір – медичні дані по суті є ланцюжком: пацієнт, його запис, зразок, результат, окремі тести [5]. Це типова реляційна структура де транзакції реально потрібні, особливо при оплаті. Prisma забезпечує типізовані запити і гнучку систему міграцій при зміні структури аналізів [4].

Безпека реалізована через JWT із двома токенами (access з TTL 1 год і refresh на 30 днів) та RBAC-middleware. Система підтримує три ролі: пацієнт, лаборант і адміністратор – кожна з чітко обмеженим набором дозволів. Усі критичні дії фіксуються в audit log разом із IP-адресою та user agent.

Найбільше часу в розробці зайшло на real-time синхронізацію. Я підключив WebSocket і тепер статуси зразків у веб-панелі оновлюються самі - адміністратор бачить актуальну чергу без жодних перезавантажень сторінки. Мобільні push-сповіщення реалізовано через Firebase Cloud Messaging: пацієнт отримує сповіщення на телефон щойно лаборант верифікував результат [6].

PDF-бланки результатів генеруються на сервері за допомогою PDFKit і зберігаються у MinIO – S3-сумісному об'єктному сховищі. Це дозволяє розвантажити основну базу даних і забезпечити швидкий доступ до архівних документів навіть при нестабільному мобільному з'єднанні. Вся інфраструктура контейнеризована через Docker Compose, що спрощує розгортання.

Тестування показало, що час від введення результату лаборантом до моменту коли пацієнт його отримав скоротився приблизно на 30% порівняно з попереднім процесом – телефон плюс пересилання файлів у месенджерах. Рис. 1 демонструє головну сторінку кабінету лаборанта, де відображається поточна черга, навантаження зміни та сповіщення в реальному часі.

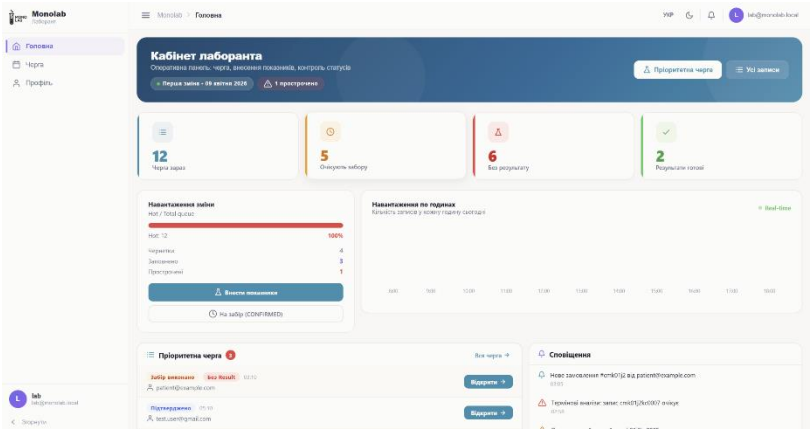

Рис. 1. Головна сторінка кабінету лаборанта у веб-панелі платформи «Monolab»

Висновки

Розроблена платформа «Monolab» демонструє, що невеликий медичний заклад може отримати повноцінну цифрову інфраструктуру без прив'язки до дорогих комерційних рішень. TypeScript-монорепозиторій з єдиною кодовою базою для API, веб і mobile виявився вдалим архітектурним підходом для проектів із кількома клієнтами, де важлива узгодженість типів даних. Практичні результати підтвердили ефективність обраних рішень: скорочення операційного часу, усунення паперового документообігу і підвищення доступності медичних послуг для пацієнтів.

Перспективи розвитку системи включають інтеграцію з державним реєстром eHealth, додавання модуля аналітики динаміки медичних показників у мобільному застосунку та впровадження біометричної авторизації.

Список використаних джерел

1. Лановий, О., & Заїка, А. (2022). Цифрова трансформація системи охорони здоров'я України: виклики та перспективи. Вісник НТУУ «КПІ». Серія «Інформатика, управління та обчислювальна техніка», 75, 12–19.

2. Synevo Romania. (2026). Synevo Mobile App. Google Play Store. https://play.google.com/store/apps/details?id=com.mysynevo&hl=uk

3. ДІЛА. (2026). Мобільний застосунок ДІЛА. Google Play Store. https://play.google.com/store/search?q=%D0%94%D1%96%D0%BB%D0%B0&c=apps&hl=uk / App Store. https://apps.apple.com/us/app/d%D1%96%D0%BB%D0%B0/id1423583919

4. Prisma. (2024). Prisma ORM documentation. https://www.prisma.io/docs

5. PostgreSQL Global Development Group. (2023). PostgreSQL 16 documentation. https://www.postgresql.org/docs/16/

6. Google LLC. (2024). Firebase Cloud Messaging documentation. https://firebase.google.com/docs/cloud-messaging

7. Meta Platforms. (2024). React Native documentation. https://reactnative.dev/docs/getting-started

Лук'янов Владислав Юрійович
студент групи ІСД-42
Державного університету
інформаційно-комунікаційних технологій
+380 68 464 43 93
vladlukyanov.30@gmail.com

Бондарчук Олександр Павлович
викладач кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних-комунікаційних технологій, м.Київ
o.bondarchuk@duikt.edu.ua

ЗАСТОСУВАННЯ ЧАТ-БОТ ТЕХНОЛОГІЙ У МОВНІЙ ОСВІТІ: РОЗРОБКА TELEGRAM-БОТА ДЛЯ ВИВЧЕННЯ ІНОЗЕМНИХ МОВ ЗАСОБАМИ PYTHON

У сучасному цифровому освітньому середовищі чат-боти поступово переходять із допоміжних сервісів у повноцінні інструменти організації навчання. Їхня актуальність у мовній освіті зумовлена доступністю месенджерів, постійною взаємодією з користувачем та можливістю пропонувати короткі персоналізовані завдання без встановлення спеціалізованого програмного забезпечення. Метою цих тез є обґрунтування доцільності застосування чат-бот технологій для підтримки вивчення іноземних мов і визначення особливостей розробки Telegram-бота засобами Python. Дослідження у сфері навчальних чат-ботів засвідчують, що такі системи можуть підтримувати автономне навчання, підвищувати залученість здобувачів освіти та створювати умови для регулярної мовної практики [1], [2], [4].

Для реалізації такого рішення доцільно використовувати платформу Telegram, оскільки офіційний Telegram Bot API надає засоби для обміну повідомленнями, використання вбудованих кнопок, мультимедійного контенту, команд і механізмів інтеграції через polling або webhook, що дає змогу будувати гнучкі навчальні сценарії [5]. Мова Python є зручною технологічною основою завдяки зрозумілому синтаксису, розвиненій екосистемі бібліотек і широким можливостям для роботи з мережевими запитами, базами даних, асинхронною логікою та тестуванням програмних модулів [3]. Поєднання Telegram і Python забезпечує швидке прототипування системи, спрощує подальшу підтримку програмного коду та дозволяє масштабувати бот для ширшого кола користувачів.

Функціональна модель Telegram-бота для вивчення іноземних мов може включати реєстрацію користувача, вибір мови й рівня підготовки, подання нової лексики, тренування граматичних конструкцій, виконання тестових завдань, перевірку відповідей, повторення складних тем і накопичення статистики успішності. Доцільно реалізувати модулі словникових карток, тематичних діалогів, мінітестів і щоденних нагадувань, що підтримують формат мікронавчання. У такому

випадку користувач отримує невеликі порції навчального матеріалу у звичному середовищі месенджера, а сам бот виступає посередником між навчальним контентом і повсякденними цифровими практиками студента.

Важливою перевагою чат-бота є персоналізація навчання. На основі попередніх відповідей система може змінювати складність вправ, повторювати проблемні теми, варіювати формат завдань і пропонувати індивідуальну траєкторію опрацювання матеріалу. Для мовної освіти особливо цінною є можливість багаторазового безпечного тренування, коли користувач отримує миттєвий зворотний зв'язок, працює у власному темпі та не боїться помилитися під час взаємодії з програмою. Наукові огляди підтверджують, що ефективність навчальних чат-ботів значною мірою залежить від якості педагогічного дизайну, чіткості сценаріїв взаємодії та відповідності контенту поставленим освітнім цілям [1], [2].

Під час проєктування такого програмного засобу необхідно враховувати не лише технічну, а й методичну складову. Контент повинен відповідати рівню володіння мовою, вправи мають містити зрозумілі критерії оцінювання, а інтерфейс повинен бути інтуїтивним і не перевантаженим зайвими командами. Практично доцільно передбачити збереження історії навчання, систему балів або досягнень, формування короткої аналітики для користувача та можливість оновлення навчального контенту без зміни базової логіки бота. Перспективним напрямом розвитку є інтеграція елементів штучного інтелекту для автоматичної адаптації складності завдань, пояснення типових помилок і підтримки більш природного діалогу з користувачем.

Отже, застосування чат-бот технологій у мовній освіті є актуальним напрямом розвитку сучасних інформаційних технологій. Telegram-бот, розроблений засобами Python, поєднує доступність, функціональність і зручність використання, що робить його ефективним інструментом підтримки вивчення іноземних мов. Запропонований підхід може бути використаний як для індивідуального навчання, так і як допоміжний цифровий сервіс у межах формальної освіти. Подальший розвиток таких систем доцільно пов'язувати з поглибленою персоналізацією, аналізом навчальних результатів і впровадженням інтелектуальних механізмів підтримки користувача.

Список використаних джерел

1. Huang, W., Hew, K. F., & Fryer, L. K. (2022). Chatbots for language learning - Are they really useful? A systematic review of chatbot-supported language learning. Journal of Computer Assisted Learning, 38(1), 237-257. https://doi.org/10.1111/jcal.12610

2. Okonkwo, C. W., & Ade-Ibijola, A. (2021). Chatbots applications in education: A systematic review. Computers and Education: Artificial Intelligence, 2, 100033. https://doi.org/10.1016/j.caeai.2021.100033

3. Python Software Foundation. (2026). Python 3 documentation. https://docs.python.org/3/

4. Smutny, P., & Schreiberova, P. (2020). Chatbots for learning: A review of educational chatbots for the Facebook Messenger. Computers & Education, 151, 103862. https://doi.org/10.1016/j.compedu.2020.103862

5. Telegram. (n.d.). Telegram Bot API. https://core.telegram.org/bots/api

Далькевич Денис Олександрович
студент 4 курсу
Державного університету інформаційно-комунікаційних технологій
den921524@gmail.com

Чернявський Ждан Анатолійович
старший викладач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ З НАСКРІЗНИМ ШИФРУВАННЯМ НА БАЗІ ASP.NET CORE ТА ANGULAR

Постановка задачі.

В сучасному світі системи обміну миттєвими повідомленнями стикаються з основною проблемою - забезпечення конфіденційності користувачів. Звичайні месенджери використовують транспортне шифрування (TLS/SSL), в результаті чого сервер має доступ до незашифрованого контенту повідомлень. Такий сценарій при компрометації серверної інфраструктури створює ризики витоку конфіденційної інформації або несанкціонованого доступу адміністраторів. Для захисту приватності користувачів виникає потреба застосування наскрізного шифрування (End-to-End Encryption, E2EE) [2], при якому криптографічні ключі зберігаються виключно на пристроях користувачів, а сервер лише виконує функцію пересилання зашифрованих повідомлень без можливості їх розшифрування.

Мета дослідження.

Метою даного проєкту є розробка та реалізація веб-застосунку для обміну миттєвими повідомленнями з інтегрованим наскрізним шифруванням на базі технологій ASP.NET Core та Angular, що забезпечує максимальний рівень конфіденційності листування при збереженні зручності використання та високої продуктивності в реальному часі.

Результати.

В результаті розроблено систему обміну повідомленнями, яка інтегрує технологію SignalR для двостороннього зв'язку в реальному часі з криптографічним модулем на основі алгоритму AES-256 (Advanced Encryption Standard) в режимі CBC (Cipher Block Chaining) [5]. Алгоритм забезпечує наскрізне шифрування всіх текстових повідомлень та файлів, гарантуючи що лише відправник та отримувач мають доступ до незашифрованого контенту.

Архітектура криптографічного модуля побудована на принципі Zero-Knowledge - сервер не має доступу до ключів шифрування. Майстер-ключ зберігається виключно на стороні клієнта і ніколи не передається на сервер. Для кожного повідомлення генеруються унікальні криптографічні параметри, які

унеможливлюють розшифрування навіть при отриманні зашифрованих даних з бази даних.

Для забезпечення криптографічної стійкості застосовано алгоритм AES-256, затверджений NIST (National Institute of Standards and Technology) [5]. AES-256 використовує 256-бітний ключ, що забезпечує 2^{256} можливих комбінацій, роблячи brute force атаки практично неможливими [4] (табл. 1).

Табл. 1.

Порівняльна характеристика методів шифрування

Параметр	**TLS/SSL**	**E2EE (AES-256-CBC)**
Доступ сервера до контенту	Так	Ні
Захист при компрометації сервера	Ні	Так
Криптографічна стійкість ключа	128-256 біт	256 біт
Можливість масового стеження	Так	Ні
Складність реалізації	Низька	Висока
Латентність шифрування	< 1 мс	2-5 мс

Для кожного повідомлення генеруються унікальні криптографічні параметри: вектор ініціалізації (IV, 128 біт) та сіль (Salt, 256 біт). На основі Salt через PBKDF2 з 100 000 ітерацій деривується сесійний ключ. Відправник шифрує текст алгоритмом AES-256-CBC та передає структуру {content, IV, Salt} через SignalR Hub; сервер зберігає зашифровані дані без можливості розшифрування; отримувач деривує ключ з того ж Salt та дешифрує повідомлення [3] (рис. 1).

Рис. 1. Схема обміну зашифрованими повідомленнями (E2EE)

Інтеграція з SignalR забезпечує доставку зашифрованих повідомлень у реальному часі з мінімальною затримкою (< 100 мс). SignalR Hub маршрутизує повідомлення до конкретних користувачів або груп без розшифрування контенту. Авторизація реалізована через JWT-токени що зберігаються в HttpOnly cookie з атрибутами Secure та SameSite=Strict [1].

Тестування через Chrome DevTools Performance Profiler показало стабільні 60 FPS при CPU throttling 4x, затримку доставки повідомлень менше 100 мс та Cumulative Layout Shift 0.08, що відповідає стандартам Google Core Web Vitals.

Висновки.

Розроблена система обміну повідомленнями з наскрізним шифруванням на базі AES-256-CBC демонструє високий рівень безпеки при збереженні прийнятної продуктивності для роботи в реальному часі. Принцип Zero-Knowledge гарантує що навіть при повній компрометації серверної

інфраструктури відкритий текст повідомлень залишається недоступним. Використання динамічних параметрів IV та Salt з функцією деривації ключа PBKDF2 забезпечує захист від сучасних криптографічних атак [2].

В подальшому можть бути розроблені слідуючі напрямки - впровадження протоколу Diffie-Hellman для Perfect Forward Secrecy [3], інтеграція цифрових підписів для верифікації відправника та підтримка групового шифрування.

Список використаних джерел

1. *Docs M. SignalR documentation. URL: https://learn.microsoft.com/en-us/aspnet/core/signalr/.*
2. *Katz J., Lindell Y. Introduction to modern cryptography. CRC Press, 2020. 640 c.*
3. *Marlinspike M., Perrin T. The double ratchet algorithm. URL: https://signal.org/docs/specifications/doubleratchet/.*
4. *Schneier B. Applied cryptography: protocols, algorithms and source code in C. Wiley, 2015. 784 c.*
5. *Standards N. I. o., Technology. Advanced encryption standard (AES). 2001. 51 c.*

Теслюк Віктор Євгенович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
tesluk.ve@duikt.edu.ua

РОЛЬ ERP-СИСТЕМ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ СУЧАСНИХ БІЗНЕС-ПРОЦЕСІВ

У сучасних умовах глобалізації та жорсткої конкуренції підприємства змушені функціонувати в середовищі постійних змін. До основних викликів належать швидкий розвиток технологій, динамічність споживчого попиту та посилення регуляторного контролю. За таких обставин для підтримання стабільності й збереження конкурентних позицій компаніям необхідні дієві інструменти управління ресурсами, бізнес-процесами та інформаційними потоками. Одним із таких інструментів є ERP-системи (Enterprise Resource Planning), які об’єднують різні функціональні підрозділи підприємства в єдину систему та забезпечують централізований доступ до актуальних даних у реальному часі.

Застосування ERP-рішень дозволяє підвищити гнучкость організації та ефективність її діяльності. Вони сприяють удосконаленню бізнес-процесів, покращенню рівня обслуговування клієнтів і підтримують ухвалення зважених управлінських рішень на стратегічному рівні. Їх значущість доцільно розглядати за такими основними напрямами як:

1. Стандартизація бізнес-процесів. Системи забезпечують уніфікацію процесів у межах організації, гарантуючи послідовність виконання та дотримання кращих практик. Такий процес мінімізує помилки, виконує підвищення якісті продукції та послуг а також посилює контроль.

2. Зростання операційної результативності. Впровадження автоматизованих рішень для виконання типових операцій та вдосконалення бізнес-процесів сприяє істотному підвищенню продуктивності підприємства. Зокрема, використання систем автоматизованого планування виробництва дає змогу мінімізувати простої, раціональніше залучати наявні ресурси та, як наслідок, скорочувати витрати й підвищувати загальну ефективність діяльності.

3. Управління на основі аналітичних даних. ERP-рішення забезпечують оперативний доступ до актуальної інформації, що створює підґрунтя для прийняття виважених управлінських рішень. Опрацювання ключових показників ефективності, фінансових індикаторів і застосування інструментів прогнозування дозволяє оцінювати потенційні ризики, передбачати зміну попиту та знаходити перспективні напрями розвитку бізнесу.

4. Покращення взаємодії з клієнтами. Завдяки інтеграції CRM-компонентів ERP-системи забезпечують більш ефективне управління клієнтськими відносинами. Фахівці з продажу отримують повну інформацію про попередні контакти, потреби та запити клієнтів, що дозволяє індивідуалізувати підхід, оперативно реагувати на звернення та підвищувати рівень задоволеності й довіри споживачів [2].

5. Забезпечення відповідності вимогам та мінімізація ризиків. ERP-системи сприяють дотриманню нормативних стандартів завдяки точному обліку, формуванню аудиторських журналів і автоматизації процесів звітності. Наприклад, організації, що працюють у межах вимог GDPR, можуть ефективно контролювати обробку персональних даних. Вбудовані механізми контролю дозволяють знижувати ймовірність операційних помилок і запобігати шахрайським діям.

6. Раціональне використання ресурсів і зниження витрат. ERP-рішення допомагають оптимально розподіляти фінансові, матеріальні та трудові ресурси. Моніторинг використання сировини дозволяє уникати як надлишків, так і дефіциту, а інструменти контролю витрат сприяють скороченню втрат, підвищенню ефективності операцій і зростанню прибутковості підприємства [3].

Аналіз показав, що ERP-системи має ключову роль у діяльності сучасних підприємств, сприяючи підвищенню результативності роботи, розвитку інновацій та зміцненню конкурентних позицій. Об’єднання інформації в єдиному середовищі, автоматизація бізнес-процесів і можливість оперативного аналізу даних дають змогу компаніям ефективніше організовувати свою діяльність і приймати зважені управлінські рішення. Узагальнення їхніх функціональних

можливостей, переваг і проблем впровадження підтверджує вагомий вплив ERP-рішень на стабільний розвиток і довгострокову ефективність бізнесу.

Список використаних джерел

1. *Huang, T. & Yasuda, K. Comprehensive review of literature survey articles on ERP. Business Process Management Journal.*
2. *Оксамитна Л. П., Пряха Р. І. Особливості сучасних ERP-систем управління бізнес-процесами підприємства. Управління розвитком складних систем, 2022.*
3. *Markuts V., Kyzenko O. ERP system as a tool for ensuring the rational use of company resources. Scientific Notes (KNEU), 2023.*

Романчук Станіслав Дмитрович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
romanchukstanislav21@gmail.com

Ткаленко Оксана Миколаївна
доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
tkalenko-oksana888@ukr.net

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ БРОНЮВАННЯ ГОТЕЛЬНИХ НОМЕРІВ З ВИКОРИСТАННЯМ МОВИ ПРОГРАМУВАННЯ PYTHON

На сьогодні інформаційні технології досить активно впроваджуються у різні сфери діяльності людини і готельний бізнес не є винятком. Якщо раніше більшість процесів виконувались вручну, то зараз усе більше підприємств переходять до автоматизованих систем, які значно спрощують роботу персоналу. Особливо це стосується бронювання номерів, адже саме цей процес є одним із основних у діяльності будь-якого готелю.

З розвитком Інтернету користувачі почали віддавати перевагу онлайн-бронюванню. Це зручно, швидко і не потребує додаткових зусиль, таких як дзвінки або особисті візити. У той же час традиційні способи ведення обліку, наприклад, записи у журналах або навіть таблиці, вже не можуть забезпечити потрібну швидкість і точність. Через це можуть виникати помилки, наприклад, подвійне бронювання або втрата інформації. Саме тому, виникає потреба у створенні спеціалізованих інформаційних систем.

Актуальність даної теми полягає в тому, що автоматизація процесу бронювання дозволяє значно покращити роботу готелю. Це стосується не тільки зручності для клієнтів, а й оптимізації внутрішніх процесів. Система дозволяє швидко отримати інформацію про вільні номери, їх вартість та інші характеристики. Крім того, вона дає можливість зберігати історію бронювань, що може бути корисним для подальшого аналізу.

Для реалізації такої системи досить часто використовується мова програмування Python. Вона є популярною завдяки своїй простоті та зрозумілості, особливо для початківців. Але при цьому Python має достатньо можливостей для створення повноцінних веб-додатків. Наприклад, за допомогою фреймворків Flask або Django можна реалізувати серверну частину системи, яка буде обробляти запити користувачів. Як правило, система бронювання складається з кількох основних частин. По-перше, це інтерфейс користувача, через який відбувається взаємодія. По-друге, серверна частина, де реалізована логіка роботи. І, звичайно, база даних, де зберігається вся інформація. Усі ці компоненти працюють разом і забезпечують коректну роботу системи.

Однією з найважливіших функцій є перевірка доступності номерів. Це означає, що система повинна “розуміти” чи вільний номер у певний період часу. Для цього враховуються вже існуючі бронювання. Якщо все реалізовано правильно, то можна уникнути ситуацій, коли один номер заброньовано двічі. Також важливо передбачити можливість змінювати або скасовувати бронювання, оскільки такі ситуації трапляються досить часто. Крім цього, система повинна дозволяти працювати з інформацією про номери. Наприклад, змінювати ціну, статус або опис. Це важливо для адміністратора, який керує готелем. У деяких випадках можна навіть реалізувати зміну цін залежно від попиту, що виглядає досить цікаво з точки зору бізнесу.

Не варто забувати і про безпеку. Оскільки система працює з персональними даними користувачів, потрібно забезпечити їх захист. Це може бути реалізовано через шифрування, використання паролів та інші методи. Хоча на практиці це часто недооцінюють, насправді це дуже важлива частина будь-якої інформаційної системи.

Ще один момент - це продуктивність. Якщо користувачів стає багато, система повинна працювати стабільно і не “гальмувати”. Для цього використовуються різні підходи, наприклад, оптимізація запитів до бази даних або кешування. У сучасних умовах такі системи часто інтегруються з іншими сервісами. Це можуть бути платіжні системи або сервіси повідомлень. Наприклад, після бронювання користувач може отримати підтвердження на електронну пошту. Це робить систему більш зручною і сучасною.

Отже, можна сказати, що інформаційна система бронювання готельних номерів є важливим інструментом для автоматизації роботи готелю.

Використання Python у цьому випадку є цілком виправданим, оскільки ця мова дозволяє швидко створювати ефективні рішення.

Висновки та перспективи. В результаті можна зробити висновок, що впровадження таких систем значно покращує роботу готелів. Це дозволяє зменшити кількість помилок, підвищити швидкість обробки інформації та зробити сервіс більш зручним для клієнтів. У майбутньому такі системи можуть розвиватися за рахунок використання нових технологій, зокрема аналізу даних або елементів штучного інтелекту.

Список використаних джерел

1. *Python Documentation. Електронний ресурс. – Режим доступу: https://docs.python.org*
2. *Flask Documentation. Електронний ресурс. – Режим доступу: https://flask.palletsprojects.com*
3. *Sommerville I. Software Engineering. – Pearson, 2016.*
4. *Pressman R. Software Engineering: A Practitioner's Approach. – McGraw-Hill, 2014.*

Матвійчук Ернест Вікторович
студент групи ІСД-42
Державного університету
інформаційно-комунікаційних технологій
(096)-987-48-11
ernestmatvijcuk@gmail.com

Сагайдак Віктор Анатолійович
PhD, доцент кафедри Інформаційних систем та технологій Державного університету інформаційно-комунікаційних технологій, м. Київ.

ЕКОНОМІЧНА ТА ЕКОЛОГІЧНА ЕФЕКТИВНІСТЬ СИСТЕМ РОЗУМНОГО ОПАЛЕННЯ В КОНТЕКСТІ SMART HOME

Постановка задачі

В умовах глобальної енергетичної кризи та постійного зростання тарифів на енергоносії в Україні, оптимізація витрат на обігрів житла стає критично важливою. За даними Міненерго, опалення може становити до 60% загального споживання енергії домогосподарством у холодний період. Впровадження IoT-рішень для керування кліматом дозволяє не лише підвищити комфорт, а й забезпечити суттєве зменшення фінансових витрат та негативного впливу на довкілля.

Мета дослідження

Аналіз економічної доцільності та екологічного впливу впровадження систем розумного опалення, а також оцінка потенціалу їхньої інтеграції з

відновлюваними джерелами енергії для підвищення автономності домогосподарств.

Результати дослідження

У роботі досліджено, що використання інтелектуальних алгоритмів керування (адаптація до присутності мешканців, врахування погодних API та зональних тарифів) дозволяє скоротити витрати на енергію на 15–30%. З економічного погляду, середня окупність обладнання для квартири при поточних тарифах становить від 2 до 4 років. Екологічний аспект впровадження полягає у прямому зниженні викидів CO2. Зокрема, перехід на розумне керування дозволяє уникати перегріву приміщень та марного витрачання ресурсів за відсутності людей (сценарій «Немає вдома»). Додатково розглянуто можливість інтеграції системи з сонячними панелями та тепловими насосами, що дозволяє акумулювати теплову енергію в періоди її найнижчої вартості або максимальної генерації з відновлюваних джерел.

Висновки та перспективи

Системи розумного опалення є інвестиційно привабливим рішенням, яке сприяє сталому розвитку та енергетичній незалежності. Подальші дослідження можуть бути спрямовані на розробку універсальних моделей прогнозування енергоспоживання на основі штучного інтелекту для багатоквартирних будинків з централізованим опаленням.

Список використаних джерел

1. Mistry, V. Smart Thermostats: Revolutionizing HVAC Control in Building Automation. IJSR, 2024.

2. Su, Y. An Intelligent Heating System Based on the Internet of Things and STM32 Microcontroller. Energy Informatics, 2024.

3. Tado. Smart Climate Control: Energy Savings Report [Електронний ресурс]. – 2023.

Зима Тимофій Андрійович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету інформаційно-комунікаційних технологій, м. Київ
st6870209@stud.duikt.edu.ua

Катков Юрій Ігорович
професор, доктор технічних наук

ОПТИМІЗАЦІЯ НЕЙРОМЕРЕЖЕВИХ МОДЕЛЕЙ ДЕТЕКЦІЇ ОБ'ЄКТІВ ДЛЯ РОБОТИ НА КІНЦЕВИХ ПРИСТРОЯХ ІОТ-МЕРЕЖ

Вступ. У сучасному світі спостерігається стрімке зростання кількості пристроїв, підключених до мережі Інтернет, що формує основу концепції

Інтернету речей (IoT). Разом із цим активно розвиваються технології штучного інтелекту, які дозволяють автоматизувати обробку великих обсягів даних [1]. Поєднання цих двох напрямів створює передумови для розробки інтелектуальних систем, здатних не лише збирати інформацію, але й аналізувати її в режимі реального часу [2]. Стрімкий розвиток концепції Internet of Things (IoT) та Edge Computing вимагає перенесення обчислень безпосередньо на кінцеві пристрої для зменшення затримки (latency) та економії смуги пропускання, тобто забезпечувати детекцію об'єктів. Детекція об'єктів – це технологія комп'ютерного зору, яка одночасно вирішує два завдання: визначає тип об'єкта (класифікація) та знаходить його точне місце розташування на зображенні або відео (локалізація) [3, 4].

Детекція об'єктів у реальному часі є критичною для розумних міст та промисловості. Проте, обмежені апаратні ресурси IoT-вузлів (пам'ять, енергоспоживання, обчислювальна потужність) створюють бар’єр для розгортання «важких» сучасних нейромереж, що робить розробку методів їх оптимізації пріоритетним науковим завданням. [5, 6].

Сучасні системи детекції об'єктів на Edge-пристроях базуються на спеціалізованих архітектурах або хмарних обчисленнях. Хмарні рішення мають необмежені ресурси, але залежать від стабільності мережі та створюють ризики для безпеки даних. Спеціалізовані архітектури (напр. MobileNet, SqueezeNet) мають низьку кількість параметрів та високу швидкість роботи, але помітна втрата точності (mAP) у порівнянні з повнорозмірними моделями типу ResNet. Апаратні прискорювачі (Coral TPU, Jetson Nano) мають високу продуктивність на ват енергії, але у них висока вартість та обмежена гнучкість для різних типів нейромереж [7, 8].

Одже основною проблемою залишається пошук балансу між точністю розпізнавання та енергоефективністю кінцевого пристрою. У зв’язку з цим виникає потреба у створенні автоматизованих систем, які здатні самостійно виявляти об’єкти, зокрема людей і домашніх тварин, у відеопотоці.

Постановка завдання. Необхідно дослідити та розробити комплексний підхід до адаптації нейромережевих моделей детекції об'єктів для роботи в умовах суворих ресурсних обмежень IoT-вузлів. Завдання включає вибір базової легкої архітектури, застосування алгоритмічних методів стиснення моделей та оцінку впливу цих маніпуляцій на швидкість обробки кадрів (FPS) та точність детекції в умовах реального часу.

Метою роботи є мінімізація обчислювальної складності нейромережевих моделей детекції об'єктів при збереженні прийнятного рівня точності для їх ефективного розгортання на кінцевих пристроях IoT-мереж. Це дозволить реалізувати автономні системи моніторингу, які здатні приймати рішення локально без залучення потужних серверів.

Основна частина. Детекція об'єктів (Object Detection) – це технологія в галузі комп’ютерного зору, яка дозволяє комп'ютерним системам не просто класифікувати зображення (визначити, «що» на ньому зображено), а й знаходити точне місце розташування кожного об'єкта. Ось ключові аспекти, що пояснюють суть цього процесу:

1. Подвійне завдання. Детекція об'єктів об'єднує в собі дві операції: класифікація - визначення категорії об'єкта (наприклад, людина, автомобіль, датчик IoT); локалізація - визначення координат об'єкта на зображенні, що зазвичай відображається у вигляді прямокутної рамки (Bounding Box).

2. Застосування в IoT. У цьому контексті детекція об'єктів є критичною для таких напрямів: розумні міста (автоматичний моніторинг трафіку та підрахунок пішоходів); промисловість (контроль якості на конвеєрах та виявлення дефектів); безпека (розпізнавання несанкціонованого доступу в реальному часі через IoT-камери).

3. Технологічні підходи. Сучасна детекція базується на використанні нейромережевих моделей. Основна проблема для IoT-мереж полягає в тому, що ці моделі зазвичай потребують значних обчислювальних ресурсів, тому зараз активно розвиваються методи їх оптимізації для роботи безпосередньо на кінцевих (Edge) пристроях.

4. Популярні алгоритми. Для задач детекції найчастіше використовують такі архітектури [9, 10, 11, 12]:

YOLO (You Only Look Once): Високошвидкісні моделі, що ідеально підходять для роботи в реальному часі.

SSD (Single Shot Multibox Detector): Баланс між швидкістю та точністю.

Faster R-CNN: Висока точність, але потребує більше ресурсів.

Ці архітектури для роботи на «краю» мережі (Edge) найчастіше використовуються одностадійні детектори (one-stage detectors). Ці моделі використовують глибинно-роздільні згортки (depthwise separable convolutions), що радикально зменшує кількість мультиплікативних операцій. В контексті IoNT (Інтернету нано-речей) розглядаються ще більш компактні структури з двійковими вагами.

Розробка системи детекції об’єктів у відеопотоці базується на використанні методів глибокого навчання та комп’ютерного зору [1]. Основною задачею є визначення типу об’єкта та його локалізація у межах кадру. Архітектура системи включає такі основні компоненти: модуль отримання даних – захоплення відеопотоку; модуль попередньої обробки – підготовка зображення до аналізу; модуль детекції – використання нейронної мережі; модуль постобробки – усунення дублювань результатів; модуль відображення результатів – виведення інформації користувачу.

У якості основного алгоритму доцільно використовувати одноетапні детектори, зокрема YOLO, які забезпечують високу швидкість роботи [2]. Це

дозволяє реалізувати обробку відео в реальному часі. Процес роботи системи включає: отримання кадру; обробку нейронною мережею; визначення координат об’єктів; застосування алгоритму фільтрації результатів; відображення результатів.

Для навчання моделі використовуються відкриті датасети, зокрема COCO [13]. Для покращення результатів застосовуються методи аугментації даних.

Порівняльний аналіз показує, що YOLOv8 Nano демонструє найкращий баланс між швидкістю та точністю на ARM-процесорах. MobileNet-SSD є більш енергоефективним, але має труднощі з детекцією дрібних об'єктів. Моделі типу EfficientDet-Lite показують високу стабільність, проте вимагають специфічної підтримки з боку бібліотек (TensorFlow Lite). Ключові метрики порівняння: розмір моделі (Мб); кількість операцій (GFLOPs); Latency на стандартному CPU (мс); Mean Average Precision (mAP); FPS (швидкість обробки відео).

Для досягнення максимальної ефективності пропонується використовувати трирівневу стратегію оптимізації:

Квантування (Quantization): Перехід від обчислень з плаваючою комою (FP32) до цілочисельних операцій (INT8). Це зменшує розмір моделі в 4 рази та прискорює вивід на пристроях з підтримкою SIMD-інструкцій без критичної втрати точності.

Прунінг (Pruning): Видалення надлишкових зв'язків (ваг) або цілих фільтрів, які мінімально впливають на результат. Це дозволяє скоротити кількість параметрів на 30-50%.

Дистиляція знань (Knowledge Distillation): Навчання малої моделі («учня») на основі прогнозів великої, попередньо навченої моделі («вчителя»). Це дозволяє «учневі» краще узагальнювати дані, маючи малу кількість параметрів.

Апаратна адаптація: Використання форматів ONNX або OpenVINO для оптимізації графів обчислень під конкретне залізо (наприклад, ESP32-S3 або Raspberry Pi).

Висновки та перспективи

В результаті дослідження визначено, що поєднання квантування INT8 та архітектури YOLO Nano є найбільш перспективним для сучасних систем IoT. Оптимізація дозволяє знизити енергоспоживання пристрою, що критично для автономних датчиків. Перспективи подальших розробок лежать у площині Neural Architecture Search (NAS) – автоматизованого пошуку архітектур, які створюються нейромережею під конкретні апаратні обмеження певного IoT-чіпа. Такі підходи дозволяють комплексно оцінити ефективність системи як за точністю, так і за швидкодією.

Список використаних джерел

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, (2021). Genetic Programming and Evolvable Machines 19(1-2), https://link.springer.com/article/10.1007/s10710-017-9314-z & https://www.deeplearningbook.org/

2. Shi W. et al. Edge Computing: Vision and Challenges. (2024) IEEE Internet of Things Journal (Volume: 3, Issue: 5, Page(s): 637 – 646, DOI: 10.1109/JIOT.2016.2579198, https://ieeexplore.ieee.org/document/7488250

3. Liang, T., et al. (2021). Optimization Methods for Deep Learning Models in Edge Computing. IEEE Access. DOI: 10.1109/ACCESS.2021.3084781 https://ieeexplore.ieee.org/document/9444394

4. Howard, A., et al. (2019). Searching for MobileNetV3. IEEE/CVF International Conference on Computer Vision. DOI: 10.1109/ICCV.2019.00141, https://ieeexplore.ieee.org/document/9008835

5. Han, S., et al. (2016). Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding. ICLR. DOI: 10.48550/arXiv.1510.00149 https://arxiv.org/abs/1510.00149

6. Gholami, A., et al. (2021). A Survey of Quantization Methods for Efficient Neural Network Inference. Low-Power Computer Vision. DOI: 10.48550/arXiv.2103.13630 https://arxiv.org/abs/2103.13630

7. Wang, C. Y., et al. (2023). YOLOv7: Trainable Bag-of-Freebies Sets New State-of-the-Art for Real-Time Object Detectors. IEEE/CVF CVPR. DOI: 10.1109/CVPR52729.2023.00721, https://openaccess.thecvf.com/content/CVPR2023/html/Wang_YOLOv7_Trainable_Bag-of-Freebies_Sets_New_State-of-the-Art_for_Real-Time_Object_Detectors_CVPR_2023_paper.html |

8. Mishra, R. K., et al. (2022). Deep Learning for Internet of Things: A Comprehensive Review. Sensors. DOI: 10.3390/s22114055, https://www.mdpi.com/1424-8220/22/11/4055

9. Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXiv. | DOI: 10.48550/arXiv.1804.02767, https://arxiv.org/abs/1804.02767

10. Redmon J. et al. YOLO: Unified, Real–Time Object Detection, 2016. https://arxiv.org/abs/1506.02640

11. Liu W. et al. SSD: Single Shot MultiBox Detector, 2016. https://arxiv.org/abs/1512.02325

12. Ren S. et al. Faster R-CNN, 2017. https://arxiv.org/abs/1506.01497

13 Lin T.-Y. et al. Microsoft COCO Dataset, 2014. https://cocodataset.org/

Кохановський Кіріл Олександрович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету інформаційно-комунікаційних технологій, м. Київ
st7958694@stud.duikt.edu.ua

Катков Юрій Ігорович
професор, доктор технічних наук

ПРОЦЕДУРНА ГЕНЕРАЦІЯ РІВНІВ У UNITY ДЛЯ ОПТИМІЗАЦІЇ РОЗРОБКИ ЦИФРОВИХ ДВІЙНИКІВ IOT-СИСТЕМ

Вступ

Сучасний розвиток систем IoT (Internet of Things) зумовлює необхідність створення інтерактивних моделей середовища існування IoT-речей – цифрових двійників (Digital Twins). У IoT системах концепція цифрових двійників є

ключовою технологією, що з’єднує фізичний світ із цифровим. Це не просто візуальна 3D-модель, а жива цифрова копія фізичного об'єкта, процесу або системи, яка оновлюється в реальному часі. Це важливе для масштабування бізнес-процесів, оптимізації використання ресурсів та створення безпечних симуляцій реальності IoT-середовища шляхом впровадження цифрових світів. Наприклад, якщо у вас є «Розумне місто», то його цифровий світ у Unity – це 3D-модель міста, яка в реальному часі отримує дані з датчиків (температура, трафік, енергоспоживання) і відображає їх.

Цифровий світ для IoT систем – це штучне віртуальне середовище, що базується на дизайні рівнів, створених комп'ютерними системами для взаємодії користувачів, обробки даних та симуляції реальних процесів. Традиційне ручне моделювання стає надто дорогим і тривалим процесом, тому виникає потреба в автоматизації рутинних завдань на основі процедурної генерації. Це дозволяє створювати унікальний контент «на льоту», забезпечуючи високу реіграбельність та значне зниження витрат. У контексті розвитку метавсесвітів та складних цифрових екосистем такі інструменти стають фундаментальною основою розробки.

Існує інструментарій Unity та Unreal Engine. Він є провідним рушієм, що визначають стандарти сучасного GameDev та промислових візуалізацій. Unity вирізняється гнучкістю, величезною екосистемою плагінів (Asset Store) та зручністю для C#-програмування, що робить його ідеальним для ітеративної розробки процедурних алгоритмів. Unreal Engine пропонує потужні графічні можливості (Lumen, Nanite) та систему візуального програмування Blueprints. Обидва рушії підтримують складні обчислення, необхідні для генерації геометрії, ландшафтів та розміщення об'єктів у реальному часі [1, 2]

Відомо, що процедурна генерація в Unity базується на використанні математичних алгоритмів (наприклад, шуму Перліна, клітинних автоматів або L-систем) для автоматичного створення ігрового простору. Замість статичного розміщення префабів, розробник створює правила, за якими рушій під час виконання або на етапі дизайну формує ландшафт, архітектуру та логіку взаємодії.

Це дозволяє створювати нескінченні світи з мінімальним обсягом вхідних даних, що критично для мобільних платформ та хмарних ігрових рішень. Звідси сутність оптимізації розробки цифрових світів полягає у переході від "ручної праці" до "алгоритмічного дизайну". Тобто, по-перше, у підвищенні швидкодії фінального продукту FPS (Frames Per Second), коли кількість кадрів, які комп'ютерна система (рушій Unity/Unreal Engine) виводить на екран за одну секунду); по-друге, у вдосконаленні самого процесу створення контенту (Workflow). Це дозволяє скоротити цикл тестування, швидко змінювати концепцію рівнів без необхідності їх повного перероблення та забезпечує масштабованість проекту. Ключовий показник оптимізації тут – відношення

обсягу створеного унікального контенту до людино-годин, витрачених на його програмування [2, 3].

Постановка завдання

Завдання полягає у розробці гібридного методу генерації в Unity через поєднання алгоритму хвильового колапсу функції та графів залежностей. Необхідно реалізувати інструмент для автоматизації створення логічно зв’язних локацій з можливістю тонкого налаштування та мінімальним впливом на продуктивність.

Метою роботи є розробка та впровадження гібридного методу процедурної генерації в середовищі Unity, що базується на поєднанні алгоритму хвильового колапсу функції (WFC) та графів залежностей, для автоматизації створення логічне зв’язних цифрових двійників в IoT-системах при забезпеченні високої продуктивності FPS.

Основна частина

Розробка гібридного підходу до процедурної генерації в середовищі Unity, що базується на синергії алгоритму хвильового колапсу функції (WFC - Wave Function Collapse) та графів залежності передбачає реалізацію програмних інструментів, які вирішують наступні підзадачі [4, 5]:

- Інтелектуальна генерація: застосування алгоритму WFC для автоматичного формування локацій, що гарантує візуальну цілісність контенту.
- Логічний контроль: впровадження графів залежності для забезпечення суворої ієрархії об'єктів та дотримання геймплейних обмежень (прохідність шляхів, логічне розміщення елементів).
- Оптимізація обчислень: мінімізація навантаження на систему під час динамічної перебудови цифрового світу для підтримки стабільного показника FPS.
- Гнучкість керування: створення системи параметричного налаштування, яка дозволяє дизайнеру поєднувати швидку автоматичну генерацію з ручним коригуванням ключових вузлів графа.

Під час дослідження були визначені наступні основні методи процедурної генерації, що застосовуються в середовищі Unity [6, 7]:

1. Випадкове розміщення об’єктів (Random Placement): Найпростіший метод, що базується на розкиданні префабів у заданих координатах за допомогою функції Random.Range. Використовується для дрібних деталей (трава, каміння).
2. Шум Перліна та Симплекс-шум (Perlin/Simplex Noise): Використання математичних функцій плавного шуму для створення природних ландшафтів, висот терайна та хмар. Забезпечує плавні переходи між висотами.
3. Клітинні автомати (Cellular Automata): Алгоритм, заснований на станах сусідніх клітинок (за принципом гри «Життя»). Ідеально підходить для генерації органічних печер та гротів.

4. L-системи (Lindenmayer Systems): Рекурсивні математичні правила, які найчастіше використовуються для моделювання фрактальних структур, таких як дерева, кущі та інші рослини.

5. Алгоритми на графах (Dungeon Digging/BSP): Використання дерев двійкового розбиття простору (BSP) або графів для створення кімнат і коридорів. Це гарантує логічну пов'язаність приміщень у лабіринтах.

6. Хвильовий колапс функції (Wave Function Collapse, WFC): Алгоритм, що збирає рівень із набору тайлів на основі правил їхньої суміжності. Він дозволяє створювати складні, візуально несуперечливі структури (міста, архітектуру).

7. Гібридний метод (WFC + Графи залежностей): Поєднання локальної точності WFC з глобальною логікою графів. Графи визначають архітектуру та ігровий шлях (геймплей), а WFC заповнює цей каркас деталізованим та візуально коректним контентом.

У роботі пропонується застосування гібридного підходу до процедурної генерації, що базується на поєднанні хвильового колапсу функції (Wave Function Collapse) та графів залежностей. На відміну від стандартного WFC, запропонований метод дозволяє інтегрувати глобальні геймплейні обмеження через графи залежностей, що гарантує логічну прохідність рівнів

Це дозволяє замість чистої випадковості використовувати системою набір пресетів із семантичними тегами для створення алгоритму розуміння контекст: наприклад, «двері мають бути в стіні», а «стіл не може перекривати шлях». Використання паралельних обчислень через Unity C# Job System дозволяє винести розрахунки генерації в окремі потоки, що усуває затримки в основному циклі програми. Також запропоноване застосування адаптивного механізму «зворотного зв'язку» між генератором і параметрами продуктивності системи. Це забезпечує механізм адаптивного керування графічними ресурсами в процедурних середовищах: якщо FPS знижується, алгоритм автоматично спрощує деталізацію (LOD) генерованих об'єктів або зменшує щільність заповнення простору без переривання сесії.

Застосування технології LOD (Level of Detail, «рівень деталізації») дозволяє оптимізацію в комп'ютерній графіці та ігрових рушіях (Unity, Unreal Engine), а також полягає у зміні складності 3D-моделі залежно від її відстані до віртуальної камери. Наприклад, коли об'єкт знаходиться близько до гравця, рушій відображає його максимально деталізованим (висока кількість полігонів, якісні текстури). Щойно об'єкт віддаляється, система автоматично підміняє його на спрощену версію. Для цього застосовуються рівні: LOD 0 (оригінальна, найбільш деталізована модель для ближніх планів; LOD 1, 2...n (спрощені копії з меншою кількістю трикутників; LOD - Culled (Відсікання) для дуже великих відстанях об'єкт взагалі перестає рендеритися, щоб не навантажувати систему. LOD є ключовим інструментом оптимізації тому, що забезпечує: продуктивність, динамічне управління, економію пам'яті.

Крім того, впроваджено систему візуальних вузлів (Node-based editor) для швидкого редагування правил генерації не-програмістами, що значно прискорює ітерацію дизайну. Такий підхід перетворює процедурний генератор з "чорної скриньки" на керований інтелектуальний інструмент. Node-based editor (вузловий редактор) – це інтерфейс візуального програмування, де логіка або контент створюються шляхом з'єднання графічних блоків (вузлів або нод) між собою за допомогою ліній (зв'язків). Замість написання сотень рядків коду, розробник використовує схему, яка наочно показує потік даних або послідовність дій. Кожен вузол (Node) виконує певну функцію (наприклад, "Створити стіну", "Повернути об'єкт", "Згенерувати шум"), має входи (Inputs) та виходи (Outputs). Під час процедурної генерації Node-based editor виступає як інструмент, що забезпечує:

- Гнучкість для дизайнера: Людина може змінювати правила генерації світу (наприклад, щільність лісу чи складність лабіринту), просто перетягуючи вузли, не заглядаючи в код C#.
- Візуалізацію графів залежностей: Оскільки ваш гібридний підхід базується на графах, вузловий редактор є найкращим способом відобразити ці зв'язки.
- Прискорення розробки: Можливість швидко створювати нові прототипи рівнів, комбінуючи готові логічні блоки.

Приклади Node-based editor в Unity: Shader Graph (для створення візуальних ефектів), Visual Scripting (раніше Bolt для написання логіки гри), VFX Graph (для складних систем частинок).

Висновки та перспективи розробок

Процедурна генерація рівнів на рушії Unity є потужним інструментом оптимізації розробки цифрових світів. Впровадження гібридного підходу до процедурної генерації в середовищі Unity, що базується на синергії алгоритму хвильового колапсу функції (WFC - Wave Function Collapse) та графів залежності передбачає реалізацію програмних інструментів дозволяє скоротити час на створення прототипів рівнів. Гібридні методи генерації забезпечують кращий баланс між продуктивністю та якістю контенту порівняно зі стандартними методами.

Перспективи: Подальші дослідження будуть спрямовані на інтеграцію нейронних мереж для аналізу стилістики дизайну, що дозволить штучному інтелекту навчатися на прикладах створених вручну рівнів та відтворювати їхню естетику. Це відкриває шлях до створення саморозвивальних цифрових світів у майбутніх IoT-системах та віртуальних тренажерах.

Список використаних джерел

1. Shaker, N., Togelius, J., Nelson, M. J. (2016) Procedural Content Generation in Games: A Textbook and an Overview of Current Research. URL: https://doi.org/10.1007/978-3-319-42716-4 . DOI: 10.1007/978-3-319-42716-4.

2. *Hendrikx, M., Meijer, S., Van Der Velden, J., Iosup, A. (2013) Procedural content generation for games: A survey. URL: https://doi.org/10.1145/2422956.2422957 . DOI: 10.1145/2422956.2422957.*

3. *De Kegel, B., Haesen, R., Suykens, J. A. K. (2013) Procedural content generation for games: a survey / recent developments in PCG. URL: https://atlarge-research.com/pdfs/2013-hendrikx-procedural.pdf*

4. *Shaan Khan (2022) Implementing Wave Function Collapse & Binary Space Partitioning for Procedural Dungeon Generation URL: https://medium.com/@ShaanCoding/implementing-wave-function-collapse-binary-space-partitioning-for-procedural-dungeon-generation-2f1a6cc376db*

5. *Paul Merrell, et al. (2023) Example-Based Procedural Modeling Using Graph Grammars. URL: https://doi.org/10.1145/3592119 . DOI: 10.1145/3592119.*

6. *Rafael Bidarra (2022) miWFC - Designer Empowerment through mixed-initiative Wave Function Collapse. URL: https://doi.org/10.1145/3555858.3563266*

7. *Anton Karpetskyi, Piotr Napieralski, Dominik Szajerman (2025) Hybrid Procedural Level Generation Using Wave Function Collapse and Genetic Algorithms. URL: https://www.iccs-meeting.org/archive/iccs2025/papers/159090105.pdf., https://dx.doi.org/10.1007/978-3-031-97564-6_9*

Кузіна Дар'я Володимирівна
студентка 4 курсу
Державного університету інформаційно-комунікаційних технологій, м. Київ
el.deschhh@gmail.com

Бажан Тетяна Олександрівна
старший викладач кафедри Технологій цифрового розвитку
Державного університету інформаційно-комунікаційних технологій, м. Київ

ВИКОРИСТАННЯ ВЕБ-ТЕХНОЛОГІЙ ТА РЕЛЯЦІЙНИХ БАЗ ДАНИХ ДЛЯ УПРАВЛІННЯ ДАНИМИ У ЦИФРОВИХ СЕРВІСАХ

Постановка задачі.

На сьогодні цифрові сервіси працюють із великими обсягами інформації, яка постійно змінюється та використовується у різних процесах. Від того, наскільки правильно організоване зберігання і обробка цих даних, залежить стабільність роботи всієї системи.

На практиці часто виникають ситуації, коли через неефективну структуру бази даних або невдало побудовану логіку взаємодії система працює повільно або нестабільно. Саме тому важливо використовувати підходи, які дозволяють упорядкувати дані та забезпечити зручну роботу з ними [1].

Мета дослідження.

Метою роботи є аналіз використання веб-технологій у поєднанні з реляційними базами даних для організації ефективного управління даними у цифрових сервісах.

Результати дослідження.

У ході дослідження було розглянуто принципи побудови веб-застосунків, що функціонують на основі клієнт-серверної архітектури. Такий підхід дозволяє розділити систему на окремі складові, які відповідають за обробку запитів, бізнес-логіку та зберігання даних, що підвищує її гнучкість і зрозумілість [5].

Реляційні бази даних забезпечують структуроване представлення інформації та дозволяють встановлювати зв’язки між окремими сутностями. Це спрощує обробку даних і знижує ризик виникнення помилок під час роботи з ними [2].

Застосування сучасних технологій, зокрема ASP.NET Core разом із MS SQL Server, дозволяє:

– забезпечити стабільну роботу веб-застосунку навіть при значному навантаженні;

– організувати контроль доступу до даних;

– спростити процес розробки та супроводу програмного забезпечення [4].

Також у роботі розглянуто використання технології об’єктно-реляційного відображення (ORM), яка дозволяє працювати з базою даних через програмний код, що значно спрощує розробку та підтримку системи [3].

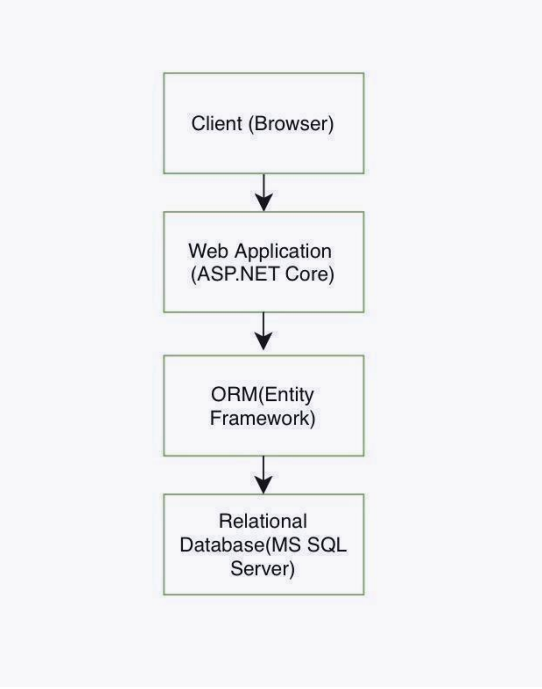

Рис. 1. Схема взаємодії веб-застосунку з базою даних

Застосування такого підходу дозволяє створювати системи, які легко масштабуються та адаптуються до змін вимог.

Висновки.

Проведений аналіз показує, що поєднання веб-технологій і реляційних баз даних є ефективним рішенням для створення сучасних цифрових сервісів. Такий підхід дозволяє забезпечити не лише зручну роботу з даними, а й стабільність функціонування системи в цілому.

Важливим є правильний розподіл функцій між компонентами системи, оскільки це впливає як на продуктивність, так і на можливість її подальшого розвитку.

У подальшому доцільно звернути увагу на використання хмарних технологій, а також на підходи, що дозволяють підвищити ефективність роботи з великими обсягами даних.

Список використаних джерел

1. *Date, C. J. (2019). An introduction to database systems (8th ed.). Pearson.*
2. *Elmasri, R., & Navathe, S. B. (2016). Fundamentals of database systems (7th ed.). Pearson.*
3. *Kleppmann, M. (2017). Designing data-intensive applications. O'Reilly Media.*
4. *Microsoft. (2026). .NET documentation. Retrieved April 8, 2026, from https://learn.microsoft.com/en-us/dotnet/*
5. *Richards, M., & Ford, N. (2020). Fundamentals of software architecture: An engineering approach. O'Reilly Media.*

Доманський Владислав Сергійович
студент 4 курсу
спеціальності «Інженерія програмного забезпечення»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
domanski0308@gmail.com

Бажан Тетяна Олександрівна
старший викладач кафедри
Технологій цифрового розвитку
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ВЕБ-ДОДАТОК ДЛЯ УПРАВЛІННЯ ПЕРСОНАЛЬНИМИ НОТАТКАМИ

У сучасних умовах стрімкого розвитку інформаційних технологій зростає потреба у зручних засобах зберігання та обробки персональних текстових даних. До таких даних належать нотатки, ідеї, плани та списки завдань, які користувачі активно використовують у повсякденному житті. Тому актуальним є створення веб-додатків, що забезпечують швидкий доступ до інформації та її ефективну організацію [3].

Сучасні веб-технології дозволяють створювати повнофункціональні додатки без використання серверної частини. Зокрема, використання мови програмування JavaScript дає можливість реалізувати логіку роботи додатку, [1, 3] а HTML і CSS – забезпечити структуру та зовнішній вигляд інтерфейсу користувача. Особливу роль відіграє технологія localStorage, яка дозволяє зберігати дані безпосередньо у браузері користувача [2].

У роботі розроблено веб-додаток для управління персональними текстовими даними, структура якого представлена на рис. 1. Додаток працює у середовищі браузера та не потребує встановлення додаткового програмного забезпечення [2,3].

Реалізований додаток забезпечує такі функціональні можливості:

– створення нових нотаток;
– редагування існуючих записів;
– видалення нотаток;
– використання категорій для систематизації інформації;
– збереження даних у локальному сховищі браузера;
– відображення списку нотаток користувача.

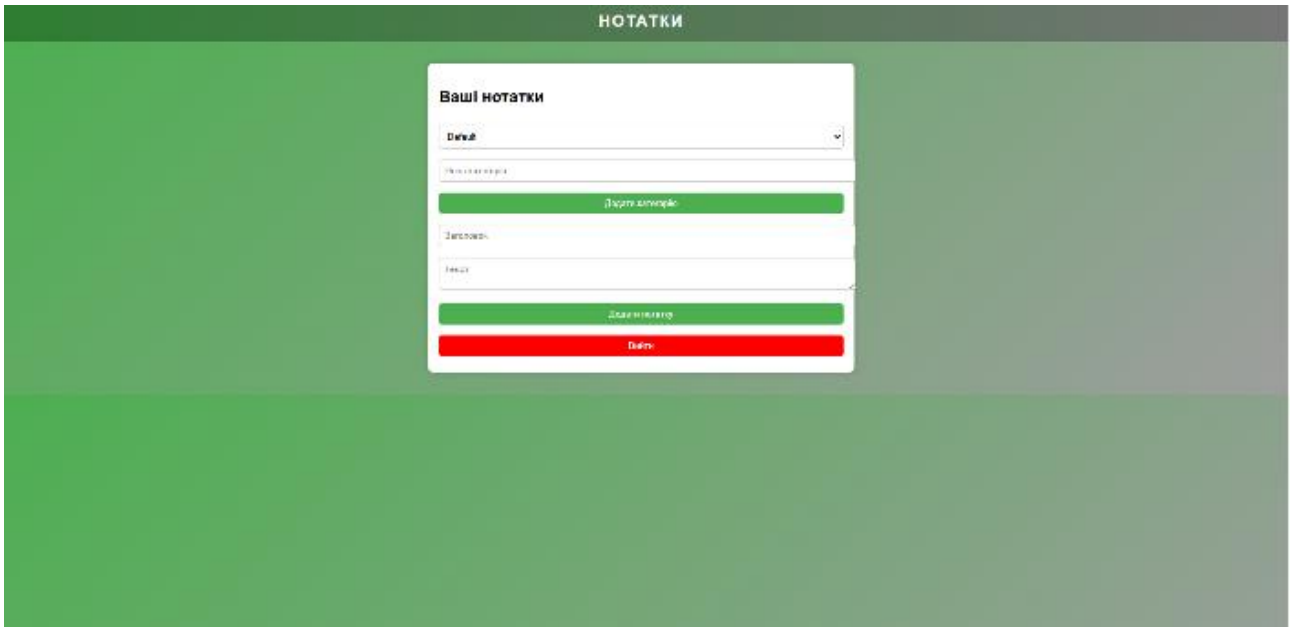

Рис. 1. Структура веб-додатку управління нотатками

Використання localStorage дозволяє зберігати дані у форматі JSON, що спрощує їх обробку та забезпечує швидкий доступ до інформації. Дані не втрачаються після перезавантаження сторінки, що підвищує надійність роботи системи [2].

Основною перевагою розробленого рішення є його автономність, оскільки всі операції виконуються на стороні клієнта без необхідності підключення до

сервера [1]. Це забезпечує високу швидкість роботи та простоту використання [3].

Таким чином, розроблений веб-додаток є ефективним інструментом для управління персональними текстовими даними користувача та може бути використаний у навчальній діяльності, роботі та повсякденному житті [1,3].

Висновки та перспективи.

Розроблений веб-додаток дозволяє ефективно вирішити задачу управління персональними текстовими даними без використання серверної частини. Використання технології localStorage забезпечує простоту реалізації та автономність роботи системи.

Перспективами подальшого розвитку є розширення функціоналу додатку, зокрема реалізація синхронізації даних між пристроями, впровадження системи авторизації з підвищеним рівнем безпеки, а також інтеграція з серверними технологіями для забезпечення віддаленого доступу до даних [1,3].

Список використаних джерел

1. *Duckett, J. (2014).* JavaScript and jQuery: Interactive Front-End Web Development. *Wiley.*
2. *Mozilla Developer Network. Web Storage API (localStorage). URL: https://developer.mozilla.org/en-US/docs/Web/API/Web_Storage_API*
3. *Flanagan, D. (2020). JavaScript: The Definitive Guide (7th ed.). O'Reilly Media.*

Федорчук Тимофій Русланович
студент групи САД-41
Державного університету
інформаційно-комунікаційних технологій
+380962893880
freeman.crazys@gmail.com

СИСТЕМА ПІДТРИМКИ РІШЕНЬ У СФЕРІ ЗАЙНЯТОСТІ НАСЕЛЕННЯ

Із розвитком цифрової економіки та стрімкими змінами на ринку праці проблема результативного управління зайнятістю населення стає особливо актуальною. Підвищення рівня безробіття, структурні трансформації економіки, міграційні процеси та вплив світових криз формують нові виклики для державних установ і роботодавців. У таких умовах виникає потреба у застосуванні сучасних інформаційних технологій для аналізу стану ринку праці та підтримки прийняття обґрунтованих управлінських рішень.

Класичні підходи до дослідження зайнятості, що базуються на статистичних даних і ручному опрацюванні інформації, не забезпечують достатньої швидкості та гнучкості. Це обмежує можливість оперативно реагувати

на економічні зміни та знижує ефективність державної політики у сфері зайнятості.

Постановка задачі

Оскільки з необхідністю підвищення ефективності управління ринком праці постає завдання створення систем підтримки прийняття рішень, які здатні обробляти значні обсяги даних, аналізувати тенденції та формувати рекомендації для користувачів. Основними труднощами є фрагментованість інформації, складність її аналізу, а також відсутність засобів прогнозування змін у сфері зайнятості.

Системи підтримки прийняття рішень дозволяють інтегрувати різнорідні дані, автоматизувати процес їх оброблення та забезпечувати формування аналітичних висновків. Використання таких рішень дає змогу підвищити точність оцінювання ситуації на ринку праці, визначати перспективні напрями розвитку та ухвалювати ефективні управлінські рішення.

Мета дослідження

Метою дослідження є розроблення та вивчення системи підтримки прийняття рішень у сфері зайнятості населення, яка забезпечує аналіз ринку праці, оброблення статистичних даних і формування рекомендацій для підвищення ефективності управління зайнятістю.

Результати дослідження

У ході дослідження було проаналізовано сучасні підходи до створення систем підтримки прийняття рішень та визначено їх значення у сфері зайнятості населення. Розглянуто ключові джерела даних, методи їх опрацювання та аналізу, а також можливості використання інформаційних технологій для прогнозування змін на ринку праці.

У процесі виконання роботи було запропоновано концепцію системи підтримки рішень, яка дозволяє здійснювати аналіз показників зайнятості, виявляти тенденції та формувати рекомендації для користувачів. Отримані результати підтверджують ефективність використання таких систем для підвищення якості управлінських рішень у сфері зайнятості.

Висновки та перспективи

У результаті проведеного дослідження встановлено, що системи підтримки прийняття рішень є важливим інструментом для аналізу та управління процесами зайнятості населення. Їх застосування дає змогу підвищити обґрунтованість рішень, забезпечити оперативний аналіз даних і покращити прогнозування ситуації на ринку праці.

Перспективи подальших досліджень полягають у вдосконаленні методів аналізу даних, інтеграції систем підтримки рішень з іншими інформаційними системами, використанні технологій штучного інтелекту для прогнозування та

розширенні функціональних можливостей системи з урахуванням потреб користувачів.

Список використаних джерел

1. Turban E., Sharda R., Delen D. Decision Support and Business Intelligence Systems. – 10th ed. – Pearson, 2015. – 812 p.

2. Power D. J. Decision Support Systems: Concepts and Resources for Managers. – Greenwood Publishing, 2002. – 250 p.

3. World Bank. Labor Market Information Systems [Електронний ресурс]. – Режим доступу: https://www.worldbank.org/ (дата звернення: 12.04.2026).

Горбунов Олексій Євгенович
студент групи САД-41
Державного університету
інформаційно-комунікаційних технологій
+380980111118
algoritm211@gmail.com

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА МОНІТОРИНГУ ХМАРНОЇ ІНФРАСТРУКТУРИ

У сучасних умовах стрімкого розвитку хмарних технологій та цифрової трансформації бізнесу використання хмарної інфраструктури стало невід'ємною складовою функціонування інформаційних систем. Хмарні платформи забезпечують масштабованість, гнучкість та доступність ресурсів, що дозволяє організаціям швидко адаптуватися до змін ринку та ефективно керувати IT-інфраструктурою. Водночас зростання складності хмарних середовищ створює нові виклики, пов'язані з моніторингом, управлінням ресурсами та забезпеченням стабільності роботи систем.

Традиційні підходи до моніторингу не завжди здатні забезпечити повний контроль за станом розподілених хмарних сервісів, особливо в умовах динамічного масштабування та великої кількості компонентів. Це зумовлює необхідність створення інформаційно-аналітичних систем, здатних здійснювати комплексний аналіз даних, виявляти відхилення та забезпечувати своєчасне реагування на інциденти.

Постановка задачі

У зв'язку зі зростанням обсягів даних, що генеруються хмарними сервісами, виникає потреба у створенні ефективних інструментів для їх збору, обробки та аналізу. Основними проблемами є розподіленість інфраструктури,

велика кількість джерел даних, складність їх інтеграції, а також необхідність забезпечення оперативного виявлення збоїв і аномалій.

Інформаційно-аналітичні системи моніторингу дозволяють централізовано обробляти дані про стан хмарної інфраструктури, здійснювати аналіз показників продуктивності, виявляти критичні події та формувати рекомендації для оптимізації роботи систем. Використання таких систем забезпечує підвищення надійності, доступності та ефективності використання ресурсів.

Мета дослідження

Метою дослідження є розробка інформаційно-аналітичної системи моніторингу хмарної інфраструктури, яка забезпечує збір, обробку та аналіз даних про стан ресурсів, виявлення аномалій і підтримку прийняття рішень для підвищення ефективності функціонування IT-систем.

Результати дослідження

У ході дослідження було проаналізовано сучасні підходи до моніторингу хмарної інфраструктури, визначено основні вимоги до інформаційно-аналітичних систем та розглянуто існуючі інструменти і технології. Досліджено методи збору та обробки метрик, логів і подій, а також підходи до виявлення аномалій у роботі систем.

Для забезпечення ефективного моніторингу хмарної інфраструктури доцільно використовувати сучасні інструменти збору, обробки та візуалізації даних. Одним із найбільш поширених підходів є використання системи Prometheus у поєднанні з Grafana, що дозволяє реалізувати повноцінний цикл обробки метрик і подій.

Як показано на рис. 1, система моніторингу базується на сервері Prometheus, який здійснює збір метрик з різних джерел за допомогою експортерів. Отримані дані зберігаються у вигляді часових рядів у базі даних та можуть бути оброблені за допомогою мови запитів PromQL. Для візуалізації показників використовується Grafana, що забезпечує зручне представлення інформації у вигляді графіків і панелей.

Крім того, система підтримує механізм сповіщень через Alertmanager, який дозволяє оперативно реагувати на критичні події, надсилаючи повідомлення через різні канали, такі як електронна пошта або месенджери. Такий підхід забезпечує комплексний моніторинг, аналіз і своєчасне реагування на зміни в стані хмарної інфраструктури.

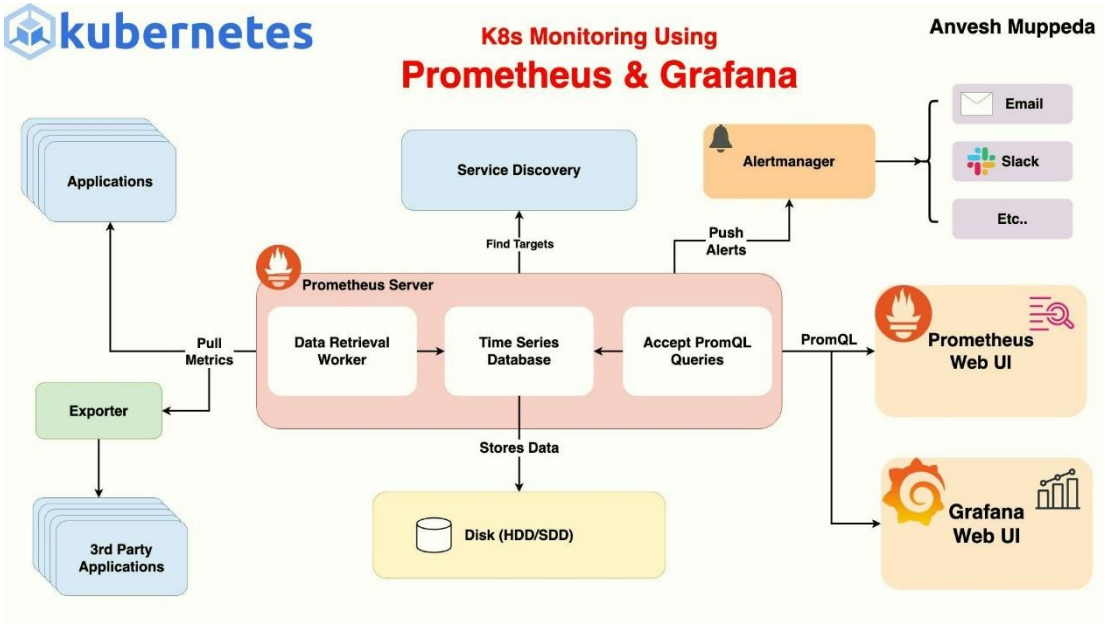

Рис. 1. Архітектура інформаційно-аналітичної системи моніторингу хмарної інфраструктури на основі Prometheus та Grafana

У процесі роботи було запропоновано концепцію інформаційно-аналітичної системи, яка забезпечує централізований моніторинг, аналіз продуктивності та виявлення критичних ситуацій у хмарному середовищі. Розроблена система дозволяє підвищити ефективність управління інфраструктурою, забезпечити своєчасне реагування на інциденти та оптимізувати використання ресурсів.

Висновки та перспективи

У результаті дослідження встановлено, що інформаційно-аналітичні системи моніторингу є ключовим елементом ефективного управління хмарною інфраструктурою. Їх використання дозволяє забезпечити безперервний контроль за станом систем, підвищити рівень надійності та оперативність реагування на збої.

Перспективи подальших досліджень полягають у впровадженні методів машинного навчання для прогнозування інцидентів, інтеграції систем моніторингу з DevOps-процесами, автоматизації реагування на події, а також розширенні функціональних можливостей системи для роботи в мультихмарних середовищах.

Список використаних джерел

1. *Turnbull J. The Art of Monitoring. – James Turnbull, 2014. – 500 p.*
2. *Burns B., Beda J., Hightower K. Kubernetes: Up and Running. – O'Reilly Media, 2022. – 350 p.*
3. *Amazon Web Services. Cloud Monitoring and Observability [Електронний ресурс]. – Режим доступу: https://aws.amazon.com/cloudwatch/ (дата звернення: 12.04.2026).*

Пасошников Андрій Петрович
студент групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій
+380989119828
pasosnikovandrej03@gmail.com

Козлов Дмитро Євгенович
старший викладач кафедри Інженерії програмного забезпечення автоматизованих систем
Державного університету інформаційно-комунікаційних технологій, м. Київ

ЕВОЛЮЦІЯ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ МЕРЕЖ ДОСТУПУ В УКРАЇНІ: ВІД FTTB ДО ЕНЕРГОНЕЗАЛЕЖНОГО GPON. ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Вступ та постановка задачі

Сьогодні швидкісний, стабільний та безперебійний Інтернет - це не просто базова потреба людей, а критично важлива система всієї інфраструктури країни [3]. Від якості та надійності мереж доступу залежить стабільність цифрової економіки, робота державних реєстрів та сервісів (зокрема екосистеми "Дія"), безперервність дистанційної освіти, ефективність віддаленої роботи бізнесу, а також функціонування об'єктів критичної інфраструктури.

Вимоги до пропускної здатності постійно зростають через масовий перехід на хмарні технології, стрімке поширення відеоконтенту у форматі 4K/8K, розвиток IoT (Інтернету речей) та геймінгу [2]. Однак стара інфраструктура "останньої милі", побудована на базі мідного кабелю, підійшла до своєї технологічної межі.

Особливо гостро ця проблема постала в Україні в умовах повномасштабної війни. Починаючи з осені 2022 року, цілеспрямовані обстріли РФ по енергетичній інфраструктурі спричинили регулярні та тривалі відключення електроенергії (блекаути) [1]. У цих екстремальних умовах стало очевидно, що головним критерієм якості мережі є не лише її пропускна здатність, а й максимальна живучість та енергонезалежність. Традиційні мідні FTTB-вузли (Fiber-to-the-Building) масово виходили з ладу під час знеструмлень, оскільки їхня архітектура критично залежить від наявності електроживлення в кожному окремому будинку. Це змусило українських провайдерів) різко прискорити модернізацію та масово переходити на пасивні оптичні мережі а саме PON чи GPON.

Мета та завдання дослідження

Метою роботи є комплексний аналіз еволюції апаратного забезпечення мереж доступу інтернет-провайдерів в Україні (перехід від архітектури FTTB Ethernet до GPON FTTH), порівняння їхньої апаратної бази, оцінка впливу

енергетичної кризи на топологію мереж та визначення нових викликів для експлуатаційних (лінійних) підрозділів.

Завдання дослідження:

1. Проаналізувати історичні передумови та технічні фундаментальні відмінності технологій FTTB та GPON.
2. Дослідити структурні зміни в апаратному забезпеченні ядра мережі та клієнтського обладнання.
3. Оцінити фактор енергонезалежності як головне питання під час переходу на оптичні мережі доступу.
4. Визначити нові операційні задачі, інструментарій та вимоги до кваліфікації лінійних інженерів після міграції на оптику.
5. Сформувати прогноз щодо подальшого розвитку апаратного забезпечення.

Історичний контекст: феномен українського ринку та епоха FTTB

Варто зазначити унікальність українського телекомунікаційного ринку. На відміну від країн Західної Європи та США, де історично домінували телефонні та телевізійні монополісти, в Україні майже не набули широкого поширення технології доступу DOCSIS (по коаксіальному телевізійному кабелю) та ADSL/VDSL (по телефонних мідних парах) [3].

Європейські оператори роками намагалися "вичавити максимум" зі старих мідних ліній, модернізуючи обладнання на вузлах зв'язку. Український ринок, завдяки високій конкуренції серед локальних провайдерів ("домашніх мереж") та відсутності "історичного багажу", фактично перестрибнув цей етап. Починаючи з 2000-х років, провайдери масово розгортали мережі за технологією FTTB.

Архітектура та апаратне забезпечення FTTB: Оптика (магістральний кабель) прокладалася до багатоквартирного будинку, де на горищі або в підвалі встановлювалася антивандальна шафа з активним обладнанням - L2-комутатором (світчем) рівня доступу. Від комутатора до квартир абонентів розводився мідний кабель - "вита пара" (UTP)[3].

- **Переваги:** Низька вартість розгортання, простота підключення абонента (не потрібне додаткове обладнання, кабель вставляється прямо в ПК або дешевий Wi-Fi роутер), висока ремонтопридатність.
- **Недоліки:** Обмеження довжини мідного кабелю (до 100 метрів)[4], схильність до електромагнітних перешкод (вигорання портів від грозових розрядів), окислення контактів, високий ризик крадіжок кабелю. Але головний недолік розкрився під час війни - **залежність від локального живлення**. Комутатор потребує 220В. Встановлення джерел безперебійного живлення (ДБЖ) з акумуляторами у кожному будинку (а це тисячі ящиків для великого провайдера) виявилося економічно нерентабельним та логістично неможливим завданням в умовах тривалих відключень.
-

GPON-революція: зміна парадигми мережевої архітектури

Технологія GPON (Gigabit Passive Optical Network) кардинально змінила філософію побудови мереж "останньої милі", запропонувавши концепцію FTTH (Fiber-to-the-Home - оптика в квартиру) [5].

Технічні фундаментальні відмінності та апаратна база: Головна особливість PON полягає у слові "пасивна". Між вузлом провайдера та обладнанням клієнта відсутні будь-які активні електронні компоненти, що потребують електроживлення. Мережа будується за деревоподібною топологією за допомогою оптичних дільників (сплітерів) - пристроїв, які фізично розщеплюють світловий сигнал через систему призм.

Ключові елементи GPON:

1. **OLT (Optical Line Terminal)** - станційне обладнання (комутатор) високої щільності, що встановлюється в центральному вузлі зв'язку провайдера (Core/Aggregation node). Один порт OLT може обслуговувати до 128 абонентів. [5]
2. **Пасивна оптична розподільча мережа (ODN)** - система оптоволоконних кабелів, муфт, кросів та пасивних сплітерів (зазвичай з коефіцієнтом ділення 1:64 або 1:128).
3. **ONT (Optical Network Terminal) або ONU (Optical Network Unit)** - абонентський термінал, який встановлюється безпосередньо у квартирі клієнта. Він перетворює оптичний сигнал назад у електричний (Ethernet) і часто виконує роль Wi-Fi маршрутизатора.

Енергонезалежність як фактор національної стійкості: Під час масових знеструмлень GPON продемонстрував свою безпрецедентну ефективність. Оскільки проміжні вузли мережі є пасивними шматками скла і пластику, для роботи Інтернету достатньо заживити лише дві точки:

- Вузол провайдера (де стоїть OLT) - провайдери забезпечили їх потужними промисловими генераторами та акумуляторними збірками LiFePO4.
- Квартиру абонента - користувачеві достатньо підключити ONU-термінал та свій роутер до звичайного павербанка за допомогою DC-DC кабелю 9V/12V [1].

Таким чином, технологія GPON перетворилася з просто "швидкісного Інтернету" на життєво необхідний інструмент виживання в умовах інформаційного вакууму під час блекаутів.

Нові виклики для лінійних інженерів та операційних відділів

Перехід від FTTB до GPON - це не просто заміна одного обладнання на інше. Це зміна професійного інструментарію та мислення технічного персоналу. Робота інженера-монтажника (техніка який відповідає за підключення абонентів) зазнала кардинальних змін.

Зміни в інструментарії та навичках:

- **Відмова від "обжимки" на користь зварювання.** Якщо раніше головними інструментами монтажника були крімпер (для обжиму конекторів RJ-45) та LAN-тестер, то тепер інженер працює з високотехнологічним обладнанням: апаратами для автоматичного зварювання оптоволокна [6] (наприклад, Fujikura, Inno, Sumitomo), прецизійними сколювачами (cleaver) та інструментами для зняття лаку з волокна.
- **Робота з оптичним бюджетом.** Замість перевірки цілісності 8 жил мідного кабелю, інженер повинен вміти розраховувати та вимірювати загасання (втрати) оптичного сигналу. Брудний конектор, мікрозгин волокна під гострим кутом або неякісне зварювання можуть "покласти" всю гілку абонентів. У повсякденний вжиток увійшли вимірювачі оптичної потужності (Optical Power Meter) та візуальні дефектоскопи (VFL, "червоні ліхтарики").
- **Складна діагностика (OTDR).** Пошук пошкоджень у пасивній оптичній мережі вимагає використання оптичних рефлектометрів (OTDR). Інженер має вміти читати рефлектограму - графік, що показує стан лінії, відображення від сплітерів та точну відстань до місця обриву з точністю до метра [6].
- **Ювелірність роботи.** Оптоволокно (товщина якого порівнянна з людською волосиною) вимагає значно обережнішого поводження, ніж товстий UTP-кабель. Робота потребує ідеальної чистоти (використання безворсових серветок, ізопропілового спирту) та дотримання техніки безпеки при поводженні зі скляними уламками.

Ця трансформація вимагала від провайдерів величезних інвестицій не лише у закупівлю дорогого обладнання для бригад, а й у масове перенавчання персоналу.

Висновки та перспективи розвитку

Проведений аналіз дозволяє зробити висновок, що еволюція апаратного забезпечення мереж доступу в Україні пройшла шлях від тимчасових компромісних рішень (FTTB з мідною розводкою) до сучасних, стійких оптичних інфраструктур.

1. **Безпека та стійкість:** В українських реаліях технологія GPON довела, що єдина стійка архітектура зв'язку - це архітектура, вільна від залежності від транзитного електроживлення. Це питання не лише комфорту користувачів, а й національної інфраструктурної безпеки.
2. **Заміна активного на пасивне:** Перенесення всієї активної електроніки в захищені та резервовані ядра мережі провайдера знизило операційні витрати на обслуговування (менше виїздів на завислі свічі, немає вигорання від гроз).
3. **Технологічний заділ на майбутнє:** Побудована сьогодні пасивна інфраструктура (ODN - кабелі та сплітери) має величезний потенціал. Оптичне волокно майже не має обмежень щодо пропускної здатності в рамках побутових потреб. Наступний етап еволюції, який вже починається в Україні - це

впровадження стандартів **XG-PON** (10 Гбіт/с на завантаження, 2.5 Гбіт/с на віддачу) та **XGS-PON** (симетричні 10 Гбіт/с) [7].

4. **Економічна доцільність:** Перехід на XGS-PON потребуватиме заміни лише активного обладнання на кінцях мережі (OLT-карт у провайдера та ONU у абонента). Сама ж вулична та будинкова кабельна інфраструктура залишиться незмінною, що робить такі інвестиції довгостроковими та високорентабельними. Більше того, технології спектрального ущільнення дозволяють передавати сигнали звичайного GPON та XGS-PON по одному й тому ж волокну одночасно, забезпечуючи плавну міграцію.

Список використаних джерел

1. Міністерство цифрової трансформації України. (2022). Як залишатися з інтернетом під час відключень електроенергії: інструкція. Посилання на сайт: https://thedigital.gov.ua/news/how-tos/iak-zalyshatysia-na-zviazku-pid-chas-znestrumlen

2. Ericsson. (2023). Ericsson Mobility Report: Data traffic growth and network evolution. Посилання на сайт: https://www.ericsson.com/en/oss-bss/data-analytics

3. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій (НКЕК). (2024). Звіт про роботу НКЕК за 2023 рік (Стан ринку електронних комунікацій України). Посилання на Сайт: https://nkek.gov.ua/diialnist/sfery-diialnosti/elektronni-komunikatsii/ekonomichne-rehuliuvannia/rehuliuvannia-v-sferi-elektronnykh-komunikatsii

4. IEEE SA. (2022). IEEE 802.3-2022 - IEEE Standard for Ethernet. Посилання на сайт: https://standards.ieee.org/ieee/802.3/10422/

5. International Telecommunication Union. (2008). Recommendation ITU-T G.984.1 : Gigabit-capable passive optical networks (GPON): General characteristics. Посилання на сайт: https://www.itu.int/rec/T-REC-G.984.1/en

6. Компанія «ДЕПС» (DEPS). (2023). Основи побудови PON мереж: від теорії до практики (технічна документація та обладнання).

Посилання на сайт: https://deps.ua/ua/knowegable-base/samples-of-the-technical-solutions/ua-pon-network-construction-scheme.html

7. International Telecommunication Union. (2016). Recommendation ITU-T G.9807.1 : 10-Gigabit-capable symmetric passive optical network (XGS-PON). Посилання на сайт: https://www.itu.int/rec/T-REC-G.9807.1/en

Мельниченко Алла Вікторівна
студентка групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
(098)-941-47-48

Заячковський Андрій Володимирович
викладач кафедри Інженерії програмного забезпечення автоматизованих систем
Державного університету інформаційно комунікаційних технологій, м. Київ

РОЗРОБКА ВЕБ-ОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ СУПРОВОДУ НАВЧАЛЬНОГО ПРОЦЕСУ В ЦЕНТРАХ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

У роботі досліджено особливості розробки веб-орієнтованих інформаційних систем для супроводу навчального процесу в центрах підвищення кваліфікації. Визначено ключові функціональні вимоги до системи, включаючи управління контингентом слухачів, навчальними програмами, результатами оцінювання та аналітикою освітнього процесу. Запропоновано архітектурну модель системи на основі клієнт-серверного підходу та сучасних веб-технологій. Обґрунтовано доцільність використання модульної структури, REST API та хмарної інфраструктури. Розглянуто питання безпеки, масштабованості та інтеграції з іншими освітніми платформами.

Постановка задачі

Цифровізація освіти зумовлює необхідність створення інтегрованих інформаційних систем, що забезпечують повний цикл супроводу навчального процесу. Існуючі рішення часто є фрагментованими, не враховують специфіку короткострокових програм підвищення кваліфікації та мають обмежені можливості аналітики.

Мета дослідження

Розробити концептуальну модель та визначити технологічні засади створення веб-орієнтованої інформаційної системи супроводу навчального процесу в центрах підвищення кваліфікації.

Результати дослідження

Визначено функціональні модулі системи (реєстрація, навчальні програми, оцінювання, аналітика),запропоновано багаторівневу архітектуру (frontend, backend, база даних), обґрунтовано використання REST API для інтеграції, визначено механізми забезпечення безпеки (аутентифікація, шифрування, контроль доступу).

Висновки та перспективи

Запропонована модель дозволяє підвищити ефективність управління навчальним процесом, забезпечити прозорість освітніх результатів та автоматизувати ключові адміністративні функції.

Список використаних джерел

1. *Al-Fraihat, D., Joy, M., Karanasios, S., & Sinclair, J. (2020). Evaluating e-learning systems success: An empirical study. Computers in Human Behavior, 102, 67–86. https://doi.org/10.1016/j.chb.2019.08.004*
2. *Bass, L., Clements, P., & Kazman, R. (2021). Software architecture in practice (4th ed.). Addison-Wesley.*
3. *Fielding, R. T. (2000). Architectural styles and the design of network-based software architectures [Doctoral dissertation, University of California, Irvine].*
4. *ISO/IEC. (2011). Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models (ISO/IEC Standard No. 25010:2011). https://www.iso.org/standard/35733.html*
5. *Moodle Docs. (n.d.). Moodle documentation. Retrieved April 13, 2026, from https://docs.moodle.org*
6. *Newman, S. (2021). Building microservices (2nd ed.). O'Reilly Media.*
7. *Pressman, R. S., & Maxim, B. R. (2019). Software engineering: A practitioner's approach (9th ed.). McGraw-Hill Education.*
8. *Sommerville, I. (2015). Software engineering (10th ed.). Pearson.*
9. *Sun, P. C., Tsai, R. J., Finger, G., Chen, Y. Y., & Yeh, D. (2008). What drives a successful e-Learning? An empirical investigation of the critical factors influencing learner satisfaction. Computers & Education, 50(4), 1183–1202. https://doi.org/10.1016/j.compedu.2006.11.007*
10. *Weyrich, M., & Ebert, C. (2016). Reference architectures for the internet of things. IEEE Software, 33(1), 112–116. https://doi.org/10.1109/MS.2016.20*

Зінченко Ілля Денисович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
zinchenko.illia.d.2003@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

АНАЛІЗ ТА ОПТИМІЗАЦІЯ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ У МЕРЕЖЕВІЙ ІНФРАСТРУКТУРІ ПІДПРИЄМСТВА

Сучасні підприємства все активніше впроваджують системи відеоспостереження як складову комплексної безпеки та контролю виробничих процесів. Використання мережевих технологій дозволяє інтегрувати відеонагляд у загальну IT-інфраструктуру підприємства, забезпечуючи централізоване управління, масштабованість та доступ до відеоданих у режимі реального часу. Разом із тим, зростання кількості камер, підвищення роздільної здатності відео та необхідність безперервного запису створюють значне навантаження на мережу та системи зберігання, що потребує оптимізації архітектурних рішень та ефективного використання ресурсів [1].

Постановка задачі.

Основною проблемою при побудові сучасних систем відеоспостереження є забезпечення стабільної роботи при великому обсязі відеопотоків, що передаються у мережевій інфраструктурі підприємства. Зі збільшенням кількості IP-камер зростає навантаження на мережеве обладнання, відеореєстратори та підсистеми зберігання даних, що може призводити до затримок, втрат кадрів або перевантаження окремих вузлів системи. Додатково виникає необхідність забезпечення відмовостійкості, захисту даних та ефективного розподілу ресурсів між компонентами системи.

Мета дослідження.

Метою дослідження є аналіз архітектури програмно-апаратного комплексу системи відеоспостереження, обґрунтування вибору мережевої NVR-архітектури, дослідження підходів до організації передачі та зберігання відеоданих, а також визначення методів оптимізації навантаження на мережеву інфраструктуру підприємства.

Результати дослідження.

У результаті дослідження розглянуто принципи побудови систем відеоспостереження, зокрема аналогових та мережевих (IP) рішень. Встановлено,

що IP-системи забезпечують значно більшу гнучкість, масштабованість та можливість інтеграції у локальну мережу підприємства завдяки використанню стандартних мережевих протоколів та адресації [1].

Реалізована система базується на використанні мережевих відеореєстраторів (NVR), які виконують функції приймання, обробки та зберігання відеопотоків. Застосування декількох відеореєстраторів різних моделей дозволяє ефективно розподіляти навантаження між вузлами системи, що підвищує її відмовостійкість та забезпечує стабільну роботу навіть у випадку часткових відмов обладнання (рис. 1).

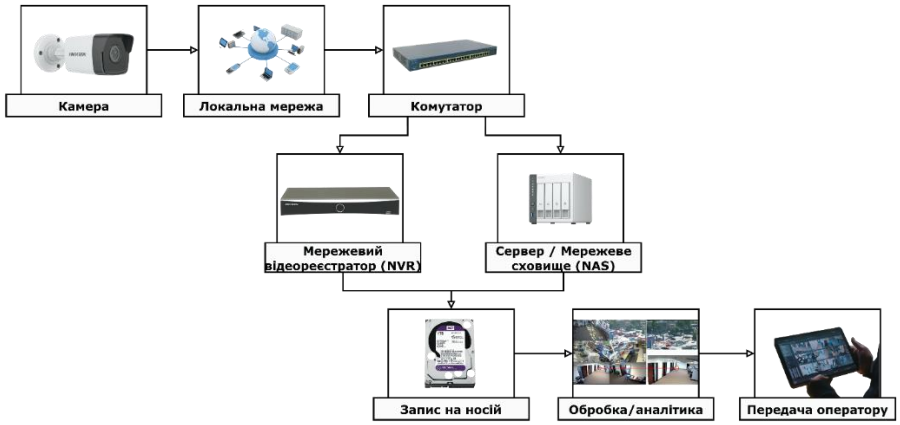

Рис. 1. Інтеграція засобів відеонагляду в мережеву інфраструктуру

Передача відеоданих організована через локальну мережу підприємства із використанням комутаторів та технології PoE, що дозволяє поєднати передачу даних і живлення камер через єдиний кабель. Це значно спрощує монтаж інфраструктури та знижує витрати на розгортання системи [2]. Додатково застосовується сегментація мережі та використання магістральних оптичних каналів, що забезпечує необхідну пропускну здатність для передачі відеопотоків високої якості.

Система зберігання даних реалізована на основі локальних накопичувачів відеореєстраторів із додатковим використанням мережевого сховища (NAS), що виконує функції резервування та централізованого доступу до відеоархіву. Такий підхід дозволяє забезпечити високу швидкість доступу до даних та незалежність від зовнішніх мережевих факторів [3].

Порівняльний аналіз показав, що використання NVR-архітектури є більш доцільним у порівнянні з DVR та хмарними рішеннями. DVR-системи поступаються за масштабованістю та гнучкістю, тоді як хмарні рішення, незважаючи на зручність, мають залежність від стабільності інтернет-з’єднання та можуть створювати ризики для конфіденційності даних.

Додатково проведено оцінку вартості системи, яка показала, що найбільшу частку витрат становлять IP-камери та мережеве обладнання, тоді як

відеореєстратори та системи зберігання мають відносно менший вплив на загальну вартість. Це підтверджує доцільність оптимізації параметрів відеопотоку та використання сучасних методів стиснення для зменшення навантаження на інфраструктуру [4].

Висновки та перспективи.

У результаті дослідження встановлено, що використання мережевої NVR-архітектури у поєднанні з сучасним мережевим обладнанням забезпечує високий рівень надійності, масштабованості та ефективності функціонування системи відеоспостереження підприємства. Реалізована структура дозволяє оптимально розподіляти навантаження, забезпечувати безперервний запис відеоданих та підтримувати централізоване управління системою.

Перспективними напрямами розвитку є інтеграція інтелектуальних методів відеоаналізу, використання технологій штучного інтелекту для автоматичної обробки подій, а також впровадження гібридних моделей зберігання даних (локально + хмара), що дозволить підвищити гнучкість системи та розширити її функціональні можливості.

Список використаних джерел:

1. Network Video Recorders vs DVR Systems. Security Today. URL: https://securitytoday.com/articles/2019/04/01/nvr-vs-dvr.aspx (дата звернення: 12.04.2026).

2. What is Power over Ethernet (PoE)? Cisco. URL: https://www.cisco.com/c/en/us/products/switches/what-is-power-over-ethernet.html (дата звернення: 12.04.2026).

3. Network Attached Storage (NAS) Explained. IBM. URL: https://www.ibm.com/topics/network-attached-storage (дата звернення: 13.04.2026).

4. Video Surveillance System Cost Guide. SafeWise. URL: https://www.safewise.com/security-system-cost/ (дата звернення: 13.04.2026).

Красюк Андрій Валерійович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
a.krasiuk1@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

АВТОМАТИЗОВАНА СИСТЕМА ЗАХИЩЕНОГО ДОСТУПУ ДО ВНУТРІШНІХ РЕСУРСІВ НА ОСНОВІ OPENVPN

Сучасні умови цифровізації та поширення віддаленої роботи обумовлюють необхідність створення надійних, масштабованих і водночас економічно доцільних рішень для забезпечення доступу користувачів до внутрішніх ресурсів організацій. Особливої актуальності набувають технології віртуальних приватних мереж (VPN), які дозволяють організувати захищене з'єднання через публічні мережі. Водночас використання традиційних підходів до розгортання інфраструктури часто потребує значних фінансових витрат та складного адміністрування, що обмежує їх застосування у малих організаціях або навчальних середовищах. У цьому контексті доцільним є дослідження можливостей побудови автоматизованих VPN-рішень із використанням наявного обладнання та відкритого програмного забезпечення [1].

Постановка задачі.

Основною проблемою є забезпечення безпечного, стабільного та продуктивного віддаленого доступу до внутрішніх ресурсів при обмежених апаратних і фінансових ресурсах. Додатковими викликами виступають складність адміністрування користувачів, ризики помилок при ручному налаштуванні, а також необхідність підтримання високого рівня безпеки в умовах нестабільних мереж (зокрема мобільних і бездротових).

Існуючі рішення часто орієнтовані на корпоративні середовища та не враховують потреби невеликих систем, де критичними є простота розгортання, автономність і можливість швидкого масштабування. Таким чином, виникає потреба у розробці автоматизованої системи VPN-доступу, яка поєднує ефективність, безпеку та економічну доцільність.

Мета дослідження.

Метою дослідження є розробка та аналіз автоматизованої системи підключення користувачів до внутрішніх ресурсів організації на основі технології OpenVPN, що забезпечує:

- захищену передачу даних через публічні мережі;
- автоматизацію процесів адміністрування;
- оптимізацію використання апаратних ресурсів;

- можливість масштабування та інтеграції з централізованими системами управління доступом.

Результати дослідження.

У межах дослідження реалізовано систему віддаленого доступу на базі клієнт-серверної архітектури, де VPN-сервер розгорнуто на основі ноутбука бізнес-класу, що дозволило суттєво знизити вартість впровадження без втрати функціональності. Використання OpenVPN забезпечило створення захищеного тунелю з підтримкою сучасних криптографічних алгоритмів і гнучких механізмів налаштування [1].

Процес функціонування системи включає етапи ініціалізації з'єднання, узгодження параметрів, автентифікації користувача та встановлення захищеного каналу зв'язку. Для підвищення рівня безпеки реалізовано багатофакторну автентифікацію, що поєднує сертифікати, пароль та одноразові коди. Такий підхід дозволяє мінімізувати ризики несанкціонованого доступу навіть у випадку компрометації одного з факторів (рис. 1) [2].

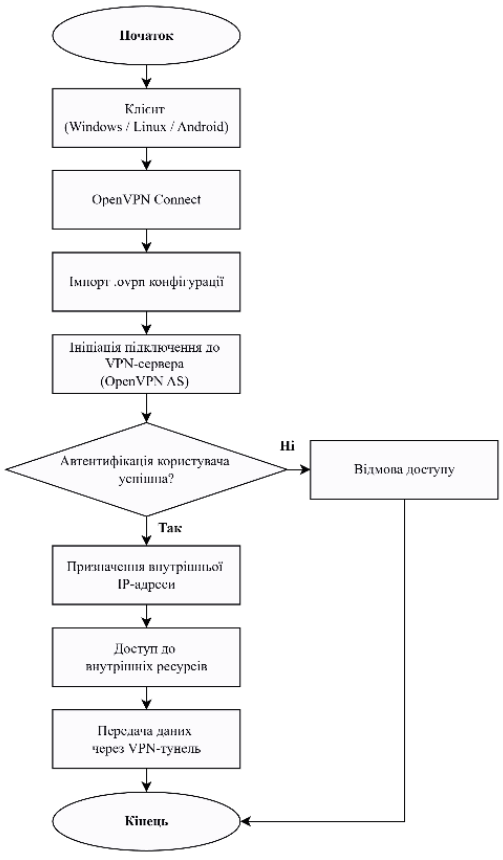

Рис. 1. Клієнт-серверна комунікація

Одним із ключових результатів є автоматизація процесу створення клієнтських конфігурацій за допомогою bash-скриптів. Це дозволило скоротити час розгортання з десятків хвилин до кількох секунд, зменшити кількість помилок і

забезпечити стандартизацію налаштувань. Автоматизація також сприяє ефективному масштабуванню системи при зростанні кількості користувачів.

Проведене тестування показало, що середня пропускна здатність системи становить близько 30 Мбіт/с у напрямку до сервера та 20 Мбіт/с у зворотному напрямку, що відповідає умовам використання мобільних і бездротових мереж. Важливим фактором оптимізації є вибір транспортного протоколу: використання UDP замість TCP дозволяє уникнути явища TCP-over-TCP meltdown та підвищити ефективність передачі даних [3].

Додатково було досліджено вплив криптографічних алгоритмів на продуктивність системи. Встановлено, що перехід від AES-256-GCM до AES-128-GCM дозволяє зменшити навантаження на процесор без суттєвого зниження рівня безпеки, що є критично важливим для систем, побудованих на обмежених апаратних ресурсах.

З економічної точки зору запропоноване рішення демонструє значні переваги: загальна вартість системи становить близько 20 000 грн, що суттєво нижче порівняно з традиційними серверними рішеннями. Це досягається завдяки використанню наявного обладнання, відкритого програмного забезпечення та енергоефективних компонентів.

Перспективи розвитку системи включають інтеграцію з централізованими системами управління доступом (Active Directory, LDAP), що дозволить реалізувати єдину точку адміністрування, а також впровадження гібридної архітектури з використанням хмарних рішень для підвищення відмовостійкості та доступності сервісу [4].

Висновки та перспективи.

У результаті дослідження розроблено та апробовано автоматизовану систему захищеного доступу до внутрішніх ресурсів на основі OpenVPN, яка поєднує ефективність, безпеку та низьку вартість впровадження. Запропонований підхід дозволяє використовувати наявне обладнання як повноцінну серверну платформу, забезпечуючи стабільну роботу навіть у складних мережевих умовах.

Подальші дослідження можуть бути спрямовані на інтеграцію системи з хмарними сервісами, впровадження інтелектуальних механізмів аналізу трафіку та автоматичного реагування на загрози, а також розширення функціональності за рахунок використання сучасних протоколів і технологій мережевої безпеки.

Список використаних джерел

1. What is a VPN? – Cloudflare. URL: https://www.cloudflare.com/learning/network-layer/what-is-a-vpn/ (дата звернення: 12.04.2026).

2. Multi-Factor Authentication (MFA) – Microsoft. URL: https://learn.microsoft.com/en-us/security/identity-protection/mfa-overview (дата звернення: 13.04.2026).

3. TCP vs UDP for VPN – OpenVPN Documentation. URL: https://openvpn.net/faq/what-is-the-difference-between-tcp-and-udp/ (дата звернення: 13.04.2026).

4. Integrating VPN with Active Directory – Microsoft Docs. URL: https://learn.microsoft.com/en-us/windows-server/remote/remote-access/vpn/vpn-top (дата звернення: 13.04.2026).

Ситник Євген Олегович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st6827393@stud.duikt.edu.ua

ЦИФРОВИЙ ДВІЙНИК МІСТА: ВІД РЕАКТИВНОГО ГАСІННЯ ПОЖЕЖ ДО ПРОАКТИВНОГО МОДЕЛЮВАННЯ

Постановка задачі

Більшість сучасних міст і досі керуються за принципом «виникла проблема - шукаємо рішення». Ми бачимо це щодня: коли на дорогах уже стоять затори, ми намагаємося регулювати рух; коли трапляється аварія на тепломережі, ми починаємо ремонт. Такий реактивний підхід вичерпав себе, адже він бореться з наслідками, а не з причинами. Виникає питання: чи можна побачити кризу до того, як вона стане реальністю?. Саме тут на сцену виходить концепція цифрового двійника (Digital Twin) - не просто 3D-карти, а живого цифрового організму, який дихає в унісон з реальним містом.

Мета дослідження

Розібратися, як перетворити масиви даних з датчиків на інструмент, що дозволяє «прокрутити» майбутнє міста на комп'ютері. Нам потрібно зрозуміти, де в цій технології закінчується красива візуалізація і починається реальна аналітика, яка допоможе зробити життя в місті безпечнішим та ефективнішим.

Результати дослідження

Цифровий двійник - це своєрідна віртуальна лабораторія. Якщо Fuller та колеги наголошують на технічній стороні збору даних, то для нас важливо, як ці дані працюють у зв'язці.

1. **Можливість безпечної помилки.** Це, мабуть, найцінніше. Ми можемо «побудувати» нову розв'язку або змінити маршрути громадського транспорту у віртуальному просторі й побачити результат ще до того, як буде витрачено першу гривню з бюджету. Це дозволяє проводити експерименти, які в реальному житті були б занадто дорогими або небезпечними.

2. **Єдиний нервовий центр.** Зазвичай дані про транспорт, екологію та енергетику живуть у різних департаментах. Цифровий двійник об’єднує їх. Як зазначає M. Batty, людський мозок просто не здатний охопити тисячі дрібних зв’язків між міськими процесами одночасно - а цифрова модель може. Це дає змогу бачити місто як цілісну систему, а не набір окремих вулиць чи труб.

3. **Економіка даних.** Згідно з дослідженнями OECD, державний сектор, який спирається на реальні цифри, а не на інтуїцію, працює в рази ефективніше. Це особливо актуально для комунальних служб: прогнозування пікових навантажень дозволяє уникати аварій та економити ресурси.

Для України ця технологія сьогодні - не розкіш, а необхідність. Під час відбудови ми маємо шанс не просто копіювати старі радянські схеми, а одразу закладати «розумний» фундамент. Це дозволить будувати міста, які будуть стійкими до нових викликів.

Де ховаються ризики?

Було б помилкою вважати Digital Twin магічною кулею. Система працює рівно настільки добре, наскільки якісні дані ми в неї завантажуємо. Якщо сенсори брешуть або база даних застаріла, двійник видасть таку ж «криву» відповідь. OECD справедливо застерігає: без чітких стандартів безпеки та, що найважливіше, довіри людей до цих алгоритмів, технологія залишиться лише дорогою іграшкою.

Висновки

Цифровий двійник - це про зміну мислення. Це перехід від гасіння пожеж до стратегічного передбачення. Ми повинні використовувати цей інструмент, щоб робити наші міста не просто «цифровими», а справді життєздатними в довгостроковій перспективі.

Список використаних джерел

1. Batty, M. (2018). Digital twins. Environment and Planning B: Urban Analytics and City Science, 45(5), 817-820. https://doi.org/10.1177/2399808318796416

2. Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access, 8, 108952-108971. https://doi.org/10.1109/ACCESS.2020.2998358

3. OECD. (2019). The Path to Becoming a Data-Driven Public Sector. OECD Publishing. https://doi.org/10.1787/059814a7-en

Сіроєдов Валерій Олександрович
студент групи ТЦР-44
Державного університету інформаційно-комунікаційних технологій м. Київ
siroedovvv@gmail.com

Бажан Тетяна Олександрівна
старший викладач кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА ВЕБ-ЗАСТОСУНКУ ДЛЯ ВЕДЕННЯ ТА АНАЛІЗУ СИЛОВИХ ТРЕНУВАНЬ ІЗ ВИКОРИСТАННЯМ PYTHON ТА DJANGO

Постановка задачі.

Сьогодні все більше людей займаються спортом та намагаються систематизувати свої тренування. При цьому багато хто веде записи у блокнотах

або нотатках на телефоні, що не є зручним та не дозволяє повноцінно аналізувати результати.

Основною проблемою є відсутність простого інструменту, який дозволяє не лише фіксувати виконані вправи, а й відстежувати прогрес у часі. Без такої системи користувачам складно оцінити ефективність тренувань, визначити власні рекорди та планувати подальше навантаження.

Також важливим є питання збереження історії тренувань та швидкого доступу до попередніх результатів. Саме тому виникає потреба у створенні програмного рішення, яке поєднує зручність використання та можливість аналізу даних [1].

Мета дослідження.

Основною метою роботи є створення веб-застосунку, який дає можливість користувачам зручно зберігати результати виконання вправ, а також переглядати попередні тренування та відстежувати зміни показників.

Результати дослідження.

Під час розробки було обрано підхід, при якому застосунок працює через браузер, а обробка даних відбувається на серверній частині. Така організація дозволяє відокремити логіку роботи системи від інтерфейсу та зробити її більш зрозумілою з точки зору реалізації [2].

Як основний інструмент використано мову програмування Python та фреймворк Django. Це рішення дозволяє швидко реалізувати основні функції застосунку, зокрема роботу з користувачами, обробку запитів та збереження інформації без необхідності створення всіх компонентів з нуля [4].

Інформація про тренування зберігається у реляційній базі даних, де окремо представлені користувачі, вправи та результати їх виконання. Такий підхід дозволяє логічно структурувати дані та забезпечує зручну роботу з ними [1].

У розробленому застосунку передбачено такі можливості:

- додавання та редагування вправ;
- внесення результатів після виконання підходів;
- перегляд попередніх тренувань;
- відображення максимальних досягнень для кожної вправи.

Для спрощення взаємодії з базою даних застосовано механізм ORM, який дозволяє працювати з даними у вигляді об’єктів, не заглиблюючись у деталі SQL-запитів [3].

Рис. 1. Загальна структура взаємодії елементів веб-застосунку

Завдяки такій організації користувач отримує можливість швидко знайти потрібну інформацію та використовувати її під час наступних тренувань. Також застосунок може відкриватися як на комп'ютері, так і на мобільному пристрої без додаткової адаптації.

Висновки.

У результаті виконаної роботи створено веб-застосунок, який дозволяє впорядкувати процес ведення тренувань та зробити його більш зручним у повсякденному використанні.

Обрані інструменти розробки дають змогу реалізувати необхідний функціонал без зайвої складності та забезпечують можливість подальшого розширення системи.

Отримане рішення може використовуватися як основа для подальшого розвитку, зокрема для додавання аналітичних функцій або інтеграції з іншими сервісами.

Список використаних джерел

1. *Elmasri, R., & Navathe, S. B. (2016). Fundamentals of database systems (7th ed.). Pearson.*
2. *Richards, M., & Ford, N. (2020). Fundamentals of software architecture: An engineering approach. O'Reilly Media.*
3. *Kleppmann, M. (2017). Designing data-intensive applications. O'Reilly Media.*
4. *Django Software Foundation. (2026). Django documentation. Retrieved April 13, 2026, from https://docs.djangoproject.com/*
5. *Richards, M., & Ford, N. (2020). Fundamentals of software architecture: An engineering approach. O'Reilly Media.*

Явдюк Тимофій Миколайович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
tima.uvdik@gmail.com

Бондарчук Олександр Павлович
викладач кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.bondarchuk@duikt.edu.ua

ВИКОРИСТАННЯ ПРОТОКОЛУ IRC ЯК СТІЙКОГО РЕЗЕРВНОГО КАНАЛУ ЗВ'ЯЗКУ ДЛЯ КРИТИЧНОЇ ІТ-ІНФРАСТРУКТУРИ

Сучасна критична ІТ-інфраструктура глибоко залежить від стабільних широкосмугових мереж. Управління центрами обробки даних та розподіленими системами вимагає безперервної координації оперативного персоналу та засобів моніторингу [1]. Тому стійкість цих комунікацій є не просто зручністю, а фундаментальним елементом загальної відмовостійкості (resilience) системи під час надзвичайних ситуацій.

Водночас, домінуючі корпоративні рішення (Slack, Microsoft Teams, Telegram) демонструють критичну вразливість до деградації мережевого середовища. Їхня архітектура, що покладається на хмарні сервери, постійні виклики REST API та важкі графічні інтерфейси, генерує надлишковий трафік і вимагає стабільного з'єднання. Під час блекаутів чи вимушеного переходу на перевантажені мережі 2G/EDGE високі затримки (latency) та втрата пакетів руйнують механізми їхньої синхронізації стану. Як наслідок, ці інструменти стають повністю недієздатними, залишаючи системних адміністраторів у комунікаційному вакуумі та без контролю над інфраструктурою.

Відтак, виникає гостра необхідність у децентралізованому резервному інструменті координації. Він має відрізнятися екстремально низькими вимогами до пропускної здатності, автономністю (self-hosted) та здатністю до швидкого розгортання в ізольованих контурах [2]. Більше того, цей інструмент повинен діяти як єдина текстова шина даних для комунікації інженерів та збору базової IoT-телеметрії. Це гарантує збереження керованості ІТ-системами навіть за повної відмови основних мереж та веб-дашбордів.

Постановка задачі

Головна проблема управління критичною ІТ-інфраструктурою під час кризових ситуацій полягає у забезпеченні гарантованої доставки управляючих текстових команд, системних алертів та мінімальної апаратної телеметрії між

адміністраторами і серверами. Коли пропускна здатність мережі екстремально звужується, а рівень втрати пакетів стрімко зростає, сучасні "важкі" протоколи прикладного рівня часто не здатні підтримувати стабільні сесії для передачі навіть життєво необхідних обсягів даних [3].

Вирішення цієї задачі вимагає дотримання жорстких архітектурних обмежень. Насамперед, комунікаційне ядро має бути повністю автономним (self-hosted) для збереження керованості у випадку фізичної ізоляції мережі. Інструмент повинен бути гранично мінімалістичним: відмова від передачі надлишкового інтерфейсного коду чи метаданих максимізує проходження корисного навантаження. З міркувань безпеки контур зобов'язаний підтримувати сучасне шифрування на транспортному рівні. Це гарантує конфіденційність команд і телеметрії, не обтяжуючи базовий протокол додатковими криптографічними надбудовами.

Мета дослідження

Метою дослідження є обґрунтування доцільності використання архітектури протоколу IRC як базового резервного комунікаційного ядра для IT-підрозділів в умовах надзвичайних ситуацій. Робота спрямована на доведення здатності цього мінімалістичного стандарту забезпечувати безперервність оперативного управління критичною інфраструктурою під час екстремальної деградації пропускної здатності мережі, компенсуючи повну відмову сучасних корпоративних платформ.

Дослідження має на меті продемонструвати, як консолідована текстова взаємодія між адміністраторами, системними ботами та IoT-датчиками – за умови повної відмови від ресурсомістких графічних інтерфейсів – дозволяє оптимізувати моніторинг та низькорівневе апаратне управління в умовах жорсткого дефіциту обчислювальних та мережевих ресурсів.

Результати дослідження

Архітектура IRC (RFC 1459/2812) демонструє виняткову ефективність за умов дефіциту пропускної здатності. Оперуючи чистим текстом поверх TCP/IP, протокол зводить мережеві витрати до мінімуму – службові дані одного повідомлення вимірюються ліченими десятками байтів. Як наслідок, обмін командами в IRC потребує на порядки менше трафіку порівняно із сучасними платформами, що критично обтяжені викликами REST API, JSON-серіалізацією та завантаженням графічних веб-інтерфейсів [4].

З точки зору безпеки пріоритетом є мінімізація поверхні атаки. Відсутність наскрізного шифрування у базовому стандарті IRC надійно компенсується інкапсуляцією трафіку в захищені TLS-тунелі. Водночас розгортання ізольованого сервера у зв'язці з консольними або кастомними мобільними клієнтами радикально знижує ризик компрометації інфраструктури через типові вразливості браузерів та сторонніх інтеграцій [5].

Окремим напрямком стала концепція інтеграції прямої IoT-телеметрії через TCP-сокети в загальне середовище. Базові мікроконтролери можуть транслювати сирі текстові дані (наприклад, рівень заряду акумуляторів джерел безперебійного живлення) безпосередньо на IRC-сервер. Це усуває архітектурну необхідність у розгортанні та підтримці складних брокерів повідомлень (на кшталт MQTT), що є критичною перевагою в умовах часткової деградації обчислювальних потужностей дата-центру [6].

Запропонований підхід формує консолідоване середовище взаємодії "Людина-Машина". У спільних текстових каналах адміністратори координують дії пліч-о-пліч із моніторинговими скриптами та IoT-пристроями. Діючи як віртуальні користувачі, останні автоматично транслюють алерти та телеметрію безпосередньо в потік повідомлень, гарантуючи оперативне інформування без потреби завантажувати ресурсномісткі зовнішні дашборди.

Водночас оцінка структурної стійкості (resilience) підтверджує надійність архітектури завдяки механізмам федерації. Об'єднання незалежних серверів у єдину логічну мережу нівелює ризики єдиної точки відмови: при знеструмленні або втраті зв'язку з одним із вузлів, решта продовжує функціонувати. Це гарантує збереження цілісного комунікаційного ядра навіть за умов масштабних інфраструктурних руйнувань та локальних блекаутів [7].

Висновки та перспективи

Проведене дослідження підтверджує, що протокол IRC є високоефективним інструментом "судного дня" для управління критичною IT-інфраструктурою. Його технологічний вік виступає не архаїзмом, а неочікуваною стратегічною перевагою: архітектура, яка проектувалася та відточувалася для роботи в умовах повільного і нестабільного зв'язку на зорі розвитку інтернету, парадоксальним чином ідеально відповідає мережевим реаліям сучасних блекаутів. Відмова від сучасного надлишкового функціоналу на користь роботи з чистим текстом гарантує збереження базової керованості серверами та апаратним забезпеченням навіть за умов майже повної деградації комунікаційних каналів.

Перспективи подальших досліджень у цьому напрямку охоплюють розширення практичного інструментарію та підвищення рівня системної автоматизації. Пріоритетним завданням є розробка стандартизованих шаблонів за методологією "Інфраструктура як код" (Infrastructure as Code) для миттєвого розгортання ізольованих резервних IRC-мереж. Крім того, значний науковий та інженерний потенціал лежить у площині створення спеціалізованих, криптографічно стійких мобільних клієнтів, а також у поглибленому вивченні концепції ChatOps – побудові комплексних систем автоматизованого реагування на інциденти безпосередньо через обробку керуючих IRC-команд.

Список використаних джерел

1. Disaster resilience in communication networks [Guest Editorial] / M. Nogueira et al. IEEE Communications Magazine. 2014. Vol. 52, no. 10. P. 44–45. URL: https://doi.org/10.1109/mcom.2014.6917400 (date of access: 8.04.2026).

2. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / A. Al-Fuqaha et al. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, no. 4. P. 2347–2376. URL: https://doi.org/10.1109/comst.2015.2444095 (date of access: 8.04.2026).

3. Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation / J. P. G. Sterbenz et al. Telecommunication Systems. 2011. URL: https://doi.org/10.1007/s11235-011-9573-6 (date of access: 8.04.2026).

4. Oikarinen J., Reed D. Internet Relay Chat Protocol. RFC Editor, 1993. URL: https://doi.org/10.17487/rfc1459 (date of access: 8.04.2026).

5. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. RFC Editor, 2008. URL: https://doi.org/10.17487/rfc5246 (date of access: 8.04.2026).

6. A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks / J. E. Luzuriaga et al. 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015. 2015. URL: https://doi.org/10.1109/ccnc.2015.7158101 (date of access: 8.04.2026).

7. Kalt C. Internet Relay Chat: Architecture. RFC Editor, 2000. URL: https://doi.org/10.17487/rfc2810 (date of access: 8.04.2026).

Зайченко Сергій Петрович
аспірант групи АІСТ-31
Державного університету інформаційно-комунікаційних технологій
м. Київ

Полоневич Ольга Володимирівна
к.т.н., доцент, доцент кафедри інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій,
o.polonevych@duikt.edu.ua

ЗАСТОСУВАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ

На сьогодняшній день, в період активного розвитку телекомунікацій та постійного зростання обсягів передаваних даних все більшого значення набуває забезпечення стабільної та безпечної роботи телекомунікаційних мереж. Збільшення кількості підключених пристроїв, особливо в умовах поширення Інтернету речей, призводить до постійного ускладнення структури мереж, що супроводжує появу нових загроз та аномальних явищ у мережевому трафіку.

Одним із сучасних рішень моніторингу мережевого трафіку є застосування методів машинного навчання, які надають змогу автоматизувати процес аналізу даних і підвищити точність виявлення аномалій. В даний час такі методи

являються ключовим інструментом розвитку інтелектуальних інформаційних систем. Особливість застосування машинного навчання полягає у здатності систем адаптуватися та покращувати результати своєї роботи на основі накопичених даних, тобто ефективність моделі збільшується в процесі її взаємодії з новими даними. Основним завданням машинного навчання є побудова моделі, яка може самостійно знаходити приховані закономірності у великих обсягах інформації використовуючи їх для прогнозування [1]. У контексті телекомунікаційних мереж це означає можливість виконувати аналіз трафік в режимі реального часу, виявляти незвичну активність та в оперативному режимі зреагувати на потенційні загрози.

До основних підходів машинного навчання слід віднести контрольоване навчання, при якому використовуються попередньо підготовлені та розмічені дані [2]. На їх базі модель встановлює залежності між параметрами та результатами, що надає змогу в подальшому виконувати класифікацію нових даних. Наприклад, у задачах бербезпеки це може бути розподілення мережевого трафіку на нормальний та той що може нашкодити. Кординально інший підход - неконтрольоване навчання, що базується на аналізі нерозмічених даних. В такому випадку система самостійно визначає структуру даних та виконує виявлення закономірностей. В більшості випадків застосовуються алгоритми кластеризації, які надають змогу групувати дані за спільними ознаками. Такий підхід є досить корисним для виявлення нових типів аномалій, які раніше не фіксувалися.

Слід зазначити, що важливу роль у побудові моделей відіграє тип даних. Розмічені дані забезпечують високу точність, однак їх підготовка є досить складною процедурою та вимагає значних затрат часового ресурсу. Натомість нерозмічені дані доступні у великих обсягах, але їх аналіз є більш складним і потребує додаткових обчислювальних ресурсів.

Таким чином, використання методів машинного навчання є ефективним підходом до виконання задачі виявлення аномалій та надає змогу автоматизувати обробку великих обсягів трафіку, виявляти відхилення у роботі системи, виконати прогноз потенційних загроз та підвищити ефективність засобів захисту [3]. Використання та поєднання різних підходів до навчання надає змогу як виявляти вже відомі загрози, так і знаходити нові. Незважаючи на складність реалізації та потребу у значних ресурсах, такі технології забезпечують високу точність, гнучкість і автоматизацію аналізу.

Список використаних джерел

1. Schummer P., del Rio A., Serrano J. Machine Learning-Based Network Anomaly Detection: Design, Implementation, and Evaluation // AI. – 2024

2. Chentoufi O., Choukhairi M. An Enhanced Machine Learning Framework for Network Anomaly Detection // AI. – 2025.

3. Krzysztoń E., Rojek I. Comparative Analysis of Anomaly Detection Methods in IoT Networks // Applied Sciences. – 2024.

Зиков Михайло Віталійович
студент групи ТЦР-44
Державний університет інформаційно-комунікаційних технологій м. Київ
zykovmihail35@gmail.com

Гавор Артур Станіславович
викладач кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій м. Київ

ЗАСТОСУВАННЯ МОВИ C++ ТА ФРЕЙМВОРКУ QT ДЛЯ РОЗРОБКИ ДЕСКТОПНОГО ЗАСТОСУНКУ З КЕРУВАННЯ КАТАЛОГОМ ФІЛЬМІВ

Постановка задачі. Зростання кількості доступного кіноконтенту ставить перед користувачами практичне питання: як зручно організувати власну кінотеку, відстежувати переглянуте і знаходити потрібне. Більшість відомих платформ - IMDb, Letterboxd - є онлайн-сервісами без офлайн-режиму. Серед десктопних рішень існує Kodi, проте він розрахований на технічно підготовлених користувачів і потребує значного налаштування. Таким чином, існує потреба у простому автономному застосунку з сучасним інтерфейсом для ведення особистої кінотеки.

Мета дослідження. Спроєктувати та реалізувати десктопний застосунок CinemaHub, який дозволяє користувачу вести особисту кінотеку в офлайн-режимі - переглядати каталог фільмів, шукати потрібні стрічки, зберігати обране і відкривати трейлери - із зручним сучасним інтерфейсом, розробленим засобами мови C++ і фреймворку Qt 6. На даному етапі виконано аналіз, проєктування та базову реалізацію застосунку.

Аналіз предметної галузі. Для вирішення поставленої задачі проаналізовано наявні програмні рішення. IMDb і Letterboxd надають широкий функціонал, але повністю залежать від мережі. Kodi працює офлайн, але має перевантажений інтерфейс і орієнтований на відтворення контенту, а не на керування каталогом. MediaMonkey розроблявся переважно для аудіо і підтримує відео лише частково. Розглянуті рішення не повністю відповідають вимогам автономної роботи, простоти інтерфейсу та орієнтації саме на керування персональною кінотекою.

Вибір та обґрунтування технологічного стеку. Для реалізації застосунку розглядалось кілька варіантів технологічного стеку. Серед мов програмування порівнювались Java, Python і C++. Java і Python мають вищий рівень абстракції, але поступаються C++ у продуктивності і контролі над ресурсами - що важливо при роботі з великою кількістю постерів і медіаданих. C++17 обрано як основну мову розробки [5].

Серед UI-фреймворків розглядались wxWidgets, Electron і Qt 6. wxWidgets має обмежені засоби стилізації. Electron потребує вбудованого браузерного рушія, що суттєво збільшує розмір застосунку. Qt 6 надає компоненти для інтерфейсу, механізм сигналів і слотів, гнучку стилізацію через QSS і вбудовану підтримку мультимедіа без підключення сторонніх бібліотек [2]. Саме тому Qt 6 обрано як основний фреймворк [4].

Архітектуру застосунку спроєктовано за компонентним принципом: кожен екран - окремий клас із власною відповідальністю. Взаємодія між компонентами відбувається через сигнали і слоти, що мінімізує залежності між модулями і дозволяє змінювати окремі частини незалежно [3].

Висновки. На основі порівняльного аналізу обґрунтовано вибір технологічного стеку. C++17 обрано за продуктивність і контроль над ресурсами; Qt 6 - за вбудовану підтримку мультимедіа і гнучкі засоби стилізації; CMake - як стандартну систему збірки для Qt 6. Порівняно з IMDb і Letterboxd, спроєктоване рішення працює офлайн і зберігає дані локально. Подальші дослідження будуть спрямовані на програмну реалізацію застосунку і тестування [1].

Список використаних джерел

1. *Myers G. J., Sandler C., & Badgett T. (2011). The art of software testing (3rd ed.). Wiley.*
2. *Ousterhout J. (2021). A philosophy of software design (2nd ed.). Yaknyam Press.*
3. *Qt Group. (2024). Qt multimedia overview. https://doc.qt.io/qt-6/multimediaoverview.html*
4. *Qt Group. (2024). Qt 6 documentation. https://doc.qt.io/qt-6/*
5. *Stroustrup B. (2022). A tour of C++ (3rd ed.). Addison-Wesley Professional.*

Куцовол Іванна Іванівна
студентка групи ТЦР-44
Державного університету інформаційно-комунікаційних технологій
+380-(50)-136-90-25
st6815720@stud.duikt.edu.ua

Бажан Тетяна Олександрівна
старший викладач кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА МАСШТАБОВАНОГО ВЕБЗАСТОСУНКУ ІНТЕРНЕТ-МАГАЗИНУ НА ОСНОВІ NEXT.JS ТА SPRING BOOT

Постановка задачі. У сучасних умовах цифрової економіки електронна комерція є одним із ключових напрямів розвитку IT-систем. Зростання кількості онлайн-магазинів створює потребу у розробці високопродуктивних, масштабованих та зручних для користувача вебзастосунків.

Основними проблемами існуючих рішень є низька швидкість завантаження сторінок, складність масштабування, обмежена інтеграція з платіжними системами та недостатній рівень персоналізації користувацького досвіду.

Мета дослідження. Метою дослідження є розробка архітектури сучасного вебзастосунку інтернет-магазину з використанням технологій **Next.js** для фронтенду та **Spring Boot** для бекенду, що забезпечить високу продуктивність, масштабованість та зручність користування. Додатковими задачами є реалізація системи управління товарами, обробки замовлень та інтеграції з базою даних для ефективного зберігання інформації відповідно до принципів REST-архітектури [1].

Результати дослідження. У ході роботи було спроєктовано та реалізовано вебзастосунок інтернет-магазину, що складається з клієнтської та серверної частин.

Фронтенд реалізовано з використанням фреймворку Next.js, який забезпечує серверний рендеринг (SSR) та генерацію статичних сторінок (SSG), що дозволяє значно покращити швидкість завантаження та SEO-оптимізацію [3]. Інтерфейс користувача побудований із застосуванням адаптивного дизайну, що забезпечує коректне відображення на різних пристроях.

Бекенд реалізовано на основі Spring Boot із використанням RESTful API для взаємодії з клієнтською частиною [2]. Для роботи з даними використовується реляційна база даних, що забезпечує структуроване зберігання інформації про товари, категорії та замовлення.

Архітектура системи побудована за принципом розділення відповідальностей, що спрощує підтримку та масштабування системи [4].

Реалізовано основні функції інтернет-магазину:

1. Перегляд каталогу товарів.
2. Фільтрація та пошук товарів.
3. Додавання товарів у кошик.
4. Оформлення замовлення.
5. Обчислення вартості з урахуванням доставки та знижок.

Застосування Docker-контейнеризації дозволяє спростити розгортання системи та забезпечує її переносимість між різними середовищами.

Висновки. У результаті дослідження було розроблено ефективну архітектуру вебзастосунку інтернет-магазину, яка відповідає сучасним вимогам до продуктивності, масштабованості та зручності використання. Використання Next.js та Spring Boot дозволило досягти оптимального поєднання швидкодії клієнтської частини та надійності серверної логіки.

Запропонований підхід може бути використаний для створення комерційних вебзастосунків у сфері електронної торгівлі. Перспективами подальших досліджень є інтеграція систем рекомендацій на

основі машинного навчання, впровадження мікросервісної архітектури та використання хмарних технологій.

Список використаних джерел

1. *Fielding R. T. Architectural styles and the design of network-based software architectures. University of California, Irvine. 2000.*
2. *Tilkov S., Vinoski S. Node.js: Using JavaScript to Build High-Performance Network Programs. IEEE Internet Computing. 2010. Vol. 14, No. 6. P. 80–83.*
3. *Vercel. Next.js Documentation. 2025. URL: https://nextjs.org/docs*
4. *VMware. Spring Boot Reference Documentation. 2024. URL: https://docs.spring.io/spring-boot/docs/current/reference/html/*
5. *Richardson C. Microservices Patterns. Manning Publications. 2018.*

Гончаренко Антон Ігорович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету інформаційно-комунікаційних технологій, м. Київ
antoniogonch2005@gmail.com

ВЕБ-ОРІЄНТОВАНА ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ФОРМУВАННЯ МАРКЕТИНГОВИХ СТРАТЕГІЙ

Веб-орієнтована інформаційна система, що підтримує прийняття рішень у розробці маркетингових стратегій. Цифровий маркетинг розглядається як один з ключових інструментів для просування товарів і послуг у сучасному середовищі цифрової трансформації бізнесу. Цифрові комунікації зростають такими швидкими темпами, що інвестиції в цифрову рекламу є однією з найважливіших тенденцій. Частка цифрової реклами на світовому ринку реклами перевищує 70% і зростає відповідно до аналітичних даних [1]. Це є доказом поступового домінування цифрових каналів у структурі маркетингових комунікацій підприємств.

Хоча можливості рекламних платформ зростають, налаштування рекламних кампаній також стає більш складним. Спеціалісту потрібна велика кількість інформації на різних етапах, таких як маркетингова мета, аудиторія на основі ринку, контроль бюджету, вибір рекламного креативу, формування воронки продажів та оптимізація рекламної кампанії для ефективної роботи. Помилки на будь-якому з цих етапів можуть значно порушити маркетингові процеси та призвести до неправильного використання бюджету [2].

Особливо для малого та середнього бізнесу, які не можуть найняти професійних маркетологів або агентства для розробки рекламних стратегій, ця

проблема має великий вплив. Підприємці змушені приймати маркетингові рішення самостійно без належного досвіду. Це призводить до поширених помилок при запуску рекламної кампанії в таких умовах.

Хорошим виходом з цієї ситуації є впровадження системи підтримки прийняття рішень. З її допомогою вхідні дані можуть оброблятися автоматично, а рекомендації на основі вбудованих алгоритмів і правил можуть розроблятися та формулюватися на автоматичній основі [3].

Хоча традиційні галузі, такі як фінанси, логістика, медицина та бізнес-аналітика, використовують ці системи в широкому сенсі, але недостатньо застосувань у секторі цифрового маркетингу. Це дослідження пропонує створення веб-орієнтованої інформаційної системи підтримки прийняття рішень для встановлення маркетингових стратегій.

Метою системи є автоматизація процесу розробки рекламної стратегії шляхом аналізу вхідних даних та надання структурованих рекомендацій для проектування та реалізації рекламних кампаній.

Передбачається, що користувачі вводять основи бізнесу, маркетингові цілі, бюджетні обмеження та інші відповідні характеристики, а потім система логічно аналізує та надає рекомендації щодо рекламних каналів, структури системи рекламної кампанії, пріоритету сегментів цільової аудиторії, приблизного розподілу рекламного бюджету та основних рекомендацій щодо рекламних креативів.

З точки зору функціональності, запропонована система також може розглядатися як інструмент автоматизації первинного маркетингового консалтингу, що дозволяє знизити бар'єр входу для початківців у сферу цифрового маркетингу.

Отже, очікується, що така система допоможе зменшити кількість помилок при запуску рекламної кампанії в майбутньому, прискорити підготовку маркетингової стратегії та підвищити ефективність використання рекламного бюджету. Крім того, автоматизація процесу прийняття рішень, пов'язаного з маркетинговим процесом, може створити стандартизований процес розробки рекламної стратегії, що зменшує вплив людського фактора.

Цікавим напрямком для розвитку запропонованого рішення є включення моделі машинного навчання та вивчення минулої маркетингової поведінки, в якій можна було б здійснювати адаптивне коригування рекомендацій на основі накопиченого досвіду використання системи.

Отже, створення веб-орієнтованої інформаційної системи підтримки прийняття рішень для розробки маркетингових стратегій є важливим для розвитку сучасних інформаційних технологій, інтеграції автоматизації бізнес-процесів, аналітики даних та інтелектуальної підтримки користувачів [3].

Список використаних джерел

1. DataReportal. Digital 2025 Global https://datareportal.com/reports/digital-2025-global-overview-report

2. Google Ads Help. About campaign goals https://support.google.com/google-ads/answer/6325025

3. IBM. Decision Support System (DSS) https://www.ibm.com/topics/decision-support-system

Маліков Дмитро Вікторович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
malikovdimaft@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

СИСТЕМА КОНТРОЛЮ ДОСТУПУ ДО ВНУТРІШНІХ СЕРВІСІВ НА БАЗІ REVERSE PROXY ТА БЕЗКОШТОВНИХ DNS-СЕРВІСІВ

У сучасних умовах розвитку інформаційних технологій значна частина сервісів розгортається не лише у промислових дата-центрах, а й у локальних середовищах – на персональних комп'ютерах, віртуальних машинах або малопотужних серверах, що працюють у режимі 24/7. Такий підхід дозволяє зменшити витрати на інфраструктуру, однак створює низку проблем, пов'язаних із організацією доступу до внутрішніх сервісів, їх адмініструванням та безпекою.

Постановка задачі.

Основною проблемою є складність централізованого доступу до різних внутрішніх ресурсів (веб-інтерфейсів, сервісів, панелей керування), які розміщені на локальних IP-адресах і використовують різні порти. Це ускладнює масштабування системи, знижує зручність використання та створює ризики помилок конфігурації. Крім того, відсутність публічної IP-адреси або її динамічний характер унеможливлює використання класичних DNS-рішень і сертифікації безпеки [1].

Мета дослідження.

Метою дослідження є розробка та аналіз підходу до організації системи контролю доступу до внутрішніх сервісів у локальній мережі з використанням технології зворотного проксі (Reverse Proxy), безкоштовних DNS-сервісів та інструментів автоматизованого керування доменами.

Результати дослідження.

У межах дослідження було розглянуто підхід до побудови системи доступу до внутрішніх сервісів, що базується на використанні зворотного проксі-сервера, зокрема рішень типу Nginx Proxy Manager, які забезпечують централізоване керування маршрутизацією HTTP/HTTPS-запитів. Основна ідея полягає у використанні доменних імен для доступу до локальних ресурсів замість прямого звернення до IP-адрес і портів [2].

Запропонована система включає такі основні компоненти:

- локальний сервер або віртуальна машина, на якій розгорнуті сервіси;
- Reverse Proxy-сервер для маршрутизації запитів;
- DNS-сервіс (наприклад, Duck DNS) для створення доменних імен;
- клієнтські пристрої, що здійснюють доступ до сервісів.

Принцип роботи системи полягає у наступному. Користувач звертається до сервісу за доменним іменем (наприклад, service.localdomain). DNS-сервіс співставляє це ім’я з локальною IP-адресою (або псевдолокальною адресацією), після чого Reverse Proxy приймає запит і перенаправляє його до відповідного внутрішнього сервісу. Таким чином, забезпечується єдина точка входу до системи (рис. 1) [3].

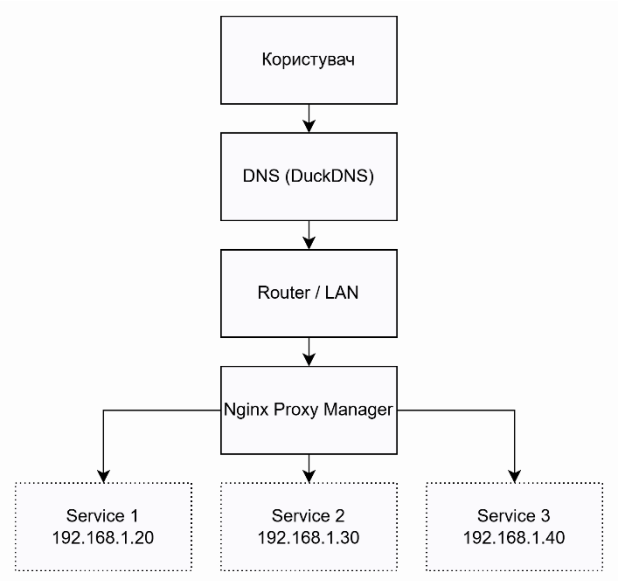

Рис. 1. Схема роботи системи доступу до внутрішніх сервісів через Reverse Proxy

Особливістю запропонованого підходу є використання безкоштовних DNS-рішень для імітації доменної інфраструктури навіть у межах локальної мережі. Це дозволяє уникнути необхідності придбання публічних доменів і використання статичних IP-адрес. При цьому доменні імена не обов’язково резолвляться у глобальному Інтернеті, а можуть функціонувати виключно в межах локальної мережі.

Ключові переваги системи:

- централізований доступ до сервісів через єдиний проксі;
- спрощення адміністрування та масштабування;
- підвищення зручності використання за рахунок доменних імен;
- можливість інтеграції з TLS-сертифікатами (наприклад, Let's Encrypt) у разі необхідності;
- мінімальні фінансові витрати на розгортання.

Крім того, використання Reverse Proxy дозволяє реалізувати додаткові механізми безпеки, такі як автентифікація користувачів, обмеження доступу за IP-адресами та журналювання запитів. Це особливо важливо для систем, які працюють у нестабільних умовах або розгорнуті на непрофесійній інфраструктурі [2].

Висновки та перспективи.

У результаті дослідження встановлено, що використання технології Reverse Proxy у поєднанні з безкоштовними DNS-сервісами є ефективним підходом до організації доступу до внутрішніх сервісів у локальних мережах. Запропонована модель дозволяє забезпечити зручний, масштабований і відносно безпечний доступ до ресурсів без необхідності використання складної або дорогої інфраструктури.

Практична цінність підходу полягає у можливості його застосування в навчальних, домашніх та малих корпоративних середовищах, де відсутні ресурси для розгортання повноцінних серверних рішень.

Список використаних джерел

1. Dynamic DNS explained. Cloudflare. URL: https://www.cloudflare.com/learning/dns/glossary/dynamic-dns/ (дата звернення: 12.04.2026)

2. NGINX Reverse Proxy. NGINX Documentation. URL: https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/ (дата звернення: 12.04.2026)

3. What is Duck DNS? Duck DNS. URL: https://www.duckdns.org/about.jsp (дата звернення: 12.04.2026)

Лузан Ярослав Дмитрович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
zhbr1pro@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ВІДДАЛЕНОГО ДОСТУПУ ДО СЕРВЕРНОЇ ІНФРАСТРУКТУРИ НА БАЗІ TAILSCALE

У сучасних умовах цифровізації підприємств, освітніх закладів та приватних IT-систем особливого значення набуває організація безпечного віддаленого доступу до серверної інфраструктури. Класичні VPN-рішення часто потребують складного налаштування маршрутизації, відкриття портів, адміністрування сертифікатів та постійного супроводу. Альтернативою є сучасні Zero Trust Network Access-рішення, одним із яких є Tailscale – програмна мережа типу mesh VPN, побудована на базі протоколу WireGuard. Такий підхід дозволяє створити захищену корпоративну або приватну мережу між пристроями без складної конфігурації та безпосереднього відкриття сервісів у глобальну мережу Інтернет [1].

Постановка задачі.

Основною проблемою традиційних систем віддаленого доступу є складність розгортання та підтримки захищених каналів зв'язку між користувачами і серверами. Для малого бізнесу, домашніх лабораторій та навчальних середовищ використання класичних VPN-серверів може бути економічно недоцільним або занадто складним в адмініструванні. Також актуальною проблемою залишається безпечний доступ до ізольованих сервісів, що працюють у контейнеризованому середовищі Docker, без відкриття портів у маршрутизаторі та без ризику зовнішнього сканування мережі [2].

Мета дослідження.

Метою дослідження є аналіз архітектурних особливостей Tailscale як сучасного рішення для побудови програмно-апаратного комплексу віддаленого доступу до серверної інфраструктури, дослідження можливостей інтеграції з Docker-контейнерами, а також оцінка практичного застосування Tailscale SSH для безпарольного адміністрування вузлів мережі.

Результати дослідження.

Програмно-апаратний комплекс реалізується на базі компактного серверного вузла – неттопа класу Lenovo ThinkCentre M920q або аналогічного

пристрою. На хост-системі під керуванням Linux встановлюється Docker Engine, після чого розгортається контейнеризоване середовище з двох сервісів: контейнера Tailscale та внутрішнього сервісу, наприклад Portainer або Nginx із тестовою веб-сторінкою. Такий підхід забезпечує ізоляцію компонентів, гнучкість масштабування та спрощує повторне розгортання системи [2].

Tailscale використовує mesh-топологію, у якій кожен авторизований пристрій може встановлювати пряме з'єднання з іншим вузлом мережі. Авторизація відбувається через зовнішнього провайдера ідентифікації (Google, Microsoft, GitHub тощо), що реалізує сучасну модель централізованого контролю доступу. Для з'єднання між вузлами застосовуються механізми NAT Traversal, які дозволяють працювати навіть за наявності «сірих» IP-адрес або подвійного NAT (рис. 1) [1].

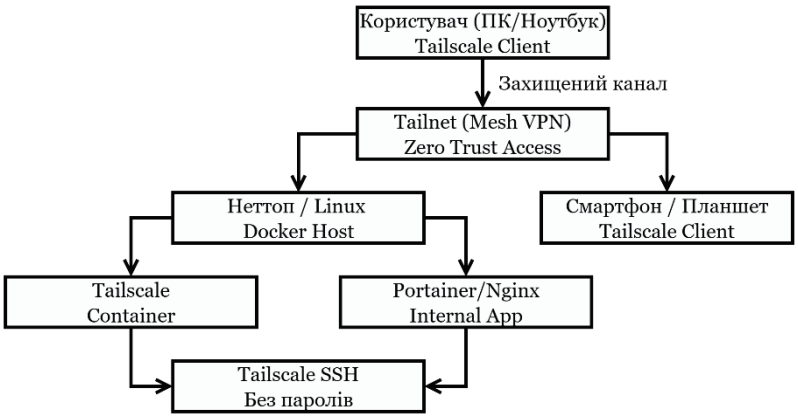

Рис. 1. Візуалізація структури та комунікацій компонентів

Практична демонстрація роботи комплексу може виглядати так: внутрішній сервіс Portainer функціонує на порту 9000, однак цей порт не відкритий у мережу Інтернет. Після підключення клієнтського пристрою до Tailnet користувач отримує доступ до веб-інтерфейсу за внутрішньою адресою виду 100.x.y.z:9000. Таким чином реалізується доступ лише для авторизованих користувачів без експонування сервісу назовні.

Окремої уваги заслуговує функція Tailscale SSH. Вона дозволяє виконувати підключення до серверного вузла командою типу ssh user@nettop-node, використовуючи внутрішнє DNS-ім'я MagicDNS. При цьому не потрібне налаштування паролів, ручний обмін SSH-ключами або відкриття порту 22 у зовнішній мережі. Контроль доступу здійснюється політиками Tailnet, що підвищує безпеку адміністрування серверів [3].

Дослідження також показало, що використання Docker-контейнерів разом із Tailscale є доцільним для побудови мікросервісної архітектури. У межах одного вузла можна ізольовано запускати веб-сервіси, бази даних, системи моніторингу

та засоби керування, надаючи до них доступ лише через внутрішню захищену мережу.

Висновки та перспективи.

У результаті дослідження встановлено, що Tailscale є ефективною платформою для створення сучасного програмно-апаратного комплексу віддаленого доступу до серверної інфраструктури. Основними перевагами рішення є простота розгортання, відсутність необхідності відкривати зовнішні порти, централізоване керування доступом, підтримка безпарольного SSH та зручна інтеграція з Docker-контейнерами. Такий підхід відповідає концепції Zero Trust та є особливо актуальним для малого бізнесу, домашніх лабораторій і навчальних IT-середовищ [1].

Перспективами подальших досліджень є аналіз продуктивності мережевого трафіку при різних режимах Docker Networking (bridge, host), інтеграція з Kubernetes-кластерами, побудова резервованих серверних вузлів та впровадження систем моніторингу доступності сервісів у Tailnet.

Список використаних джерел

1. What is Tailscale? Tailscale Docs. URL: https://tailscale.com/kb/1151/what-is-tailscale (дата звернення: 13.04.2026)

2. Docker Documentation. Overview of Docker Containers. URL: https://docs.docker.com/get-started/docker-overview/ (дата звернення: 13.04.2026)

3. Tailscale SSH. Tailscale Docs. URL: https://tailscale.com/kb/1193/tailscale-ssh/ (дата звернення: 13.04.2026)

Груша Данило Романович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
starsitien@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ЗАХИЩЕНОГО КЕРУВАННЯ БПЛА З ВИКОРИСТАННЯМ СУЧАСНИХ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

Стрімкий розвиток безпілотних літальних апаратів (БПЛА) у цивільній та військовій сферах зумовлює необхідність підвищення рівня захищеності каналів зв'язку між мобільною платформою та наземною станцією управління. Особливу

актуальність набуває проблема забезпечення конфіденційності, цілісності та доступності даних у процесі передачі команд керування та телеметричної інформації. Застосування сучасних мережевих технологій, таких як VPN-тунелювання, шифрування та сегментація мереж, дозволяє значно знизити ризики несанкціонованого доступу та атак типу «людина посередині» (Man-in-the-Middle) [1].

Постановка задачі.

Основною проблемою при організації зв'язку між БПЛА та пунктом управління є забезпечення надійного і захищеного каналу передачі даних в умовах нестабільних мереж, обмежених ресурсів та потенційних кіберзагроз. Відкриті бездротові канали зв'язку можуть бути вразливими до перехоплення, підміни або блокування даних. Існуючі підходи часто не враховують комплексного використання механізмів шифрування, автентифікації та ізоляції трафіку, що призводить до зниження загального рівня безпеки системи [2].

Мета дослідження.

Метою дослідження є розробка та аналіз апаратно-програмного комплексу захищеного керування БПЛА, який забезпечує безпечну передачу керуючих команд і телеметричних даних шляхом використання VPN-тунелювання, сучасних криптографічних алгоритмів та сегментації мережевого трафіку. Додатково передбачається дослідження ефективності запропонованої моделі в умовах імітації реального мережевого середовища.

Результати дослідження.

У процесі дослідження було розроблено узагальнену модель взаємодії між БПЛА та наземною станцією, яка включає такі компоненти: модуль збору телеметрії, модуль передачі керуючих команд, VPN-шлюз, система шифрування та механізми автентифікації. Основна увага приділяється створенню захищеного каналу зв'язку на основі VPN-протоколів (наприклад, OpenVPN або WireGuard), що дозволяє інкапсулювати весь трафік у зашифрований тунель [1].

Для забезпечення ізоляції даних використано підхід сегментації мережі, при якому трафік керування та телеметрії розділяється на окремі логічні канали. Це дозволяє зменшити ризик впливу компрометації одного сегмента на інші компоненти системи. Крім того, застосування криптографічних алгоритмів (AES, RSA) забезпечує захист даних навіть у випадку їх перехоплення (рис. 1) [3].

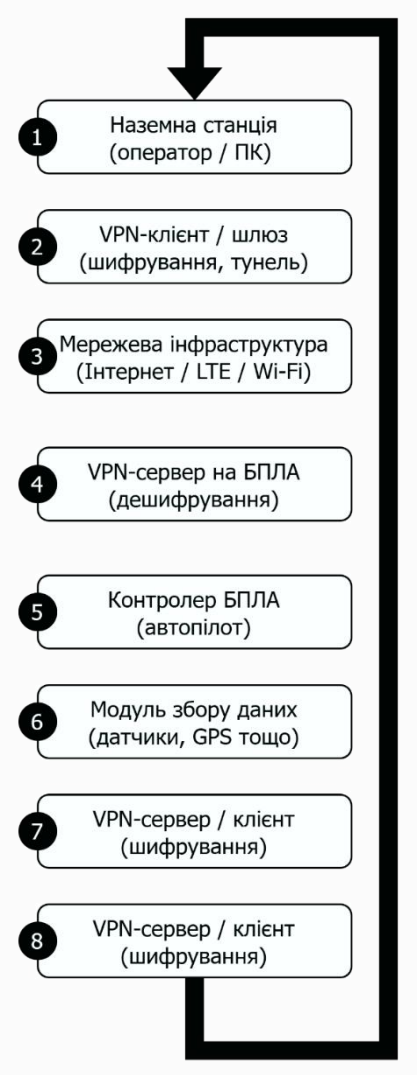

Рис. 1. Логіка зв’язків у системі

У рамках роботи було реалізовано тестове середовище з використанням емуляції передачі даних між вузлами. Проведені експерименти показали, що використання VPN-тунелювання збільшує затримку передачі даних незначно, проте значно підвищує рівень захищеності. Також встановлено, що сегментація мережі сприяє підвищенню стабільності системи при високих навантаженнях та дозволяє ефективно управляти потоками даних [2].

Додатково було проаналізовано можливість інтеграції системи з IoT-платформами та використання протоколів MQTT для передачі телеметричних даних. Це дозволяє підвищити масштабованість системи та забезпечити гнучкість у розгортанні мережевої інфраструктури [4].

Висновки та перспективи.

У результаті дослідження встановлено, що використання комплексного підходу до захисту мережевої взаємодії БПЛА, який включає VPN-тунелювання, шифрування та сегментацію трафіку, дозволяє значно підвищити безпеку та

надійність системи керування. Запропонована модель забезпечує захист від основних типів мережевих атак та може бути адаптована до різних умов експлуатації.

Перспективами подальших досліджень є інтеграція технологій штучного інтелекту для виявлення аномалій у мережевому трафіку, використання блокчейн-технологій для автентифікації вузлів, а також оптимізація протоколів передачі даних для зменшення затримок у реальному часі.

Список використаних джерел

1. Virtual Private Networks Explained. Cisco. URL: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html (дата звернення: 13.04.2026)

2. Network Segmentation Best Practices. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/network-segmentation (дата звернення: 13.04.2026)

3. Cryptography and Network Security Principles. IBM. URL: https://www.ibm.com/topics/cryptography (дата звернення: 13.04.2026)

4. MQTT Protocol for IoT Systems. HiveMQ. URL: https://www.hivemq.com/mqtt/ (дата звернення: 13.04.2026)

Проць Максим Русланович
студент групи МТД-42
Державного університету
інформаційно-комунікаційних технологій, м. Київ
procmaksim55@gmail.com

Галаган Наталія Вікторівна
кандидат технічних наук, доцент,
завідувач кафедри Мобільних та відеоінформаційних технологій
Державного університету
інформаційно комунікаційних технологій, м. Київ

ДОСЛІДЖЕННЯ ХМАРНИХ СЕРВІСІВ ДЛЯ ПОБУДОВИ IT-ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

У сучасних умовах цифрової трансформації підприємств хмарні технології стають ключовим інструментом для побудови гнучкої, масштабованої та економічно ефективної IT-інфраструктури. Використання хмарних сервісів дозволяє значно знизити витрати на апаратне забезпечення, забезпечити віддалений доступ до ресурсів та швидко адаптувати систему до змін бізнес-потреб. Особливу роль відіграють платформи, що надають інфраструктуру як сервіс (IaaS), зокрема рішення, які дозволяють створювати віртуальні сервери,

організовувати мережеву взаємодію та забезпечувати надійне зберігання даних [1].

Постановка задачі.

Основною проблемою, що постає перед підприємствами, є необхідність створення IT-інфраструктури, яка одночасно відповідає вимогам безпеки, продуктивності та економічної доцільності. Традиційні підходи до розгортання фізичних серверів потребують значних початкових інвестицій, часу на впровадження та складного обслуговування.

Крім того, підприємства стикаються з труднощами масштабування ресурсів у разі зростання навантаження, що може призводити до простоїв або перевитрат ресурсів. Відсутність централізованого управління доступом та резервного копіювання також створює ризики втрати даних та несанкціонованого доступу [2].

Мета дослідження.

Метою дослідження є аналіз можливостей хмарних сервісів для побудови IT-інфраструктури підприємства, розробка спрощеної моделі інфраструктури з використанням основних компонентів хмарної платформи, а також оцінка ефективності такого підходу з точки зору масштабованості, безпеки та економічної доцільності.

Результати дослідження.

У рамках дослідження було запропоновано модель IT-інфраструктури підприємства, що базується на трьох основних компонентах:

1. Обчислювальні ресурси (EC2) – віртуальний сервер, який виконує роль центрального вузла системи (наприклад, хостинг корпоративного сайту або облікової системи).
2. Мережева інфраструктура (VPC) – забезпечує ізольоване середовище з контрольованим доступом до ресурсів.
3. Система зберігання (S3) – використовується для резервного копіювання та зберігання файлів підприємства.

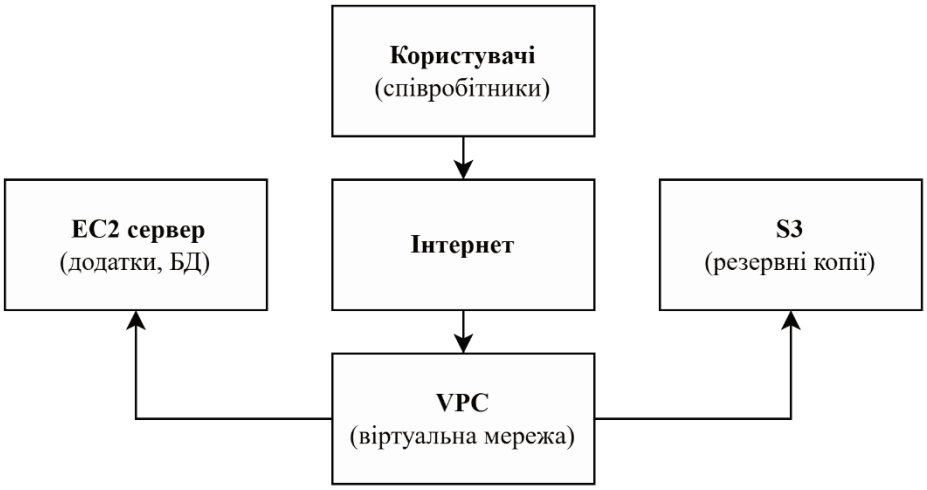

Рис. 1. Схема хмарної IT-інфраструктури підприємства

Запропонована модель дозволяє:

- забезпечити централізоване управління ресурсами;
- гнучко масштабувати обчислювальні потужності;
- реалізувати резервне копіювання даних;
- обмежити доступ до системи через налаштування мережевих політик.

У процесі дослідження також проведено порівняння хмарних платформ (AWS, Microsoft Azure, Google Cloud). Встановлено, що обрана платформа має переваги у вигляді гнучкості налаштувань, широкого набору сервісів та доступності безкоштовного тестового середовища (Free Tier) [1].

Окрему увагу приділено економічному аспекту. Використання хмарної інфраструктури дозволяє уникнути значних капітальних витрат на придбання серверного обладнання. За допомогою калькулятора вартості можна оцінити щомісячні витрати та порівняти їх із традиційною моделлю, що підтверджує економічну ефективність хмарних рішень на початкових етапах розвитку підприємства [3].

Також досліджено механізми безпеки, зокрема управління доступом користувачів (IAM). Встановлено, що розмежування прав доступу дозволяє мінімізувати ризики несанкціонованого доступу та підвищити рівень захисту інформації [2]

Висновки та перспективи.

У результаті дослідження встановлено, що використання хмарних сервісів є ефективним рішенням для побудови сучасної IT-інфраструктури підприємства. Запропонована модель дозволяє забезпечити високу гнучкість, масштабованість та безпеку системи при мінімальних початкових витратах.

Практична реалізація інфраструктури на базі хмарних технологій демонструє значні переваги порівняно з традиційними підходами, зокрема

швидкість розгортання, зручність адміністрування та можливість оперативного масштабування ресурсів.

Перспективними напрямами подальших досліджень є:

- інтеграція хмарних сервісів із системами штучного інтелекту;
- автоматизація управління інфраструктурою (Infrastructure as Code);
- використання контейнеризації для підвищення ефективності розгортання додатків;
- дослідження гібридних та мультихмарних рішень.

Список використаних джерел

1. Amazon Web Services Overview – AWS. URL: https://aws.amazon.com/what-is-aws/ (дата звернення: 13.04.2026)

2. AWS Identity and Access Management (IAM) – AWS. URL: https://aws.amazon.com/iam/ (дата звернення: 13.04.2026).

3. AWS Pricing Calculator – AWS. URL: https://calculator.aws/#/ (дата звернення: 13.04.2026).

Кулик Ілля Олегович
студент групи МТД-42
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kuilja2005@gmail.com

Блаженний Назарій Валерійович
доцент кафедри Мобільних та відеоінформаційних технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

МОДЕЛЮВАННЯ ВІДМОВОСТІЙКОЇ IP-МЕРЕЖІ З ВИКОРИСТАННЯМ БПЛА У РОЛІ ПОВІТРЯНИХ ВУЗЛІВ ЗВ'ЯЗКУ

Розгортання тимчасових бездротових мереж на базі безпілотних літальних апаратів набуває особливої актуальності в умовах відсутності, пошкодження або перевантаження наземної телекомунікаційної інфраструктури. Для рятувальних, тактичних і спеціальних завдань повітряні вузли можуть виконувати функції ретрансляції, маршрутизації та швидкого відновлення зв'язності між ізольованими сегментами мережі. У сучасних дослідженнях такі мережі розглядаються як засіб оперативного розгортання зв'язку в середовищі зі складною геометрією покриття, мінливою топологією та підвищеними вимогами до стійкості передавання даних [1, 2].

Постановка задачі.

Основною проблемою при побудові мережі зв’язку на базі БПЛА є поєднання високої мобільності повітряних вузлів із вимогою стабільного передавання IP-пакетів у тривимірному просторі. Часті зміни топології, ризик втрати лінії прямої видимості, обмеженість енергоресурсу акумуляторів і неоднорідність каналів зв’язку ускладнюють маршрутизацію та можуть призводити до збільшення затримки, втрати пакетів або розриву з’єднань. Це зумовлює потребу в такій архітектурі мережі, яка забезпечує резервування маршрутів і автоматичну перебудову шляхів передавання даних у разі відмови окремого повітряного вузла [1, 2].

Мета дослідження.

Метою дослідження є обґрунтування архітектури відмовостійкої мережі зв’язку на базі БПЛА, що виконують роль літаючих маршрутизаторів, а також моделювання логічної IP-топології із застосуванням протоколу динамічної маршрутизації для перевірки автоматичної перебудови маршрутів при відмові окремих вузлів.

Результати дослідження.

Мережі типу FANET доцільно розглядати як розвиток концепції MANET, адаптований до середовища з тривимірною мобільністю та значно вищою динамікою зміни топології. У такій мережі БПЛА можуть виступати одночасно джерелами трафіку, транзитними вузлами та маршрутизаторами. Для практичних задач зв’язку використовуються централізована, багатогрупова та mesh-архітектури, а самі БПЛА можуть виконувати функції ретрансляторів, динамічних шлюзів або повітряних базових станцій [1, 2].

Під час проєктування такої мережі необхідно враховувати не лише фізичну наявність каналу зв’язку, а й мережеві показники, що безпосередньо впливають на стійкість системи. До ключових показників належать [1, 2, 5]:

1. Ймовірність втрати прямої видимості або виходу сусіднього вузла із зони впевненого радіозв’язку.
2. Час оновлення маршрутної інформації та швидкість реконвергенції після топологічних змін.
3. Енергоспоживання повітряних вузлів під час передавання та ретрансляції даних.
4. Затримка end-to-end, кількість переходів між вузлами та ймовірність втрати пакетів.
5. Наявність резервного шляху між наземними сегментами мережі.

Підходи до маршрутизації в мережах БПЛА зазвичай поділяють на кілька груп [1]:

1. Топологічна маршрутизація, яка базується на інформації про зв’язки між вузлами мережі.
2. Позиційна або географічна маршрутизація, у якій рішення приймаються з урахуванням координат і напрямку руху БПЛА.

3. Ієрархічна маршрутизація, що використовує кластеризацію повітряних вузлів для зменшення службового навантаження та кращого масштабування мережі.

Для перевірки запропонованої архітектури доцільно використовувати логічну модель у програмному симуляторі. У межах такої моделі повітряний вузол інтерпретується як маршрутизатор, а зв'язки між БПЛА - як канали передавання IP-трафіку. Для практичної реалізації обрано підхід Link-State, оскільки OSPF підтримує єдину топологічну базу, обчислення shortest-path tree, поділ на області та швидкий перерахунок маршрутів при зміні топології. У документації Cisco також виокремлюються LSDB, таблиця сусідів і таблиця маршрутизації як ключові компоненти механізму перебудови маршрутів. Це дає змогу перевірити, чи зберігається зв'язність між наземними сегментами мережі після виходу одного з дронів з ладу [3, 4].

Рис. 1 Логічна модель відмовостійкої IP-мережі з повітряними вузлами зв'язку

Висновки та перспективи.

Використання БПЛА у ролі літаючих маршрутизаторів дозволяє будувати тимчасові відмовостійкі мережі зв'язку в умовах, коли застосування лише наземної інфраструктури є неможливим або недостатнім. Застосування динамічної маршрутизації дає змогу зменшити ризик втрати зв'язності між віддаленими пунктами та забезпечити автоматичну перебудову маршрутів у разі відмови окремого повітряного вузла. Перспективи подальших досліджень пов'язані з інтеграцією таких мереж із супутниковим зв'язком, стільниковими системами нового покоління та сервісами U-space/UTM для побудови гібридної повітряно-наземної інфраструктури [2, 5].

Список використаних джерел

1. Almansor M. J., Md Din N., Baharuddin M. Z., Ma M., Alsayednoor H. M., Al-Shareeda M. A., Al-asadi A. J. Routing protocols strategies for flying ad-hoc network (FANET): Review, taxonomy, and open research issues. Alexandria Engineering Journal. URL:

https://www.sciencedirect.com/science/article/pii/S1110016824010469 (дата звернення: 11.04.2026).

2. Cisco Systems. OSPF Configuration Guide. Cisco IOS XE 17.18.1. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/lyr3-fwd/ospf/ospf-configuration-guide/ospf.html (дата звернення: 11.04.2026).

3. Ghamari M., Rangel P., Mehrubeoglu M., Tewolde G. S., Sherratt R. S. Unmanned aerial vehicle communications for civil applications: a review. IEEE Access. URL: https://centaur.reading.ac.uk/107540/ (дата звернення: 12.04.2026).

4. Marks T., Fuger K. Using generic cities to assess flying ad-hoc network (FANET) performance. CEAS Aeronautical Journal. URL: https://link.springer.com/article/10.1007/s13272-024-00801-2 (дата звернення: 12.04.2026).

5. Moy J. RFC 2328: OSPF Version 2. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/html/rfc2328 (дата звернення: 12.04.2026).

НАПРЯМ 2. ІОТ ТА ШТУЧНИЙ ІНТЕЛЕКТ

Фуркало Даниіл Юрійович
студент 3 курсу
спеціальності «Інженерія програмного забезпечення»
Київського національного університету імені Тараса Шевченка, м. Київ
daniilf077@knu.ua

СУЧАСНІ ТЕНДЕНЦІЇ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНТЕРНЕТІ РЕЧЕЙ

Стрімкий розвиток Інтернету речей (Internet of Things, IoT) призводить до експоненційного зростання обсягів даних, що генеруються сенсорами, вбудованими пристроями та кіберфізичними системами. Традиційні методи обробки таких даних часто виявляються недостатньо ефективними з огляду на вимоги до масштабованості, адаптивності та автономності систем. У цьому контексті штучний інтелект (ШІ) виступає ключовим інструментом підвищення інтелектуальності IoT-систем, забезпечуючи автоматичний аналіз даних, прогнозування та підтримку прийняття рішень у реальному часі. Актуальним завданням є аналіз сучасних тенденцій інтеграції методів ШІ в IoT та визначення перспектив їх подальшого розвитку.

Ціллю даної роботи є огляд і систематизація сучасних підходів до застосування штучного інтелекту в Інтернеті речей, а також визначення ключових напрямів розвитку інтелектуальних IoT-систем у різних прикладних галузях.

У процесі дослідження було використано методи аналізу наукових публікацій, аналітичних звітів та статистичних даних, присвячених розвитку технологій штучного інтелекту в середовищі Інтернету речей. Основу дослідження становили сучасні наукові статті, матеріали міжнародних аналітичних компаній, а також результати досліджень у сфері AioTx [1].

Для систематизації отриманої інформації застосовувалися методи порівняльного аналізу, узагальнення та класифікації підходів до інтеграції штучного інтелекту в IoT-системи. Особливу увагу приділено аналізу основних технологічних напрямів, зокрема методів машинного навчання, глибинного навчання, інтелектуального аналізу даних, а також концепції Edge AI. Крім того, було виконано аналіз сучасних тенденцій розвитку ринку AIoT на основі прогнозних статистичних даних, що дозволило оцінити динаміку зростання та визначити перспективні напрями подальшого розвитку інтелектуальних IoT-систем [2].

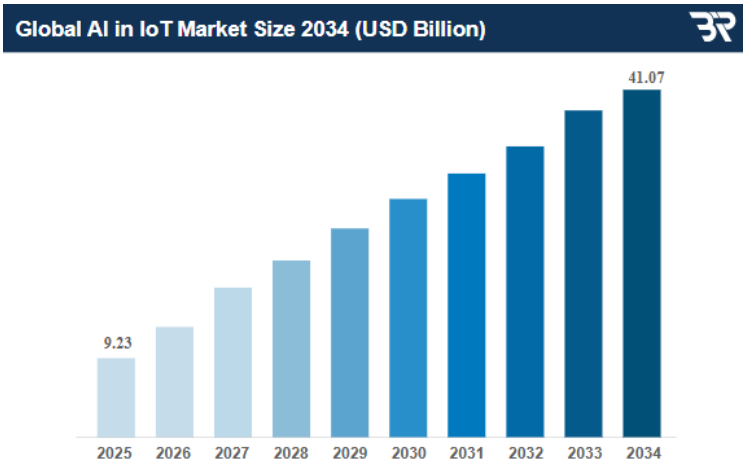

Рис. 1. Прогноз динаміки зростання світового ринку штучного інтелекту в Інтернеті речей (AIoT) у 2025–2034 рр., млрд дол. США

Стрімкий розвиток Інтернету речей зумовлює зростаючу потребу в інтелектуальних методах обробки великих обсягів даних, що надходять від розподілених сенсорних систем. У цьому контексті штучний інтелект відіграє ключову роль у підвищенні ефективності, автономності та адаптивності IoT-рішень. Сучасні аналітичні дослідження свідчать про стабільну позитивну динаміку розвитку ринку AIoT. Зокрема, прогнозується значне зростання обсягів глобального ринку штучного інтелекту в Інтернеті речей у період з 2025 по 2034 роки, що обумовлено активним впровадженням інтелектуальних технологій у промисловості, енергетиці, транспорті, охороні здоров'я та системах «розумних» міст [3].

У результаті дослідження встановлено, що найбільш поширеними напрямами використання штучного інтелекту в IoT є машинне навчання, глибинне навчання та методи інтелектуального аналізу даних. Зазначені підходи забезпечують можливість прогнозування технічного стану обладнання, виявлення аномалій у режимі реального часу, оптимізації енергоспоживання та підвищення якості прийняття управлінських рішень. Особливого значення набуває застосування ШІ в промисловому Інтернеті речей, де інтелектуальні алгоритми дозволяють реалізувати концепції предиктивного обслуговування та автоматизованого контролю виробничих процесів. Однією з провідних тенденцій розвитку AIoT є перехід від централізованих хмарних обчислень до обробки даних на периферії мережі, відомої як Edge AI. Такий підхід сприяє зменшенню затримок, підвищенню надійності функціонування систем та зниженню навантаження на мережеву інфраструктуру. Водночас значна увага приділяється питанням інформаційної безпеки та захисту персональних даних, зокрема застосуванню методів штучного інтелекту для виявлення кіберзагроз у середовищі Інтернету речей.

Інтеграція штучного інтелекту в Інтернет речей є одним із ключових чинників формування інтелектуальних, автономних та адаптивних систем нового покоління. Сучасні тенденції свідчать про зростання ролі Edge AI, самонавчальних моделей та гібридних архітектур обробки даних. Перспективними напрямами подальших досліджень є розробка енергоефективних алгоритмів ШІ, підвищення рівня безпеки IoT-систем та створення стандартизованих підходів до інтеграції інтелектуальних компонентів у різнорідні середовища Інтернету речей.

Список використаних джерел

1. *AI in IOT Market Size, Share, Growth, and Industry Analysis, By Type Source URL: https://www.businessresearchinsights.com/market-reports/ai-in-iot-market-119209*

2. *AIoT: навіщо Інтернету речей потрібен штучний інтелект URL: https://iotji.io/aiot-navischo-internetu-rechei-potriben-shtuchnyi-intelekt/*

3. *Recent Trends and Emerging Applications of the Internet of Things: Transforming the Way We Live and Work URL: https://www.researchgate.net/publication/394305233_Recent_Trends_and_Emerging_Applications_of_the_Internet_of_Things_Transforming_the_Way_We_Live_and_Work*

Закревський Сергій Миколайович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
Zakrevskysn@gmail.com

Ткаленко Оксана Миколаївна
доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
tkalenko-oksana888@ukr.net

ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ КЛАСИФІКАЦІЇ ДАНИХ ІНТЕРНЕТУ РЕЧЕЙ

Сучасний етап розвитку інформаційних технологій характеризується стрімким поширенням концепції Інтернету речей (IoT), яка передбачає інтеграцію великої кількості фізичних пристроїв, сенсорів і систем в єдину мережну інфраструктуру. Такі пристрої безперервно генерують великі обсяги даних різної природи, що використовуються для моніторингу, аналізу та управління процесами у різних сферах людської діяльності. У зв’язку з цим

задача класифікації даних IoT є досить актуальною, оскільки дозволяє ефективно структурувати інформаційні потоки, виявляти типи сервісів, а також приймати обгрунтовані управлінські рішення.

Актуальність класифікації даних Інтернету речей зумовлена наступними факторами. По-перше, IoT-середовище характеризується високою динамічністю та гетерогенністю даних, що надходять від різних типів пристроїв з різними параметрами якості обслуговування (QoS). По-друге, обсяги даних постійно зростають, що ускладнює їх обробку традиційними методами. По-третє, для ефективного функціонування мереж необхідно своєчасно ідентифікувати типи трафіку та сервісів з метою оптимізації використання ресурсів, зменшення затримок та підвищення надійності передавання даних.

Традиційні підходи до класифікації даних, які основані на фіксованих правилах або простих статистичних моделях, часто не здатні ефективно обробляти складні багатовимірні дані з нелінійними залежностями. Тому, особливої актуальності набуває застосування алгоритмів машинного навчання, які дозволять автоматично виявляти приховані закономірності в даних та адаптуватися до змін у середовищі. Методи машинного навчання зможуть забезпечити більш високу точність класифікації, стійкість до шуму та можливість роботи з великими обсягами даних без необхідності ручного налаштування правил.

Для класифікації даних Інтернету речей доцільно використовувати алгоритми, які добре працюють із багатовимірними, зашумленими та зачасту нелінійними даними, які є характерними для IoT-середовища. До них слід віднести як базові лінійні алгоритми (Logistic Regression, Linear SVM), так і більш складні нелінійні та ансамблеві методи (RBF SVM, Decision Tree, Random Forest), які здатні враховувати складні взаємозв’язки між параметрами QoS. Додатково можуть застосовуватися методи KNN та Naive Bayes для порівняльного аналізу, а також глибокі нейронні мережі як перспективний напрям подальших досліджень.

Застосування алгоритмів машинного навчання для класифікації даних IoT дозволить підвищити точність та швидкість обробки даних, що є критично важливим для систем реального часу. По-друге, буде забезпечене більш ефективне використання мережних ресурсів за рахунок адаптивного управління трафіком. Підвищить надійність і стійкість систем до збоїв, та перевантажень. Крім того, автоматизація процесів аналізу даних зменшить необхідність втручання людини та сприятиме зниженню експлуатаційних витрат.

Важливим напрямом є інтеграція методів машинного навчання з технологіями edge computing, що дозволить здійснювати обробку даних безпосередньо на рівні пристроїв IoT, зменшуючи затримки та навантаження на мережу. Також перспективним є використання адаптивних та самонавчальних

систем, здатних змінювати свою поведінку залежно від умов функціонування мережі.

Застосування алгоритмів машинного навчання для класифікації даних Інтернету речей є ефективним і перспективним підходом, який дозволить підвищити якість функціонування сучасних мережних систем, забезпечити їх масштабованість та адаптивність до змінних умов середовища. Перспективи подальших досліджень у даному напрямку можуть бути пов'язаними з розвитком більш складних моделей машинного навчання, зокрема глибокого навчання, які дозволять обробляти ще більші обсяги даних і враховувати часові залежності.

Список використаних джерел

5. Huang Y.-F., Lin C.-B., Chung C.-M., Chen C.-M. Research on QoS classification of network encrypted traffic behavior based on machine learning // Electronics. – 2021. – Vol. 10, No. 12. – Article 1376. – Режим доступу: https://doi.org/10.3390/electronics10121376

6. Rahmayanti D. Predicting quality of service on cellular networks using artificial intelligence // Jurnal Elektronika dan Energi Indonesia. – 2023. – Vol. 5, No. 2. – Режим доступу: https://doi.org/10.55606/jeei.v5i2.3901

Шевчук Олег Олексійович
студент 5 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st01243597@stud.duikt.edu.ua

Гаврилюк Анжеліка Русланівна
студент 5 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
aanzelikaa23@gmail.com

Сагайдак Віктор Анатолійович
PhD, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ІНТЕЛЕКТУАЛЬНІ АЛГОРИТМИ В ЗАДАЧАХ МАРШРУТИЗАЦІЇ ТРАНСПОРТНИХ ЗАСОБІВ

Стрімкий розвиток транспортно-логістичних систем, електронної комерції та цифрових технологій зумовлює значне зростання складності задач маршрутизації транспортних засобів. Сучасні логістичні процеси

характеризуються великою кількістю обмежень, динамічністю середовища та необхідністю обробки значних обсягів даних у реальному часі. У таких умовах традиційні методи оптимізації виявляються недостатньо ефективними, що зумовлює необхідність застосування інтелектуальних алгоритмів для підвищення ефективності планування маршрутів та управління транспортними потоками.

Метою дослідження є аналіз сучасних інтелектуальних алгоритмів, що застосовуються для розв'язання задач маршрутизації транспортних засобів, а також визначення їх ефективності в умовах динамічних транспортних систем і багатокритеріальних обмежень.

Задача маршрутизації транспортних засобів (Vehicle Routing Problem) належить до класу складних комбінаторних задач оптимізації. Вона передбачає визначення оптимальних маршрутів для набору транспортних засобів з урахуванням обмежень, таких як час доставки, місткість транспорту, пріоритети замовлень та характеристики дорожньої мережі. Для її розв'язання активно застосовуються метаевристичні алгоритми, які дозволяють знаходити наближено оптимальні рішення у задачах із великою кількістю параметрів і обмежень [1]. Такі методи забезпечують ефективний пошук у складному просторі рішень та зменшують обчислювальні витрати.

Суттєвий розвиток у цій галузі пов'язаний із застосуванням методів штучного інтелекту, зокрема алгоритмів глибинного та підкріплювального навчання. Використання таких підходів дозволяє враховувати динамічні зміни транспортного середовища, зокрема зміну трафіку, попиту та стану дорожньої інфраструктури [5]. Це забезпечує підвищення точності прийняття рішень і дозволяє будувати адаптивні системи маршрутизації, здатні реагувати на зміну умов у режимі реального часу.

У сучасних дослідженнях також активно використовуються гібридні підходи, що поєднують різні алгоритмічні методи оптимізації. Зокрема, багатокритеріальні моделі дозволяють одночасно враховувати час доставки, енергоспоживання, вартість перевезень та екологічні фактори [3]. Такі підходи є особливо актуальними для задач маршрутизації електричних транспортних засобів, де необхідно враховувати обмеження зарядної інфраструктури та енергетичних ресурсів.

Важливим напрямом розвитку є інтеграція інтелектуальних алгоритмів із технологіями Інтернету речей. Використання даних від сенсорів і підключених транспортних систем дозволяє здійснювати адаптивну маршрутизацію в реальному часі та підвищувати ефективність управління транспортними потоками [2]. Такий підхід забезпечує оперативне реагування на зміну дорожньої ситуації та дозволяє мінімізувати затримки доставки.

Сучасні дослідження демонструють ефективність використання цифрових двійників для моделювання транспортних процесів. Застосування таких

технологій дозволяє створювати віртуальні моделі транспортних систем і прогнозувати поведінку маршрутів у різних умовах експлуатації [4]. Це сприяє підвищенню точності оптимізації та покращенню якості логістичних рішень.

Отримані результати свідчать, що використання інтелектуальних алгоритмів дозволяє суттєво підвищити ефективність задач маршрутизації транспортних засобів, забезпечити адаптацію до динамічних умов та зменшити витрати логістичних операцій. Комплексне застосування різних підходів дає змогу досягти кращих результатів порівняно з використанням окремих методів.

Інтелектуальні алгоритми є ключовим інструментом оптимізації транспортних процесів у сучасних логістичних системах. Перспективними напрямами подальших досліджень є розроблення адаптивних гібридних моделей, інтеграція методів штучного інтелекту з IoT-технологіями та створення ефективних систем підтримки прийняття рішень у сфері транспортної логістики.

Список використаних джерел

1. Liu, Y., Tang, Y., & Hua, C. (2025). A hybrid metaheuristic algorithm for dynamic heterogeneous vehicle routing problem with stochastic demand considering environmental aspects. International Journal of Electrical Power & Energy Systems, 172, 111135. https://doi.org/10.1016/j.ijepes.2025.111135

2. Narsimhulu, P., Chithaluru, P., Al-Turjman, F., Guda, V., Inturi, S., Stephan, T., & Kumar, M. (2024). An intelligent FL-based vehicle route optimization protocol for green and sustainable IoT connected IoV. Internet of Things, 101240. https://doi.org/10.1016/j.iot.2024.101240

3. Sbayti, O., & Housni, K. (2026). MOACO-OLSR : Application of Multi-Objective Ant Colony Optimization to optimal path search for enhanced routing algorithm OLSR in vehicular networks. Scientific African, Стаття e03329. https://doi.org/10.1016/j.sciaf.2026.e03329

4. Shamani, M., Foroud, A. A., & Rastgoo, R. (2026). Intelligent management of mobile charging fleet with traffic prediction-based routing and emergency vehicle servicing. Results in Engineering, 109360. https://doi.org/10.1016/j.rineng.2026.109360

5. Ye, S., Xu, L., Xu, Z., & Wang, F. (2024). A deep reinforcement learning-based intelligent QoS optimization algorithm for efficient routing in vehicular networks. Alexandria Engineering Journal, 107, 317–331. https://doi.org/10.1016/j.aej.2024.07.045

Білоус Владислав Володимирович
старший викладач кафедри комп'ютерних наук,
факультету інформаційних технологій та математики
Київського столичного університету
імені Бориса Грінченка, м. Київ
v.bilous@kubg.edu.ua

ІНТЕГРАЦІЯ IOT, OSINT ТА КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ РАННЬОГО ВИЯВЛЕННЯ UAV З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Сучасна війна вже давно перестала бути лише фізичним зіткненням сил і техніки. Це, насамперед, боротьба за швидкість: хто швидше побачить загрозу, проаналізує її і прийме рішення - той отримує вирішальну перевагу. У 2024–2025 роках безпілотні літальні апарати (UAV) радикально змінили характер бойових дій. FPV-дрони та баражуючі боєприпаси стали одним із головних інструментів як розвідки, так і точного ураження. Щодня фіксується велика кількість інцидентів із застосуванням FPV-дронів. Вони з'являються раптово, діють швидко і коштують відносно недорого, тому раннє виявлення таких загроз та прогнозування їхньої траєкторії стали критичним фактором для збереження життя особового складу.

Класичні радіолокаційні системи, хоч і потужні, мають серйозні обмеження. Вони дорогі, складні в розгортанні, погано працюють у щільній міській забудові та легко пригнічуються засобами електронної боротьби. Саме тому сьогодні набуває популярності зовсім інший, більш гнучкий і доступний підхід. Йдеться про гібридну систему, яка розумно поєднує чотири ключові технології: Інтернет речей (IoT), відкриті джерела розвідки (OSINT), комп'ютерний зір (Computer Vision) та штучний інтелект (AI) [3].

Така інтеграція дає відразу кілька важливих переваг. По-перше, система виходить відносно недорогою - її можна зібрати на базі доступного обладнання, без необхідності купувати дорогі військові радари. По-друге, вона легко масштабується: від одного окремого поста спостереження до цілої мережі сенсорів, розгорнутої вздовж лінії фронту чи навколо важливих об'єктів. По-третє, вся обробка даних відбувається швидко й ефективно, завдяки чому система здатна працювати в реальному часі навіть у складних умовах - при обмеженому зв'язку, активній радіоелектронній боротьбі, в міській забудові чи за поганої видимості. Саме тому такий гібридний підхід сьогодні виглядає одним із найперспективніших напрямків розвитку систем раннього попередження

По суті, вся система являє собою єдину гібридну розвідувальну платформу. Фізичні сенсори IoT збирають дані безпосередньо з навколишнього середовища - звук, радіосигнали, температуру. Відеопотоки з камер обробляються сучасними алгоритмами комп'ютерного зору. OSINT додає цінний контекст із відкритих

джерел - повідомлення, геолокації, інформацію від волонтерів. А центральне AI-ядро виступає «мозком» системи: воно поєднує всі ці дані, аналізує їх і видає чітке, своєчасне попередження [1].

Рис. 1. Загальна архітектура системи (розроблено автором) (IoT-сенсори, Відео (CV) та OSINT дані сходяться в центральне AI-ядро, яке передає результат у блок «Система попередження»

Основним модулем комп’ютерного зору є нейромережева модель YOLO11 (Ultralytics). Вона характеризується високою швидкістю роботи, відмінною підтримкою edge-пристроїв і покращеною здатністю виявляти малі об’єкти, такі як FPV-дрони [6]. Система демонструє стабільну детекцію навіть у складних умовах: шумний міський фон, часткове закриття об’єкта та несприятливе освітлення.

Для стабільного відстеження виявлених об’єктів використовується алгоритм ByteTrack. Він забезпечує мінімальну кількість перепризначень ідентифікаторів, стабільне утримання треку та точне обчислення швидкості об’єкта [7]. ByteTrack показує найкраще співвідношення точності та швидкості серед сучасних алгоритмів трекінгу. Це особливо важливо для динамічних загроз від UAV, які характеризуються високою швидкістю польоту, різкими маневрами та частими змінами траєкторії під впливом оператора. Завдяки ефективній асоціації кожної детекції алгоритм мінімізує втрати треків навіть у складних сценах з перетинами об’єктів або тимчасовим зникненням дрона з кадру.

Табл. 1

Порівняння алгоритмів трекінгу (адаптовано за даними MOT benchmarks)

Алгоритм	MOTA	FPS	ID switches
SORT	54,7 %	143	831
DeepSORT	61,4 %	61	781
ByteTrack	77,3 %	171	558

Прогнозування траєкторії реалізовано гібридним методом: Kalman Filter для швидкого лінійного прогнозу [4] у поєднанні з LSTM-мережею, яка враховує нелінійну поведінку FPV-дронів під керуванням оператора [2]. Kalman Filter забезпечує блискавичну обробку та високу точність на коротких лінійних ділянках руху, тоді як LSTM-мережа навчається на реальних патернах поведінки дронів, передбачаючи різкі повороти, корекцію курсу та маневри ухилення. Такий гібридний підхід дозволяє системі не лише відстежувати поточне положення, але й з високою ймовірністю прогнозувати майбутню точку удару, що дає операторам цінні секунди на реагування.

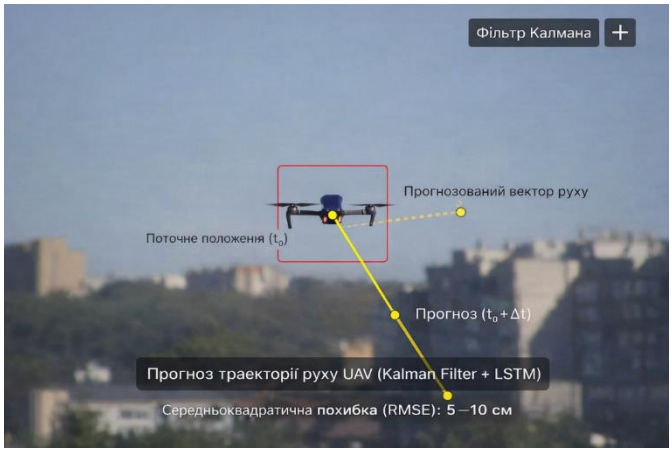

Рис. 2. Прогноз траєкторії дрона (Kalman Filter + LSTM) (Кадр відеопотоку з червоним bounding box навколо FPV-дрона на фоні міської забудови; жовта лінія показує прогнозовану траєкторію на 5–10 секунд вперед)

Точність прогнозу становить приблизно 0,80 м на горизонті 1 секунди та 1,09 м на 5 секундах, що дозволяє розрахувати ймовірну точку удару та вчасно відреагувати.

IoT-компонент доповнює візуальний аналіз акустичними сенсорами (розпізнавання звуку дронів), SDR-модулями (фіксація радіочастот керування) та додатковими камерами. Типовий сценарій: камера виявляє об’єкт → AI класифікує його як «drone» → SDR підтверджує активність сигналу → система автоматично надсилає сповіщення.

OSINT інтегрується для додавання географічного та контекстного шару (повідомлення в каналах, дані волонтерів). Шум у відкритих джерелах фільтрується за допомогою AI-моделей класифікації тексту. При збігу даних OSINT із сенсорними та візуальними джерелами точність системи сягає 90 % і вище [5].

Реальний прототип системи вже функціонує в польових умовах і включає детекцію UAV, стабільний трекінг, прогноз траєкторії, зручний інтерфейс та підтримку відеопотоків з IP-камер і мобільних пристроїв (наприклад, DroidCam) (рис.3).

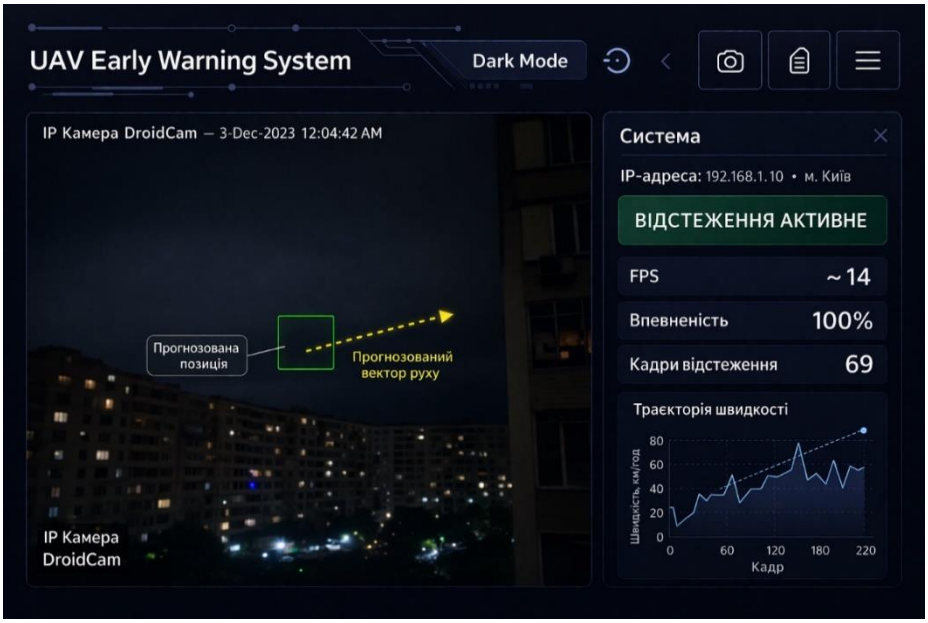

Рис. 3. Інтерфейс прототипу системи раннього попередження

Табл. 2

Ефективність різних підходів до виявлення UAV

№	Підхід	Приблизна точність	Основні переваги	Головні обмеження	Коментар / Рекомендації
1	Традиційний активний радар	70-78 %	Велика дальність, працює в будь-яку погоду, вимірює швидкість і відстань	Висока вартість, погано виявляє малі дрони, легко пригнічується РЕБ	Класичний, але дорогий варіант для дальнього виявлення
2	Тільки Computer Vision (YOLO та подібні)	78-82 %	Висока швидкість, низька вартість, добра класифікація типу дрона	Сильно залежить від освітлення, погоди та фону, багато хибних спрацьовувань	Базовий рівень для денних умов
3	Тільки акустичні сенсори	75-85 %	Пасивний, недорогий, добре працює вночі та при обмеженій видимості	Коротка дальність (до 200-500 м), чутливий до зовнішнього шуму	Добре для ближньої зони
4	Тільки RF (радіочастотний аналіз)	80-88 %	Виявляє керуючий сигнал і місцезнаходження оператора, відносно дешевий	Не працює з автономними (RF-silent) дронами	Ефективний проти комерційних FPV-дронів

№	Підхід	Приблизна точність	Основні переваги	Головні обмеження	Коментар / Рекомендації
5	CV + IoT (камера + акустика + SDR)	84-88 %	Мультимодальне підтвердження загрози, краща робота вночі та при поганій видимості	Зростає складність інтеграції сенсорів	Добрий баланс ціна/якість для передової
6	CV + IoT + Kalman Filter	86-90 %	Додає базовий прогноз траєкторії, покращує стабільність трекінгу	Слабко справляється з різкими маневрами	Перехідний варіант з елементами прогнозування
7	CV + IoT + OSINT + AI (повна інтеграція)	91-95 %	Максимальна точність, контекстна фільтрація шуму, прогноз траєкторії, низький рівень хибних тривог	Найвища складність розробки та налаштування	Оптимальний варіант для реальних бойових умов
8	CV + IoT + OSINT + AI + Thermal Imaging	93-96 %	Відмінна робота вночі, в тумані та при сильному задимленні	Значно дорожче через тепловізори	Рекомендується для захисту критичної інфраструктури
9	Радар + CV + RF (класична мультисенсорна фьюжн)	92-96 %	Широка дальність + візуальне підтвердження + ідентифікація оператора	Висока вартість і складність системи	Використовується в професійних військових системах
10	Повна мультимодальна фьюжн з AI (Radar + CV + RF + Acoustic + OSINT)	95-98 %+	Найвища надійність, мінімальна кількість хибних спрацьовувань, робота в усіх умовах	Найвища вартість і складність інтеграції та обробки даних	Майбутнє систем раннього попередження

Запропонована система має ряд суттєвих переваг порівняно з традиційними засобами виявлення повітряних цілей. По-перше, вона значно дешевша за класичні радіолокаційні станції: вартість одного комплекту на базі edge-пристроїв (наприклад, NVIDIA Jetson, Raspberry Pi 5 або промислових mini-PC) у кілька разів нижча, ніж у спеціалізованих військових радарів. По-друге, система повністю працює на edge-пристроях, що дозволяє проводити всю обробку даних безпосередньо на місці без необхідності постійного підключення до хмарних серверів. Це критично важливо в умовах обмеженого зв'язку, активної радіоелектронної боротьби та вимог до автономності.

По-третє, архітектура легко масштабується - від окремого спостережного поста до розгалуженої мережі сенсорів, розгорнутої вздовж лінії фронту чи навколо критичних об'єктів інфраструктури. По-четверте, система забезпечує

роботу в реальному часі з частотою 30–60 FPS навіть на доступному апаратному забезпеченні, що достатньо для своєчасного виявлення швидкісних FPV-дронів.

Основні інженерні виклики, з якими стикається розробка такої системи, пов'язані насамперед з підготовкою якісного та репрезентативного датасету для навчання моделей комп'ютерного зору. Якість анотацій, різноманітність умов зйомки (денне/нічне освітлення, різні погодні умови, фони, ракурси) та баланс класів безпосередньо впливають на точність детекції. Не менш важливим є правильне налаштування конфігураційних файлів (зокрема, шляхів до датасету в YAML-файлах, параметрів аугментації та гіперпараметрів навчання), оскільки навіть найсучасніша модель YOLO11 демонструє низьку ефективність при неправильній організації даних.

Підсумовуючи, можна сказати що, інтеграція технологій Інтернету речей (IoT), відкритих джерел розвідки (OSINT), комп'ютерного зору та штучного інтелекту створює принципово новий клас доступних, гнучких і високоефективних інтелектуальних систем раннього попередження про UAV-загрози. Завдяки мультимодальному підходу система не тільки підвищує швидкість виявлення та реакції на загрозу, але й суттєво знижує когнітивне навантаження на операторів, автоматизуючи рутинний аналіз даних. У кінцевому підсумку це сприяє підвищенню рівня захисту особового складу, критичної інфраструктури та цивільного населення в умовах сучасної високотехнологічної війни.

Список використаних джерел

1. *European Commission. (2025). Artificial intelligence (AI) in defence. Directorate-General for Defence Industry and Space. https://data.europa.eu/doi/10.2889/1453267*
2. *Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735*
3. *Insecurity Insight. (2025). Hovering threats: The challenges of armed drones in humanitarian contexts. https://shorturl.at/MeAbt*
4. *Kalman, R. E. (1960). A new approach to linear filtering and prediction problems. Journal of Basic Engineering, 82(1), 35–45. https://doi.org/10.1115/1.3662552*
5. *NATO. (2024). Summary of NATO's revised Artificial Intelligence Strategy. https://www.nato.int/cps/en/natohq/official_texts_227237.htm*
6. *Ultralytics. (2024). YOLO11 documentation. https://docs.ultralytics.com/models/yolo11/*
7. *Zhang, Y., Sun, P., Jiang, Y., Yu, D., Weng, F., Yuan, Z., Luo, P., Liu, W., & Wang, X. (2022). ByteTrack: Multi-object tracking by associating every detection box. In Proceedings of the European Conference on Computer Vision (ECCV) (pp. 1–21). Springer. https://arxiv.org/abs/2110.06864*

Крест’янінов Ігор Олександрович
аспірант групи АКН-21
Державного університету
інформаційно-комунікаційних технологій
(063)-268-06-95
i.krestiyaninov@stud.duikt.edu.ua

Катков Юрій Ігорович
доктор технічних наук, доцент

ГІБРИДНИЙ ПІДХІД PARETO-NASH-MPC ДЛЯ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ СИСТЕМАМИ «РОЗУМНОГО БУДИНКУ»

Сучасні системи «розумного будинку» (Smart Home) трансформуються у складні кіберфізичні системи, що функціонують як мультиагентні середовища з високим рівнем автономності. Зростання кількості інтелектуальних пристроїв, інтеграція відновлюваних джерел енергії та необхідність взаємодії з електричними мережами формують нові вимоги до підходів управління. Однією з ключових проблем є забезпечення узгодженої роботи агентів в умовах стохастичної невизначеності, що виникає через зміни зовнішнього середовища, наприклад погодні умови або динаміку тарифів, а також внутрішні фактори, такі як поведінка користувачів і режим експлуатації обладнання.

Традиційні методи керування, зокрема rule-based control (RBC), обмежені у гнучкості та не здатні враховувати складну динаміку системи. Широке застосування набув метод Model Predictive Control (MPC), який дозволяє здійснювати керування з урахуванням прогнозу майбутніх станів системи та наявних обмежень [2]. Проте класичні MPC-моделі переважно орієнтовані на одноцільову оптимізацію і не враховують багатокритеріальність задачі та мультиагентну природу взаємодій.

У цьому контексті актуальною є інтеграція багатокритеріальної оптимізації на основі Pareto-ефективності для знаходження компромісних рішень [4], а також методів теорії ігор, зокрема концепції рівноваги Неша, яка забезпечує узгодження стратегій агентів у конфліктному середовищі [2]. Це створює передумови для формування гібридного підходу Pareto–Nash–MPC.

Постановка задачі

Система «розумного будинку» моделюється як стохастична мультиагентна структура, де кожен агент – наприклад, кліматичний, енергетичний або освітлювальний – прагне мінімізувати власну функцію вартості, що відображає його локальні цілі. Дії агентів взаємопов’язані, що може викликати конфлікти між забезпеченням комфорту користувачів та оптимізацією енергоспоживання. Основна мета полягає у формуванні керуючої політики, яка мінімізує загальну функцію ефективності системи, що агрегує локальні критерії з урахуванням їхніх

пріоритетів. Координація агентів забезпечується через рівновагу Неша, що запобігає одностороннім змінам стратегій окремих агентів і підтримує стабільність системи.

Мета дослідження

Розробка гібридної моделі Pareto–Nash–MPC для мультиагентних систем «розумного будинку», яка забезпечує адаптивне прогнозне керування з урахуванням стохастичності системи та оптимальний баланс між комфортом користувачів і енергоспоживанням, а також виявлення та узгодження конфліктів між агентами через механізми рівноваги Неша.

Результати дослідження

Запропонований підхід поєднує MPC, Pareto-оптимізацію та теорію ігор у єдину архітектуру управління. Система прогнозує стани на горизонті H і розв'язує оптимізаційну задачу для прийняття рішень з урахуванням майбутніх змін. Глобальна функція якості системи визначається як агрегування локальних критеріїв:

$$J_{global} = \sum_k w_k J_k$$

де J_k відображає окремі критерії (енергія, комфорт, безпека), а w_k – вагові коефіцієнти, що визначають пріоритетність кожного критерію. Динаміка системи описується стохастичним рівнянням:

$$x_{t+1} = f(x_t, u_t, \xi_t)$$

де x_t – стан системи у момент часу t, u_t – керуючі дії, а ξ_t – випадкові збурення. Взаємодія агентів моделюється через рівновагу Неша:

$$J_i(a_i' a_{-i}^{)} J_i(a_i, a_{-i}^*)$$

що гарантує відсутність стимулу у жодного агента змінювати стратегію односторонньо, якщо стратегії інших агентів залишаються незмінними. Оптимізація відбувається в просторі Pareto-ефективних рішень, що дозволяє гнучко балансувати різні показники.

Важливою особливістю підходу є використання градієнтного аналізу та потенціальних функцій для виявлення конфліктів між агентами та їх узгодження. Це дозволяє інтегрувати ігрову логіку безпосередньо в контур MPC та забезпечити узгодженість локальних і глобальних цілей. Архітектура реалізована як замкнений цикл із збором даних із сенсорів і зовнішніх джерел, аналізом мультиагентних взаємодій, прогнозуванням та оптимізацією керуючих дій, а також нейромережевим оператором для адаптації параметрів на основі накопиченого досвіду.

Моделювання показало, що запропонований підхід забезпечує зниження енергоспоживання на 10–15% порівняно з традиційними алгоритмами, підвищує рівень комфорту користувачів завдяки прогнозуванню потенційних конфліктів і демонструє стійкість до випадкових збурень та змін тарифів. Результати підтверджують ефективність мультиагентного координаційного механізму та

узгоджуються з сучасними дослідженнями щодо MPC та Pareto-орієнтованих підходів [1], [2], [3], [4].

Висновки та перпективи

Гібридний підхід Pareto–Nash–MPC ефективний для інтелектуального управління системами «розумного будинку», оскільки дозволяє враховувати динаміку системи, багатокритеріальність та конфліктність інтересів агентів. Інтеграція Pareto-оптимізації забезпечує гнучкість у виборі рішень, рівновага Неша гарантує узгодженість дій агентів, а MPC надає адаптивність і проактивність управління.

Результати дослідження підтверджують доцільність використання підходу для підвищення енергоефективності та комфорту у системах «розумного будинку». Подальші дослідження можуть зосередитися на інтеграції методів глибокого навчання, масштабуванні підходу до рівня Smart Grid і Smart City, а також на експериментальній перевірці на реальних об’єктах.

Список використаних джерел

1. Elgammal, A. (2026, січень). Real-Time thermal–water management energy dispatch co-optimization in pemfc-evs via metaheuristic pareto tuning of MPC with rl-based disturbance adaptation. International Journal of Modern Research in Engineering and Technology. https://www.ijmret.org/paper/V11I1/41478451375.pdf

2. Morteza, A., Nazari, H. K., & Pahlevani, P. (2024, 23 серпня). An iot framework for building energy optimization using machine learning-based MPC. arXiv.org. https://arxiv.org/abs/2408.13294

3. Saroha, P., Singh, G., Lilhore, U. K., Khan, M., Masud, M., Khalid, A., & Algarni, S. (2025, 4 грудня). Enhancing smart home energy efficiency using a hybrid genetic algorithm and improved dandelion optimizer - international journal of computational intelligence systems. SpringerLink. https://link.springer.com/article/10.1007/s44196-025-01076-z

4. Scarabaggio, P., Mignoni, N., Jantzen, J., Carli, R., & Dotoli, M. (2024, жовтень). Model predictive control with recursive multi-step input convex lipschitz neural networks: An application to smart buildings. IEEE Xplore. https://ieeexplore.ieee.org/document/10831606

Лисенко Микола Миколайович
аспірант 3 року навчання
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
andrew.strazh@gmail.com

Бондарчук Андрій Петрович
д.т.н., професор
завідувач кафедри комп'ютерних наук
Київського столичного університету імені Бориса Грінченка, м. Київ
a.bondarchuk@kubg.edu.ua

ЗАСТОСУВАННЯ МЕТОДІВ КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ ІНТРАОПЕРАЦІЙНОЇ НАВІГАЦІЇ ТА ВІЗУАЛІЗАЦІЇ АНАТОМІЧНИХ СТРУКТУР У РЕАЛЬНОМУ ЧАСІ

Постановка задачі. Сучасний етап цифровізації медицини потребує розробки високонавантажених інформаційних систем, здатних інтегрувати гетерогенні дані діагностики у відеопотік хірургічних втручань у реальному часі. Актуальність дослідження зумовлена необхідністю подолання обмежень традиційної візуалізації шляхом впровадження алгоритмів комп'ютерного зору, що автоматично суміщають цифрові двійники органів (КТ/МРТ) із динамічним операційним полем. Метою роботи є розробка наукового підходу для інтраопераційної навігації, що забезпечує мінімальну затримку візуалізації та високу точність просторової орієнтації, створюючи єдиний інтелектуальний простір для підтримки прийняття рішень хірургом. Основою дослідження є процес сегментації медичних зображень, отриманих за допомогою комп'ютерної томографії. Використовуючи нейронні мережі архітектури U-Net, ми проводимо автоматичне виділення цільових об'єктів (органів, новоутворень) та реконструкцію їхніх тривимірних моделей у форматі STL або OBJ.

Результати дослідження. В основі запропонованого підходу лежить конвеєрна обробка даних, що включає автоматичну сегментацію анатомічних структур за допомогою нейронних мереж архітектури U-Net та їх подальшу 3D-реконструкцію. Для забезпечення просторової синхронізації віртуальних моделей із реальним відеопотоком застосовано комбінований метод на основі дескрипторів ознак ORB та ітераційного алгоритму ICP, реалізований за допомогою мови Python та бібліотек PyTorch.

Аналіз результатів досліджень вказує на високу стійкість алгоритмів до візуальних шумів та артефактів, проте виявляє потребу у впровадженні методів нежорсткої реєстрації для корекції динамічних деформацій м'яких тканин. Результатом роботи є вдосконалення методів інтраопераційного трекінгу, що дозволяє автоматизувати ідентифікацію критичних анатомічних зон та значно

знизити когнітивне навантаження на оператора в умовах складних інформаційних потоків.

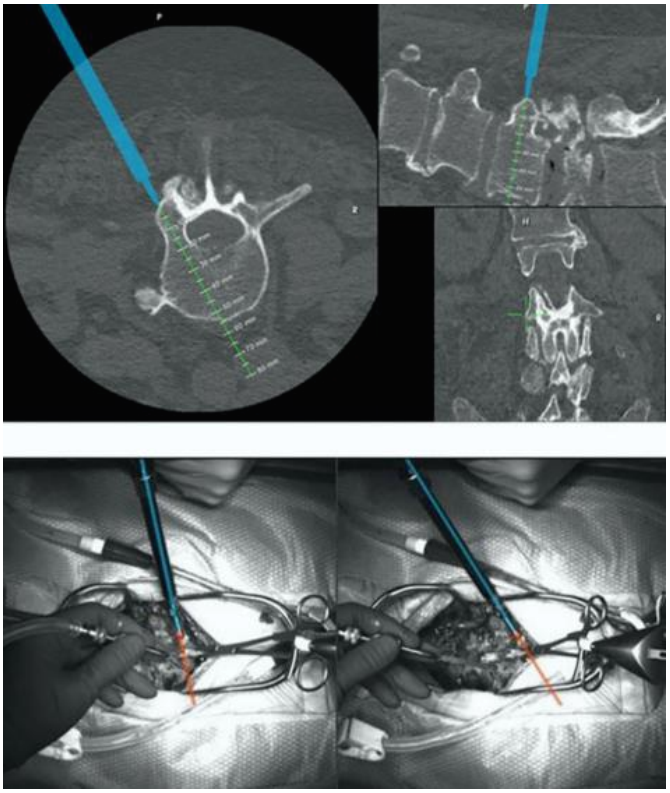

Рис. 1. Застосування комп’ютерного зору при операції хребта

Висновки. Розроблена інформаційна система підтвердила ефективність використання методів комп’ютерного зору для підвищення точності та безпеки хірургічних маніпуляцій завдяки створенню середовища змішаної реальності. Отримані показники швидкодії та точності відповідають стандартам сучасних медичних навігаційних комплексів, а запропонований підхід до архітектури системи створює надійну базу для подальшої інтеграції засобів штучного інтелекту в клінічну практику. Подальші дослідження будуть спрямовані на адаптацію системи до динамічних змін геометрії органів, що дозволить розширити сферу її застосування в автоматизованих госпітальних мережах.

Список використаних джерел

1. Сокольцов, А. О., Кандауров, І. В., Привалов, Б. В., Носова, Т. В., Шушляпіна, Н. О., Носова, Я. В., & Аврунін, О. Г. (2025). Натурні 3D–моделі як ефективний інструмент для відпрацювання навичок риноендоскопічних втручань. Оптико-електронні інформаційно-енергетичні технології, 50(2), 233-243. DOI: 10.31649/1681-7893-2025-50-2-233-243

2. Касянчук, Андрій Валентинович.. "Вплив штучного інтелекту, комп'ютерного зору та машинного навчання на життя людини." Управління розвитком складних систем 55 (2023): 175-185.

Pidhornyi Andrii
3rd year student
majoring in «Computer Engineering»
National Technical University
«Kharkiv Polytechnic Institute», Kharkiv
Andrii.Pidhornyi@cs.khpi.edu.ua

Brechko Veronika
docent, Associate Professor
at the Department of Computer Engineering and Programming
National Technical University
«Kharkiv Polytechnic Institute», Kharkiv
Veronika.Brechko@khpi.edu.ua

DEVELOPMENT OF ELEMENTS OF A SMART HOME SYSTEM

This paper presents the development and analysis of key elements of a smart home system within the Internet of Things paradigm. The system architecture, functional components, and interaction mechanisms are examined. Special attention is given to communication protocols, data security, energy efficiency, and the integration of artificial intelligence methods. A conceptual model of a scalable and adaptive smart home system is proposed.

The rapid evolution of information technologies and the widespread adoption of the Internet of Things (IoT) have significantly influenced the development of smart environments, particularly smart home systems [1]. These systems aim to improve the quality of life by automating routine processes, enhancing security, and optimizing energy consumption. Smart homes integrate heterogeneous devices into a unified network, enabling efficient monitoring and control. The development of smart home systems requires a comprehensive approach that includes hardware components, software solutions, and communication infrastructure. The purpose of this work is to design and analyze the main elements of such a system and to investigate their interaction within a unified architecture. A typical smart home system consists of four main components: sensors, actuators, a central controller, and a software interface. Each component plays a crucial role in ensuring the system's functionality and efficiency.

Sensors are responsible for collecting real-time data about environmental conditions. Common types of sensors include temperature, humidity, light, motion, and smoke detectors. These devices generate continuous data streams that reflect the current state of the environment. The collected data is transmitted to the central controller for further processing and decision-making [3]. The accuracy and reliability of sensors significantly influence the overall system performance.

Actuators serve as execution units that respond to commands generated by the controller. They include lighting systems, heating, ventilation, and air conditioning (HVAC) units, smart locks, alarms, and other devices. Actuators enable the system to

automatically adjust environmental parameters based on predefined rules or real-time data analysis.

The central controller is the core of the smart home system. It acts as a processing unit that receives data from sensors, analyzes it, and generates appropriate control signals for actuators. The controller can be implemented as an embedded microcontroller, a local server, or a cloud-based solution. The choice of implementation depends on system requirements such as latency, scalability, and computational complexity.

The software component provides an interface between the user and the system. It enables real-time monitoring, configuration of automation scenarios, and manual control of devices. A well-designed user interface is essential for ensuring usability and accessibility. Modern smart home systems often include web-based or cross-platform applications. Security is one of the most important aspects of smart home systems. Since these systems manage sensitive data and control physical devices, they are potential targets for cyberattacks. To ensure data protection, various security mechanisms are implemented, including authentication, authorization, encryption, and secure communication channels. Access control policies restrict unauthorized users from interacting with the system [4].

In addition to traditional automation, modern smart home systems increasingly incorporate artificial intelligence techniques. Machine learning algorithms can analyze historical data to identify user preferences and predict future behavior. This enables the system to adapt dynamically and provide personalized services. For instance, predictive models can optimize heating schedules or detect anomalies in system operation [5].

Another important aspect is system scalability and interoperability. A well-designed smart home system should support the integration of new devices and technologies without requiring significant modifications. Standardization of communication protocols and modular architecture design are essential for achieving this goal.

The proposed conceptual model integrates all the discussed components into a unified system. It emphasizes modularity, flexibility, and adaptability. The system supports both centralized and distributed control approaches, allowing it to operate efficiently under different conditions.

Список використаних джерел

1. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications // IEEE Communications Surveys & Tutorials. – 2023.

2. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // IEEE Internet of Things Journal. – 2022.

3. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions // Future Generation Computer Systems. – 2023.

4. Li S., Da Xu L., Zhao S. The Internet of Things: A Survey // Information Systems Frontiers. – 2022.

5. Yang G., Xie L., Mäntysalo M., et al. A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box // IEEE Transactions on Industrial Informatics. – 2023.

Гелман Амін Акімович
студент 4 курсу
спеціальності «Штучний інтелект»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st7977927@stud.duikt.edu.ua

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ІНТЕРНЕТІ РЕЧЕЙ

Інтенсивний розвиток цифрових технологій зумовлює широке впровадження Інтернету речей (IoT) та штучного інтелекту (ШІ) у різноманітні сфери діяльності. Синергія цих технологій формує нові підходи до автоматизації процесів, підвищення ефективності управління та побудови інтелектуальних систем. Динаміка розвитку ринку ШІ в IoT характеризується стійким зростанням: з 7,47 млрд доларів США у 2023 році до прогнозованих 29,08 млрд доларів США до 2032 року, що свідчить про актуальність і перспективність даного напряму [1].

Інтеграція штучного інтелекту в середовище Інтернету речей істотно розширює можливості збору, обробки та аналізу даних. Використання алгоритмів машинного навчання забезпечує ефективну роботу з великими масивами інформації в режимі реального часу, що підвищує оперативність і точність прийняття управлінських рішень.

Одним із ключових напрямів застосування є прогнозне обслуговування. Інтелектуальні IoT-системи здатні здійснювати моніторинг технічного стану обладнання та виявляти аномальні відхилення, що дозволяє завчасно запобігати відмовам і оптимізувати витрати на технічне обслуговування. Особливої актуальності це набуває в умовах промислового виробництва [2].

Важливою перевагою є також підвищення рівня персоналізації сервісів. IoT-пристрої, зокрема в системах розумного дому, здатні адаптуватися до поведінкових моделей користувачів, автоматично регулюючи параметри середовища відповідно до індивідуальних потреб.

Окрему увагу привертає застосування технологій ШІ та IoT у концепції «розумного міста». Їх використання дозволяє оптимізувати транспортні системи, управління відходами та інші міські процеси, що сприяє раціональному використанню ресурсів і підвищенню якості життя населення.

Крім того, значний потенціал інтеграції ШІ та IoT спостерігається у сфері охорони здоров’я. Носимі пристрої забезпечують безперервний моніторинг життєво важливих показників, що дає змогу своєчасно виявляти відхилення та підвищувати ефективність медичного обслуговування [3].

Таким чином, інтеграція штучного інтелекту в Інтернет речей є одним із пріоритетних напрямів розвитку сучасних інформаційних технологій. Вона сприяє підвищенню ефективності обробки даних, надійності функціонування

систем та рівня автоматизації в різних галузях. Подальший розвиток даного напряму забезпечить створення більш інтелектуальних, адаптивних і безпечних технологічних рішень.

Список використаних джерел

1. Alakkari K., Ali B. Artificial Intelligence of Things: A Review // Babylonian Journal of Internet of Things. – 2025. – Vol. 2025. – P. 113–120

2. Hamidi S. A., Hashimi F. U., Rahmati A. Integrating Artificial Intelligence in IoT Systems: A Systematic Review of Recent Advances and Application // Journal of Computer Science Advancements. – 2024.

3. Aleran A. et al. Artificial Intelligence and the Internet of Things in Energy Preservation: Research Prototypes, Trends, and Future Directions // Computing (Springer). – 2025. – Vol. 107. – Article 209.

Гульчук Дмитро Сергійович
студент групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
gds6686@gmail.com

Бондарчук Олександр Павлович
викладач кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.bondarchuk@duikt.edu.ua

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УПРАВЛІННЯ ПРИВАТНИМ БУДИНКОМ

Сьогодні прогрес розвитку Інтернету речей (IoT) у поєднанні із штучним інтелектом (ШІ) відкриває нові можливості для автоматизації та оптимізації квартир та будинків. Приватний будинок може стати наявним прикладом інтегрованої системи, де сенсори, пристрої та програмні модулі взаємодіють для забезпечення комфорту, безпеки та енергоефективності [1]. Така концепція отримала назву “розумний будинок” і є одним із ключових напрямів розвитку сучасних інформаційних технологій.

Використання ШІ у сфері “розумного будинку” дає змогу перейти від простих сценаріїв автоматизації (такі як вмикання світла за датчиком руху) до складних адаптивних систем, що враховують поведінку мешканців, зовнішні умови та індивідуальні потреби [2]. Алгоритми машинного навчання здатні

аналізувати великі масиви даних, отриманих від сенсорів, і приймати оптимальні рішення в реальному часі.

Основні напрями застосування ШІ в приватному будинку можна поділити на кілька категорій:

1. Енергозбереження та оптимізація ресурсів. Алгоритми прогнозування дозволяють визначати пікові години споживання електроенергії та оптимізувати роботу освітлення, опалення й кондиціонування. Система може враховувати температуру зовнішнього середовища, скільки людей у приміщенні та їхні звички, щоб автоматично регулювати клімат-контроль [3]. Це не лише знижує витрати, а й сприяє екологічній сталості.

2. Безпека та моніторинг. Використання комп'ютерного зору та систем розпізнавання звуку дозволяє виявляти підозрілу активність, інтегруватися з камерами та сигналізаціями. ШІ може спостерігати та аналізувати поведінку відвідувачів, розпізнавати обличчя, а також навіть відрізняти звичайні звуки (такі як падіння предмета наприклад) від потенційно небезпечних (розбиття скла чи подібне) [4].

3. Комфорт та персоналізація. Голосові асистенти, інтегровані з IoT-пристроями, створюють персоналізоване середовище. Система може "навчитися" звичкам мешканців ,наприклад: автоматично вмикати улюблену музику вранці для пробудження чи регулювати освітлення для читання ввечері. Це створює індивідуальний простір, що адаптується до потреб користувача.

4. Інтеграція з Big Data та прогнозування. Використання великих масивів даних дозволяє прогнозувати потреби мешканців та підвищувати ефективність системи. Аналіз історичних даних може допомогти передбачити, коли скоріш за все знадобиться підвищення температури в будинку, або коли навпаки мешканці зазвичай залишають приміщення [5].

Таким чином, використання ШІ в приватному будинку показує перспективність поєднання IoT та інтелектуальних алгоритмів. Це не лише підвищує якість життя окремих користувачів, а й сприяє розвитку концепції "розумних міст" та цифрової трансформації побуту. Водночас важливим залишається питання безпеки даних та захисту приватності, адже інтелектуальні системи працюють із великими масивами персональної інформації. Тому майбутні дослідження мають бути спрямовані на створення надійних механізмів кіберзахисту та етичного використання технологій.

Список використаних джерел

1. Лановський, М. О. (2022). Впровадження цифрових технологій Інтернету речей для поліпшення енергоощадних технологій у будівлях. Комп'ютерні науки та інноваційні технології, 37, 145–152. https://doi.org/10.32782/2663-5682/2022/37/35

2. Smith, J. (2023). Artificial Intelligence in Smart Homes: Applications and Challenges. Journal of IoT Research, 12(3), 45–58.

3. Brown, L., & Chen, Y. (2024). Energy Efficiency through AI-driven IoT Systems. IEEE Transactions on Smart Grid, 15(2), 210–220.

4. Кузнецов, Я. В. (2025). Модифікований метод підвищення безпеки розумного будинку за рахунок штучного інтелекту. Наукові праці КПІ ім. Ігоря Сікорського, 4(25), 88–96.

5. Білик, О. В., & Білик, М. Ю. (2025). Перспективи розвитку ринку розумних електротехнічних пристроїв (Smart Home) в Україні. Вісник Кременчуцького національного університету імені М. Остроградського, 7(5), 33–41. https://doi.org/10.32782/2079-5009.krnu25.7.5

Абраменко Олександра Андріївна
студентка групи ІСД-42
Державного університету
інформаційно-комунікаційних технологій, м. Київ
(095)-329-68-10
j67062423@gmail.com

Бондарчук Олександр Павлович
викладач кафедри Інформаційних систем та технологій Державного університету
інформаційно-комунікаційних технологій, м. Київ

ВИКОРИСТАННЯ ГЕНЕРАТИВНИХ АЛГОРИТМІВ У СТВОРЕННІ КНИЖКОВИХ ІЛЮСТРАЦІЙ

Генеративні алгоритми значно пришвидшують процес формування концепцій майбутніх ілюстрацій, дозволяючи митцям миттєво отримувати численні варіанти стилю, композиції та образної системи й оперативно відбирати найвдаліші рішення; одночасно вони відкривають нові творчі межі, поєднуючи традиційні прийоми і несподівані візуальні поєднання, що збагачують інтерпретацію літературних творів. Використання штучного інтелекту у книжковому ілюструванні тому є не лише технологічною інновацією, а й важливим напрямом сучасного дизайну, який потребує окремого дослідження з погляду методик генерації образів, авторських прав та естетичних критеріїв відбору результатів.

Постановка задачі

У сучасній практиці створення книжкових ілюстрацій дедалі ширше застосовуються інструменти штучного інтелекту, що дозволяють прискорити візуалізацію художніх образів, урізноманітнити стилістичні рішення та розширити горизонти творчого пошуку. Водночас постає завдання з’ясувати, яким чином генеративні алгоритми можуть бути інтегровані у процес ілюстрування літературних творів так, щоб не втратити художньої цілісності, смислової виразності та авторського задуму. Тому актуальним є комплексне дослідження особливостей використання ШІ у книжковій ілюстрації, його взаємодії з

традиційними і цифровими методами графічного дизайну та розробка рекомендацій для балансування технологічних можливостей і художньої автономії автора.

Мета дослідження

Метою дослідження є всебічний аналіз можливостей застосування штучного інтелекту у процесі створення книжкових ілюстрацій та уточнення його ролі у формуванні художньо виразного візуального образу літературного твору. Особливу увагу приділено використанню генеративних алгоритмів як інструменту для пошуку композиційних, стилістичних та образних рішень у сучасній ілюстративній практиці, а також оцінці їх впливу на збереження авторського задуму, цілісності візуального наративу й художньої виразності твору.

Результати дослідження

У ході дослідження встановлено, що генеративні алгоритми є ефективним інструментом у процесі створення книжкових ілюстрацій. Їх використання дає змогу прискорити пошук візуальних рішень, розробку ескізів і формування художніх образів відповідно до змісту літературного твору. Визначено, що застосування генеративних алгоритмів сприяє урізноманітненню стилістичних і композиційних рішень, а також розширює можливості творчого експерименту під час роботи над ілюстраціями. Отримані результати підтвердили, що використання таких алгоритмів у поєднанні з авторським баченням ілюстратора дає змогу створювати цілісний, виразний і сучасний візуальний супровід книги.

Висновки та перспективи

Отже, застосування генеративних алгоритмів у створенні книжкових ілюстрацій виявляється перспективним напрямом сучасного графічного дизайну: воно дозволяє оптимізувати окремі етапи творчого процесу, прискорити пошук візуальних рішень і розширити можливості художньої інтерпретації літературного твору. Проведене дослідження підтвердило, що генеративні підходи є ефективним допоміжним інструментом для ілюстратора, оскільки поєднання алгоритмічної генерації з авторським баченням сприяє створенню цілісних, виразних і сучасних візуальних образів, збереженню змістовної взаємодії тексту й ілюстрації та підвищенню продуктивності творчих ітерацій.

Список використаних джерел

1. *Li, H., Xue, T., Zhang, A., Luo, X., Kong, L., & Huang, G. (2024). The application and impact of artificial intelligence technology in graphic design: A critical interpretive synthesis. Heliyon, 10(21), e40037. https://doi.org/10.1016/j.heliyon.2024.e40037*
2. *Adobe. Photoshop Desktop Help. Adobe Help Center. URL: https://helpx.adobe.com/photoshop/desktop.html*
3. *Lewis, N. (2025). Teaching Illustration in the Age of Generative AI. URL: https://sure.sunderland.ac.uk/id/eprint/19286/1/12%2BLewis.pdf*
4. *A Study on the Use of AI Image Generation Tools for Picture Book Illustration Development. (2026). ResearchGate. URL: https://shorturl.at/k7OD9*
5. *Liu, W., et al. (2025). The visual communication using generative artificial intelligence in the context of new media. Scientific Reports. URL: https://www.nature.com/articles/s41598-025-96869-9*

Зима Олексій Андрійович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету інформаційно-комунікаційних технологій, м. Київ
st6870209@stud.duikt.edu.ua

Катков Юрій Ігорович
професор, доктор технічних наук

ІНТЕЛЕКТУАЛЬНА IOT-СИСТЕМА ДЛЯ АВТОМАТИЗОВАНОЇ ОБРОБКИ ПАПЕРОВИХ БЛАНКІВ ТЕСТУВАННЯ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОГО РОЗПІЗНАВАННЯ.

Вступ

Цифровізація освіти вимагає швидкої обробки великих обсягів паперових даних. Попри розвиток онлайн-тестування, паперові бланки залишаються стандартом для державних іспитів та сертифікацій через надійність та відсутність потреби в індивідуальних гаджетах. Проблема полягає у тривалості ручної перевірки та високій вартості професійних сканерів. Створення IoT-системи, що використовує доступні камери та нейромережеве розпізнавання, дозволить автоматизувати процес, знизити помилки людського фактора та забезпечити миттєву передачу результатів у хмару.

Сьогодні існують системи типу OMR (Optical Mark Recognition), OMR - це технологія автоматизованого зчитування даних з паперових форм, де інформація позначена спеціальними мітками (галочками, кружечками або зафарбованими областями) [1, 2]. Система OMR працює шляхом розпізнавання наявності або відсутності відбитого світла від паперу. Оскільки технологія дозволяє обробляти тисячі документів за годину з мінімальною кількістю помилок, вона незамінна в таких сферах: освіта (перевірка тестів, екзаменаційних бланків та анкет); вибори (автоматизований підрахунок голосів у паперових бюлетенях); лотереї (зчитування ігрових комбінацій на квитках); медицина (заповнення карток пацієнтів та опитувальників) [3, 4]..

Такі системи мають переваги (швидкість: можливість миттєвої обробки великих масивів даних без участі людини; точність: виключається «людський фактор» при підрахунку балів). Але є обмеження - технологія зазвичай не розпізнає рукописний текст (для цього потрібна технологія OCR – Optical Character Recognition), а лише мітки. Також вона вимагає використання якісного паперу та чіткого дотримання меж маркування користувачем.

OMR використовується у мобільних додатках. Існують рішення для смартфонів (наприклад, ZipGrade), проте вони мають обмежену точність при розпізнаванні рукописного тексту (OCR) і часто не інтегровані в єдину IoT-інфраструктуру закладу, що ускладнює централізований моніторинг у реальному

часі. Використання стандартних алгоритмів комп'ютерного зору без нейромереж часто призводить до помилкового зчитування через низьку якість зображення. [5, 6].

Постановка завдання

Необхідно рознобити архітектуру IoT-системи, яка здатна отримувати зображення бланків з периферійних пристроїв (камер, підключених до мікрокомп'ютерів), проводити їх попередню обробку та застосовувати нейронну мережу для класифікації міток і розпізнавання ідентифікаторів студентів. Система має забезпечувати стійкість до геометричних спотворень зображення та передавати оброблені дані в базу даних через захищені канали зв'язку.

Метою є розробка концепції та прототипу інтелектуальної IoT-системи для автоматизації збору та аналізу результатів тестування. Основний акцент робиться на підвищенні точності розпізнавання за допомогою архітектур згорткових нейронних мереж (CNN) та забезпеченні мобільності системи шляхом використання концепції Edge Computing, де первинна обробка відбувається безпосередньо на місці сканування.

Основна частина

Архітектура IoT-системи базується на трирівневій архітектурі:

1. Рівень сприйняття (Perception Layer): Модулі захоплення зображення на базі Raspberry Pi з камерою або ESP32-CAM. Пристрій фіксує бланк.

2. Мережевий рівень (Network Layer): Передача стиснутих даних через Wi-Fi/Ethernet до локального сервера або хмарного шлюзу.

3. Прикладний рівень (Application Layer): Хмарна платформа, де розгорнута нейромережа (наприклад, MobileNetV2), яка виконує сегментацію бланка та виділення відповідей. Така структура дозволяє масштабувати систему на велику кількість аудиторій одночасно.

У порівнянні з класичними алгоритмами (OpenCV-фільтри, порогове перетворення), нейромережевий підхід демонструє вищу точність на «шумних» зображеннях. На відміну від закритих комерційних систем, запропонована модель на базі IoT є гнучкою до зміни шаблонів бланків без перепрограмування всього пристрою - достатньо оновити модель нейромережі в хмарі.

Запропоновані нові підходи до створення інтелектуальної IoT-системи для автоматизованої обробки паперових бланків тестування на основі нейромережевого розпізнавання. Цім підходом є використання Transformer-based архітектур для корекції перспективи бланка. Компоненти системи:

- Edge AI Node: Використання алгоритмів квантизації моделі для запуску нейромереж безпосередньо на мікроконтролерах, що мінімізує трафік.
- Data Augmentation Pipeline: Метод генерації синтетичних даних для навчання мережі, що імітує різні умови освітлення та дефекти друку.
- Блок верифікації: Модуль, що автоматично маркує «сумнівні» бланки (де нейромережа має низьку впевненість) для ручної перевірки оператором.

- API-шлюз: Для інтеграції з системами управління навчанням (LMS, наприклад Moodle). Це дозволяє реалізувати концепцію «розумного деканату», де результати з'являються в системі через секунди після здачі роботи студентом.

Висновки та перспективи

Розроблена концепція інтелектуальної IoT-системи вирішує проблему оперативності та вартості обробки паперових тестів. Використання нейромереж забезпечує високу стійкість до артефактів зображення. Перспективи розвитку полягають у впровадженні розпізнавання рукописних відкритих відповідей (Handwritten Text Recognition) та створенні мобільних автономних боксів для сканування, які не потребують постійного підключення до мережі під час роботи, накопичуючи дані у внутрішній пам'яті.

Список використаних джерел

1. Authors: Mohamed Labrassi, Aziz Ouaarab (2025) Improved Deep Learning-Based Optical Mark Recognition for Automated Correction. Intelligent Data Engineering and Automated Learning – IDEAL 2025: 26th International Conference, Jaén, Spain, November 13–15, 2025, Proceedings, Part I. Pages 324 – 330. https://doi.org/10.1007/978-3-032-10486-1_30

2. MOHAMMED ALI, SUHEL HAMMOUD, ALIDA ESPER (2025) Optical Mark Recognition Techniques for Multiple-Choice Tests: A Comprehensive Review. Received 2 July 2025, accepted 11 August 2025, date of publication 19 August, date of current version 11 September 2025. Digital Object Identifier 10.1109/ACCESS.2025.3600106

3. Dutta, A., & Gupta, S. (2022). Deep Learning-Based OMR for Automated Exam Correction International Journal of Interactive Multimedia and Artificial Intelligence. URL: https://www.linkedin.com/posts/mohamed-labrassi-375566208_deeplearning-computervision-research-activity-7392825733078740992-_DIF

4. Jia Li, Shiva Nejati, Mehrdad Sabetzadeh, Michael McCallen (2025) A domain-specific language for simulation-based testing of IoT edge-to-cloud solutions. Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems. Pages 367 – 378.https://doi.org/10.1145/3550355.3552405

5. Priyabrata Karmakar Shyh Wei Teng Guojun Lu (2024) A survey on attention-based artificial neural networks for automatic speech recognition https://doi.org/10.1016/j.iswa.2024.200406

6. Urmi Kushwah (2025) Integrating IoT and Smart Technologies in Education: A Pathway to Personalized and Adaptive Learning. August 2025Vidhyayana 11(si1):117-136. DOI:10.58213/cksnqh76

Угрімов Денис Володимирович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
denis.ugrimov04@gmail.com

ЗАСТОСУВАННЯ МУЛЬТИМОДАЛЬНИХ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ ДЛЯ РОЗПІЗНАВАННЯ ВІЗУАЛЬНИХ ОБ'ЄКТІВ У ВЕБ-ЗАСТОСУНКАХ

Стрімкий розвиток штучного інтелекту зумовив появу нового класу моделей - мультимодальних великих мовних моделей (МВММ), здатних одночасно обробляти текстові та візуальні дані. На відміну від класичних підходів комп'ютерного зору, що потребували окремого навчання під конкретні категорії об'єктів, МВММ реалізують підхід відкритого світу (open-world classification), за якого модель здатна ідентифікувати довільні об'єкти без додаткового донавчання [1].

Постановка задачі та технічні обмеження класичних підходів.

Традиційні методи розпізнавання зображень, засновані на згорткових нейронних мережах, мають суттєве архітектурне обмеження: вони здатні класифікувати лише наперед визначені категорії об'єктів і потребують повторного навчання при зміні предметної області. Згідно з оглядом, опублікованим у IEEE Transactions on Pattern Analysis and Machine Intelligence, МВММ усувають цей недолік завдяки попередньому навчанню на масштабних наборах пар «зображення-текст» з відкритого інтернету, що забезпечує здатність до узагальнення на нові категорії об'єктів без додаткового розмічення даних [3]. Інтеграція класичних моделей комп'ютерного зору у веб-застосунки також вимагає розгортання власної серверної інфраструктури, тоді як МВММ доступні через стандартний REST API, що суттєво спрощує архітектуру системи та скорочує час розробки.

Мета дослідження.

Дослідити практичну застосовність мультимодальних великих мовних моделей для задач розпізнавання візуальних об'єктів у контексті веб-застосунків, а також оцінити переваги та обмеження їх інтеграції через хмарний API порівняно з класичними підходами.

Результати дослідження.

Як зазначається в огляді A Survey on Multimodal Large Language Models, сучасні МВММ формують єдину уніфіковану архітектуру обробки тексту та зображень, що принципово відрізняє їх від попередніх підходів, де візуальні та мовні модулі функціонували незалежно [2]. Дослідження, проведене у межах оцінки готовності моделей до задач харчового аналізу, підтверджує, що сучасні

VLM демонструють точність розпізнавання харчових продуктів понад 80% навіть без спеціалізованого донавчання, перевершуючи ряд класичних CNN-підходів у сценаріях з широким діапазоном категорій [4]. У процесі практичної реалізації веб-застосунку з розпізнаванням візуальних об'єктів було підтверджено, що передача зображення у форматі base64 через REST API та отримання структурованої JSON-відповіді є достатнім для побудови повнофункціональної клієнт-серверної системи без необхідності розгортання власної моделі на сервері.

Табл. 1

Ефективність методів контролю якості даних

Параметр порівняння	Класичні CNN-моделі	Мультимодальні LLM (MBMM)
Типи об'єктів	Фіксований набір класів	Довільні об'єкти (відкритий світ)
Формат виводу	Клас + ймовірність	Структурований текст / JSON
Потреба у донавчанні	Висока (під кожну задачу)	Відсутня (zero-shot)
Інтеграція у веб	Складна (власна інфраструктура)	Проста (REST API)

Висновки.

Мультимодальні великі мовні моделі є перспективним інструментом для інтеграції функціоналу комп'ютерного зору у веб-застосунки. Вони усувають необхідність навчання спеціалізованих моделей під конкретні предметні області, забезпечують гнучкий структурований формат виводу та доступні через стандартний API. Разом з тим, залежність від зовнішніх хмарних сервісів залишається обмеженням для застосунків із підвищеними вимогами до конфіденційності даних. Подальші дослідження доцільно спрямувати на порівняльну оцінку точності MBMM у вузькоспеціалізованих предметних областях та дослідження можливостей їх локального розгортання.

Список використаних джерел

1. *Conti A. et al. On Large Multimodal Models as Open-World Image Classifiers. ICCV 2025. URL: https://tinyurl.com/39htca3c*
2. *Yin S. et al. A Survey on Multimodal Large Language Models. National Science Review. 2024. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11645129/*
3. *Zhang W. et al. Vision-Language Models for Vision Tasks: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2024. URL: https://ieeexplore.ieee.org/document/10423421*
4. *Cioffi R. et al. Are Vision-Language Models Ready for Dietary Assessment? Exploring the Next Frontier in AI-Powered Food Image Recognition. arXiv. 2025. URL: https://arxiv.org/html/2504.06925v1*

Роговенко Максим Олександрович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
maksimrogovenko224@gmail.com

Сагайдак Віктор Анатолійович
PhD, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ІНТЕГРАЦІЯ IOT ТА ШТУЧНОГО ІНТЕЛЕКТУ ЯК НОВИЙ РІВЕНЬ АВТОМАТИЗАЦІЇ ПОВСЯКДЕННОГО ЖИТТЯ

Сьогоднішній день поєднання Інтернету речей (IoT) та штучного інтелекту вже не виглядає як щось футуристичне – це поступово стає частиною звичайного життя. Суть IoT полягає в тому, що різні пристрої (від фітнес-браслетів до побутової техніки) підключені до мережі та постійно обмінюються даними. Але самі по собі ці дані мало що дають, якщо їх не аналізувати. Саме тут підключається штучний інтелект – він дозволяє не просто збирати інформацію, а «витягувати» з неї сенс і на основі цього приймати рішення [1].

Найбільш доступний приклад – системи «розумного будинку». Вони вже давно вийшли за межі простого дистанційного керування технікою. Зараз такі системи можуть автоматично підлаштовувати освітлення, температуру чи навіть рівень безпеки залежно від поведінки користувача. Це здається дрібницею, але саме з таких деталей і формується відчуття «розумного середовища». Наприклад, якщо людина щодня повертається додому в один і той самий час система може заздалегідь увімкнути опалення або світло[2].

Окремо варто звернути увагу на те, що сучасні IoT-системи вже не є статичними. Завдяки алгоритмам машинного навчання вони поступово адаптуються до змін і стають точнішими у своїх рішеннях. Тобто мова йде не просто про автоматизацію, а про перехід до систем, які можуть частково прогнозувати потреби користувача. У перспективі це означає, що повсякденні процеси – від побуту до організації робочого простору – будуть все більше переходити в напівавтоматичний режим. Саме тому поєднання IoT та штучного інтелекту сьогодні розглядається як один із ключових напрямів розвитку цифрового суспільства [1; 2].

Табл. 1

Основні компоненти IoT-системи та їх функції

Компонент системи	Функції	Приклади використання
Датчики (Sensors)	Збирають інформацію з навколишнього середовища	Температура, рух, освітлення
Мережа (Network)	Передає дані між пристроями та серверами	Wi-Fi, Bluetooth, мобільний інтернет
Обробка даних (AI/Cloud)	Аналізує отримані дані та приймає рішення	Алгоритми штучного інтелекту
Користувацький інтерфейс	Дозволяє людині взаємодіяти з системою	Мобільні додатки, панелі керування

З таблиці видно, що всі елементи IoT-системи тісно пов’язані між собою і працюють як єдине ціле. При цьому ключову роль відіграє обробка даних, оскільки саме вона дозволяє системі не просто збирати інформацію, а приймати рішення. Саме завдяки штучному інтелекту IoT переходить від звичайної автоматизації до більш «розумного» функціонування.

Список використаних джерел

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks.URL: https://doi.org/10.1016/j.comnet.2010.05.010

2. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson. URL: https://aima.cs.berkeley.edu/

3. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2021). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. URL: https://doi.org/10.1016/j.future.2013.01.010

Чорнобривець Дмитро Віталійович
студент групи ІП-21
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського", м. Київ
chornobruveyets@gmail.com

Поперешняк Світлана Володимирівна
доцент кафедри Інформатики та програмної інженерії
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського", м. Київ
spopereshnyak@gmail.com

ОПТИМІЗАЦІЯ ПРОСТОРОВОГО АНАЛІЗУ ЗАЙНЯТОСТІ ПАРКОМІСЦЬ В EDGE-IOT СИСТЕМАХ З ВИКОРИСТАННЯМ МЕТРИКИ IOU

Анотація. Досліджується інтелектуальна IoT-система моніторингу паркувальних місць на основі комп'ютерного зору з використанням парадигми граничних обчислень (Edge Computing). Запропоновано метод визначення статусу паркомісця за допомогою метрики перекриття площ (IoU) замість аналізу центральної точки, що мінімізує похибки при нестандартному паркуванні.

Ключові слова: Internet of Things, Edge Computing, комп'ютерний зір, YOLO, IoU, гомографія, розумне місто, ROI.

Мета дослідження. Метою дослідження є розробка та апробація автоматизованої системи блокування зарядних місць для електромобілів, яка використовує інтелектуальні технології для розпізнавання електрокарів, управління паркувальними бар'єрами та інтегрується з зарядними станціями, забезпечуючи їх ефективне використання. Така система має забезпечувати автоматичне опускання паркувального бар'єра після підключення електромобіля до зарядної станції, гарантуючи доступ лише для електрокарів [1].

Архітектура Edge-IoT. Суть запропонованої архітектури полягає в тому, що ресурсомістка обробка відео (детекція та просторовий аналіз) виконується локально – безпосередньо на мікрокомп'ютері, підключеному до камери (рис. 1). На центральний IoT-сервер передається не "важкий" відеопотік, а лише "легкі" пакети даних у форматі JSON, що містять ідентифікатор місця, його статус (вільно/зайнято) та часову мітку. Це забезпечує масштабованість системи та суттєво зменшує вимоги до пропускної здатності мережі.

Детекція та еволюція просторового аналізу. Першим етапом обробки кадру є виявлення транспортних засобів. У роботі використано однопрохідну нейромережеву модель YOLO, яка забезпечує оптимальний баланс між точністю та швидкістю інференсу (висновку) на малопотужних Edge-пристроях. Модель генерує обмежувальні рамки (Bounding Boxes) [2] для кожного виявленого автомобіля. На другому етапі виконується геометричне співставлення виявлених автомобілів із заздалегідь сконфігурованими зонами інтересу (Region of Interest - ROI) [3], що відповідають розмітці паркомісць.

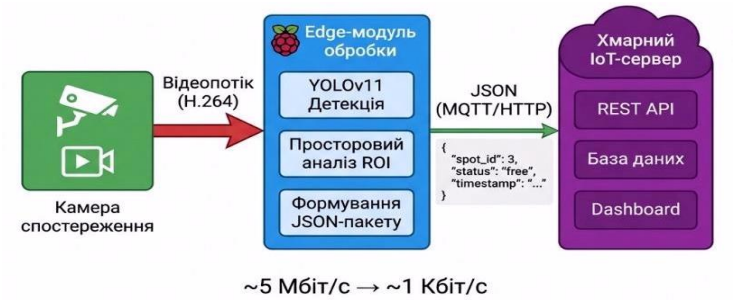

Рис. 1. Блок-схема Edge-архітектури

Класичний підхід, який використовує тест входження центральної точки автомобіля P у полігон паркомісця R, має суттєвий недолік: він є вразливим до випадків "неправильного" паркування (коли габаритний транспортний засіб займає два суміжних місця). Для підвищення надійності системи (робастності) запропоновано оптимізований метод просторового аналізу на основі метрики Intersection over Union (IoU)[4] або коефіцієнта перекриття. Система розраховує відношення площі перетину обмежувальної рамки виявленого автомобіля B та полігону паркомісця R до загальної площі паркомісця:

$$Coverage(B,R) = \frac{fracArea(B \cap R)}{Area(R)},$$

Якщо значення *Coverage* перевищує емпірично встановлений поріг (наприклад, 0.45), місце класифікується як "Зайняте". Цей підхід дозволяє коректно обробляти часткові перекриття та виявляти порушників правил паркування.

Висновки та перспективи. Розроблена архітектура Edge-IoT системи на основі комп'ютерного зору доводить свою ефективність у задачах моніторингу паркувального простору. Впровадження метрики перекриття площ (IoU) усуває алгоритмічні похибки класичних методів при нестандартному паркуванні. Використання граничних обчислень вирішує проблему перевантаження міських мереж, а застосування перетворень дозволяє інтегрувати дані про паркомісця у глобальні навігаційні системи Smart City.

Подальші дослідження будуть спрямовані на використання зібраних Big Data для тренування предиктивних моделей завантаженості паркінгів.

Список використаних джерел

1. Giampaoli, L. E., & Hessel, F. (2021). Parking Space Occupancy Monitoring System Using Computer Vision and IoT. IEEE 7th World Forum on Internet of Things (WF-IoT), 7-12. https://doi.org/10.1109/WF-IoT51360.2021.9595935

2. Чорнобривець, Д. В., Поперешняк, С. В. (2024). Система моніторингу місць для паркування з використанням комп'ютерного зору. Телекомунікаційні та інформаційні технології, 4(85), 62-72. https://doi.org/10.31673/2412-4338.2024.045775

3. S. V. Popereshnyak, D. V. Chornobryvets. COMPUTER VISION-BASED APPROACH TO PARKING SPACE AVAILABILITY DETECTION, 83-91 DOI: https://doi.org/10.32782/2521-6643-2025-1-69.10

4. Bradski, G. (2000). The OpenCV Library. Dr. Dobb's Journal of Software Tools. https://opencv.org/

Асмолов Сергій Олександрович
студент групи ТЦР-51
Державного університету інформаційно-комунікаційних технологій
asmolov@gmail.com

РОЗУМНІ СТЕНДИ ДЛЯ ТЕСТУВАННЯ ЕЛЕКТРООБЛАДНАННЯ З ВИКОРИСТАННЯМ ЦИФРОВИХ ДВІЙНИКІВ (DIGITAL TWIN)

Сучасна електроенергетика потребує точних і швидких методів контролю стану обладнання. Традиційні підходи до тестування часто є трудомісткими та обмеженими у можливостях аналізу. Розвиток цифрових технологій відкриває нові підходи до вирішення цих завдань, зокрема через використання концепції цифрового двійника.

Цифровий двійник - це віртуальна модель фізичного об’єкта, яка відтворює його стан у реальному часі. Вона базується на даних, що надходять із сенсорів. Такий підхід дозволяє аналізувати поведінку об’єкта без прямого втручання.

Система цифрового двійника складається з трьох частин: фізичного об’єкта, цифрової моделі та каналу обміну даними. Дані з обладнання передаються у модель. Модель обробляє їх і відображає поточний стан. Це забезпечує постійний контроль і можливість прогнозування [1].

Розумні стенди застосовуються для контролю технічного стану електрообладнання шляхом вимірювання його основних параметрів. Вони забезпечують виявлення відхилень від нормативних значень і дозволяють оцінити працездатність обладнання.

Сучасні стенди виконують не лише вимірювання, а й діагностику: на основі отриманих даних визначають можливі несправності та ступінь їх розвитку. Це дає змогу виявляти дефекти на ранніх етапах і зменшувати ризик відмов у роботі обладнання.

Автоматизація процесу тестування знижує вплив оператора, підвищує точність результатів і забезпечує повторюваність вимірювань [2].

Типовий стенд складається з датчиків, контролера та програмного забезпечення (рис.1). Датчики перетворюють фізичні величини (струм, напруга, температура) у електричні сигнали. Контролер обробляє ці сигнали та передає їх у систему аналізу.

Рис. 1. Структурна схема типового діагностичного стенда (датчики, контролер та система аналізу даних)

Системи збору даних забезпечують швидке отримання і обробку інформації в реальному часі. Програмне забезпечення виконує аналіз результатів, виявляє відхилення та формує висновок про стан обладнання. [2]

У сучасних рішеннях використовуються комп’ютерні методи діагностики, що дозволяють автоматично обробляти великі обсяги даних і підвищують ефективність технічного контролю.

Розумні стенди забезпечують поточне та стабільне вимірювання параметрів, що підвищує достовірність результатів. Автоматизація дозволяє швидко обробляти дані, виявляти відхилення та зменшувати вплив оператора. Використання цифрових технологій дає можливість працювати в реальному часі, прогнозувати несправності та підвищувати надійність обладнання.

Впровадження таких систем потребує значних витрат на обладнання та програмне забезпечення. Ефективність роботи залежить від якості даних і налаштування системи. Також виникають складнощі інтеграції з існуючим обладнанням і потреба у підготовці персоналу. [1]

Цифрові двійники завзято використовуються в промисловості як засіб збільшення ефективності та сталості устаткування. В енергетиці їх залучають для вдосконалення робочих режимів агрегатів у добу. Це дає змогу скоротити витрати ресурсів та підняти віддачу процесів.

У виробничих комплексах цифрові двійники гарантують нагляд за технічним станом устаткування впродовж усього терміну служби. Вони дають змогу з'єднати відомості з різноманітних джерел у єдину інформаційну модель. Це полегшує оцінку та ухвалення рішень.

У галузі електроагрегатів цифрові двійники вживаються для випробування роз’єднувачів, трансформаторів та інших приладів. Вони надають можливість моделювати робочі стани, звіряти параметри та передбачати ймовірні збої без загрози для справжнього устаткування.

У навчальних майстернях подібні технології застосовуються для імітації дійсних процесів. Студенти можуть вивчати функціонування систем без

фізичного втручання. Це покращує рівень підготовки кадрів та формує практичні уміння роботи із сучасними засобами.

Цифрові двійники є ефективним інструментом модернізації тестових систем. Вони забезпечують точний контроль і глибокий аналіз даних. Подальший розвиток технології пов'язаний із розширенням можливостей моделювання. Очікується зростання ролі таких рішень у автоматизації та діагностиці електрообладнання.

Список використаних джерел

1. Семененко Ю. С. Моделювання цифрових двійників бізнес-процесів як інструмент управління ефективністю компанії // Наукові записки Національного університету «Острозька академія». Серія «Економіка». – Острог: Вид-во НаУОА, 2025. – № 38(66). – С. 99–106. URL : http://doi.org/10.25264/2311-5149-2025-38(66)-99-106

2. Цифрові двійники для промислового застосування : біла книга / Industrial Internet Consortium. – Версія 1.0. – 2020. – 21 с.

Бученко Ігор Анатолійович
старший викладач кафедри
Комп'ютерної інженерії
Державного університету
інформаційно-комунікаційних технологій, м. Київ
i.buchenko@duikt.edu.ua

ЗАСТОСУВАННЯ ПЕРИФЕРІЙНИХ ОБЧИСЛЕНЬ ТА ФІЗИЧНОГО ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ РОЗУМНОГО ЗЕМЛЕРОБСТВА

Сучасна галузь сільського господарства перебуває у незручному становищі. Не тільки в Україні, але й у світі з'являється дефіцит кадрів, змінюється клімат, бур'яни адаптуються до існуючих хімічних засобів. Актуальність дослідження полягає в потребі зміни старих підходів масової обробки полів на перехід до екологічних, безпечних систем точного землеробства, які керуються автономними кіберфізичними системами. Мета роботи полягає в комплексному аналізі багаторівневої архітектури аграрного Інтернету речей (IoT) на базі периферійних обчислень та практичного застосування фізичного штучного інтелекту (ШІ) в агроробототехніці, що в перспективі дозволить оптимізувати алгоритми управління комп'ютерними мережами.

Еволюція інтелектуальних систем знаменується переходом до концепції фізичного штучного інтелекту. У цій парадигмі алгоритми машинного навчання глибоко інтегруються у фізичні структури (мобільні роботи, безпілотні апарати),

дозволяючи їм безпосередньо сприймати реальний світ та виконувати прецизійні дії у непередбачуваних середовищах. [2] Для забезпечення безперебійного функціонування таких систем в умовах нестабільного сільського зв'язку розгортається трирівнева архітектура взаємодії: хмарний рівень, периферійний рівень та рівень кінцевих пристроїв. [7] Периферійні обчислення переносять обчислювальні потужності безпосередньо до джерела виникнення даних на борту техніки, що повністю усуває критичні мережеві затримки.

Впровадження концепції фізичного ШІ безпосередньо на мобільних аграрних платформах потребує використання обчислювальних модулів новітнього зразка. Провідним індустріальним стандартом у цьому сегменті виступає платформа NVIDIA, а саме вбудовані системи лінійки Jetson Orin Nano. Дані мікрокомп’ютери гарантують обчислювальну потужність на рівні 67 TOPS за умов мінімального енергоспоживання, відкриваючи можливість безперервного виконання інференсу ресурсоємних нейромережевих архітектур локально та в режимі реального часу. (табл.1) [5]

Табл. 1

Специфікації комплекту для розробників Jetson Orin Nano Super [5]

Компонент	Характеристики
Продуктивність ШІ	67 INT8 TOPS
Графічний процесор	Архітектура NVIDIA Ampere з 1024 ядрами CUDA та 32 тензорними ядрами
Процесор	6-ядерний процесор Arm® Cortex®-A78AE версії 8.2, 64-бітний, 1,5 МБ пам'яті L2 + 4 МБ пам’яті L3
Пам’ять	8 ГБ 128-бітної LPDDR5 102 ГБ/с
Пам’ять для зберігання даних	Підтримує слот для SD-карти та зовнішній NVMe
Потужність	7 Вт–25 Вт

Дослідження показують, що розгортання моделей комп’ютерного зору (наприклад, архітектур сімейства YOLO) на платформі Jetson Orin для завдань семантичної сегментації дозволяє з високою точністю ідентифікувати рослини (рис. 1) та миттєво генерувати керуючі сигнали для виконавчих механізмів. [6]

Аграрна промисловість на основі ШІ без хімікатів стає більш реалістичною за рахунок роботів Aigenio на сонячній енергії (рис. 2), які використовують ШІ для виявлення та видалення бур’янів на рівні рослин, допомагаючи фермерам зменшити використання гербіцидів та впроваджувати більш стійкі методи завдяки симуляції, реальним даним та периферійному штучному інтелекту (edge AI). [4] Комунікація всередині рою таких роботів здійснюється через інтелектуальну mesh-мережу, що дозволяє ботам координувати дії без втручання оператора. (рис. 3)

Рис. 1. Ідентифікація рослин штучним інтелектом [1]

Рис. 2. Компоненти робота Aigenio [1]

Рис. 3. Рій роботів Aigenio [1]

Стрімке розширення ройових систем призводить до експоненційного зростання обсягів мережевого трафіку. Зважаючи на обмеженість енергетичних та обчислювальних ресурсів периферійних вузлів, виникає необхідність переходу до децентралізованих моделей управління, де кожен окремий дрон чи наземний робот функціонує як незалежний раціональний агент. Інтеграція математичних моделей на основі теорії ігор для розподілу мережевих ресурсів є стратегічно важливим вектором розвитку. Такий підхід дає змогу раціоналізувати розподіл завдань (task offloading) і побудову маршрутів передачі даних всередині рою роботів, що мінімізує ризики перевантаження окремих вузлів і підвищує надійність всієї аграрної IoT-інфраструктури. [3]

Здійснено комплексний аналіз сучасних архітектурних рішень для сільськогосподарських розумних систем, що ґрунтуються на глибокій синергії парадигм периферійних обчислень та фізичного штучного інтелекту. Підтверджено, що міграція обчислювальних навантажень безпосередньо на бортові мікропроцесори мобільних агророботів з використанням платформ NVIDIA Jetson Orin є критичною вимогою для для усунення мережевих затримок і гарантування безперебійної роботи алгоритмів комп’ютерного зору в режимі реального часу. Наукова новизна роботи полягає у формуванні концептуального підґрунтя для поєднання апаратних засобів аграрної кіберфізики на базі автономних ройових комплексів Aigen із математичним математичним апаратом теорії ігор. Рекомендації щодо практичного застосування здобутих результатів передбачають їх використання як базису для розробки оптимізаційних алгоритмів маршрутизації. Впровадження таких теоретико-ігрових моделей забезпечить високоефективне балансування обчислювальних потужностей та енерговитрат в умовах нестабільних бездротових мереж, притаманних інфраструктурі точного землеробства.

Список використаних джерел

1. Aigen • robotics • AI generated agriculture. (б. д.). Aigen • Robotics • AI Generated Agriculture. https://www.aigen.io/

2. Fontani, M., Luglio, S. M., Gagliardi, L., Peruzzi, A., Frasconi, C., Raffaelli, M., & Fontanelli, M. (2025). A systematic review of 59 field robots for agricultural tasks: Applications, trends, and future directions. Agronomy, 15(9), 2185. https://doi.org/10.3390/agronomy15092185

3. Gong, R., Zhang, H., Li, G., & He, J. (2025). Edge computing-enabled smart agriculture: Technical architectures, practical evolution, and bottleneck breakthroughs. Sensors, 25(17), 5302. https://doi.org/10.3390/s25175302

4. Huskey, L., & Cook, V. (б. д.). Feeding the world with AI. https://institute.bankofamerica.com/transformation/ai-agriculture.html

5. Jetson orin nano super developer kit. (б. д.). NVIDIA. https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-orin/nano-super-developer-kit/

6. Lytridis, C., & Pachidis, T. (2024). Recent advances in agricultural robots for automated weeding. AgriEngineering, 6(3), 3279–3296. https://doi.org/10.3390/agriengineering6030187

7. Rasool, I., Yadav, P., Parmar, A., Mirzakhaninafchi, H., Budhathoki, R., Usmani, Z. U. A., Jone, E., Paudel, S., & Olivera, I. P. (2025). Robotic system with AI for real time weed detection, canopy aware spraying, and droplet pattern evaluation. ArXiv preprint arXiv:2507.05432. https://doi.org/10.48550/arXiv.2507.05432

Чернєв Іван Юрійович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету інформаційно-комунікаційних технологій, м. Київ
ivan.cherniev@duikt.edu.u

ПРОГНОЗУВАННЯ СЦЕНАРІЇВ ЖИТТЄДІЯЛЬНОСТІ В СИСТЕМАХ РОЗУМНОГО БУДИНКУ ЗА ДОПОМОГОЮ АНАЛІТИКИ ПОВЕДІНКОВИХ ПАТЕРНІВ

Постановка задачі

Сучасний етап розвитку концепції Інтернету речей (IoT) характеризується переходом від простих систем автоматизації до складних інтелектуальних середовищ, що здатні генерувати та обробляти колосальні обсяги даних у реальному часі. Проте більшість існуючих рішень для «Розумного будинку» досі базуються на жорстко детермінованих сценаріях, які потребують постійного ручного коригування з боку користувача. Така архітектурна обмеженість створює додаткове когнітивне навантаження на людину та знижує загальну ефективність системи. Актуальність дослідження полягає у необхідності створення адаптивної моделі управління, яка б використовувала аналітику поведінкових патернів для проактивного прийняття рішень [1]. При цьому критично важливим аспектом залишається забезпечення конфіденційності та

цілісності даних, оскільки аналіз звичок мешканців передбачає роботу з надчутливою персональною інформацією [4].

Мета дослідження

Метою даної роботи є проектування та наукове обґрунтування моделі управління системою «Розумний будинок», яка інтегрує методи машинного навчання для аналізу користувацької поведінки. Дослідження спрямоване на розробку архітектурного рішення, що гармонізує високий рівень побутового комфорту, оптимізацію енергоспоживання та впровадження надійних протоколів безпеки для захисту IoT-мереж від несанкціонованого втручання.

Результати дослідження

У результаті проведеного аналізу була сформована трирівнева інтелектуальна модель, яка забезпечує гнучке управління житловим простором:

1. Шар збору та агрегації контекстних даних: На відміну від традиційних систем, запропонована модель розглядає кожну дію користувача як елемент великого цифрового сліду. Використання мережі гетерогенних сенсорів дозволяє фіксувати не лише події, а й їхній контекст: тривалість перебування у зонах, часові кореляції між використанням різних приладів та реакцію на зміну зовнішніх умов [1]. Це створює надійний фундамент для побудови точних прогнозних моделей.

2. Модуль поведінкової аналітики: Центром системи є аналітичне ядро, що використовує алгоритми навчання без учителя для виявлення прихованих закономірностей у поведінці мешканців. Модель здатна самостійно класифікувати поточний стан системи (наприклад, «сон», «робота», «відсутність») і адаптувати параметри освітлення, температури та безпеки без прямих команд користувача. Такий підхід дозволяє виявляти аномалії, які можуть сигналізувати про вихід з ладу обладнання або потенційні загрози здоров'ю людини [3].

3. Екосистема безпеки та конфіденційності: Враховуючи специфіку даних, особлива увага приділяється захисту комунікаційних каналів. Модель передбачає впровадження стандартизованих рішень кібербезпеки, зокрема використання протоколів TLS 1.3 для шифрування трафіку між IoT-вузлами та центральним хабом [4]. Використання криптографічних бібліотек (наприклад, OpenSSL) забезпечує надійну автентифікацію пристроїв, мінімізуючи ризики перехоплення даних або логічних атак на систему управління [2, 4].

Висновки

Запропонована модель управління доводить, що інтеграція аналітики користувацької поведінки є ключовим фактором трансформації «Розумного будинку» у справді автономну систему. Це дозволяє не лише покращити якість життя, а й досягти суттєвої економії енергоресурсів завдяки предиктивному управлінню. Подальші дослідження будуть зосереджені на впровадженні методів граничних обчислень (Edge Computing) для локальної обробки даних, що

дозволить підвищити швидкість реакції системи та забезпечити ще вищий рівень приватності користувачів.

Список використаних джерел

1. AltexSoft. (2023, July 10). IoT Architecture: Layers and Components in Smart Systems. https://www.altexsoft.com/blog/iot-architecture/

2. ISO/IEC. (2022). Cybersecurity – IoT security and privacy – Guidelines and infrastructure (ISO/IEC Standard No. 27400:2022). https://www.iso.org/standard/74140.html

3. Kotevski, A., Koceska, N., & Koceski, S. (2022). Security and monitoring in smart home systems: Current trends. Journal of Applied Informatics, 15, 45–52.

4. Осипчук, С. О., Мошинська, А. В., & Кіращук, В. В. (2019). Прикладні аспекти реалізації рішень передавання інформації в технологіях інтернету речей. Перспективи телекомунікацій: матеріали конференції, 17–21.

5. MokoSmart. (2024). IoT technologies for smart home and systems: A comprehensive review of 2024 trends. https://www.mokosmart.com/

Кудринський Павло Олегович
аспірант кафедри Комп'ютерних наук
Державного університету інформаційно-комунікаційних технологій, м. Київ
pavlo.kudrinskiy@gmail.com

Звенігородський Олександр Сегрійович
к. т. н., доцент кафедри штучного інтелекту
Державного університету інформаційно-комунікаційних технологій, м. Київ
zvenigas56@gmail.com

ОПТИМІЗАЦІЯ АЛГОРИТМІВ КРАЙОВИХ ОБЧИСЛЕНЬ (EDGE COMPUTING) ДЛЯ МІНІМІЗАЦІЇ ЗАТРИМКИ В IOT-СИСТЕМАХ РЕАЛЬНОГО ЧАСУ

Актуальність теми. Зі зростанням кількості пристроїв Інтернету речей (IoT) традиційна хмарна модель обробки даних стикається з проблемою високих затримок (latency) та перевантаження каналів зв'язку. Для систем реального часу (автономний транспорт, промислова автоматизація IIoT, телемедицина) критично важливим є прийняття рішень за мілісекунди. Технологія Edge Computing дозволяє перенести обчислювальне навантаження ближче до джерела даних, проте обмеженість ресурсів крайових вузлів вимагає створення інтелектуальних алгоритмів розподілу завдань (offloading).

Постановка задачі. Метою дослідження є розробка алгоритму динамічного розподілу обчислювальних завдань між IoT-пристроєм, крайовим сервером (Edge node) та центральною хмарою (Cloud) для мінімізації сумарної затримки T_{total} при дотриманні обмежень на енергоспоживання.

Виклад основного матеріалу. Затримка в системах Edge Computing складається з часу передачі даних мережею T_{comm} та часу безпосередньої обробки T_{proc} . У запропонованому підході використовується метод зваженої черги пріоритетів, де кожне завдання J_i характеризується параметрами: обсяг даних D_i обчислювальна складність C_i та критичний поріг затримки T_{max}.

Математична модель оптимізації базується на мінімізації цільової функції: $T_{total} = \sum_{i=1}^{n} (x_i * T_{edge} + (1 - x_i) * T_{cloud})$ – де $x_i \in \{0,1\}$ - рішення про розвантаження завдання на крайовий вузол або в хмару. [1][2]

На відміну від стандартних алгоритмів (наприклад, Round Robin), запропонований адаптивний алгоритм враховує поточну завантаженість процесора (CPU load) крайового вузла та стан пропускної здатності каналу (Bandwidth). Якщо прогнозний час обробки на Edge-рівні перевищує T_{max}через чергу завдань, система автоматично перенаправляє частину низькопріоритетних запитів до хмари, звільняючи ресурси для критичних операцій.[3]

Результати дослідження. Шляхом імітаційного моделювання в середовищі iFogSim було проведено порівняльний аналіз запропонованого алгоритму з традиційною хмарною архітектурою. Результати показали:

1. Середнє зниження затримки для критичних завдань на 25-35%.[4]
2. Зменшення обсягу трафіку до центрального ядра мережі на 40%.[5]
3. Стабільність системи при пікових навантаженнях (понад 100 активних вузлів на один Edge-сервер).

Висновки. Оптимізація алгоритмів розвантаження в Edge Computing є ключовим фактором розвитку сучасних IoT-мереж. Запропонований метод дозволяє ефективно використовувати обмежені ресурси крайових пристроїв, забезпечуючи виконання вимог реального часу для критично важливих застосунків. Подальші дослідження будуть спрямовані на впровадження методів машинного навчання (Reinforcement Learning) для прогнозування навантаження мережі.

Список використаних джерел

1. Buyya, R., Srirama, S. N. Fog and Edge Computing: Principles and Paradigms. Wiley, 2019. 448 p.

2. Шевченко О. В. Методи оптимізації обчислень у мережах IoT. Наукові праці КНТУ, 2024. №12. С. 45–52.

3. Kumar, A., & Gupta, S. Latency Optimization in IoT-Edge Systems Using Federated Learning: A Comprehensive Review. Journal of Network and Computer Applications. 2023. Vol. 215. 103632.

4. Кучук Г. А., Коваленко А. О., Гацевич П. О. Методи та засоби управління ресурсами хмарно-орієнтованих систем. Сучасні інформаційні системи. 2023. Т. 7, № 2. С. 15–22.

5. Теленик С. Ф., Ролик О. І., Букасов М. М. Динамічне управління обчислювальними ресурсами в ієрархічних крайових мережах. Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка. 2024. № 71. С. 34–41.

Кудринський Павло Олегович
аспірант кафедри Комп'ютерних наук
Державного університету інформаційно-комунікаційних технологій, м. Київ
pavlo.kudrinskiy@gmail.com

Звенігородський Олександр Сегрійович
к. т. н., доцент кафедри штучного інтелекту
Державного університету інформаційно-комунікаційних технологій, м. Київ
zvenigas56@gmail.com

ВИКОРИСТАННЯ IoMT (INTERNET OF MEDICAL THINGS) ДЛЯ ДИСТАНЦІЙНОЇ РЕАБІЛІТАЦІЇ ПАЦІЄНТІВ

Актуальність теми. Традиційні методи реабілітації вимагають постійної присутності пацієнта в медичному закладі, що створює логістичні та фінансові бар'єри. Впровадження концепції Інтернету медичних речей (IoMT) дозволяє трансформувати цей процес у дистанційну форму (telerehabilitation), забезпечуючи безперервний моніторинг фізіологічних показників та правильності виконання вправ у домашніх умовах. Це особливо критично для пацієнтів з порушеннями опорно-рухового апарату, серцево-судинними захворюваннями та при відновленні після мінно-вибухових травм.

Постановка задачі. Метою роботи є розробка архітектури системи дистанційної реабілітації на основі IoMT-пристроїв, яка забезпечує біологічний зворотний зв'язок (biofeedback) у реальному часі та автоматизований збір даних для лікаря-реабілітолога.[1]

Виклад основного матеріалу. Запропонована система базується на трирівневій ієрархії:

1. Рівень сенсорів (Perception Layer): Використання інерційних вимірювальних модулів (IMU), що включають акселерометри та гіроскопи, для фіксації кутів нахилу кінцівок, а також датчиків ЧСС та SpO2 для контролю загального стану організму.[2]
2. Мережевий рівень (Network Layer): Передача даних через протокол Bluetooth Low Energy (BLE) на смартфон пацієнта (Gateway) з подальшою синхронізацією з хмарним сервером за стандартами шифрування AES-256.[3]
3. **Прикладний рівень (Application Layer):** Програмне забезпечення для пацієнта, яке за допомогою алгоритмів машинного навчання (наприклад, Dynamic Time Warping) порівнює поточну траєкторію руху кінцівки з еталонною моделлю вправи.[4]

Ключовою інновацією є використання алгоритму класифікації активності для автоматичного підрахунку повторень та оцінки амплітуди рухів. Це дозволяє лікарю дистанційно корегувати план лікування на основі об'єктивних даних, а не суб'єктивних відчуттів пацієнта.

Результати дослідження. Впровадження прототипу системи на базі контролера ESP32 та набору сенсорів MPU6050 показало високу точність розпізнавання типів вправ (до 94%) при затримці передачі даних не більше 120 мс. Використання системи дозволяє підвищити прихильність пацієнтів до виконання вправ на 30% завдяки елементам гейміфікації та постійному контролю.[5]

Висновки. Технології IoMT створюють фундамент для персоналізованої медицини, дозволяючи проводити ефективну реабілітацію поза межами стаціонару. Запропонована архітектура вирішує проблему браку кваліфікованих кадрів шляхом автоматизації рутинного моніторингу, що дозволяє одному фахівцю одночасно вести у 3-4 рази більше пацієнтів без втрати якості терапії.

Список використаних джерел

1. Joyia, D. M., Liaqat, R. M., et al. Internet of Medical Things (IoMT): Applications, Challenges and Future Opportunities. World Wide Web. 2023. Vol. 26, No. 4. P. 1255–1280.

2. Gatouillat, A., Badr, Y., et al. Internet of Medical Things: A Review of Recent Contributions from a Process Perspective. IEEE Access. 2018. Vol. 6. P. 37641–37663. (Класичний огляд архітектури).

3. Kashyap, S., & Sharda, S. Artificial Intelligence and IoMT in Healthcare: Next-Generation Rehabilitation Systems. Medical Devices & Sensors. 2024. Vol. 7, No. 1. 10214.

4. Коваленко А. О., Кучук Г. А. Методи управління трафіком у мережах Інтернету медичних речей. Сучасні інформаційні системи. 2025. Т. 9, № 1. С. 12–19. (Актуальне українське джерело).

5. World Health Organization (WHO). Global Strategy on Digital Health 2020–2025. Geneva: WHO Press, 2021. 60 p.

Фоменко Віолетта Володимирівна
студентка групи ІСД-42
Державного університету
інформаційно-комунікаційних технологій, м.Київ
(050)-049-82-26
fomenkoviola2016@gmail.com

Данильченко Валентина Миколаївна
PhD, доцент Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м.Київ
y.danylchenko@duikt.edu.ua

ЗАСТОСУВАННЯ МЕТОДІВ КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ АВТОМАТИЗОВАНОГО АНАЛІЗУ ВІЗУАЛЬНИХ ДАНИХ

Обсяги візуальної інформації стрімко зростають завдяки розвитку цифрових технологій, систем відеоспостереження, мобільних пристроїв та інтернету речей. Це створює необхідність ефективної обробки та аналізу зображень у різних сферах – від безпеки та медицини до промисловості та транспорту. Традиційні методи аналізу візуальних даних, які базуються на ручній обробці або простих алгоритмах, уже не забезпечують достатньої швидкості, точності та масштабованості, що обмежує їхнє практичне застосування.

Методи комп'ютерного зору відкривають широкі можливості для автоматизованого аналізу зображень і відеопотоків. Використання сучасних алгоритмів дозволяє системам розпізнавати об'єкти, класифікувати сцени, виявляти події та аналізувати поведінку в реальному часі. Це значно підвищує ефективність обробки візуальних даних, зменшує залежність від людського фактора та забезпечує можливість швидкого прийняття рішень у складних і динамічних середовищах.

Постановка задачі

У зв'язку зі стрімким зростанням обсягів візуальної інформації, що генерується сучасними цифровими системами, виникає необхідність у створенні ефективних засобів її автоматизованої обробки та аналізу. Візуальні дані активно використовуються у різних сферах діяльності – від медицини та транспорту до промисловості, безпеки та інтелектуальних інформаційних систем. Однак традиційні підходи до аналізу зображень, які передбачають ручну обробку або використання простих алгоритмів, мають обмежену продуктивність, низьку адаптивність та не здатні ефективно працювати з великими масивами даних у реальному часі.

Методи комп'ютерного зору дозволяють автоматизувати процеси обробки візуальної інформації, забезпечуючи можливість виявлення, розпізнавання та класифікації об'єктів, а також аналізу складних сцен. Завдяки використанню

сучасних алгоритмів, зокрема моделей глибокого навчання, системи комп'ютерного зору здатні виконувати складні завдання з високою точністю та швидкістю, що значно розширює можливості їх практичного застосування.

Особливо актуальним є впровадження таких систем у задачах автоматизованого аналізу візуальних даних, де необхідна обробка інформації у реальному часі, мінімізація впливу людського фактора та підвищення ефективності прийняття рішень. Це обумовлює необхідність дослідження методів комп'ютерного зору, аналізу їхніх можливостей і обмежень, а також розробки програмних рішень для реалізації автоматизованих систем аналізу зображень.

Мета дослідження

Метою дослідження є аналіз та застосування методів комп'ютерного зору для автоматизованого аналізу візуальних даних, а також розробка програмного застосунку, здатного виконувати розпізнавання та обробку зображень із використанням сучасних алгоритмів машинного навчання. Дослідження спрямоване на підвищення ефективності обробки візуальної інформації, забезпечення високої точності розпізнавання об'єктів та можливості роботи системи в умовах реального часу.

Результати дослідження

У ході дослідження було проаналізовано сучасні підходи та методи комп'ютерного зору, що застосовуються для автоматизованого аналізу візуальних даних. Розглянуто принципи роботи алгоритмів розпізнавання зображень, зокрема методів, заснованих на використанні глибоких нейронних мереж, та визначено їхні переваги і обмеження в практичному застосуванні.

У процесі роботи було розроблено програмний застосунок для розпізнавання зображень, який забезпечує автоматичну обробку візуальних даних, виявлення та класифікацію об'єктів. Проведене тестування системи показало її здатність ефективно працювати з вхідними зображеннями, забезпечуючи достатній рівень точності та швидкодії.

Отримані результати підтверджують доцільність використання методів комп'ютерного зору для автоматизації аналізу візуальної інформації та демонструють перспективність їх застосування в різних галузях, зокрема у системах безпеки, моніторингу, медицини та інтелектуальних інформаційних системах.

Висновки та перспективи

У результаті проведеного дослідження встановлено, що методи комп'ютерного зору є ефективним інструментом для автоматизованого аналізу візуальних даних. Їх застосування дозволяє значно підвищити швидкість і точність обробки зображень, мінімізувати вплив людського фактора та забезпечити можливість роботи систем у режимі реального часу. Проаналізовані підходи та алгоритми підтверджують доцільність використання сучасних

моделей машинного навчання для вирішення задач розпізнавання об’єктів і класифікації зображень.

Розроблений програмний застосунок демонструє практичну реалізацію досліджуваних методів і підтверджує можливість їх ефективного використання у прикладних задачах. Отримані результати свідчать про перспективність впровадження систем комп’ютерного зору в різних сферах діяльності, де необхідний швидкий та точний аналіз візуальної інформації.

Перспективи подальших досліджень полягають у вдосконаленні алгоритмів розпізнавання, підвищенні точності моделей за рахунок використання більш складних архітектур глибокого навчання, оптимізації продуктивності систем для роботи на обмежених обчислювальних ресурсах, а також розширенні функціональних можливостей програмного застосунку. Крім того, актуальним напрямом є інтеграція систем комп’ютерного зору з іншими інтелектуальними технологіями, що дозволить створювати більш складні та адаптивні рішення для аналізу візуальних даних.

Список використаних джерел

1. *Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016. – 775 p.*
2. *Szeliski R. Computer Vision: Algorithms and Applications. – 2nd ed. – Springer, 2022. – 979 p.*
3. *OpenCV. Open Source Computer Vision Library [Електронний ресурс]. – Режим доступу: https://opencv.org/ (дата звернення: 12.04.2026).*

Шабля Анастасія Вікторівна
студентка 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st8147685@stud.duikt.edu.ua

Данильченко Валентина Миколаївна
доктор філософії, доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

АВТОМАТИЗАЦІЯ ГЕНЕРАЦІЇ ТА ВЕРИФІКАЦІЇ ТЕХНІЧНОЇ ДОКУМЕНТАЦІЇ ДЛЯ IOT-РІШЕНЬ НА ОСНОВІ АРХІТЕКТУРИ LLM

Вступ. З кожним роком концепція Інтернету речей (IoT) охоплює все більше сфер, об'єднуючи тисячі пристроїв у складні мережі. Звісно, кожна така інфраструктура вимагає детального опису. Розробники змушені постійно

документувати API, протоколи та налаштування безпеки. Проблема полягає в тому, що при використанні гнучких методологій розробки документація просто не встигає за змінами в коді. Якщо писати та оновлювати її вручну, це займає надто багато часу. Як наслідок – накопичується «документаційний борг», що суттєво підвищує ризик помилок під час інтеграції нових пристроїв.

Аналіз останніх досліджень. Сьогодні великі мовні моделі (LLM) вже стали звичним інструментом для написання коду. Проте їхній потенціал у генеруванні технічної документації досі розкрито не до кінця [1,4]. На практиці нам потрібен не просто автоматичний текст, а точний технічний документ, який піддається програмній перевірці. Для IoT-проєктів це взагалі критична вимога, оскільки опис має на 100% збігатися з фізичними характеристиками обладнання [3].

Постановка завдання. Головна мета нашої роботи – створити інформаційну систему на основі архітектури трансформерів, яка зможе автоматично генерувати та одразу верифікувати технічні специфікації. Ідея полягає в тому, щоб система вміла не лише читати вхідні конфігураційні файли, але й самостійно знаходила логічні помилки в архітектурі.

Методологія та архітектура системи. У розробленій системі ми поєднали можливості сучасних мовних моделей (таких як GPT або Llama) із зовнішніми алгоритмами перевірки. Весь процес ми розбили на три логічні етапи. Спочатку система витягує дані з JSON/YAML файлів конфігурації. Потім модель формує базовий опис, спираючись на спеціально підготовлені промпти. На фінальному етапі відбувається порівняння згенерованого результату з галузевими вимогами безпеки.

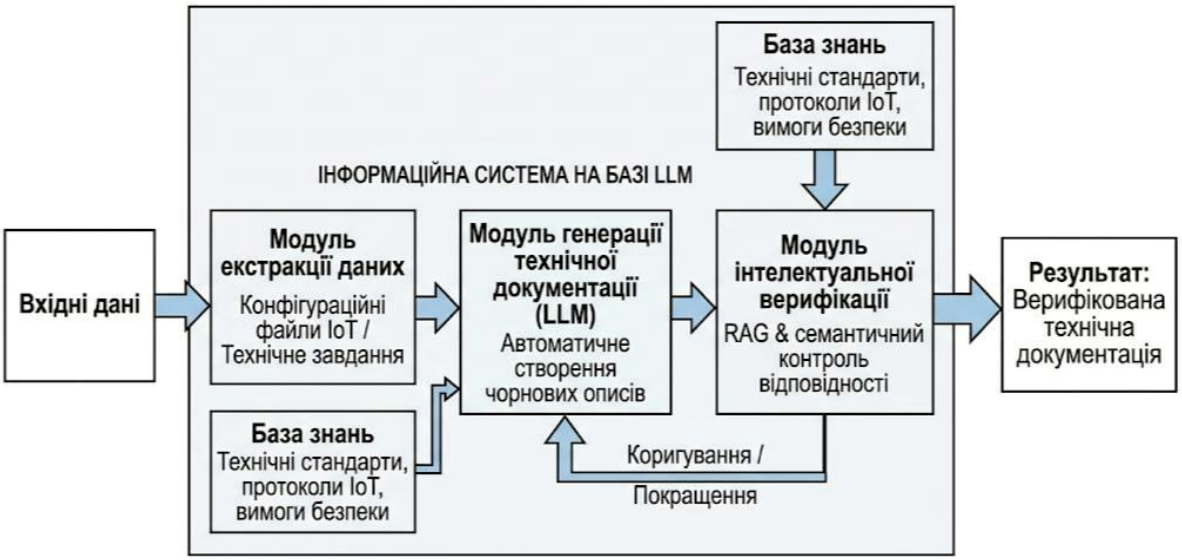

Рис. 1. Схема інтелектуальної генерації та верифікації документації

Щоб модель не вигадувала неіснуючих фактів (так звані «галюцинації» ШІ), ми застосували підхід RAG (Retrieval-Augmented Generation) [2]. Завдяки цьому система бере інформацію виключно із завантаженої бази стандартів, а не з власних «спогадів».

Результати дослідження. Під час експериментальної перевірки ми протестували систему на конфігурації фрагменту мережі «Розумний будинок». Результати виявилися досить показовими: час на генерацію специфікацій для протоколів MQTT/CoAP зменшився на 80%. Крім того, автоматичний модуль верифікації знайшов близько 15% дрібних розбіжностей у призначенні портів, які людина просто пропустила б під час ручного аудиту. Порівняння традиційного методу та нашого підходу наведено у табл. 1.

Табл. 1

Порівняльна характеристика методів підготовки документації

Параметр порівняння	**Традиційний метод**	**Система на основі LLM**
Час створення документа (умовні год)	10-12	1-2
Рівень автоматизації	Низький	Високий
Точність технічних параметрів	Залежить від людини	Верифікується алгоритмом
Вартість підтримки актуальності	Висока	Мінімальна

Висновки. Отже, впровадження LLM для автоматизації документації – це вже не просто цікавий тренд, а реальна необхідність, яка дозволяє прискорити випуск IoT-продуктів. Розроблений механізм верифікації гарантує, що згенеровані специфікації будуть дійсно надійними та придатними для використання. У майбутньому ми плануємо оптимізувати цю систему під більш суворі стандарти промислового Інтернету речей (IIoT).

Список використаних джерел

1. Bakhshi, R. (2024). LLMs for Automated Technical Writing: Challenges and Perspectives. Journal of Artificial Intelligence Research.

2. OpenAI. (2024). GPT-4 Technical Report. arXiv. https://doi.org/10.48550/arXiv.2303.08774

3. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview. Internet Society. https://www.internetsociety.org/resources/doc/2015/iot-overview/

4. Zhu, J., et al. (2023). Application of Large Language Models in Software Engineering: A Systematic Review. IEEE Access, 11, 45210-45225. https://doi.org/10.1109/ACCESS.2023.3271418

Козачок Марія Сергіївна
студентка 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st6300045@stud.duikt.edu.ua

ІНТЕЛЕКТУАЛЬНІ РОБОТИЗОВАНІ СИСТЕМИ В СЕРЕДОВИЩІ ІНТЕРНЕТУ РЕЧЕЙ: СУЧАСНЙ СТАН ТА ПЕРСПЕКТИВИ

Інтернет речей (IoT) є технологічною парадигмою, що забезпечує інтеграцію фізичних пристроїв у єдину мережу для обміну даними. У цьому середовищі інтелектуальні роботизовані системи поєднують робототехнічні платформи (мобільні роботи, безпілотні літальні апарати, стаціонарні сенсорні вузли) з алгоритмами штучного інтелекту та засобами мережевої взаємодії. У військовому застосуванні такі системи розглядаються в межах концепції «Інтернету військових речей» (Internet of Military Things).

Функціонування зазначених систем базується на використанні сенсорних компонентів (камери, радіолокаційні системи, лідари тощо), які здійснюють збір даних, а також комунікаційних каналів (Wi-Fi, LTE/5G, супутниковий зв'язок) для їх передачі. Інтеграція цих компонентів забезпечує можливість дистанційного спостереження, розвідки та моніторингу з передачею інформації в режимі реального часу. Застосування алгоритмів комп'ютерного зору дозволяє роботизованим платформам виконувати задачі розпізнавання об'єктів і підтримки прийняття рішень оператором.

Збройний конфлікт на території України сприяв прискоренню розвитку безпілотних систем. Сучасні безпілотні платформи оснащуються мультисенсорними комплексами та використовуються для виконання завдань спостереження без залучення людини безпосередньо в небезпечну зону. Одним із технологічних підходів є використання безпілотних апаратів як повітряних вузлів зв'язку (UxNB), що дозволяє забезпечити покриття в умовах відсутності або пошкодження традиційної інфраструктури. Зокрема, застосування супутникових систем зв'язку, таких як Starlink, дає змогу організувати стабільну передачу даних у складних умовах. Завдяки мобільності та висоті розміщення безпілотні апарати здатні виконувати функції ретрансляторів, формуючи гнучкі мережеві структури.

Подальший розвиток інтелектуальних роботизованих систем визначається кількома ключовими технологічними напрямками. По-перше, впровадження мереж зв'язку нового покоління (5G/6G) забезпечує зменшення затримок і підвищення пропускної здатності, що є критично важливим для передачі відеопотоків і телеметричних даних у реальному часі. По-друге, використання методів штучного інтелекту сприяє підвищенню рівня автономності роботів,

зокрема у задачах навігації, розпізнавання об’єктів та планування дій. По-третє, розвиток енергоефективних технологій та обчислювальних засобів дозволяє збільшити тривалість роботи пристроїв і реалізувати обробку даних безпосередньо на борту (edge computing). Додатково досліджуються роєві підходи, у межах яких групи роботів здійснюють координацію дій шляхом обміну даними, що підвищує стійкість системи до втрат окремих елементів та впливу засобів радіоелектронної боротьби.

Важливим аспектом розвитку є питання інформаційної безпеки, етики та правового регулювання. Застосування автономних роботизованих систем вимагає визначення відповідальності за їх використання та впровадження механізмів контролю. На міжнародному рівні тривають дискусії щодо обмеження автономних озброєнь (LAWs) та необхідності збереження принципу «людина в циклі» (human-in-the-loop). Технічна безпека систем передбачає використання криптографічних методів захисту даних, автентифікації та протидії несанкціонованому доступу до каналів управління.

Окрему увагу слід приділити розвитку інтелектуальних роботизованих систем у Китаї, який є одним із лідерів у сфері IoT та штучного інтелекту. Державні програми, зокрема ініціативи цифрової трансформації та «розумної промисловості», сприяють інтеграції робототехніки, мережевих технологій і аналітики даних. Китайські дослідницькі центри та компанії активно розробляють автономні безпілотні системи, роботизовані платформи для логістики, а також інфраструктурні IoT-рішення для міських середовищ. Значна увага приділяється розвитку 5G-мереж, які використовуються як основа для взаємодії між пристроями, а також впровадженню edge computing для зниження навантаження на хмарні сервіси. Такий підхід забезпечує масштабованість і високу ефективність інтелектуальних систем.

Висновки

Інтелектуальні роботизовані системи є невід’ємною складовою сучасного Інтернету речей, виконуючи функції сенсорних і комунікаційних вузлів. Їх застосування трансформує підходи до обробки інформації та управління складними системами. Подальший розвиток визначається вдосконаленням мережевих технологій, алгоритмів штучного інтелекту та енергоефективних рішень. Водночас необхідним є формування нормативно-правової бази та забезпечення інформаційної безпеки для контролю використання таких систем.

Сучасний стан інтелектуальних роботизованих систем в IoT визначається бурхливим розвитком мережевих технологій і зростанням ролі дронів у збройних конфліктах. Основні висновки: ці системи стають складовою Інтернету речей, де безпілотні платформи виконують функції сенсорів і комунікаційних вузлів. Укріплення поля бою «мережею» дронів змінює тактику війни. Технічні перспективи: потрібно розвивати 5G/6G зв’язок, автономні алгоритми та енергоефективні рішення для розумних роботів. Етичні/правові: необхідно

встановити правила застосування автономних систем (нормативи ООН, національне законодавство).

Список використаних джерел

1. Розумні дрони України: роль штучного інтелекту та машинного зору на фронті - . VGI-9. URL: https://vgi.com.ua/rozumni-drony-ukrayiny-rol-mashynnogo-zoru-i-shi-na-fronti/

2. Дрони та штучний інтелект: робота поза онлайн-середовищем. Експерт про новації під час застосування БПЛА. АрміяInform | Інформаційне агентство. URL: https://armyinform.com.ua/2025/06/19/drony-ta-shtuchnyj-intelekt-robota-poza-onlajn-seredovyshhem-ekspert-pro-novacziyi-pid-chas-zastosuvannya-bpla/

3. AI for drone piloting – defense tech for ukraine. Defense Tech for Ukraine. URL: https://defensetechforukraine.org/ua/volunteer/ai-for-drone-piloting/

4. Китай створив військові дрони під керуванням DeepSeek. ITC.ua. URL: https://itc.ua/ua/novini/kytaj-stvoryv-vijskovi-drony-pid-keruvannyam-deepseek/

Сокульський Олег Євгенович
доцент, к.т.н.
Військового інституту телекомунікацій та інформатизації імені Героїв Крут
mortimer@ukr.net

Топольськов Євгеній Олександрович
доцент, к.т.н.
Київського національного університету імені Тараса Шевченка
y.topolskov@knu.ua

Москаленко Наталія Володимирівна
асистент
Київського національного університету імені Тараса Шевченка
moskalenkonv@ukr.net

ТЕХНОЛОГІЯ AWS ДЛЯ IoT ПРОЕКТІВ

Максимальна функціональність при мінімальних витратах часу та вартості – це мрія всіх розробників проектів. З появою IoT почався розвиток апаратного та програмного забезпечення для розробки IoT проектів. Багато компаній, які спочатку створювали свої IoT проекти, почали втілювати свій досвід в засобах розробки. Так виникла дочірня компанія Amazon – Amazon Web Services або AWS, яка створила свою технологію розробки проектів на відповідній платформі хмарнних обчислень, серверні кластери якої розташовані по всьому світу. Технологія AWS дозволяє розробникам створювати проекти різної складності та функціональності, заощаджуючи на закупівлі відповідних апаратних та програмних засобах[1]. Технологія AWS надає можливість клієнтам мати у своєму розпорядженні:

- Віртуальні комп’ютери AWS, які мають атрибути реального комп'ютера, включаючи апаратні пристрої (жорсткий диск або SSD-накопичувач процесор, відеокарту, локальну та оперативну пам'ять,).
- Операційну систему. Клієнти можуть обрати необхідну з переліку.
- Мережу та прикладні програми, наприклад, базу даних та інше.
- Консольний ввід/вивід (клавіатура, дисплей і миша).

Набір та конфігурацію засобів розробник може підібрати згідно своїх потреб. Основні сервіси у складі AWS IoT:

- AWS IoT Core: Центральний вузол, який з'єднує пристрої з хмарою.
- AWS IoT Device Management: Інструмент для реєстрації, організації та відстеження великої кількості пристроїв.
- AWS IoT Greengrass: Забезпечує обробку даних пристроями локально.
- AWS IoT Analytics: Сервіс для глибокого аналізу інформації.

Сервіси технології постійно оновлюються, а їх кількість постійно збільшується, що забезпечує постійну популярність серед розробників.[2].

Список використаних джерел

1. Б. Ю. Жураковский, Н.В. Федорова, Є.В. Гаврилко, І. О. Зенів, Технології створення інтернету речей. Комп’ютерний gрактикум. Навчальний посібник [Електронний ресурс] / // КПІ ім. Ігоря Сікорського. – 2021. – 128 с. Режим доступу до ресурсу: https://ela.kpi.ua/handle/123456789/46169

2. Сайт компанії AWS [Електронний ресурс]. Режим доступу: https://aws.amazon.com/ru/iot/

Мадінов Микола Леонідович
аспірант кафедри мобільних та відеоінформаційних технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ
https://orcid.org/0009-0005-5910-8774
e-mail: nmadinov@gmail.com

Галаган Наталія Вікторівна
кандидат технічних наук, доцент, інструктор академії Cisco,
завідувач кафедри мобільних та відеоінформаційних технологій
Державного університету інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-8582-3126

МІНІМІЗАЦІЯ ПРОСТОЇВ ФІЗИЧНОГО РІВНЯ В ЕКОСИСТЕМАХ IOT ШЛЯХОМ НАЛЕЖНОГО УПРАВЛІННЯ ПАРАЛЕЛЬНОЮ ПОЛЯРНІСТЮ

Стрімке зростання екосистем Інтернету речей, розширення edge-обчислень і збільшення кількості високошвидкісних сервісів ускладнюють проєктування

інтегрованих IoT-систем і підвищують вимоги до безперервності передавання даних [1]. Для віддалених IoT-застосувань, зокрема систем моніторингу, стійкість інфраструктури безпосередньо впливає на надійність спостереження, своєчасність отримання даних і загальну ефективність експлуатації [2]. У магістральних сегментах це посилює потребу у волоконно-оптичних рішеннях, здатних забезпечувати високу пропускну здатність, малу затримку та стабільність роботи каналів [3], [4]. Саме тому фізичний рівень сьогодні розглядається не як допоміжний компонент, а як критична основа надійності всієї IoT-екосистеми [1], [2].

У високощільних оптичних системах центри обробки даних, транспортні вузли та кампусні магістралі дедалі частіше використовують паралельну оптику з багатоволоконними конекторами MPO/MTP. Такі рішення дають змогу передавати дані через кілька паралельних ліній, але одночасно підвищують чутливість мережі до помилок фізичного рівня. Однією з найнебезпечніших серед них є помилка оптичної полярності, коли сигнал із передавача потрапляє не до приймача, а до іншого передавача або повертається на хибну позицію масиву [3]. У таких умовах навіть правильно змонтований за механічними ознаками канал може виявитися непрацездатним [4].

Під оптичною полярністю в системах MPO/MTP слід розуміти узгодження логічного шляху передавання між позиціями Tx і Rx в межах усього лінку: від трансивера і патч-корда до магістрального кабелю, адаптера та касети. Стандарт ANSI/TIA-568.3-E регламентує п’ять базових методів організації полярності - A, B, C, U1 та U2 - і прямо наголошує, що змішування цих підходів у межах одного каналу призводить до помилкової комутації та відмов лінку [4]. Матеріали оновлення ANSI/TIA додатково підкреслюють, що універсальні методи U1 і U2 були введені саме для зменшення кількості помилок під час багатодуплексних реалізацій та спрощення експлуатації мереж високої щільності [3].

Практика експлуатації показує, що більшість простоїв фізичного рівня пов’язана не з дефектами волокна як такого, а з помилками підключення, неузгодженістю типів компонентів та відсутністю єдиної політики полярності. За спостереженнями галузевих фахівців, традиційні методи A і C ускладнюють адміністрування, оскільки вимагають нестандартних поєднань патч-кордів або погано масштабуються для сучасної паралельної оптики [5]. У результаті операції Moves, Adds, Changes перетворюються на джерело ризику, а час відновлення працездатності лінку зростає через складну ручну діагностику [5].

Для задач мінімізації простоїв особливе значення має правильний вибір методу полярності залежно від сценарію використання. Метод B залишається ефективним рішенням для наскрізних з’єднань типу array-to-array, оскільки забезпечує логічно передбачувану інверсію волокон і дає змогу застосовувати однакові стандартні патч-корди на обох кінцях лінку [4]. Водночас під час побудови модульних систем із MPO-to-LC переходами більшу практичну цінність мають універсальні методи, оскільки вони краще підтримують типові сценарії розгалуження і спрощують обслуговування [3].

Метод U1 доцільно розглядати як базовий варіант для одномодових магістралей IoT, особливо там, де використовуються конектори з кутовим фізичним контактом APC. Застосування адаптерів типу A у складі U1 дає змогу зберегти правильну геометрію стикування APC-конекторів і тим самим контролювати зворотні втрати, що є критичним для протяжних та чутливих до відбиття лінків [3]. Такий підхід зменшує ймовірність прихованих деградацій каналу, які можуть не проявлятися одразу після монтажу, але викликати нестабільність у процесі експлуатації [4].

Метод U2, навпаки, є особливо привабливим для багатомодових середовищ і сценаріїв direct breakout усередині щільно насичених центрів обробки даних. Його перевага полягає у справжній топологічній незалежності: правильна полярність досягається без використання нестандартних комутаційних шнурів, а отже зменшується кількість дій, у яких персонал може припуститися помилки [3]. Для IoT-інфраструктур із частими змінами конфігурації це безпосередньо означає скорочення часу простою, спрощення інвентаризації та зниження експлуатаційних витрат [5].

Окремої уваги потребує дисципліна комплектації елементів каналу. На практиці стабільність лінку визначається не лише вибором методу A, B, C, U1 чи U2, а й правильним поєднанням гендеру конекторів, типу адаптерів, магістральних кабелів і модулів. Нормативні вимоги ANSI/TIA-568.3-E щодо узгодження Female-Female магістралей із відповідними модулями та портами трансиверів спрямовані саме на усунення прихованих причин простою ще до етапу введення системи в експлуатацію [4]. Якщо ж монтаж виконується без жорсткого дотримання цієї логіки, мережа отримує додаткові точки відмови, які важко локалізувати вже після запуску сервісу [3].

Не менш важливою є організаційна складова. Для зменшення часу аварійного відновлення оператор повинен заздалегідь фіксувати вибрану стратегію полярності в проєктній документації, використовувати однозначне маркування збірок та уніфікувати перелік компонентів на складі. Коли в одній інфраструктурі одночасно присутні різні типи касет, перехідників і патч-кордів без належного опису, навіть незначна модернізація може призвести до каскадного простою декількох сервісів [5]. Тому управління полярністю слід розглядати як окремий процес технічного менеджменту, а не лише як разову монтажну операцію [3].

Для магістралей, що пов’язують віддалені edge-вузли, шлюзи та центральні майданчики обробки даних, критичною стає не тільки працездатність каналу, а й стабільність оптичних параметрів протягом тривалого часу. Для віддалених IoT-систем безперервність обміну даними прямо впливає на стійкість моніторингу й керування, тому вимоги до надійності фізичного рівня тут є особливо високими [2]. Саме тому вибір U1 для одномодових APC-конфігурацій є не просто стандартним рішенням, а засобом профілактики майбутніх відмов, зумовлених зростанням зворотних втрат або нестійким контактом [3], [4]. У цьому випадку мінімізація простою досягається ще на етапі архітектурного вибору, коли правильна полярність

поєднується з фізично коректним типом конектора для конкретного класу навантаження [4].

У внутрішніх spine-leaf сегментах, де характерні часті перемикання та висока щільність портів, перевагу мають рішення, що зменшують залежність від людського фактора. Саме за цією логікою метод U2 є особливо цінним для багатомодових середовищ: він не потребує нестандартних шнурів у сценаріях direct breakout і полегшує Day-2 administration, тобто поточну експлуатацію після завершення інсталяції [3]. Для операторів IoT-платформ це означає швидше виконання змін конфігурації, меншу кількість помилкових підключень і нижчу ймовірність появи прихованих простоїв при масштабуванні ресурсів [5].

Табл. 1

Рекомендоване застосування методів полярності для зменшення простоїв

Сценарій	**Рекомендований метод**	**Підстава вибору**
Одномодова магістраль IoT з APC	U1	Сумісність із Type-A та контроль зворотних втрат
Наскрізне MPO-MPO з’єднання	B	Стабільна інверсія волокон і стандартизовані патч-корди
Багатомодовий direct breakout	U2	Топологічна незалежність без нестандартних шнурів
Нові інсталяції на A або C	Не рекомендовано	Підвищений ризик помилок і складність адміністрування

Окремим елементом мінімізації простоїв є верифікація оптичної інфраструктури до введення її в експлуатацію. Для високощільних кабельних систем стандартний візуальний контроль є недостатнім, оскільки помилки полярності, надмірні втрати або неправильне картування волокон можуть залишатися непоміченими до моменту запуску сервісу. Тому приймально-здавальні випробування мають включати вимірювання внесених втрат, перевірку безперервності каналу та підтвердження полярності згідно з обраною схемою [6]. Автоматизовані засоби сертифікації суттєво скорочують час виявлення проблем і перетворюють пошук несправності з аварійної процедури на планову частину розгортання [6].

Практична цінність такого підходу полягає в тому, що система тестування перестає бути останнім формальним етапом перед здачею об’єкта і стає інструментом попередження простою. Якщо карта волокон, полярність і бюджет втрат підтверджені до запуску, ризик аварійного виїзду на майданчик після введення сервісу помітно зменшується [6]. Для IoT-інфраструктур, де один оптичний сегмент може обслуговувати критичні сенсорні мережі, промислові контролери та edge-сервери одночасно, такий ефект має не лише технічне, а й економічне значення [2], [6].

З практичного погляду доцільно виділити чотири послідовні кроки мінімізації простоїв. Перший крок - це вибір єдиної схеми полярності для всього сегмента ще

на стадії проєкту. Другий - застосування стандартизованих збірок без змішування несумісних методів, адаптерів і патч-кордів під час монтажу [4]. Третій - документування карти волокон, маркування магістралей і перевірка фактичного картування перед введенням у роботу [6]. Четвертий - підтримання тієї самої логіки під час подальших змін конфігурації, коли будь-яке розширення або заміна обладнання виконується не «за місцем», а відповідно до заздалегідь прийнятого стандарту [5]. Саме така послідовність дає змогу перевести проблему полярності з категорії аварійних інцидентів у категорію керованих інженерних процедур, що особливо важливо для IoT-екосистем, де зупинка фізичного каналу часто призводить до втрати доступу одразу до великої кількості сенсорних, аналітичних і керуючих сервісів [2], [5].

У перспективі подальшого переходу до швидкостей 800G та 1.6T вимоги до безпомилковості фізичного рівня лише зростатимуть. Чим вищою є щільність портів і чим складнішою стає інтеграція оптичних трактів у комутаційному обладнанні, тим дорожчою виявляється будь-яка помилка полярності, оскільки вона зачіпає вже не окремий кабельний сегмент, а великий блок сервісів, що працюють поверх спільної транспортної платформи [3], [4]. Для майбутніх архітектур, пов’язаних із ко-пакетованою оптикою та дедалі тіснішою інтеграцією оптичних модулів із обчислювальними системами, правильне управління полярністю стає елементом технологічної сумісності всієї інфраструктури, а не лише локальної кабельної схеми [3]. Отже, рішення щодо методу полярності повинно прийматися з урахуванням не тільки поточної конфігурації, а й майбутнього масштабування IoT-платформи, щоб модернізація не супроводжувалася повторним кабельним перепроєктуванням і супутніми простоями [4].

Отже, мінімізація простоїв фізичного рівня в IoT-екосистемах досягається не окремою дією, а комплексом взаємопов’язаних рішень: стандартизованим вибором методу полярності ще на етапі проєктування, відмовою від застарілих схем A і C для нових інсталяцій, вибором U1 для одномодових APC-лінків і U2 для багатомодових direct breakout сегментів, а також обов’язковою сертифікацією з’єднань перед запуском [3 - 6]. За таких умов фізичний рівень перестає бути джерелом непередбачуваних простоїв і перетворюється на надійну основу масштабованої IoT-інфраструктури [1], [2].

Список використаних джерел

1. Reis, R. (2019). Challenges in the design of integrated systems for IoT. DOI: https://doi.org/10.1007/978-3-030-43605-6_11

2. Perdana, D., Lorenz, P., & Aditya, B. (2025). Optimized dual-battery system with intelligent auto-switching for reliable soil nutrient monitoring in remote IoT applications. Journal of Sensor and Actuator Networks, 14, 53. DOI: https://doi.org/10.3390/jsan14030053

3. TIA FOTC. ANSI/TIA-568.3-E Optical Fiber Cabling and Components Standard Updates. Telecommunications Industry Association Fiber Optics Tech Consortium. 2022. URL: https://tiaonline.org/standardannouncement/tia-issues-updated-optical-fiber-cabling-component-standard-ansi-tia-568-3-e/

4. ANSI/TIA-568.3-E. Optical Fiber Cabling and Components Standard. Telecommunications Industry Association. 2022. URL: https://www.tiafotc.org/tia-standards-update/tia-568-3-e/

5. Casteel, R. The Perpetual Perplexities of Optical Fiber Polarity. CommScope / TIA FOTC Webinar Series. 2024. URL: https://www.tiafotc.org/event/the-perpetual-perplexities-of-optical-fiber-polarity/

6. EXFO. Certifying High Density Data Center Fiber Cabling to TIA-568.3E Standards. EXFO Application Notes. 2024. URL: https://www.tiafotc.org/event/certifying-high-density-data-center-fiber-cabling-to-tia-568-3e-standards/

НАПРЯМ 3. І ОТ ДЛЯ РОЗУМНИХ МІСТ ТА ПРОМИСЛОВОСТІ

Гаврилюк Анжеліка Русланівна
студент 5 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
aanzelikaa23@gmail.com

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ У РОЗПОДІЛЕНИХ СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Активний розвиток цифрових технологій сприяв широкому впровадженню концепції Інтернету речей, що передбачає інтеграцію фізичних об'єктів, сенсорних пристроїв та обчислювальних систем у єдине інформаційне середовище. Такі системи забезпечують безперервний збір, передачу та обробку даних у режимі реального часу. Сфера застосування Інтернету речей охоплює різноманітні галузі, зокрема транспортні системи, промислову автоматизацію, охорону здоров'я, енергетику та інфраструктуру розумних міст [3].

Збільшення кількості підключених пристроїв і обсягів даних, що генеруються у таких системах, призводить до формування складних інформаційних потоків між різними компонентами мережі. У результаті виникають додаткові вимоги до ефективної організації передачі даних, їх обробки та забезпечення узгодженості інформації у розподіленому середовищі. Наявність великої кількості взаємопов'язаних вузлів, різноманітних комунікаційних протоколів та різних типів обчислювальних ресурсів значно ускладнює процес управління такими потоками.

У таких умовах особливої актуальності набуває моделювання інформаційних потоків у розподілених системах Інтернету речей. Використання відповідних моделей дозволяє досліджувати структуру взаємодії між елементами системи, визначати оптимальні маршрути передачі даних та забезпечувати ефективне використання обчислювальних ресурсів. Крім того, моделювання інформаційних потоків сприяє підвищенню надійності функціонування системи та забезпеченню контролю над процесами обміну інформацією.

Метою дослідження є аналіз підходів до моделювання інформаційних потоків у розподілених системах Інтернету речей та визначення сучасних технологічних рішень, що дозволяють підвищити ефективність передачі й обробки даних у таких системах.

Функціонування систем Інтернету речей базується на взаємодії великої кількості сенсорних пристроїв, комунікаційних мереж та обчислювальних платформ. У процесі їх роботи формується складна система інформаційних потоків, що забезпечує передачу даних від джерел їх генерації до систем обробки та кінцевих користувачів. Ефективна організація цих потоків є важливим фактором забезпечення стабільної та продуктивної роботи системи [1].

Традиційні архітектури обробки даних передбачають передачу інформації до централізованих хмарних сервісів, де виконуються основні обчислювальні операції. Однак зі зростанням кількості пристроїв та обсягів інформації такий підхід може призводити до перевантаження мережі та збільшення затримок передачі даних. У зв'язку з цим у сучасних IoT-системах широко використовуються розподілені обчислювальні моделі, які поєднують можливості периферійних пристроїв і хмарних обчислювальних ресурсів [1].

Використання периферійних обчислень дозволяє виконувати частину обробки даних безпосередньо на вузлах, розташованих поблизу джерел їх генерації. Це сприяє зменшенню затримок передачі інформації, зниженню навантаження на мережеву інфраструктуру та підвищенню швидкості реакції системи на зміни зовнішнього середовища. У таких умовах інформаційні потоки розподіляються між різними рівнями інфраструктури (рис. 1), що потребує застосування відповідних моделей для їх аналізу та оптимізації.

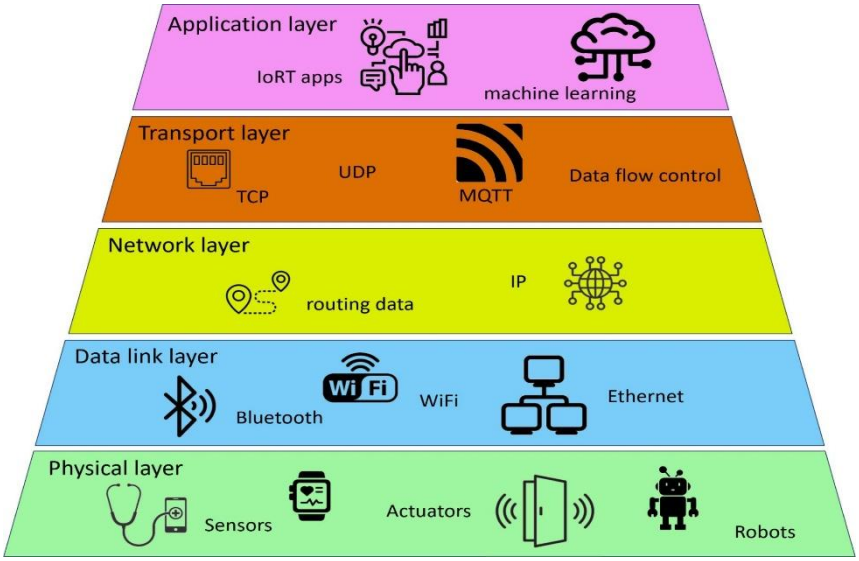

Рис. 1. Шарова організація системи Інтернету речей та інформаційних потоків між її компонентами [5]

Важливим аспектом функціонування розподілених систем є забезпечення узгодженості даних між різними вузлами мережі. У випадках, коли інформація зберігається або обробляється на декількох пристроях, виникає необхідність її синхронізації. Для вирішення цієї задачі використовуються спеціальні механізми, що дозволяють підтримувати узгодженість даних навіть у випадку нестабільного мережевого з'єднання або тимчасового відключення окремих вузлів [5].

Забезпечення безпеки передачі даних також є важливим елементом організації інформаційних потоків у розподілених системах. У мережах Інтернету речей існує ризик несанкціонованого доступу до інформації або її модифікації під час передачі між вузлами мережі. Застосування моделей

контролю інформаційних потоків дозволяє визначати правила доступу до даних та регулювати їх поширення між компонентами системи, що сприяє підвищенню рівня захисту інформації [4].

Сучасні дослідження також приділяють значну увагу інтеграції технологій штучного інтелекту з інфраструктурою Інтернету речей. Аналіз великих обсягів даних дозволяє визначати закономірності у роботі системи та оптимізувати процеси передачі інформації між її компонентами. Використання інтелектуальних алгоритмів сприяє адаптації системи до змінних умов функціонування та підвищенню ефективності використання обчислювальних ресурсів [3].

Підвищення ефективності функціонування IoT-мереж також досягається шляхом використання алгоритмів оптимізації маршрутів передачі даних між пристроями. Такі алгоритми дозволяють визначати найбільш ефективні шляхи обміну інформацією з урахуванням характеристик мережі та рівня навантаження на її вузли. Це сприяє зменшенню затримок передачі даних і підвищенню надійності комунікацій у складних мережевих середовищах [2].

Моделювання інформаційних потоків у розподілених системах Інтернету речей є важливим інструментом для аналізу структури мережі, оптимізації передачі даних та забезпечення ефективного функціонування сучасних інформаційних систем.

Проведений аналіз показав, що ефективне моделювання інформаційних потоків є важливою складовою процесу проєктування та функціонування розподілених систем Інтернету речей. Зростання кількості підключених пристроїв та обсягів даних потребує використання сучасних підходів до організації передачі й обробки інформації.

Застосування розподілених обчислювальних архітектур дозволяє зменшити затримки передачі даних, оптимізувати використання мережевих ресурсів і підвищити продуктивність системи. Використання механізмів синхронізації даних і моделей контролю інформаційних потоків сприяє підвищенню надійності та безпеки функціонування IoT-інфраструктури.

Перспективи подальших досліджень пов’язані з розробкою нових методів управління інформаційними потоками у складних розподілених середовищах, а також із застосуванням алгоритмів машинного навчання та штучного інтелекту для автоматичної оптимізації мережевих процесів і підвищення ефективності роботи систем Інтернету речей.

Список використаних джерел

1. Almurshed, O., Kaushal, A., Meshoul, S., Muftah, A., Almoghamis, O., Petri, I., Auluck, N., & Rana, O. (2024). Enhancing performance of machine learning tasks on edge-cloud infrastructures: A cross-domain internet of things based framework. Future Generation Computer Systems, 107696. https://doi.org/10.1016/j.future.2024.107696

2. *Al-Rasheed, A., Khan, R., Alturise, F., & Alkhalaf, S. (2025). Distributed computing-based optimal route finding algorithm for trusted devices in the internet of things. Computers, Materials & Continua, 1–10. https://doi.org/10.32604/cmc.2025.064102*

3. *Anthony, B. (2024). Artificial intelligence of things and distributed technologies as enablers for intelligent mobility services in smart cities-a survey. Internet of Things, 101399. https://doi.org/10.1016/j.iot.2024.101399*

4. *Denis, N., Laurent, M., & Chabridon, S. (2024). A decentralized model for usage and information flow control in distributed systems. Computers & Security, 103975. https://doi.org/10.1016/j.cose.2024.103975*

5. *Galeas, J., Tudela, A., Pons, Ó., Bandera, J. P., Bandera, A., & Bustos, P. (2025). CRDT-based knowledge synchronization in an internet of robotics things ecosystem for ambient assisted living. Computer Vision and Image Understanding, 104437. https://doi.org/10.1016/j.cviu.2025.104437*

Юхимович Світлана Валеріївна
студентка групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
(063)-247-58-50
svetik.iukhymovych@gmail.com

Полоневич Ольга Володимирівна
кандидат технічних наук, доцент,
доцент кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ

АПАРАТНІ ПЛАТФОРМИ ІОТ У ЦИФРОВІЙ ТРАНСФОРМАЦІЇ РОЗУМНИХ МІСТ ТА ПРОМИСЛОВОСТІ

Стрімкий розвиток технологій Інтернету речей (IoT) є одним із ключових факторів цифрової трансформації міського середовища та промислового сектору. Сучасні апаратні засоби, зокрема мікропроцесорні системи, сенсорні мережі та комунікаційні модулі, формують основу інтелектуальних інфраструктур, здатних забезпечувати безперервний моніторинг і керування об’єктами в режимі реального часу.

Інтеграція цих компонентів сприяє підвищенню ефективності використання ресурсів, покращенню якості міських сервісів та оптимізації виробничих процесів, що робить IoT невід’ємною складовою сучасних цифрових екосистем.

Постановка задачі

Масове впровадження IoT-рішень у міських і промислових системах призводить до суттєвого ускладнення їхньої структури та функціонування, що формує нові вимоги до апаратного забезпечення. У таких умовах актуалізується задача визначення ключових характеристик апаратних платформ IoT, які мають забезпечувати стабільну та ефективну роботу в гетерогенних середовищах.

Ці платформи повинні поєднувати енергоефективність, масштабованість і надійність із можливістю роботи в мережах із низькими затримками передачі даних і підтримкою сучасних стандартів зв'язку, таких як 5G, LTE-M і LoRaWAN.

Додатковою складністю є інтеграція новітніх рішень із застарілим обладнанням, що потребує використання універсальних апаратних шлюзів і адаптивних інтерфейсів, а також забезпечення належного рівня кібербезпеки на рівні апаратних компонентів.

Мета дослідження

Метою даної роботи є аналіз впливу технологій IoT на архітектуру апаратних платформ у контексті розумних міст і промислових систем, а також визначення параметрів, які забезпечують їхню ефективність, надійність і безпеку.

У центрі уваги перебуває дослідження взаємодії фізичних компонентів, зокрема сенсорів, виконавчих механізмів і мережевих модулів, із хмарними сервісами та системами обробки даних у реальному часі.

Результати дослідження

У результаті проведеного аналізу встановлено, що впровадження IoT-технологій суттєво підвищує ефективність управління як міською, так і промисловою інфраструктурою. Використання сенсорних мереж у міському середовищі забезпечує оптимізацію транспортних потоків, підвищення ефективності систем освітлення та вдосконалення обліку енергоресурсів.

Інтелектуальні системи моніторингу сприяють зниженню енергоспоживання та покращенню екологічних показників. У промисловості застосування Industrial IoT дозволяє реалізувати підходи прогнозного обслуговування, що зменшує кількість відмов обладнання та мінімізує простої.

Важливим результатом є також підтвердження ефективності використання універсальних шлюзів для інтеграції застарілих систем у сучасні цифрові мережі. Окремо встановлено, що критичну роль відіграє апаратна безпека, яка реалізується через механізми шифрування, автентифікації та контролю доступу.

Висновки та перспективи

Отримані результати свідчать про те, що апаратні платформи є фундаментальним елементом IoT-систем у розумних містах і промисловості, оскільки саме вони визначають рівень масштабованості, надійності та безпеки всієї інфраструктури.

Подальший розвиток галузі пов'язаний із розширенням високошвидкісних мереж зв'язку, поглибленням інтеграції з хмарними технологіями та системами

обробки великих даних, а також із застосуванням методів машинного навчання для автоматизації прийняття рішень.

Перспективним напрямом є створення адаптивних апаратних систем, здатних ефективно функціонувати в умовах динамічних навантажень і забезпечувати тісну інтеграцію фізичного та цифрового середовищ.

Список використаних джерел

1. *Gerlée K. 8 wegweisende IoT-Lösungen für Smart Cities | Freeeway. Freeeway. URL: https://freeeway.com/de/8-iot-loesungen-fuer-smart-cities/*
2. *Was ist das Industrial Internet of Things (IIoT)? | PTC. Global Leader in Product Lifecycle Management Software | PTC. URL: https://www.ptc.com/de/technologies/iiot?srsltid=AfmBOoqys02N-lGLBoNS3dIkYAe-JPHDj224iyLwVBNgkf6WndgTdYLz*

Кухаренко Артем Русланович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kuharenkoartem131104@gmail.com

Бондарчук Олександр Павлович
викладач кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.bondarchuk@duikt.edu.ua

СИСТЕМА БЕЗПЕРЕБІЙНОГО ЕЛЕКТРОЖИВЛЕННЯ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ

Доцільність обраного напряму підготовки зумовлена високим ступенем залежності сучасних інформаційно-комунікаційних систем від стабільності параметрів електроживлення в умовах глобальної цифровізації. Навіть короткочасні вимкнення електрики можуть спричиняти порушення цілісності інформаційних потоків, зупинку роботи енергозалежних пристроїв або ставити під загрозу безпеку як інформаційних, так і промислових об’єктів. Створені джерела безперебійного живлення (або UPS) забезпечують автономність об’єкта на деякий час, що достатньо для коректного завершення системних процесів або переходу на резервну лінію. Але можливості цих пристроїв обмежені - вони не мають інтелектуальних механізмів для прогнозу несправностей або для

керування режимами роботи. Інтернет речей допомагає нівелювати зазначені недоліки шляхом використання засобів моніторингу та аналізу телеметричних даних. Це забезпечить високоточне керування енергосистемами та оптимізацію фінансових витрат.

Під якістю енергопостачання розуміють ступінь відхилення фізичних величин (напруги, частоти та сили струму) від встановлених еталонних значень. Враховуючи високу чутливість сучасної мікропроцесорної техніки до параметрів мережі, виникає гостра необхідність у застосуванні інтелектуальних систем контролю. Ефективним рішенням заданої проблеми є використання систем PQA (Power Quality Analyzers) - аналізаторів показників якості електроенергії. Ці пристрої здійснюють безперервний моніторинг ключових характеристик, зокрема коефіцієнта потужності, стабільності амплітуди та гармонійних спотворень. Аналіз зазначених показників дозволяє своєчасно виявляти такі аномалії, як мерехтіння (флікер), критичні для обладнання коливання напруги або її перехідні процеси. Подана концепція створює передумови для комплексної діагностики та верифікації ключових параметрів електроенергії у розгалужених локальних та магістральних мережах [1, 2].

Практична реалізація системи безперебійного живлення потребує строгої ієрархічної структури, що зазвичай базується на чотирирівневій архітектурі IoT. Поданий підхід гарантує забезпечення наскрізного потоку даних від фізичного обладнання до кінцевого користувача [3].

1. **Рівень пристроїв (перцептивний рівень)**: даний етап включає в себе безпосередньо задіяні датчики виконавчих механізмів (інверторів, реле), температури акумуляторних батарей, сили струму, напруги або частоти. В межах заданого шару відбувається первинний збір телеметричної інформації про параметри мережі та стан UPS. Інтеграція периферійних обчислень (edge computing) на першому рівні дозволяє системі оперативно реагувати на мінімальні критичні відхилення без очікування відповіді від сервера.

2. **Мережевий рівень (транспортний)**: фундаментальним завданням цього шару визначена стабільна передача зібраних даних до центрального обробчого вузла. Залежно від масштабу об’єкта можуть бути задіяні енергоефективні протоколи передачі даних, до яких належать LoRaWAN (для територіально розподілених систем) або Ethernet/Wi-Fi (для серверних кімнат локального рівня). Вирішальним фактором мережевого рівня є впровадження механізмів шифрування та автентифікації з метою унеможливлення несанкціонованого доступу до контурів управління даною енергосистемою.

3. **Рівень обробки даних**: відбувається акумуляція масивів даних для подальшого аналізу. Використання хмарних платформ (наприклад, Azure або AWS IoT) забезпечує масштабування системи та застосування потужних обчислювальних ресурсів. Це уможливлює фільтрацію шумів у показниках якості електроенергії. Практичне використання доводить ефективність

багаторівневої моделі edge-fog-cloud computing, за допомогою якої ефективніше розподіляється навантаження між різними рівнями обробки.

- Edge computing відповідає за первинну обробку безпосередньо на сенсорах, як наслідок - миттєва реакція на критичні відхилення без залучення основного сервера.
- Fog computing є проміжним рівнем, де відбувається попередня аналітика на шлюзах та мікросерверах.
- Cloud computing забезпечує централізоване зберігання великих масивів даних. У хмарних платформах застосовано алгоритми машинного навчання, що допомагають прогнозувати потенційні відмови або пікові навантаження.

Взаємозв'язок трьох шарів створює чіткий баланс між швидкістю та глибиною аналітики. Це один із вирішальних критеріїв якості роботи систем UPS [4].

4. **Рівень прикладних об'єктів**: інтерфейсна частина, в межах якої оброблена інформація візуалізується для користувача даної системи у доступному вигляді. Через вебпанелі або мобільні додатки людина має доступ до звітів про стан електроенергії в режимі реального часу, прогнозів щодо ресурсу акумуляторів або сповіщень про необхідність проведення технічного обслуговування [5].

Інтеграція IoT в енергетичну галузь уможливлює максимально оперативний контроль та керування енергетичними системами. Це полегшує налаштування системи максимально ефективно та підтримання сталих параметрів. Водночас застосування інтелектуальних алгоритмів аналізу даних забезпечує користувачу можливість прогнозування пікових навантажень на систему та потенційних відмов обладнання [6]. Задані алгоритми підвищують рівень надійності електропостачання, уникаючи перепадів напруги, що негативно впливатимуть на об'єкти системи. Крім того, використання інтернету речей сприяє формуванню адаптивних моделей управління, що дозволяють інтегрувати методи безперебійного живлення безпосередньо у комплексні енергетичні платформи, забезпечуючи їхню масштабованість та відповідність сучасним вимогам сталого розвитку.

Таким чином, розробка та впровадження системи безперебійного електроживлення на основі концепції інтернету речей є фундаментальним кроком для забезпечення енергетичної стійкості сучасних приладів. Чотирирівнева архітектура стимулює трансформувати традиційні джерела електрики з пасивних резервних пристроїв у активні інтелектуальні вузли мережі. Аналізатори якості енергії уможливлюють не лише констатацію факту збою в мережі, а й превентивний моніторинг стану обладнання, що позитивно впливає на якість та тривалість експлуатації роботи батарей.

Перспективами у даному напрямі є впровадження машинного навчання на рівні обробки даних. Це дає змогу створити самонавчальні моделі, що здатні прогнозувати ймовірність аварій з високою точністю. Дана концепція забезпечить новий рівень надійності та автономності критично важливих інформаційних систем.

Список використаних джерел

1. *Моделювання та проектування аналізатора якості електроенергії на основі FPGA - Springer Nature Link. URL: https://link.springer.com/chapter/10.1007/978-981-99-0412-9_39*
2. *Алгоритми виявлення та класифікації порушень якості електроенергії з використанням вейвлетів - Science Publications. URL: https://thescipub.com/abstract/ajassp.2006.2049.2053*
3. *Чотири рівні архітектури інтернету речей - Zipit. URL: https://www.zipitwireless.com/blog/4-layers-of-iot-architecture-explained*
4. *Багаторівнева архітектура периферійних обчислень - MDPI. URL: https://www.mdpi.com/1999-5903/17/1/22*
5. *Основи інтернету речей - Школа автоматики. URL: http://edu.asu.in.ua/mod/book/view.php?id=112&chapterid=230*
6. *Інтернет речей в енергетиці - Springer Nature Link. URL: https://link.springer.com/article/10.1007/s12083-024-01725-8*

Порицька Варвара Володимирівна
студенка групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій
(095)-437-58-33
varvaraporytska@gmail.com

Полоневич Ольга Володимирівна
к.т.н., доцент,
доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ АВТОТРАНСПОРТУ ІЗ ЗАСТОСУВАННЯМ АЛГОРИТМІВ ІНТЕЛЕКТУАЛЬНОЇ ВІДЕОАНАЛІТИКИ

Вступ

В умовах стрімкого зростання кількості автомобілів та підвищення вимог до безпеки об'єктів різного призначення, традиційні методи контролю доступу

(перепустки, радіобрелоки, ручна перевірка охороною) стають менш ефективними та створюють незручності у вигляді черг. На зміну їм приходять автоматизовані системи контролю доступу (АСКД) автотранспорту, в основі яких лежать алгоритми інтелектуальної відеоаналітики, зокрема технології розпізнавання номерних знаків (LPR/ANPR). Впровадження таких систем є надзвичайно актуальним для організації закритих паркувань у житлових комплексах, бізнес-центрах, на промислових підприємствах, логістичних складах та платних дорогах.

Мета роботи

Дослідження та обґрунтування принципів побудови автоматизованої системи контролю доступу автотранспорту з використанням сучасних алгоритмів інтелектуальної відеоаналітики (на прикладі автономних обчислювальних модулів LPR BOX та спеціалізованого програмного забезпечення).

Основний зміст дослідження

Автоматизовані системи контролю доступу на базі відеоаналітики (LPR/ANPR) ефективно замінюють застарілі ручні методи пропуску. Вони працюють за двома основними сценаріями: автономна аналітика «на борту» (пристрої обробляють відео самостійно, без підключення до інтернету) та серверна аналітика (обробка RTSP-потоку з будь-яких IP-камер на центральному сервері).

В основі таких систем лежать інтелектуальні алгоритми, які розпізнають номерні знаки понад 50 країн світу з точністю вище 98%. Швидкість обробки складає всього 50 мілісекунд, що дозволяє фіксувати автомобілі на швидкостях до 260 км/год. Для максимальної безпеки система здійснює розширену ідентифікацію: визначає не лише номер, а й марку, модель та колір авто, що унеможливлює шахрайство з підробленими номерами.

Процес пропуску повністю автоматизований: алгоритм миттєво звіряє розпізнаний номер із базами даних («білими» та «чорними» списками) і самостійно дає команду реле на відкриття шлагбаума. Керування комплексом здійснюється через єдиний WEB-інтерфейс або Telegram-бот, куди надходять моментальні сповіщення з фотофіксацією.

Ключова перевага системи – її висока відмовостійкість. При обриві зв'язку з сервером камери та модулі продовжують працювати автономно, зберігаючи всі події на локальні карти пам'яті. Після відновлення мережі архів автоматично синхронізується (технологія ANR). Це повністю виключає людський фактор та забезпечує безперебійний контроль доступу на об'єкт.

Висновки

Впровадження автоматизованих систем контролю доступу автотранспорту із застосуванням алгоритмів інтелектуальної відеоаналітики вирішує проблему заторів на пунктах пропуску та виключає вплив людського фактора (дозволяє

системі працювати повністю без оператора). Такі системи забезпечують найвищий рівень безпеки об'єкта, ведуть точний автоматизований облік транспортного потоку (підрахунок авто, ліміти паркомісць) та надають вичерпні дані для аналітики. Гнучкість в інтеграції з існуючим обладнанням робить їх економічно вигідним рішенням для модернізації систем безпеки підприємств та житлової інфраструктури.

Список використаних джерел

1. *LPR BOX "Orthus" / "Hydra" [Електронний ресурс] // Kobi: [вебсайт компанії]. – Режим доступу: https://kobi.ua/solutions/reshenie-6/ (дата звернення: 05.04.2026).*
2. *LPR BOX Cyclops [Електронний ресурс] // Kobi: [вебсайт компанії]. – Режим доступу: https://kobi.ua/solutions/reshenie-7/ (дата звернення: 05.04.2026).*
3. *Камери ZetPro для розпізнавання автомобільних номерів [Електронний ресурс] // Kobi: [вебсайт компанії]. – Режим доступу: https://kobi.ua/solutions/rozpiznavannya-nomeriv-cameras/ (дата звернення: 05.04.2026).*

Бочеєв Ілля Дмитрович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету інформаційно-комунікаційних технологій, м. Київ
st6870209@stud.duikt.edu.ua

Катков Юрій Ігорович
професор, доктор технічних наук

РОЗРОБКА IoT-ОРІЄНТОВАНОЇ ВЕБ-ПЛАТФОРМИ ДЛЯ МОНІТОРИНГУ ТА ВІЗУАЛІЗАЦІЇ ЕКОЛОГІЧНОГО СТАНУ РЕГІОНУ

Вступ.. Сучасні екологічні виклики – зміна клімату, промислове забруднення, деградація ґрунтів і водних ресурсів – вимагають оперативного моніторингу стану довкілля регіонів. Виникає проблема погіршення екологічної ситуації через антропогенний вплив. Традиційні методи (лабораторний аналіз, стаціонарні пости) не забезпечують реального часу, повного покриття території та доступності даних для широкого кола користувачів. Використання технологій Internet of Things (IoT) дозволяє отримувати дані про стан повітря, води та радіаційного фону в режимі реального часу з високою дискретністю. IoT-орієнтовані веб-платформи інтегрують сенсори, хмарні технології та інтерактивну візуалізацію, дозволяючи збирати дані про якість повітря, води, ґрунту, температуру та інші параметри в режимі реального часу [1, 2]. Створення таких веб-платформ є необхідним кроком для оперативного реагування на екологічні загрози та забезпечення відкритого доступу громадян до екологічної

інформації. Це дає змогу виявляти аномалії, прогнозувати ризики та підтримувати прийняття рішень органами влади, екологічними службами, бізнесом і громадськістю. Для України, з її промислово-аграрними регіонами та наслідками воєнних дій, така платформа є особливо актуальною для сталого розвитку, моніторингу забруднення та виконання міжнародних зобов'язань (ЄС Green Deal). Розробка забезпечує масштабованість, низьку вартість розгортання та відкритість даних, що підвищує екологічну свідомість суспільства [3, 4].

Аналіз переваг та недоліків існуючих розробок систем для моніторингу та візуалізації екологічного стану регіону. На сучасному ринку системи моніторингу екологічного стану класифікуються за рівнем доступу та архітектурою [2, 3, 5, 6]:

- Комерційні платформи (AWS IoT, ThingSpeak, Clarity IoT): Пропонують високу надійність та готові інструменти аналітики, проте мають високу вартість підписки та закритий вихідний код, що ускладнює кастомізацію під специфічні потреби регіону.
- Системи з відкритим кодом (ConnecSenS, Soc-IoT, Yeelink): Забезпечують гнучкість у розробці та можливість інтеграції будь-яких типів датчиків, але потребують значних ресурсів на підтримку власної інфраструктури.
- Спеціалізовані оглядові рішення (PurpleAir, SaveEcoBot): Орієнтовані на широке коло користувачів і часто базуються на енергоефективних технологіях передачі даних, таких як LoRaWAN або NB-IoT.

Головним недоліком більшості цих систем є фрагментарність: дані часто існують в ізольованих екосистемах. Крім того, комерційні рішення часто є надлишковими для локального моніторингу, а відкриті платформи можуть мати складні інтерфейси для пересічного громадянина. Це створює нішу для розробки спеціалізованої веб-платформи, яка б поєднувала простоту візуалізації SaveEcoBot із потужністю аналітичних інструментів комерційних платформ.

Сучасні системи моніторингу екологічного стану мають [6, 7, 8]:

А) Переваги:

- Реальний час даних завдяки MQTT/LoRaWAN, що дозволяє оперативне виявлення забруднень (наприклад, PM2.5, CO2, pH води).
- Масштабованість і низька вартість розгортання (дешеві сенсори ESP32, сонячне живлення).
- Інтеграція візуалізації (дашборди, GIS-карти Leaflet) для простого сприйняття трендів і теплових карт регіону.
- Віддалений доступ через веб/мобільні інтерфейси, раннє попередження та підтримка прийняття рішень.
- Енергоефективність у віддалених зонах (LoRaWAN), інтеграція з хмарою для аналізу великих даних і ML-прогнозів. В огляді [7] підкреслюється зниження витрат на 30–50% порівняно з традиційними системами та покращення оперативності.

Б) недоліки:

- Низька точність дешевих сенсорів (потрібне калібрування, похибка до 20–30% порівняно з референсними приладами).
- Проблеми безпеки (кібератаки на IoT-пристрої, витік даних).
- Складність інтероперабельності різних протоколів і вендорів.
- Високе енергоспоживання в Wi-Fi-мережах, обмежене покриття в сільській місцевості.
- Перевантаження даними, складність аналізу без AI, високі витрати на хмарні сервіси при масштабуванні.
- Обмежена візуалізація в базових рішеннях (відсутність мультипараметричних карт, слабка адаптація до регіональних особливостей).
- Проблеми з довговічністю в агресивних умовах (волога, пил).

Загалом, існуючі розробки добре працюють у контрольованих середовищах (міста, промисловість), але бракує комплексних регіональних рішень з відкритим кодом, адаптованих до локальних екологічних ризиків і простої візуалізації для непрофесійних користувачів.

Мета роботи. Метою роботи є підвищення ефективності моніторингу навколишнього середовища шляхом обґрунтування архітектури IoT-орієнтованої веб-платформи для комплексного моніторингу та візуалізації екологічного стану регіону. Платформа повинна забезпечити безперервний збір даних з розподілених сенсорів, їх обробку, зберігання та представлення у зручному інтерактивному вигляді для оперативного аналізу, прогнозування ризиків і підтримки екологічного менеджменту. Досягнення мети дозволить підвищити ефективність реагування на забруднення, забезпечити доступність даних для стейкхолдерів та внести вклад у цифровізацію екологічного моніторингу в Україні

Постановка завдання Необхідно розробити IoT-орієнтовану веб-платформу, яка інтегрує мережу сенсорів для збору даних про ключові екологічні параметри регіону (якість повітря – PM, CO2, NO2; вода – pH, мутність, розчинений кисень; ґрунт – вологість, температура; метеопараметри). Платформа повинна забезпечувати передачу даних у реальному часі через бездротові протоколи, зберігання в хмарній БД, обробку (фільтрація, агрегація, аномалії), інтерактивну візуалізацію на GIS-картах і дашбордах, систему сповіщень та доступ з різних пристроїв. Завдання включає забезпечення безпеки даних, масштабованість для регіонального рівня, відкритий API для інтеграції з державними системами та простоту розгортання в умовах обмеженої інфраструктури.

Результати дослідження

Архітектура IoT-орієнтованої веб-платформи. Запропонована архітектура IoT-орієнтованої веб-платформи для реалізації функціоналу моніторингу та візуалізації екологічного стану регіону, яка базується на чотиришаровій моделі IoT з акцентом на регіональну адаптивність,

масштабованість і безпеку. Архітектура IoT-орієнтованої веб-платформи має наступні компоненти.

1. Сенсорний (Perception Layer) шар для збору даних: мережа автономних вузлів (ESP32/NodeMCU + модулі LoRa). Сенсори: повітря (MQ-135, SDS011 для PM2.5/PM10, BME680), вода (DFRobot pH, turbidity), ґрунт (VH400), метео (анемометр, дощ). Живлення – сонячні панелі + акумулятори. Edge-обробка на вузлах (фільтрація).

2. Мережевий (Network Layer) шар: протоколи – LoRaWAN (для віддалених зон, дальність до 15 км), Wi-Fi/MQTT (Message Queuing Telemetry Transport) для щільних зон, NB-IoT як резерв. Gateways (Raspberry Pi) агрегають дані та передають у хмару. Підтримка failover.

3. Шар обробки та зберігання (Application Server Processing/Cloud): хмарний сервер (AWS IoT Core / власний на Ubuntu + Node.js/Flask). БД: TimescaleDB (time-series) + PostgreSQL з PostGIS (геодані). Обробка: Python (Pandas, Scikit-learn для аномалій і простих прогнозів), Apache Kafka для потоків. API – RESTful + GraphQL.

4. Візуалізаційний (Presentation Layer) шар: фронтенд – React.js + Material-UI. Компоненти: інтерактивна карта регіону (Leaflet з тайлами OpenStreetMap + Heatmap.js), реал-тайм дашборди (Chart.js + Recharts), панелі сповіщень, користувацькі фільтри. WebSocket (Socket.io) для оновлень кожні 10–60 с. Ролі: admin (налаштування), operator (аналіз), public (перегляд).

Можуть бути додаткові компоненти:

- Безпека: JWT/OAuth2, TLS 1.3, шифрування даних на пристроях, firewall, регулярні аудити.
- Інтеграції: Telegram/SMS-алерти, експорт даних, API для державних реєстрів.
- Масштабування: контейнеризація (Docker + Kubernetes), мікросервіси.
- Моніторинг платформи: Prometheus + Grafana.

Структура потів даних даних наступна: сенсор → gateway → MQTT broker → cloud → БД → API → frontend. Час затримки <5 с у щільних зонах. Загальна вартість розгортання на 100 вузлів – низька завдяки open-source. Архітектура забезпечує повний цикл: збір → обробка → візуалізація → дії.

*Висновки та перспективи розробок***.** Розроблена архітектура IoT-орієнтованої веб-платформи забезпечує комплексне рішення для моніторингу та візуалізації екологічного стану регіону: реальний час даних, інтуїтивну GIS-візуалізацію, масштабованість і безпеку. Вона перевершує існуючі аналоги за адаптивністю до регіональних умов, відкритим кодом і низькою вартістю. Основні результати: запропонована чотиришарова архітектура, прототипи сенсорних вузлів і дашбордів, що дозволяють оперативно виявляти екологічні аномалії та підтримувати прийняття рішень.

Перспективи розвитку: інтеграція ML/AI для прогнозування (LSTM-моделі забруднення); розширення на мобільні додатки та AR-візуалізацію; підтримка 5G/6G для вищої щільності сенсорів; інтеграція з супутниковими даними та big data; відкритий репозиторій для спільноти (GitHub) та адаптація під державні стандарти України; розробка модулів для конкретних регіонів (Карпати, Причорномор'я). Подальші роботи включатимуть повномасштабне тестування в реальному регіоні, оцінку точності та економічної ефективності. Платформа сприятиме цифровій трансформації екологічного менеджменту та сталому розвитку.

Список використаних джерел

1. *Mahajan S. et al. (2022) Design and development of an open-source framework for citizen-centric IoT: environmental sensing and data visualisation. DOI: 10.1038/s41598-022-18700-z. URL: https://www.nature.com/articles/s41598-022-18700-z*
2. *Witczak D., Szymoniak S. (2024) Review of Monitoring and Control Systems Based on Internet of Things. DOI: 10.3390/app14198943. URL: https://doi.org/10.3390/app14198943*
3. *Olatomiwa L. et al. (2023) A Review of Internet of Things-Based Visualisation Platforms for Tracking Household Carbon Footprints. DOI: 10.3390/su152015016. URL: https://doi.org/10.3390/su152015016*
4. *Mokrani, H., et al. (2024). Smart Environmental Monitoring: Architecture and Protocols. Sensors (Basel). https://doi.org/10.3390/s24010123*
5. *Wang, J., et al. (2022). Web-based Platform for Regional Environmental State Visualization. Environmental Modelling & Software. https://doi.org/10.1016/j.envsoft.2022.105412*
6. *Choudhary A. et al. (2024) Internet of Things: a comprehensive overview, architectures, enabling technologies, and applications. DOI: 10.1007/s43926-024-00084-3. URL: https://doi.org/10.1007/s43926-024-00084-3*
7. *Laha S.R., Pattanayak B.K., Pattnaik S. (2022) Advancement of Environmental Monitoring System Using IoT and Sensor: A Comprehensive Analysis. DOI: 10.3934/environsci.2022044. URL: https://doi.org/10.3934/environsci.2022044*
8. *Moiroux-Arvis L. et al. (2023) ConnecSenS, a Versatile IoT Platform for Environment Monitoring: Bring Water to Cloud. DOI: 10.3390/s23062896. URL: https://doi.org/10.3390/s23062896*

Кулішенко Юлія Петрівна
студентка 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kulishenko.up@duikt.edu.ua

Кулішенко Ярослав Валерійович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kulishenko.yv@duikt.edu.ua

КЛАСИФІКАЦІЯ ТЕХНОЛОГІЙ ЗВ'ЯЗКУ ІНТЕРНЕТУ РЕЧЕЙ

Сучасні технології Інтернету речей (IoT) орієнтовані на забезпечення енергоефективного зв'язку, низької вартості апаратного забезпечення, значної дальності передачі даних та підтримки масового підключення пристроїв. Зазначені вимоги реалізуються в межах концепції мереж низької потужності з широким радіусом дії (LPWAN), розвиток яких здійснюється як міжнародними організаціями стандартизації, так і промисловими об'єднаннями.

Серед LPWAN-рішень значного поширення набули технології SIGFOX та LoRaWAN, що функціонують у неліцензованих частотних діапазонах. Технологія SIGFOX характеризується використанням ультравузькосмугових сигналів, що забезпечує мінімальне енергоспоживання, проте обмежує швидкість передачі даних і обсяг повідомлень. У свою чергу, LoRaWAN підтримує декілька схем модуляції та кодування, що дозволяє підвищити швидкість передачі даних і розширити спектр застосувань, однак обмежена стандартизація стримує її глобальне впровадження [1].

Альтернативний підхід представлений технологіями, розробленими в рамках 3GPP, які орієнтовані на масштабні IoT-сценарії. Зокрема, LTE Cat.M1, EC-GSM та NB-IoT забезпечують зниження складності пристроїв, розширене покриття та підтримку великої кількості підключень. Серед них NB-IoT вирізняється високою енергоефективністю, низькою вартістю обладнання та можливістю обслуговування значної кількості пристроїв, що робить її найбільш перспективною технологією для масового впровадження IoT, рис.1.

Таким чином, аналіз сучасних LPWAN-технологій свідчить, що рішення на основі пропрієтарних стандартів мають обмеження щодо масштабування та стандартизації. Натомість технології сімейства 3GPP, зокрема NB-IoT, забезпечують кращі умови для широкомасштабного впровадження Інтернету речей, що підтверджується їх архітектурними особливостями та технічними характеристикам.

Рис. 1. Класифікація сучасних технологій Інтернету речей [2]

Мобільні IoT-технології, NB-IoT та LTE-M, сьогодні забезпечують надійні та економічно ефективні можливості низькопотужного широкого спектру, закладаючи основу майбутнього 5G і підтримуючи масштабне зростання IoT. Технологія 5G значно прискорить розвиток IoT завдяки високій швидкості передачі даних, низькій затримці та можливості одночасного підключення великої кількості пристроїв. Це дасть змогу сенсорам і розумним системам швидко обмінюватися інформацією та працювати майже в реальному часі. Завдяки 5G IoT-рішення стануть більш надійними, масштабованими та придатними для використання у розумних будівлях, промисловості, транспорті та міській інфраструктурі. Крім того, технологія сприятиме зменшенню енергоспоживання пристроїв і підвищить ефективність автоматизованого моніторингу та керування процесами.

Список використаних джерел

1. D. Orlovs, A. Rusins, V. Skrastiņš & J. Judvaitis, "LPWAN Technologies for IoT: Real-World Deployment Performance and Practical Comparison," IoT, vol. 6, no. 4, p. 77, 2025.

2. M. Jouhari, N. Saeed, M.-S. Alouini, E. M. Amhoud, "A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges," arXiv preprint, 2022.

Дубовський Володимир Васильович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
dubovskiy.vv@duikt.edu.ua

Полоневич Ольга Володимирівна
к.т.н., доцент, доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.polonevych@duikt.edu.ua

ГЕТЕРОГЕННА IOT-СИСТЕМА МОНІТОРИНГУ ТА КЕРУВАННЯ ЖИТЛОВИМ ПРИМІЩЕННЯМ НА ОСНОВІ МУЛЬТИПРОТОКОЛЬНОЇ ВЗАЄМОДІЇ

Постановка задачі. Стрімкий розвиток технологій Інтернету речей (IoT) створив передумови для широкого впровадження інтелектуальних систем моніторингу та керування в житлових приміщеннях. Однак практичне впровадження таких систем у реальних об'єктах стикається з суттєвою проблемою – нестабільністю бездротового зв'язку в умовах складної архітектури будівель. Переважна більшість житлових будинків в Україні побудована з використанням залізобетонних конструкцій, які є ефективними екранами для радіохвиль. Підвальні приміщення, технічні поверхи та гаражі утворюють так звані «радіозатінені зони», де стандартні протоколи Wi-Fi та Bluetooth не здатні забезпечити надійний зв'язок. Комерційні системи «розумного дому», що базуються на одному протоколі, виявляються вразливими до ефекту екранування, що обумовлює необхідність розробки гетерогенної системи, яка поєднує переваги різних протоколів.

Мета дослідження. Розробка гетерогенної IoT-системи моніторингу та керування житловим приміщенням на основі мультипротокольної взаємодії технологій LoRa, Wi-Fi та Zigbee, що забезпечує стабільний збір та передачу даних у радіозатінених зонах залізобетонних будівель.

Результати дослідження. У роботі розроблено трирівневу структурну модель гетерогенної IoT-мережі, що включає рівень сприйняття (LoRa, Wi-Fi, Zigbee), рівень мережевої агрегації (мультипротокольний шлюз на базі NanoPi NEO2) та прикладний рівень (MQTT-брокер Mosquitto, Node-RED Dashboard).

Виконано математичне обґрунтування вибору частотних діапазонів. Розрахунки за моделлю FSPL (Free Space Path Loss) та аналіз енергетичного бюджету лінії зв'язку підтвердили, що технологія LoRa (868 МГц) зберігає запас потужності 73,8 дБ при проходженні крізь два залізобетонні перекриття, тоді як

Wi-Fi (2,4 ГГц) у тих самих умовах не забезпечує мінімально необхідного рівня сигналу (дефіцит 15,1 дБ відносно порогу чутливості).

Спроєктовано мультипротокольний комунікаційний хаб – плату розширення Gateway Interface, що об'єднує LoRa-трансивер SX1278 та Zigbee-координатор CC2530. Розроблено двошарову друковану плату. Створено автономні LoRa-вузли на базі ATmega328P з розрахунковим часом роботи від батареї 18650 до 2,5 років та Wi-Fi вузли на базі ESP32 для зон із стабільним покриттям.

Розроблено логічну схему мультипротокольної конвергенції: шина MQTT виступає як уніфікований транспорт, кожне повідомлення нормалізується у єдиний JSON-формат незалежно від фізичного рівня походження. Реалізовано багаторівневу систему інформаційної безпеки (HMAC-SHA256 для LoRa-каналу, TLS 1.2 для MQTT, VPN для віддаленого доступу).

Висновки та перспективи. Розроблена гетерогенна IoT-система демонструє ефективність мультипротокольного підходу для забезпечення повного покриття житлового об'єкта, включаючи радіозатінені зони. Поєднання технологій LoRa, Wi-Fi та Zigbee дозволяє компенсувати обмеження кожного окремого протоколу та забезпечити надійний моніторинг критичних параметрів (протікання, мікроклімат, безпека) навіть у найскладніших умовах поширення радіохвиль. Подальший розвиток системи може бути спрямований на інтеграцію з хмарними IoT-платформами, впровадження алгоритмів машинного навчання для предиктивного аналізу та розширення підтримки нових протоколів (Thread, Matter).

Список використаних джерел

1. Augustin A. et al. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors. 2016. Vol. 16, No. 9. P. 1466.

2. Propagation data and prediction methods for the planning of indoor radiocommunication systems: Recommendation ITU-R P.1238-11. Geneva: ITU, 2021. 32 p.

3. Al-Fuqaha A. et al. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, No. 4. P. 2347–2376.

Слєпченко Олександр Романович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету інформаційно-комунікаційних технологій, м. Київ
alexslepchenko71@gmail.com

Бондарчук Олександр Павлович
викладач кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ

IOT-АРХІТЕКТУРА ДЛЯ МОНІТОРИНГУ МІСЬКОЇ ІНФРАСТРУКТУРИ: EDGE COMPUTING ТА LPWAN

Цифровізація міського середовища перетворила розподілені мережі датчиків з інструменту академічних досліджень на повноцінний елемент комунального управління. Сучасне розуміння розумного міста передбачає не лише збір даних, а й прийняття рішень у режимі реального часу – з мінімальною затримкою та без обов'язкової участі хмарного центру обробки. Саме ця вимога зумовлює перехід від централізованих SCADA-систем до гібридних IoT-архітектур із локальною обробкою на рівні edge [4].

Ключовою тенденцією останніх років є поєднання хмарних та крайових обчислень в єдину гнучку платформу. Хмарний рівень забезпечує довгострокове зберігання та масштабну аналітику, тоді як edge-вузли виконують фільтрацію аномалій та реакцію на критичні події локально – без очікування відповіді від центрального сервера. Такий підхід суттєво скорочує затримку і зменшує обсяг трафіку, що передається через мережу [4].

Для передачі даних у масштабах міста широко застосовуються LPWAN-протоколи, зокрема LoRaWAN. Реальне розгортання мережі з 20 вузлів у місті Саутгемптон (Велика Британія) показало: 72,4% пакетів доставляється протягом 10 секунд з моменту відправлення, а рівень доставки залежить насамперед від наявності надлишковості на серверному рівні, а не від якості радіоканалу [5]. Порівняно з NB-IoT, LoRaWAN демонструє кращу гнучкість у зонах із нерівномірним покриттям мережі оператора, хоча NB-IoT підходить для щільно забудованих районів із розвиненою стільниковою інфраструктурою [1].

Для уточнення переваг децентралізованого підходу нижче наведено порівняння традиційної SCADA-архітектури та IoT edge-рішення за ключовими критеріями (табл. 1).

Табл. 1

Порівняння SCADA та IoT edge-архітектури для моніторингу міської інфраструктури

Характеристика	**SCADA (централізована)**	**IoT edge-архітектура**	**Перевага IoT**
Відмовостійкість	Єдина точка відмови	Mesh-топологія	Висока
Доступ персоналу	Фізичний виїзд	Дистанційно	Безпечно
Протокол зв'язку	Proprietary	MQTT / CoAP	Відкритий стандарт
Доставка пакетів LoRaWAN	–	72,4% за 10 с	Висока надійність

На рівні комунікаційних протоколів основними стандартами передачі даних між IoT-пристроями та edge-шлюзами є MQTT і CoAP. MQTT використовує модель публікація/підписка (pub/sub) та оптимізований для каналів із нестабільною якістю зв'язку, тоді як CoAP орієнтований на пристрої з жорсткими обмеженнями за пам'яттю й живленням. Для реалізації гібридних рішень дослідники комбінують обидва протоколи разом з технологіями LoRaWAN та NB-IoT, що дозволяє охоплювати різнорідні сценарії розгортання [3].

Edge-шлюз виконує кілька ключових функцій безпосередньо на місці розгортання. По-перше, первинний аналіз і фільтрація: шлюз відкидає шумові значення та надлишкові показники ще до передачі, що суттєво знижує навантаження на канал зв'язку. По-друге, функція гейтвею – агрегація потоків від датчиків різних протоколів у єдиний уніфікований формат. По-третє, розподіл рішень: якщо значення перевищує критичний поріг, шлюз негайно надсилає команду актуатору – клапану, вентилятору або сигналізації – без очікування відповіді від хмари. Лише зведені або аномальні дані передаються далі на хмарну платформфу для довгострокової аналітики [3].

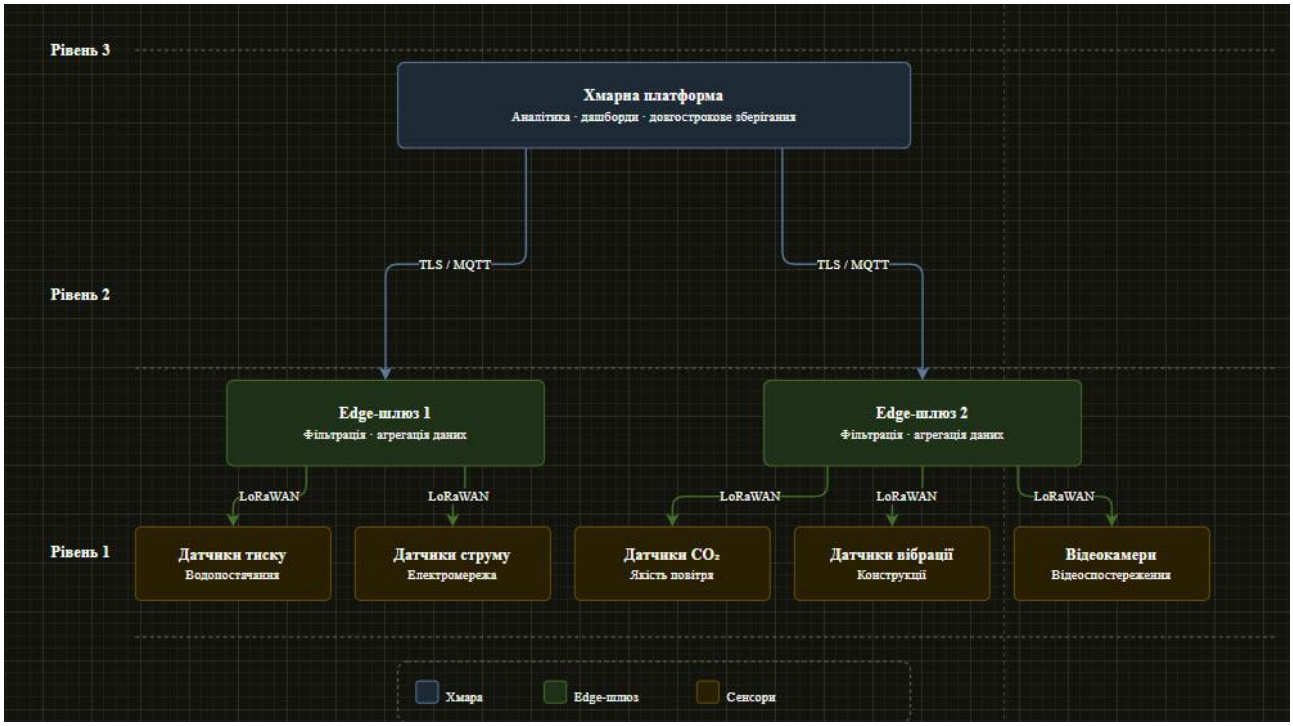

Рис. 1. Трирівнева IoT-архітектура моніторингу міської інфраструктури [2]

Архітектура, зображена на рис. 1, складається з трьох рівнів: рівень сенсорів, рівень edge-шлюзів та хмарна платформа для довгострокової аналітики. Edge-шлюзи виконують попередню фільтрацію та агрегацію даних: лише аномальні значення або зведені показники передаються до хмари, що зменшує навантаження на мережу та хмарні ресурси [4]. Такий розподіл обчислень забезпечує роботу системи навіть при тимчасовій втраті з'єднання з хмарним рівнем.

Дослідження Chan et al. (2024) підтверджує практичну ефективність такого підходу: система моніторингу якості повітря на базі LoRa та MQTT досягла стабільної передачі даних на відстані до 1,65 км у міських умовах. При цьому NB-IoT виявився більш надійним у районах зі щільною забудовою, а LoRa – переважним у відкритих або промислових зонах [1]. Це свідчить про доцільність гетерогенних мереж, де різні LPWAN-технології доповнюють одна одну залежно від специфіки місцевості.

Таким чином, впровадження IoT з edge-обчисленнями для моніторингу міської інфраструктури є технічно зрілим рішенням, підтвердженим реальними розгортаннями. Перевагами є відмовостійкість за рахунок mesh-топологій, енергоефективна передача даних через LPWAN, а також можливість локальної реакції на аномалії без залежності від хмарного центру. Водночас відкритими залишаються питання стандартизації протоколів безпеки для edge-вузлів та розробки ефективних механізмів виявлення аномалій безпосередньо на пристроях із обмеженими ресурсами.

Список використаних джерел

1. Chan, Y. W., Kristiani, E., & Fathoni, H. (2024). A smart edge computing infrastructure for air quality monitoring using LPWAN and MQTT technologies. The Journal of Supercomputing, 80, 9961–9985. https://doi.org/10.1007/s11227-023-05837-5

2. Ficili, I., Giacobbe, M., Tricomi, G., & Puliafito, A. (2025). From sensors to data intelligence: Leveraging IoT, cloud, and edge computing with AI. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC11945247/

3. Gkonis, P., Giannopoulos, A., Trakadas, P., Masip-Bruin, X., & D'Andria, F. (2025). Edge and cloud computing in smart cities. Future Internet, 17(3), 118. https://doi.org/10.3390/fi17030118

4. Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-computing architectures for Internet of Things applications: A survey. Sensors, 20(22), 6441. https://doi.org/10.3390/s20226441

5. Langford, J., Fernandez, P., Voss, S., & Blair, B. (2020). LoRaWAN for smart city IoT deployments: A long term evaluation. Sensors, 20(3), 648. https://doi.org/10.3390/s20030648

Антоненко Ярослав Миколайович
студент 3 курсу
спеціальності «Комп'ютерні науки»
Харківського національного університету
Радіоелектроніки, м. Харків
yaroslav.antonenko@nure.ua

Петрова Роксана Вадимівна
Доцент, кандидат технічних наук
Каф. Комп'ютерного моделювання та інтелектуальних технологій
Харківського національного університету
радіоелектроніки, м. Харків
roksana.petrova@nure.ua

ІНТЕЛЕКТУАЛЬНА IOT-СИСТЕМА УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ У СИСТЕМІ «РОЗУМНИЙ ДІМ»

У сучасних умовах зростання енергоспоживання та підвищення вартості енергоресурсів особливого значення набуває впровадження інтелектуальних систем управління енергією. Одним із перспективних напрямів є використання технологій Інтернету речей (IoT), які забезпечують збір, передачу та аналіз даних у режимі реального часу, що дозволяє оптимізувати споживання енергії в житлових приміщеннях [1].

Системи «розумного дому» дозволяють автоматизувати керування освітленням, опаленням та побутовими пристроями. Проте більшість існуючих рішень працює за фіксованими сценаріями і не враховує поведінку користувача та змінні умови середовища, що знижує ефективність використання енергоресурсів [2].

Метою даної роботи є розробка концепції інтелектуальної IoT-системи управління енергоспоживанням, яка забезпечує адаптивне керування ресурсами на основі аналізу поведінки користувача та параметрів середовища.

Запропонована система включає IoT-пристрої (сенсори температури, руху, освітленості та енергоспоживання), серверну частину для обробки даних та користувацький інтерфейс. Зібрані дані передаються до серверу, де аналізуються з використанням сучасних методів обробки інформації, що дозволяє формувати ефективні керуючі рішення [3].

Ключовою особливістю системи є її адаптивність. Наприклад, у разі відсутності користувача система автоматично знижує споживання електроенергії, вимикаючи освітлення або переводячи пристрої у режим енергозбереження. При поверненні користувача забезпечується відновлення комфортних умов.

Для оцінювання ефективності функціонування системи використовується показник енергоефективності:

$$E_{\text{ефект.}} = \frac{E_{\text{баз}} - E_{\text{опт}}}{E_{\text{баз}}}$$

де:

- Ебаз – базове енергоспоживання;
- Еопт – оптимізоване енергоспоживання.

Принцип роботи системи полягає у безперервному зборі та аналізі даних із сенсорів, що дозволяє оперативно реагувати на зміни умов та оптимізувати роботу обладнання.

На рис. 1 представлено загальну структуру інтелектуальної IoT-системи управління енергоспоживанням.

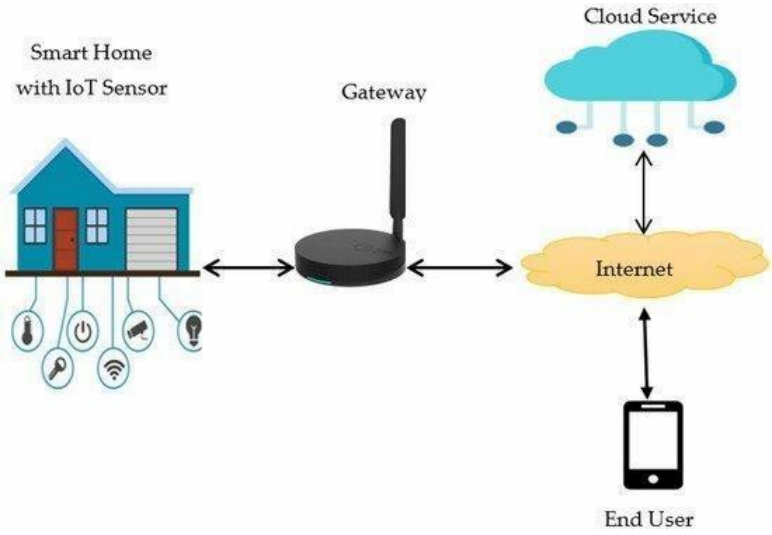

Рис. 1. Структура інтелектуальної IoT-системи управління енергоспоживанням

Для більш наочного аналізу ефективності запропонованого підходу наведено порівняння традиційних систем та IoT-рішення в табл. 1.

Табл. 1.

Порівняння систем управління енергоспоживанням

Характеристика	Традиційні системи	IoT-системи
Тип управління	Статичний	Адаптивний
Аналіз даних	Обмежений	Інтелектуальний
Урахування поведінки	Відсутнє	Присутнє
Реакція на зміни	Повільна	Автоматична
Енергоефективність	Середня	Висока

Отже, впровадження інтелектуальних IoT-систем дозволяє підвищити ефективність використання енергоресурсів та забезпечити комфортні умови проживання. Перспективним напрямом розвитку є використання методів машинного навчання для прогнозування енергоспоживання та автоматичного керування системою [3].

Список використаних джерел

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.

2. Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT architectures for smart buildings and energy optimization. IEEE Internet of Things Journal, 4(1), 269–283.

3. Al-Ali, A. R., Zualkernan, I. A., Rashid, M., Gupta, R., & Alikarar, M. (2017). Smart home energy management system using IoT. IEEE Transactions on Consumer Electronics, 63(4), 426–434.

Павлючик Андрій Михайлович
студент групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій
(050)-658-81-23
a.pavliuchyk1408@gmail.com

Заячковський Андрій Володимирович
викладач кафедри Інформаційних систем та технологій
Державного університету інформаційно-комунікаційних технологій, м. Київ

ЕКОЛОГІЧНІ ТА ЕКОНОМІЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНОГО ВУЛИЧНОГО ОСВІТЛЕННЯ В КОНЦЕПЦІЇ SMART CITY

Стрімка урбанізація та збільшення щільності населення у великих містах ставлять перед муніципалітетами нові виклики щодо управління міською інфраструктурою. Одним із найважливіших елементів життєзабезпечення населеного пункту є система вуличного освітлення, яка безпосередньо впливає на безпеку дорожнього руху, рівень злочинності та загальний комфорт містян. Проте глобальний курс на сталий розвиток вимагає перегляду традиційних підходів до експлуатації таких мереж з огляду на їхню високу енергоємність.

Постановка задачі

Сьогодні забезпечення безперебійного функціонування системи зовнішнього освітлення забирає значну частку коштів із муніципальних бюджетів. За даними енергетичних аудитів, ця стаття експлуатаційних витрат може сягати від 20% до 40% усього обсягу спожитої містом електроенергії [3].

Головна проблема полягає у відсутності адаптивності традиційних мереж. Класичне каскадне керування, що базується на астрономічних таймерах або сутінкових реле, змушує систему працювати на повній номінальній потужності протягом усієї ночі. У період глибокої ночі (з 02:00 до 05:00), коли вулиці практично повністю порожні від пішоходів та автомобілів, мережа продовжує споживати максимальну кількість енергії. Окрім прямих фінансових збитків, така перевитрата ресурсів призводить до збільшення вуглецевого сліду та поглиблює проблему "світлового забруднення" міського середовища. Отже, виникає об’єктивна потреба у переході до розумних систем освітлення, здатних балансувати між нормативною безпекою та економічною доцільністю.

Мета дослідження

Метою дослідження є комплексний аналіз економічних та екологічних переваг переходу від традиційних мереж вуличного освітлення до інтелектуальних адаптивних систем управління в рамках розбудови концепції "Розумного міста" (Smart City).

Результати дослідження

Впровадження інтелектуальних систем вуличного освітлення передбачає заміну застарілих джерел світла на енергоефективні LED-світильники, обладнані мікропроцесорними драйверами та сенсорами присутності (руху). На відміну від традиційної бінарної логіки ("увімкнено/вимкнено"), такі системи здатні динамічно змінювати рівень яскравості залежно від фактичної дорожньої ситуації [1].

З економічної точки зору, перехід на розумне освітлення генерує економію за двома основними напрямками:

1. Зниження капітальних витрат на електроенергію. Алгоритми адаптивного димірування дозволяють знижувати рівень освітленості до 20-30% від номіналу на порожніх ділянках доріг, миттєво підвищуючи його до 100% при фіксації наближення автомобіля або пішохода. Це дозволяє скоротити загальне енергоспоживання на 40-60%.

2. Оптимізація операційних витрат *(OPEX).* Традиційні мережі не мають зворотного зв'язку, тому виявлення перегорілих ламп чи обривів ліній вимагає регулярних нічних об'їздів ремонтними бригадами. Розумні світильники постійно передають телеметричні дані (напругу, струм, температуру матриці) на центральний диспетчерський пункт [3]. Це дозволяє впровадити стратегію предиктивного обслуговування: система автоматично генерує сповіщення про поломку з точними GPS-координатами, що радикально зменшує витрати на пальне та утримання штату технічних працівників.

З екологічної точки зору, оптимізація енергоспоживання має прямий наслідок у вигляді пропорційного зменшення викидів парникових газів ($CO2$) тепловими електростанціями. Крім того, адаптивне освітлення є найефективнішим інструментом боротьби зі "світловим забрудненням" (Light Pollution) [2]. Науково доведено, що надлишкове нічне освітлення дезорієнтує перелітних птахів, порушує життєві цикли комах та негативно впливає на циркадні ритми людей, пригнічуючи вироблення мелатоніну. Зниження фонової яскравості вулиць у нічний час сприяє відновленню локальних міських екосистем та покращує якість сну мешканців прилеглих будинків.

Більше того, модернізована мережа ліхтарних стовпів стає базовим фізичним каркасом для подальшого розгортання технологій Smart City. Оскільки до кожного ліхтаря вже підведено живлення та канал зв'язку, вони стають ідеальними точками для розміщення датчиків якості повітря, метеостанцій, камер відеоаналітики та точок доступу громадського Wi-Fi [1].

Висновки та перспективи

Модернізація вуличного освітлення не повинна обмежуватися простою заміною натрієвих ламп на світлодіодні. Максимальний економічний та екологічний ефект досягається виключно шляхом впровадження адаптивних систем керування на базі технологій Інтернету речей. Такі системи дозволяють

муніципалітетам не лише скоротити бюджетні витрати на електроенергію та обслуговування вдвічі, але й суттєво покращити екологічну ситуацію в регіоні за рахунок зменшення викидів CO2 та подолання проблеми світлового забруднення.

Подальші перспективи розвитку цього напрямку полягають у розробці стандартизованих протоколів обміну даними між різними підсистемами розумного міста, що дозволить інтегрувати керування освітленням із системами контролю дорожнього трафіку та екологічного моніторингу в єдину диспетчерську платформу.

Список використаних джерел

1. Wojnicki I. Intelligent Street Lighting in a Smart City Concepts–A Direction to Energy Saving in Cities: An Overview and Case Study [Електронний ресурс]. – Energies, 2021. – Режим доступу: https://doi.org/10.3390/en14113018.

2. Szulczewska B., et al. Integrating Sustainable Lighting into Urban Green Space Management: A Case Study of Light Pollution [Електронний ресурс]. – Sustainability, 2024. – Режим доступу: https://www.mdpi.com/2071-1050/17/17/7833.

3. Кліщ Т. В. Розвиток концепції розумного міста: публічно-управлінський аспект [Електронний ресурс]. – Актуальні проблеми державного управління, 2024. – Режим доступу: https://periodicals.karazin.ua/apdu/article/view/24059.

Стрельбіцький Вадим Юрійович
студент групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій,м. Київ
(068)-186-64-74
youfriend471@gmail.com

ЗАСТОСУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ У СИСТЕМАХ АВТОМАТИЗАЦІЇ ТА МОНІТОРИНГУ

Постановка задачі

Сучасні інформаційні системи потребують високого рівня автоматизації та оперативного збору даних. Традиційні підходи до моніторингу та управління часто є неефективними через відсутність гнучкості та можливості обробки даних у реальному часі.

Застосування технологій Інтернету речей дозволяє інтегрувати фізичні пристрої у цифрове середовище, що забезпечує безперервний обмін даними. Проте виникають проблеми масштабованості, сумісності пристроїв та забезпечення безпеки.

Мета дослідження

Дослідити можливості використання IoT у системах автоматизації та моніторингу, визначити ключові компоненти архітектури та оцінити ефективність їх впровадження.

Результати дослідження

Запропоновано трирівневу архітектуру системи IoT, яка включає сенсорний рівень, рівень передачі даних та рівень обробки інформації.

Сенсорний рівень представлений пристроями збору даних, такими як датчики температури, руху та освітлення. Рівень передачі даних використовує сучасні протоколи, зокрема MQTT та CoAP.

Рівень обробки інформації базується на хмарних технологіях та дозволяє здійснювати аналіз даних у реальному часі.

Використання запропонованої моделі дозволяє підвищити ефективність систем моніторингу, зменшити витрати ресурсів та забезпечити масштабованість.

Окрему увагу приділено питанням безпеки, зокрема використанню шифрування, автентифікації пристроїв та сегментації мережі.

Висновки та перспективи

Інтернет речей є перспективним напрямом розвитку інформаційних систем, що забезпечує автоматизацію процесів та підвищення ефективності управління.

Подальші дослідження можуть бути спрямовані на інтеграцію IoT з технологіями штучного інтелекту та оптимізацію обробки даних.

Список використаних джерел

1. Atzori L., Iera A., Morabito G. Internet of Things: A survey. Computer Networks, 2010.

2. LoRa Alliance. LoRaWAN Specification 1.0.3.

3. MQTT Version 3.1.1. OASIS Standard.

4. Shelby Z., Hartke K., Bormann C. The Constrained Application Protocol (CoAP). RFC 7252.

5. Шпак О., Федорка П. Розумні міста та Інтернет речей. 2023.

Корепанов Максим Валерійович
аспірант 2 курсу спеціальності
«Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
maksym.korepanov@gmail.com

Сагайдак Віктор Анатолійович
PhD, доцент кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

МЕТАЕВРИСТИЧНІ АЛГОРИТМИ ОПТИМІЗАЦІЇ ДЛЯ РОЗПОДІЛУ РЕСУРСІВ У IoT-ІНФРАСТРУКТУРІ ПІДПРИЄМСТВ

Вступ.

Інтернет речей (IoT) розширює можливості інформаційних систем підприємств шляхом підключення датчиків, виконавчих пристроїв, шлюзів та програмних сервісів, що забезпечують збір і обробку телеметрії у режимі, наближеному до реального часу. Для промислових IoT-систем, “розумних” будівель, логістичних платформ, систем моніторингу обладнання характерні нерівномірні потоки повідомлень (пікові навантаження, сезонність, подієві “сплески”), а також комбіновані вимоги QoS/SLA: допустима затримка, доступність, пропускна здатність, рівень втрат, інколи – енергоспоживання та автономність вузлів. У таких умовах виникає багатокритеріальна задача керування ресурсами (edge/fog/cloud-обчислення, пропускна здатність каналів, буфери/черги, квоти CPU/RAM), де цілі можуть бути суперечливими: підвищення якості сервісу зазвичай потребує більших витрат на інфраструктуру.

З огляду на високу розмірність, нелінійність, а також наявність дискретних рішень (вибір вузла, маршрут, політика черги), застосування класичних градієнтних методів часто обмежене. Тому перспективними є метаевристичні алгоритми оптимізації, зокрема генетичний алгоритм (GA) [2], алгоритм рою частинок (PSO) [3], диференціальна еволюція (DE) [4] та їхні гібридні комбінації [1], які здатні знаходити раціональні конфігурації без вимоги до диференційовності цільової функції.

Основний матеріал.

Узагальнено задачу ресурсного керування IoT-інфраструктурою підприємства можна подати як вибір конфігурації, що визначає: (1) розподіл обчислень між edge/fog/cloud (offloading), (2) параметри масштабування та лімітування сервісів (кількість екземплярів, CPU/RAM-квоти, політики

автоскейлінгу), (3) мережеві параметри (маршрутизація, пріоритизація трафіку, керування смугою), (4) керування чергами повідомлень (класи пріоритетів, дедлайни, правила відкидання/повторів), (5) за потреби – обмеження енергоспоживання для автономних вузлів. З огляду на комбінаторний характер частини параметрів (вибір вузлів розміщення, маршрутизація, політики черг) та нелінійний вплив навантаження на метрики QoS, задача, як правило, не має зручної аналітичної форми та містить множину локальних екстремумів. Тому для пошуку раціональних конфігурацій доцільно застосовувати метаевристичні алгоритми оптимізації (GA, PSO, DE тощо), а за потреби – їх гібридні поєднання, які забезпечують кращий баланс між швидкістю збіжності та якістю рішення.На практиці це дає низку типових задач оптимізації, наведені у табл. 1.

Табл. 1.

Типові задачі оптимізації ресурсів у IoT-інфраструктурі підприємств

Задача в IoT-інфраструктурі	**Оптимізовані параметри**	**Ключові критерії**
Розподіл обчислень між edge/fog/cloud	рішення offloading, вибір вузлів, квоти CPU/RAM	затримка, вартість, SLA
Масштабування шлюзів/мікросервісів	кількість екземплярів, ліміти ресурсів	затримка/пропускна здатність, витрати
Керування потоками телеметрії	пріоритети, правила черг, політики повторів	втрати, дедлайни, SLA
Баланс ресурсів у IoT-мережі	маршрутизація, смуга, буфери	пропускна здатність, енергія

Критерії ефективності доцільно формувати на основі метрик експлуатації: середня та перцентильна затримка (наприклад, 95-й перцентиль), пропускна здатність, завантаження вузлів, частка порушень SLA, рівень втрат/прострочених повідомлень, а також агрегована вартість інфраструктури. Для практичного використання багатокритеріальність зручно зводити до зваженої інтегральної оцінки (scoring), де ваги відображають бізнес-пріоритети (наприклад, “SLA критичніші за економію” у виробничих системах). Обмеженнями можуть виступати максимальні квоти ресурсів, граничні рівні затримки для критичних потоків, ліміти мережевої смуги, обмеження на енергоспоживання, а також регламентні вимоги до надійності/відмовостійкості.

Додатковою складністю IoT є неоднорідність середовища: edge-вузли мають обмежені ресурси, але дають мінімальні затримки; хмарні ресурси масштабовані, проте збільшують затримку через мережу. Через це рішення часто потребують адаптації до зміни профілю трафіку. Практично корисною є побудова циклу керування: телеметрія та профіль навантаження → оцінювання

конфігурації (за вимірюваннями/симуляцією) → оптимізаційний пошук → застосування рекомендацій (масштабування/перерозподіл).

У ролі оптимізатора можуть виступати метаевристики. PSO часто обирають за простоту реалізації та швидку збіжність у задачах налаштування параметрів [3]. DE є ефективним для оптимізації у неперервних просторах і придатний для пошуку ресурсних квот та коефіцієнтів політик [4]. GA зручний у задачах зі змішаними (дискретно-неперервними) змінними – наприклад, одночасний вибір вузлів розміщення та ресурсних лімітів [2]. У сучасних роботах також підкреслюється доцільність гібридних підходів, які поєднують глобальний і локальний пошук, забезпечуючи кращий баланс "якість/час" для практичних IoT-сценаріїв [1].

Висновки.

Задачі оптимізації ресурсів у IoT-інфраструктурі підприємств природно формулюються як багатокритеріальна оптимізація з обмеженнями QoS/SLA та економічними критеріями. Метаевристичні алгоритми (GA, PSO, DE) є придатними для таких задач завдяки гнучкості, здатності працювати зі змішаними змінними та ефективному пошуку раціональних конфігурацій без вимоги градієнтної інформації. Практично доцільно використовувати контур "телеметрія/оцінювання → оптимізація → рекомендації масштабування/перерозподілу", який може виконуватись періодично для адаптації до змін навантаження. Подальші дослідження можуть бути спрямовані на уточнення моделей QoS для різних класів IoT-трафіку, порівняння ефективності метаевристик на типових сценаріях та розвиток гібридних схем оптимізації.

Список використаних джерел

1. *Dankolo, N. M., Radzi, N. H. M., Mustaffa, N. H., Arshad, N. I., Nasser, M., Gabi, D., & Yusuf, M. N. (2025). Optimizing resource allocation for IoT applications in the edge cloud continuum using hybrid metaheuristic algorithms.* Scientific Reports, 15*, 14409. doi:10.1038/s41598-025-97648-2*

2. *Goldberg, D. E. (1989).* Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley.*

3. *Kennedy, J., & Eberhart, R. (1995). Particle swarm optimization. In* Proceedings of ICNN'95 *(Vol. 4, pp. 1942–1948).*

Storn, R., & Price, K. (1997). Differential evolution–A simple and efficient heuristic for global optimization over continuous spaces. Journal of Global Optimization, 11(4), 341–359.

студент групи ІСД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
reserveusername2@gmail.com

Заячковський Андрій Володимирович
викладач кафедри інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
andrii.zaiachkovskyi@duikt.edu.ua

ІОТ-СИСТЕМИ МОНІТОРИНГУ ЕКОЛОГІЧНИХ ПАРАМЕТРІВ ДЛЯ РОЗУМНИХ МІСТ ТА ПРОМИСЛОВИХ ЗОН З ІНТЕГРОВАНОЮ ВІЗУАЛІЗАЦІЄЮ ДАНИХ

Постановка задачі

Активний розвиток розумних міст та цифровізація промислових зон вимагають ефективних систем моніторингу екологічних параметрів у реальному часі. Традиційні методи екологічного контролю, що базуються на стаціонарних постах і періодичних лабораторних вимірюваннях, не забезпечують достатньої просторової щільності та оперативності обробки даних від розподілених сенсорів. Це призводить до запізнілої реакції на підвищення рівнів забруднення повітря (PM2.5, PM10, NO_2, CO_2), шуму, температури, вологості та інших параметрів [1; 4].

У промислових зонах такі обмеження створюють додаткові ризики для здоров'я населення та довкілля, а в міському середовищі ускладнюють прийняття оперативних управлінських рішень. Сучасні IoT-системи з інтеграцією edge computing, хмарних платформ і інструментів візуалізації дозволяють збирати, обробляти та представляти дані в реальному часі, що відкриває можливості для проактивного моніторингу та зниження екологічного навантаження [2; 5].

Мета дослідження

Метою дослідження є аналіз сучасних IoT-систем моніторингу екологічних параметрів (якість повітря, мікроклімат, шум, якість води) для розумних міст та промислових зон з обов'язковою інтеграцією візуалізації даних у реальному часі. Робота спрямована на оцінку ефективності архітектур, алгоритмів обробки даних та інструментів візуалізації, а також на визначення перспектив впровадження в українському контексті. Дослідження передбачає оцінку потенціалу скорочення часу реагування на забруднення на 50–70 % та підвищення точності прогнозування до 90–99 % порівняно з традиційними методами.

Результати дослідження

Сучасні IoT-системи моніторингу екологічних параметрів будуються на базі низьковартісних сенсорів (PMS5003/SDS011 для PM2.5 і PM10, MQ-серії для

газів, SCD40 для CO_2, BME680 для температури, вологості та VOC), мікроконтролерів ESP32/ESP8266 та бездротових протоколів передачі даних MQTT і LoRaWAN. Це забезпечує розгортання щільної мережі сенсорів як у міському просторі, так і на території промислових підприємств [1; 3].

Дані, зібрані сенсорами, проходять попередню обробку на edge-вузлах для фільтрації шумів (зокрема, за допомогою фільтра Кальмана) та зменшення обсягу інформації, що передається в хмару. Далі дані надходять до хмарних платформ (InfluxDB, HiveMQ), де застосовуються алгоритми машинного навчання. Зокрема, LSTM-мережі добре справляються з прогнозуванням часових рядів (температура, вологість, концентрація CO_2), а Random Forest – з класифікацією рівнів забруднення PM2.5, демонструючи R^2 до 99 % для мікрокліматичних параметрів і до 84 % для твердих частинок [2; 6].

Важливим компонентом є інтегрована візуалізація даних. Інструменти Node-RED дозволяють обробляти MQTT-потоки та зберігати інформацію в часових базах даних, тоді як Grafana формує інтерактивні дашборди з тепловими картами, трендами в реальному часі, індикаторами та системою алертів. Такий підхід забезпечує просторове моделювання за допомогою GIS-даних і допомагає оперативно виявляти «гарячі точки» забруднення в промислових зонах та густонаселених міських районах [3; 4; 7].

Поєднання IoT з edge computing суттєво зменшує затримки обробки даних і підвищує стійкість системи до перебоїв у мережі. У промислових умовах такі рішення дозволяють автоматично активувати вентиляцію або системи оповіщення при прогнозованому перевищенні нормативів. У контексті розумних міст системи забезпечують громадський доступ до відкритих дашбордів, сприяючи підвищенню екологічної обізнаності населення [5; 8].

В українському контексті впровадження подібних IoT-систем підтримує цифровізацію екологічного моніторингу в містах і промислових регіонах, сприяє зменшенню витрат на традиційний контроль та підвищенню оперативності реагування на екологічні ризики.

Висновки та перспективи

IoT-системи моніторингу екологічних параметрів з інтегрованою візуалізацією даних формують ефективний інструмент для забезпечення стійкого розвитку розумних міст та промислових зон. Аналіз літератури підтверджує їхній високий потенціал для оперативного управління довкіллям, цифрової трансформації та зниження негативного впливу на навколишнє середовище. Перспективи впровадження включають масштабування з використанням 5G/LoRaWAN, інтеграцію з цифровими двійниками міст, розширення предиктивної аналітики на базі AI та створення відкритих громадських дашбордів. Подальші дослідження доцільно зосередити на питаннях кібербезпеки IoT-мереж, енергетичної ефективності сенсорних вузлів та захисту даних [2; 5; 8].

Список використаних джерел

1. Guerbaoui, M., El Faiz, S., Ed-Dahhak, A., Lachhab, A., Benhala, B., Bakziz, Z., Ichou, I., & Selmani, A. (2025). From data to decisions: A smart IoT and cloud approach to environmental monitoring. E3S Web of Conferences, 601, Article 00008. https://doi.org/10.1051/e3sconf/202560100008

2. Mota, A., et al. (2025). Implementation of an Internet of Things architecture to monitor indoor air quality parameters. Sensors, 25(6), 1683. https://doi.org/10.3390/s25061683

3. Ramadan, M. N. A., et al. (2024). Real-time IoT-powered AI system for monitoring and forecasting of air pollution in industrial environment. Ecotoxicology and Environmental Safety. https://doi.org/10.1016/j.ecoenv.2024.

4. Yildiz, O., et al. (2025). Development of real-time IoT-based air quality forecasting system using machine learning approach. Sustainability, 17(19), 8531. https://doi.org/10.3390/su17198531

5. AlSalehy, A. S., et al. (2025). Environmental data analytics for smart cities: A machine learning approach. Smart Cities, 8(3), 90. https://doi.org/10.3390/smartcities8030090

6. Garcia, A., et al. (2025). Advancements in air quality monitoring: A systematic review of IoT-based systems. Artificial Intelligence Review. https://doi.org/10.1007/s10462-025-11277-9

7. Rajesh, M., et al. (2025). Machine learning-driven framework for realtime air quality assessment and health risk prediction. Scientific Reports. https://doi.org/10.1038/s41598-025-14214-6

8. Wijeratne, L. O. H., et al. (2025). The design and deployment of a self-powered, LoRaWAN-enabled air quality monitoring system. Air, 3(1), 9. https://doi.org/10.3390/air3010009

Сокульський Олег Євгенович
доцент, к.т.н.
Військового інституту телекомунікацій та інформатизації імені Героїв Крут
mortimer@ukr.net

Топольськов Євгеній Олександрович
доцент, к.т.н.
Київського національного університету імені Тараса Шевченка
y.topolskov@knu.ua

Москаленко Наталія Володимирівна
асистент
Київського національного університету імені Тараса Шевченка
moskalenkonv@ukr.net

МОВИ ПРОГРАМУВАННЯ ТЕНОЛОГІЙ IoT

В сучасному світі все більше набувають популярності технології IoT, які не тільки підвищують ефективність в промисловості та бізнесі, але й суттєво впливають на якість життя людини. Це може бути автоматизація процесів, дистанційного керування технікою, збору аналітики в реальному часі та інше.

IoT технології можна поділити на наступні складові:

- Збір даних про середовище.
- Передача даних через інрернет(Wi-Fi, Bluetooth, мобільні мережі (5G), LoRaWAN).
- Обробка даних.
- Інтерфейс користувача.

Проект IoT зазвичай включає розробку як апаратного так і програмного забезпечення в кожній зі складових, від якості та співвідношення їх в значній мірі залежить ефективність функціонування та поширення продукту на ринку.

Велика кількість мов програмування може бути використана розробником для рішення задач IoT технологій, але, як свідчить досвід, найбільш ефективними та популярними є наступні:

- **C / C++**. Оскільки збір даних про середовище здійснюється в основному з використанням сенсорів та датчиків, ці мови програмування забезпечують прямий доступ до пам'яті та апаратних ресурсів, що дає можливість отримати найвищу продуктивність на етапі збору даних. Стандарти розробки вбудованих систем (embedded systems) та мікроконтролерів (Arduino, ESP32) також базуються на використанні мов C / C++.
- **Java**. Ця мова існує понад 25 років, популярність якої тримається вже багато років завдяки постійним оновленням, розширення спектру сумісних інструментів, створення нових бібліотек та розширення можливостей. Завдяки кросплаторменності (JVM) ця мова широко використовується в промисловому IoT та великих системах. Використання віртуальної машини забезпечує високий рівень безпеки, надійність та простоту інтеграції з корпоративними системами,
- **JavaScript**. IoT технології використовують різні архітектурні рішення інформаційних систем, але для серверної частини та зв'язку між пристроями у реальному часі використовується саме ця мова програмування, як єдина мова для front-end та back-end.
- **Rust.** Сучасна багатопарадигмова мова програмування загального призначення. Робота над мовою почалася в 2006 році працівником Mozilla Ґрейдоном Гоаром. В 2010 році мова була офіційно представлена. За структурою схожа на C++, але має багато переваг для низькорівневого програмування. На відміну від C++ мова Rust забезпечує автоматичне управління пам'яттю (модель ownership/borrowing без збирача сміття) позбавляючи тим самим використання вказівників, які спричиняють проблеми при низькорівневій роботі з пам'яттю, наприклад, таких як звернення до ділянки пам'яті після її звільнення, розіменовування нульових вказівників, вихід за межі буфера тощо. Мова Rust забезпечує паралелізм, високу продуктивність та підтримує суміш імперактивних, процедурних та об'єктно-орієнтованих методів з такими парадигмами, як фукціональне, узагальнене та метапрограмування, а також

програмування як у статичних так і динамічних стилях. Мова набуває все більшої популярності як ефективна та безпечна альтернатива мові C++ для низькорівневого програмування.

- **Python**. Інтерпретована об’єктно-орієнтована мова програмування високого рівня з жорсткою динамічною типізацією Розроблена на початку 1990-років Гвідо ван Россумом. Структури даних високого рівня, динамічна семантика та зв'язування дозволяють швидко та ефективно здійснювати розробку програм. Мова Python підтримує обєктно-орієнтовану, процедурну, аспектно-орієнтовану та функціональну парадигми програмування. Python має багато бібліотек ,кількість яких постійно збільшується, легка у вивченні та застосуванні, завдяки чому є найкращим вибором для швидкої та ефективної розробки, прототипування, аналізу даних та рішення задач з використанням методів штучного інтелекту.

На етапі створення проектів IoT перед розробниками постає питання вибору мови програмування для ефективного рішення задач. Враховуючи особливості та різноманітність складових проектів .Необхідно зауважити, що тільки комбінація мов програмування може забезпечити якість розробки проектів, наприклад:

- Для мікроконтролерів (Low-level): C / C++.
- Для шлюзів та серверів (Backend): Java, Python, Node.js.
- Для аналітики та штучного інтелекту: Python.
- Для хмарних платформ та аналітики: Python та Java.

Список використаних джерел

1. TajDini, M., & Sokolov, V. (2017). Internet of Things Security Problems. Zenodo. https://doi.org/10.5281/ZENODO.2528814

Що таке Інтернет Речей? – Internet of Things. IoT NULP ukr – Lviv IT Cluster. URL: http://iot.lviv.ua/що-таке-інтернет-речей/

Кравченко Ірина Петрівна
студентка 4 курсу
спеціальності «Комп'ютерна інженерія»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st8070699@stud.duikt.edu.ua

Бученко Ігор Анатолійович
старший викладач кафедри Комп'ютерної інженерії
Державного університету
інформаційно-комунікаційних технологій, м. Київ
i.buchenko@duikt.edu.ua

МЕТОДИ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ IoT-МЕРЕЖ ШЛЯХОМ МІНІМІЗАЦІЇ МАРШРУТИЗАЦІЙНИХ МІКРОПЕТЕЛЬ

Сучасні мережі Інтернету речей (IoT) вимагають високого рівня доступності та мінімального часу затримки, особливо у промислових (IIoT) та медичних сегментах. Однією з головних проблем при відмовах каналів зв'язку є виникнення маршрутизаційних мікропетель (microloops), які спричиняють втрату пакетів та перевантаження каналів під час збіжності протоколів маршрутизації (OSPF/IS-IS).

Для вирішення цієї проблеми пропонується використання технології Loop-Free Alternate (LFA). Алгоритм LFA дозволяє заздалегідь обчислити резервний шлях (Backup Next Hop) до вузла призначення. Основною умовою вибору такого сусіда є нерівність:

$$Distance(N, D) < Distance(N, S) + Distance(S, D)$$

де N – потенційний резервний вузол, D – призначення, S – джерело. Виконання цієї умови гарантує, що резервний вузол не направить трафік назад через джерело, тим самим виключаючи утворення петлі.

Традиційні алгоритми SPF (Shortest Path First) під час збіжності спричиняють ефект «штилю» або масової втрати пакетів. В умовах обмежених ресурсів кінцевих пристроїв IoT (сенсорів, контролерів), повторні запити на передачу даних через мікропетлі призводять до швидкого вичерпання енергоємності автономних датчиків

У роботі розглянуто застосування механізму Remote LFA, який розширює можливості базового LFA у складних топологіях за рахунок використання тунелювання до віддаленого вузла (P-space та Q-space). Це забезпечує захист понад 90% трафіку в IoT-мережах зі складною топологією.

Висновок: впровадження механізмів LFA дозволяє скоротити час збіжності мережі до рівня менше 50 мс, що є критичним для стабільного функціонування критичних сервісів IoT. Це мінімізує вплив мікропетель на якість обслуговування (QoS) та підвищує загальну відмовостійкість інфраструктури.

Список використаних джерел

1. RFC 5286. Basic Specification for IP Fast Reroute: Loop-Free Alternates. IETF, 2008. URL: https://datatracker.ietf.org/doc/html/rfc5286 (дата звернення: 10.04.2026).

2. RFC 7490. Remote Loop-Free Alternate (LFA) Fast Reroute (FRR). IETF, 2015. URL: https://datatracker.ietf.org/doc/html/rfc7490 (дата звернення: 10.04.2026).

3. Stewart B. Loop-Free Alternates: Implementation and Best Practices in Modern ISP Networks. Cisco Press, 2021. 320 p.

Богдан Станіслав Валентинович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st8034580@stud.duikt.edu.ua

Патракеєв Ігор Михайлович
доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ІОТ ЯК ФУНДАМЕНТ ТРАНСФОРМАЦІЇ РОЗУМНИХ МІСТ ТА ПРОМИСЛОВИХ ОБ'ЄКТІВ

Сьогодні концепція «розумного міста» та «цифрового заводу» (Industry 4.0) перестала бути теоретичною. Зростання кількості населення в містах та необхідність зниження собівартості виробництва вимагають автоматизації, яка базується на реальних даних, а не на припущеннях. Інтеграція IoT-рішень дає можливість створити єдину екосистему, де кожен об'єкт – від вуличного ліхтаря до промислового преса – стає джерелом даних. **Основні переваги інтеграції включають:**

Предиктивна аналітика: Моніторинг обладнання в реальному часі дозволяє виявляти несправності до того, як вони призведуть до зупинки конвеєра або аварії на міських електромережах. Так наприклад датчик вологості допоможе запобігти запобігти засуху у теплицях, а сенсори витоку газу в миттєво перекриють подачу палива житлових масивах та сповістять екстрені служби у разі виникнення загрози

Оптимізація ресурсів: Розумні системи керування трафіком можуть зменшувати затори, а інтелектуальне управління енергоспоживанням у промисловості знижує витрати на електрику завдяки автоматичному регулюванню навантаження.

Централізоване адміністрування: Використання сучасних серверних архітектур дає можливість ефективно агрегувати дані з тисяч датчиків, забезпечуючи високу відмовостійкість системи.

Компанія ITenterprice передбачає, що до 2030 року інтернет речей буде застосовуватися в самих різних галузях. Перш за все це промисловість, транспорт, розумний будинок, комунальні служби (мільярд датчиків, істотне зниження втрат енергії), охорону здоров'я, аграрний сектор. Крім того, Інтернет речей буде застосовуватися в торгівлі, логістиці, громадському харчуванні, готельному бізнесі, банківській системі, будівництві та в збройних силах.

Реалізація IoT у масштабах розумного міста чи великого підприємства потребує переходу від хмарних обчислень до моделі Edge Computing . Це дозволяє обробляти критично важливі дані безпосередньо на місці їх виникнення (наприклад, за допомогою серверів HPE ProLiant), що мінімізує затримки в мережі. Такий підхід є вирішальним для систем автономного керування транспортом або автоматизованих систем безпеки, де швидкість реакції вимірюється мілісекундами.

Висновок: Таким чином, IoT для розумних міст та промисловості – це не просто мережа датчиків, а інструмент прийняття управлінських рішень. І це може впливати не тільки на зручність роботи, а й на екологію та оточуюче середовище. І на мою думку головним викликом залишається створення надійної IT-інфраструктури, здатної обробляти великі масиви даних та забезпечувати безпеку критичних вузлів від зовнішніх кіберзагроз.

Список використаних джерел

1. TajDini, M., & Sokolov, V. (2017). Internet of Things Security Problems. Zenodo. https://doi.org/10.5281/ZENODO.2528814

2. Що таке Інтернет Речей? – Internet of Things. IoT NULP ukr – Lviv IT Cluster. URL: http://iot.lviv.ua/що-таке-інтернет-речей/

3. Інтернет речей - Internet of Things, IoT URL: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot

Омелько Яна Вікторівна
студентка 4 курсу
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
omelkoana589@gmail.com

Дальниченко Валентина Миколаївна
PhD, доцент Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
v.danylchenko@duikt.edu.ua

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ РОБОТИЗОВАНИМ МАНІПУЛЯТОРОМ ДЛЯ ВИКОРИСТАННЯ В МЕДИЧНИХ ЛАБОРАТОРІЯХ

Вступ. Сучасний етап розвитку медичної галузі характеризується стрімким зростанням обсягів лабораторних досліджень, що зумовлено підвищенням вимог до якості діагностики, швидкості отримання результатів та безпеки роботи персоналу. Автоматизація лабораторних процесів є одним з ключових напрямків розвитку Healthcare 4.0, який дозволяє суттєво підвищити точність аналізів, зменшити вплив людського фактора та оптимізувати використання ресурсів [1].

В Україні проблема автоматизації медичних лабораторій набуває особливої актуальності через кадровий дефіцит спеціалістів, високе навантаження на існуючі лабораторії та необхідність відповідності міжнародним стандартам якості (ДСТУ EN ISO 15189:2015). Ручна обробка біологічних матеріалів залишається джерелом помилок, ризику контамінації та зниження продуктивності.

Метою даної роботи є розробка автоматизованої системи керування роботизованим маніпулятором, адаптованої до умов медичних лабораторій.

Для досягнення поставленої мети необхідно вирішити такі завдання: провести аналіз існуючих рішень роботизованої автоматизації лабораторій; розробити архітектуру системи керування; створити алгоритми позиціонування, траєкторного руху та розпізнавання об’єктів; реалізувати програмне забезпечення та провести експериментальну перевірку ефективності системи.

Об’єктом дослідження є процеси автоматизації лабораторних операцій у медичних закладах. Предметом дослідження – методи та засоби керування роботизованим маніпулятором у лабораторному середовищі.

Аналіз існуючих рішень та постановка проблеми. Сучасні медичні лабораторії активно використовують автоматизовані системи на базі роботизованих маніпуляторів. Серед провідних рішень виділяються платформи Tecan Freedom EVO та Fluent, Hamilton Microlab STAR, Beckman Coulter Biomek

серії i5/i7. Ці системи забезпечують високу точність дозування рідин, сортування пробірок, транспортування зразків та інтеграцію з аналітичним обладнанням [4, 5].

Перевагами комерційних рішень є висока надійність, вбудовані системи контролю якості, можливість роботи в режимі 24/7 та значне зниження ризику помилок порівняно з ручною працею. Вони ефективно вирішують завдання високопродуктивного скринінгу та рутинних аналізів.

Водночас існують суттєві недоліки. По-перше, висока вартість обладнання та експлуатації робить такі системи недоступними для більшості державних та невеликих приватних лабораторій України. По-друге, комерційні платформи часто мають закриту архітектуру, що ускладнює їх інтеграцію з існуючими лабораторними інформаційними системами (ЛІС) та адаптацію під специфічні робочі процеси. По-третє, спостерігається недостатня гнучкість при роботі в умовах обмеженого лабораторного простору та високих вимог до стерильності [1, 2].

В Україні ситуація ускладнюється додатковими проблемами: недостатнім фінансуванням на модернізацію, труднощами з кваліфікованим обслуговуванням імпортного обладнання та необхідністю відповідності національним регуляторним вимогам. Багато лабораторій продовжують використовувати переважно ручну працю, що призводить до низької продуктивності, втоми персоналу та підвищеного ризику професійних захворювань.

Існує нагальна потреба у розробці власної автоматизованої системи керування роботизованим маніпулятором, яка поєднуватиме прийнятну вартість, відкритість архітектури, високу адаптивність до українських медичних лабораторій та можливість глибокої інтеграції з національними ЛІС. Це дозволить підвищити доступність сучасних технологій автоматизації в медичній галузі України.

Архітектура запропонованої системи. Система керування роботизованим маніпулятором для медичних лабораторій розроблена за модульним принципом і складається з апаратної та програмної частин. Основна мета архітектури – забезпечити високу точність, безпеку, гнучкість та інтеграцію з існуючими лабораторними процесами.

Апаратна частина включає промислового або колаборативного роботизованого маніпулятора, оснащеного системою сенсорів (відеокамери, датчики сили та моменту, RFID-зчитувачі). Обчислювальний модуль представлений industrial PC або потужним Raspberry Pi 5, який виконує функції edge-обробки даних у реальному часі.

Програмна архітектура побудована на базі ROS 2, що дозволяє забезпечити модульність, надійність та масштабованість системи. Передбачена глибока інтеграція з лабораторною інформаційною системою (ЛІС) для автоматичного отримання завдань та логування виконаних операцій.

Рис. 1. Структурна архітектура запропонованої автоматизованої системи

Алгоритми керування та програмна реалізація. Програмна реалізація системи побудована на трирівневій архітектурі керування. На високому рівні виконується планування завдань та взаємодія з ЛІС. Середній рівень відповідає за планування траєкторій руху, кінематичні розрахунки та обробку даних з комп'ютерного зору. Нижній рівень забезпечує безпосереднє керування приводами маніпулятора з використанням алгоритмів зворотного зв'язку.

Для позиціонування використовується математична модель маніпулятора з розрахунком прямої та зворотної кінематики. Алгоритми уникнення перешкод та точного захоплення об'єктів реалізовано за допомогою бібліотеки OpenCV та нейромереж YOLO. Система керування зворотним зв'язком поєднує класичні PID-регулятори з елементами модельного прогнозуючого керування.

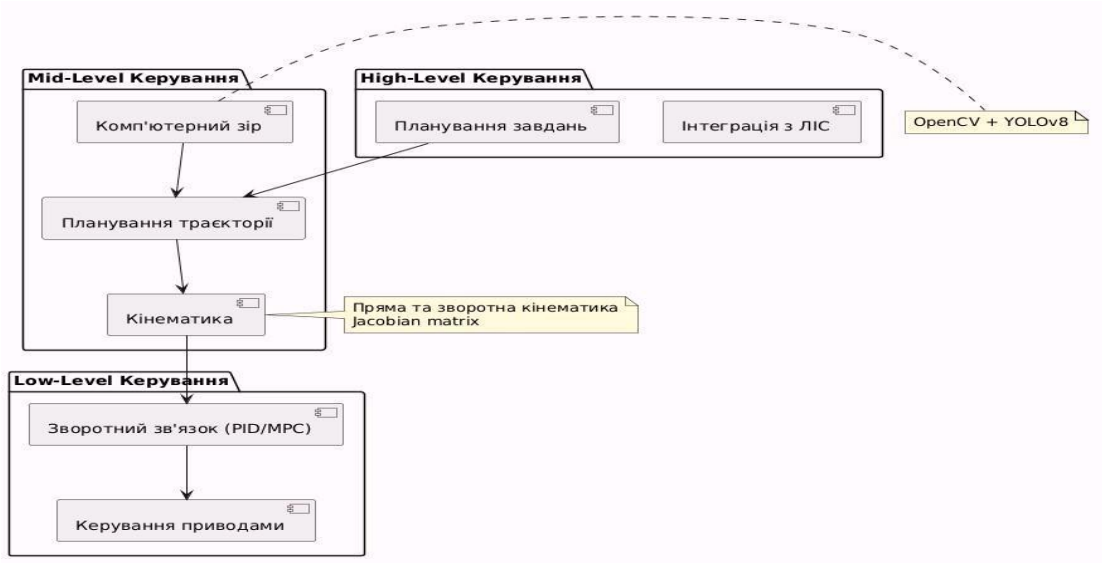

Рис. 2. Архітектура алгоритмів керування

Експериментальні дослідження та результати. Експериментальні дослідження проводилися на лабораторному стенді, що імітує реальні умови медичної лабораторії. Стенд включав колаборативний роботизований маніпулятор UR5e, оснащений системою комп'ютерного зору (камера Intel RealSense D435), датчиками сили та моменту, а також набором стандартного лабораторного обладнання (пробірки, піпетки, мікропланшети).

Обчислювальний модуль базувався на industrial PC з ROS 2.

Випробування здійснювалися за типовими лабораторними операціями: захоплення та транспортування пробірок, точне дозування рідин, переміщення мікропланшетів та сортування зразків. Кожна операція повторювалася 100 разів для забезпечення статистичної достовірності.

Критеріями оцінки ефективності стали: точність позиціонування (мм), час виконання операції (с), коефіцієнт успішності (%) та рівень безпеки (відсутність пошкоджень посуду та контамінації). Результати порівнювалися з ручним методом та комерційними системами.

Табл. 1.

Порівняльні результати точності та продуктивності запропонованої системи

Операція	Ручний метод (точність, мм / час, с / успішність, %)	Запропонована система (точність, мм / час, с / успішність, %)	Покращення (%)
Захоплення та переміщення пробірки	±2,5 / 18 / 92	±0,4 / 7 / 99	68 / 61 / 8
Точне дозування рідини (100 мкл)	±1,8 / 25 / 88	±0,3 / 9 / 98	83 / 64 / 11
Сортування мікропланшетів	±3,0 / 35 / 85	±0,5 / 12 / 97	83 / 66 / 14
Транспортування зразка між модулями	±2,2 / 22 / 90	±0,4 / 8 / 99	82 / 64 / 10

Аналіз результатів показав, що запропонована система забезпечує суттєве підвищення точності (в середньому на 80 %) та продуктивності (скорочення часу виконання на 62–66 %). Коефіцієнт успішності перевищує 97 %, що відповідає вимогам ДСТУ EN ISO 15189:2015. Отримані дані підтверджують ефективність розроблених алгоритмів керування та архітектури системи в реальних лабораторних умовах.

Висновки. У роботі досягнуто поставленої мети – розроблено автоматизовану систему керування роботизованим маніпулятором, адаптовану для використання в медичних лабораторіях. Вирішено всі поставлені завдання: проведено аналіз існуючих рішень, спроєктовано архітектуру системи, розроблено алгоритми керування та програмне забезпечення, а також виконано експериментальну перевірку.

Наукова новизна полягає в створенні модульної відкритої архітектури на базі ROS 2 з інтеграцією комп'ютерного зору та адаптивного керування, орієнтованої на умови українських медичних лабораторій. Практична значущість розробки полягає в можливості суттєвого підвищення точності, продуктивності та безпеки лабораторних досліджень при збереженні прийнятної вартості системи.

Перспективами подальших досліджень є інтеграція штучного інтелекту для адаптивного планування завдань, розширення функціоналу на маніпулятори різних типів та впровадження системи в реальних лабораторіях України.

Список використаних джерел

1. *ДП «УкрНДНЦ». (2016). ДСТУ EN ISO 15189:2015. Медичні лабораторії. Вимоги до якості та компетентності.* https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_ei_ivo_15189_2015.pdf
2. *Кравченко, О. О., Харченко, О. І., & Остапченко, Л. І. (2022). Техніка лабораторних робіт. Київський національний університет імені Тараса Шевченка.* https://biomed.knu.edu.ua/images/stories/Kafedry/Biochimiya/Biblioteka/Tekhnika_laboratornykh_robit.pdf
3. *Conrad, S., Auth, P., Masselter, T., & Speck, T. (2025). Lowering the entrance hurdle for lab automation: An artificial intelligence-supported, interactive robotic arm for automated, repeated testing procedures. Advanced Intelligent Systems, 7, Article 2401086.*
4. *Paw, J. K. O. H. S. (2002). Development of SCARA robotic arm and control system for laboratory automation [Thesis]. Universiti Putra Malaysia.* http://psasir.upm.edu.my/id/eprint/12085/1/FK_2002_51.pdf

НАПРЯМ 4. БЕЗПЕКА В ІОТ-МЕРЕЖАХ

Дьоміна Вікторія Михайлівна
кандидат техн. наук, доцент,
доцент кафедри інформаційних технологій, кібернетики та захисту інформації
Державного біотехнологічного університету, м. Харків
0667217120@btu.kharkov.ua

ІНТЕЛЕКТУАЛЬНЕ ВИЯВЛЕННЯ АНОМАЛІЙ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ МОЛОЧНОЇ ФЕРМИ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Актуальність застосування цифрових технологій у молочному тваринництві визначається необхідністю переходу до прецизійного управління виробничими процесами в умовах зростання вимог до якості продукції, біобезпеки та ефективності використання ресурсів. Традиційні підходи до контролю стану тварин і параметрів середовища мають епізодичний характер і значною мірою залежать від людського фактору, що обмежує можливості своєчасного виявлення прихованих патологій і технологічних відхилень [7]. Інтеграція бездротових сенсорних мереж (БСМ), аналітики даних і методів машинного навчання забезпечує безперервний контроль технологічних параметрів та раннє виявлення аномальних змін, створюючи підґрунтя для підвищення надійності, енергоефективності та економічної результативності молочного виробництва. БСМ формують інфраструктурну основу моніторингу, забезпечуючи розподілений збір, передавання та обробку даних [2].

Водночас ефективність функціонування БСМ обмежується ресурсними характеристиками сенсорних вузлів, зокрема обчислювальною потужністю, енергоспоживанням і пропускною здатністю каналів зв’язку. Спотворенню даних сприяє також наявність кіберзагроз. За цих умов особливої актуальності набуває розроблення методів раннього виявлення аномалій, здатних забезпечити своєчасну ідентифікацію відхилень при збереженні ресурсної ефективності мережі [4].

Мета досліджень полягає у розробленні та обґрунтуванні підходу до інтелектуального виявлення аномалій у бездротових сенсорних мережах молочної ферми на основі методів машинного навчання, зокрема методу опорних векторів, з урахуванням ресурсних обмежень сенсорних вузлів і вимог до достовірності даних.

Основні матеріали досліджень. Інтелектуальні системи моніторингу молочної ферми є складовою концепції точного тваринництва та базуються на інтеграції БСМ, інформаційно-комунікаційних технологій і методів аналізу даних. Для інтелектуалізації даних систем можна використовувати методи машинного навчання, які дозволяють виявляти приховані закономірності й аномальні зміни у даних, що важко своєчасно встановити в межах традиційного візуального або періодичного контролю. Такі методи дають змогу зіставляти

поточні значення фізіологічних, поведінкових і середовищних показників із типовими профілями функціонування системи та виявляти нетипові комбінації ознак, що можуть свідчити про початкові стадії захворювань тварин, порушення мікроклімату, збої в роботі обладнання або аномальну поведінку сенсорних вузлів. На відміну від жорстко заданих порогових правил, алгоритми машинного навчання здатні враховувати багатофакторний характер змін, їх часову динаміку та контекст виробничого процесу [3].

Формування аналітичних висновків у цьому випадку означає перехід від простого накопичення даних до їх інтерпретації у вигляді класифікаційних рішень, оцінок ризику або попереджень про можливі відхилення. Наприклад, на основі сукупності показників активності тварини, температури тіла, параметрів мікроклімату та технологічних характеристик доїння система може не лише зафіксувати зміну окремого параметра, а й встановити, чи має ця зміна ознаки фізіологічної норми, виробничої варіації або потенційно небезпечної аномалії. Рішення базується на узагальнених аналітичних висновках. Це створює передумови для більш своєчасного реагування на критичні ситуації, підвищення достовірності моніторингу та зниження ризику помилкових дій у системах управління молочною фермою [6].

При формалізації задачі виявлення аномалій у багатовимірному просторі ознак є доцільним застосування методів машинного навчання, здатних забезпечити узагальнення за обмеженої вибірки та стійкість до шумів у даних. Одним із таких підходів є метод опорних векторів [8], який базується на побудові оптимальної розділяючої гіперплощини у просторі ознак $w \cdot x + b = 0$, яка максимізує зазор (margin) між двома класами, де w – вектор ваг, b – зсув, x – вектор ознак. Сама оптимізаційна задача має вигляд:

$$\min_{w,b,\xi} \left[\frac{1}{2} \|w\|^2 + c \sum_{i=1}^{n} \xi_i \right]$$

за умов

$$y_i(w \cdot x_i + b) \geq 1 - \xi_i,\ \xi_i \geq 0,$$

де ξ_i – змінні послаблення; C – параметр регуляризації, що визначає компроміс між шириною зазору та штрафом за помилки класифікації; $y_i \in \{-1, +1\}$ – мітки класів; x_i – вектор ознак і-го об’єкта; y_i – класова мітка; w – вектор ваг (нормаль до гіперплощини); b – зсув; $\| w \|$ – евклідова норма вектора ваг.

У випадку лінійно нероздільних даних використовується ядерне перетворення $K(x_i, x_j)$, яке реалізує відображення у простір вищої розмірності без явного обчислення координат. Водночас для задач із обмеженими обчислювальними ресурсами, характерних для вузлів БСМ, доцільним є використання лінійного ядра, що забезпечує нижчу обчислювальну складність.

Для багатокласових задач, зокрема класифікації станів у системах моніторингу, застосовується схема «один проти всіх», у межах якої будується γ двокласових класифікаторів (де Г – кількість класів), кожен із яких відокремлює один клас від усіх інших. Рішення приймається за максимальним значенням функції відгуку:

$$f_\gamma(x) = w_\gamma^T x + b_\gamma, \text{ де } \gamma = 1, \dots, \Г.$$

Правило вибору класу можна сформулювати так: об'єкт відноситься до того класу, для якого відповідний класифікатор дає максимальне значення функції відгуку

$$\hat{y} \ = \arg\max_{\gamma}(w_\gamma^T x + b_\gamma),$$

де $\hat{y}$ – прогнозований (визначений) клас об'єкта; $\arg\max_{\gamma}(.)$ – оператор вибору індексу γ, для якого значення функції є максимальним; γ – індекс класу, $\gamma = 1, \dots, \Г$; w_γ – вектор ваг (параметрів) γ-го класифікатора; x – вектор ознак об'єкта; b_k – зсув γ-го класифікатора; $w_\gamma^T x$ – скалярний добуток, що визначає значення лінійної функції відгуку. Таким чином, метод опорних векторів забезпечує формалізований підхід до класифікації аномалій у багатовимірних даних із контрольованим балансом між точністю та узагальнюючою здатністю, що є важливим для ресурсообмежених БСМ.

Для класифікації аномалій у бездротових сенсорних мережах поряд із методом опорних векторів існують альтернативні підходи, які характеризуються інтерпретованістю та відносною простотою реалізації. Зокрема, дерев рішень – методу класифікації, у межах якого прийняття рішення здійснюється шляхом послідовного розбиття простору ознак на підмножини відповідно до значень окремих параметрів [5]. У задачах моніторингу молочної ферми такий підхід дозволяє класифікувати стан сенсорного вузла або фрагмента даних як нормальний, підозрілий або аномальний на основі сукупності ознак, що характеризують як поведінку вузла, так і параметри середовища. До таких ознак можуть належати рівень довіри до вузла, частота передавання пакетів, відсоток втрачених повідомлень, залишковий заряд батареї, затримка передавання, а також показники фізіологічного чи мікрокліматичного моніторингу. Перевагою дерева рішень є інтерпретованість, оскільки кожне рішення подається у вигляді послідовності логічних правил, однак за високої варіативності даних та динамічності середовища такий метод може бути чутливим до шуму й нестійких локальних змін.

Нехай для кожного сенсорного вузла i БСМ молочної ферми у момент часу t формується вектор ознак

$$x_i\ (t) = \ \big(T_i(t), P_i(t), L_i(t), E_i(t), D_i(t), S_i(t)\big),$$

де $T_i(t)$ – інтегральний показник довіри до вузла; $P_i(t)$ – частка успішно переданих пакетів; $L_i(t)$ – частка втрачених пакетів; $E_i(t)$ – залишковий рівень

енергії вузла; $D_i(t)$ – затримка передавання даних; $S_i(t)$ – узагальнений показник узгодженості сенсорних даних із сусідніми вузлами або з очікуваним технологічним режимом.

Дерево рішень реалізує відображення

$$f: x_i(t) \to y_i(t),$$

де $y_i(t) \in \{K_1, K_2, K_3\}$, а класи K_1, K_2, K_3 відповідають, наприклад, нормальному, ризиковому та аномальному стану вузла.

Кожен внутрішній вузол дерева відповідає перевірці умови виду

$$x_j \leq \theta,$$

де x_j – одна з ознак вектора $x_i(t)$, θ – порогове значення, за яким виконується розбиття множини спостережень.

Якість такого розбиття в задачі класифікації можна визначити через функцію нечистоти, наприклад індекс Джині:

$$G(Q) = 1 - \sum_{m=1}^{M} p_m^2,$$

де Q – множина об'єктів у поточному вузлі дерева; M – кількість класів; p_m – частка об'єктів класу m у множині Q.

Оптимальним вважається таке розбиття, яке мінімізує зважену нечистоту дочірніх підмножин:

$$J(j, \theta) = \frac{|Q_{left}|}{|Q|} G(Q_{left}) + \frac{|Q_{right}|}{|Q|} G(Q_{right}),$$

де Q_{left} – підмножина об'єктів, для яких виконується умова $x_j \leq \theta$; Q_{right} – підмножина об'єктів, для яких $x_j > \theta$; $|Q|$, $|Q_{left}|$, $|Q_{right}|$ – кількість об'єктів у відповідних множинах.

У задачі нашої БСМ молочної ферми це означає, що дерево послідовно вибирає такі ознаки та пороги, які найкраще розділяють вузли з нормальною поведінкою, вузли з підвищеним ризиком та вузли з ознаками аномалій або компрометації. Наприклад, одним із правил може бути перевірка умови низького рівня довіри за одночасного зростання частки втрачених пакетів і затримки передавання, що може свідчити про нестабільну або шкідливу поведінку вузла. Таким чином, дерево рішень у цій постановці виступає інтерпретованим класифікатором станів сенсорних вузлів і може використовуватися як базовий альтернативний підхід до SVM у задачах виявлення аномалій у бездротовій сенсорній мережі молочної ферми.

Потужним інструментом класифікації для даних БСМ молочної ферми, здатним моделювати складні нелінійні залежності між ознаками, є нейронні мережі [1]. У задачах виявлення аномалій вони дозволяють враховувати взаємозв'язки між параметрами вузлів (довіра, затримка, втрата пакетів,

енергетичний стан) та середовищними показниками. Це забезпечує високу точність класифікації навіть за складної структури даних.

Нехай для сенсорного вузла формується вектор ознак $x_i(t) \in \mathbb{R}^n$, тоді вихід нейронної мережі визначається як $y_i = f(x_i;\, W, b)$, де f – функція нейронної мережі, нелінійне відображення, задане композицією шарів; $x_i(t)$ – вектор ознак вузла; W, b – матриці ваг і вектори зсувів; y_i – вихід мережі (ймовірності класів).

На рівні окремого шару:

$$h^l = \sigma\left(W^{(l)}\, h^{(l-1)} + b^{(l)}\right),$$

де $\sigma(\cdot)$ – нелінійна активаційна функція.

Навчання мережі здійснюється шляхом мінімізації функції втрат, наприклад:

$$L = -\sum_i \sum_k y_{ik} \log \hat{y}_{ik},$$

де L – функція втрат; y_{ik} – істинна мітка; $\hat{y}_{ik}$ – прогнозована ймовірність.

Попри високу точність, застосування нейронних мереж у БСМ обмежується значними обчислювальними витратами та енергоспоживанням, що ускладнює їх використання безпосередньо на сенсорних вузлах. Це визначає доцільність використання більш ресурсоефективних методів у розподілених аграрних мережах.

Висновок. Аналіз альтернативних підходів до класифікації аномалій у бездротових сенсорних мережах показує, що дерева рішень забезпечують інтерпретованість і простоту реалізації, однак є чутливими до шумів і нестійких змін у даних, тоді як нейронні мережі демонструють високу точність за рахунок здатності моделювати складні нелінійні залежності, проте потребують значних обчислювальних ресурсів і обсягу навчальних даних. У контексті БСМ молочної ферми, де характерними є обмеження енергоспоживання, обчислювальної потужності та пропускної здатності, зазначені підходи мають обмежену ефективність або потребують додаткової оптимізації.

За цих умов доцільним є використання підходів, орієнтованих не лише на класифікацію даних, а й на оцінювання надійності джерел інформації. Це зумовлює необхідність інтеграції моделей довіри, які дозволяють враховувати поведінкові характеристики сенсорних вузлів, узгодженість переданих даних і історію взаємодії в мережі. Поєднання методів машинного навчання з моделями довіри створює передумови для підвищення стійкості системи до атак, зменшення впливу хибних рішень та забезпечення більш достовірної інтерпретації даних у динамічних умовах функціонування бездротової сенсорної мережі молочної ферми.

Список використаних джерел

1. *Haque A., Chowdhury M. N.-U.-R., Soliman H., Hossen M. S., Fatima T., Ahmed I. Wireless Sensor Networks anomaly detection using machine learning: A survey // arXiv. 2023. URL: https://arxiv.org/abs/2303.08823*
2. *Leliveld L.M.C., Brandolese C., Grotto M., Marinucci A., Fossati N., Lovarelli D., Riva E., Provolo G. Real-time automatic integrated monitoring of barn environment and dairy cattle behaviour: Technical implementation and evaluation on three commercial farms // Computers and Electronics in Agriculture. 2024. Vol. 216. Art. 108499. DOI: 10.1016/j.compag.2023.108499.*
3. *Liu N., Qi J., An X., Wang Y. A Review on Information Technologies Applicable to Precision Dairy Farming: Focus on Behavior, Health Monitoring, and the Precise Feeding of Dairy Cows // Agriculture. 2023. Vol. 13, No. 10. Art. 1858. DOI: 10.3390/agriculture13101858*
4. *Neethirajan S. Safeguarding digital livestock farming – a comprehensive cybersecurity roadmap for dairy and poultry industries // Frontiers in Big Data. 2025. Vol. 8. Art. 1556157. DOI: 10.3389/fdata.2025.1556157.*
5. *Pachauri G., Sharma S. Anomaly Detection in Medical Wireless Sensor Networks using Machine Learning Algorithms // Procedia Computer Science. 2015. Vol. 70. P. 325–333. DOI: 10.1016/j.procs.2015.10.078*
6. *Rifkin R., Klautau A. In Defense of One-Vs-All Classification // Journal of Machine Learning Research. 2004. URL: https://www.jmlr.org/papers/volume5/rifkin04a/rifkin04a.pdf*
7. *Shafi F. B., Ahamed M. F., Nabi M. F., Khandakar A., Rohouma W., Ayari M. A., Thomas K., Rahman A., Reaz M. B. I., Haq F., Refaat S. S. Review of sensor technologies, DC-DC converters, and power electronics for sustainable monitoring in precision livestock farming // Results in Engineering. 2025. Vol. 28. Art. 107975. DOI: 10.1016/j.rineng.2025.107975.*
8. *Tariq H., Majeed M., Ahmad M. Optimizing SVM performance through combinatorial hyperparameter tuning and model selection // International Journal of Bioautomation. 2025. Vol. 29, No. 2. P. 117-144. DOI: 10.7546/ijba.2025.29.2.000981.*

Анісімов Дмитро Олегович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
dmitrikanisimov@gmail.com

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ БЕЗПЕКИ В IOT-МЕРЕЖАХ

Інтернет речей стрімко інтегрується у транспорт, енергетику, промисловість, медицину, освіту та муніципальну інфраструктуру. Таке розширення цифрового середовища забезпечує оперативний збір даних і автоматизацію процесів, проте одночасно збільшує площу атаки, оскільки кожен сенсор, контролер, шлюз або хмарний сервіс стає потенційною точкою несанкціонованого доступу. За цих умов питання безпеки IoT-мереж переходить

із суто технічної площини в стратегічну, а використання штучного інтелекту стає одним із найперспективніших підходів до виявлення та стримування кіберзагроз [2], [4].

Специфіка IoT полягає в неоднорідності пристроїв, обмежених обчислювальних ресурсах, тривалому життєвому циклі обладнання та залежності від безперервного мережевого обміну. Саме тому класичні механізми захисту, які добре працюють у традиційних IT-системах, часто не забезпечують належного рівня стійкості в IoT-середовищі. Серед найтиповіших вразливостей виділяють використання слабких паролів, відсутність безпечного оновлення прошивки, недостатній контроль конфігурацій, неналежний захист телеметрії та відсутність повноцінного журналювання подій [3], [4], [5].

Нормативні підходи NIST, ENISA та ETSI демонструють, що захист IoT має будуватися на принципах security by design і охоплювати весь життєвий цикл продукту: від етапу проєктування до виведення пристрою з експлуатації. Для цього необхідно забезпечити ідентифікацію пристроїв, керування конфігураціями, захист даних у каналах зв'язку й у сховищах, безпечні механізми оновлення, контроль логічного доступу та здатність системи фіксувати власний кібербезпековий стан [2], [4], [5]. Утім, навіть за наявності цих вимог проблема оперативного виявлення нових аномалій залишається актуальною.

Штучний інтелект доповнює базові організаційні та технічні заходи завдяки здатності аналізувати великі потоки телеметрії, знаходити нетипові патерни поведінки пристроїв і виявляти загрози, які не покриваються заздалегідь створеними сигнатурами. Алгоритми машинного навчання застосовують для класифікації мережевого трафіку, виявлення ботнетів, розпізнавання атак типу denial-of-service, аналізу відхилень у роботі сенсорів і побудови систем поведінкової аналітики. Особливу цінність мають підходи, здатні працювати в режимі майже реального часу на edge-рівні, коли рішення ухвалюється без значної затримки та без передачі всіх сирих даних у хмару [1], [6].

На рис. 1 подано узагальнену схему багаторівневого захисту IoT-мережі із застосуванням штучного інтелекту. Її зміст полягає в тому, що первинна фільтрація та сегментація виконуються на рівні шлюзу, а модуль інтелектуального аналізу оцінює телеметрію, виявляє аномалії та передає результати до системи реагування. Такий підхід зменшує навантаження на центральну інфраструктуру та підвищує стійкість системи до масових інцидентів.

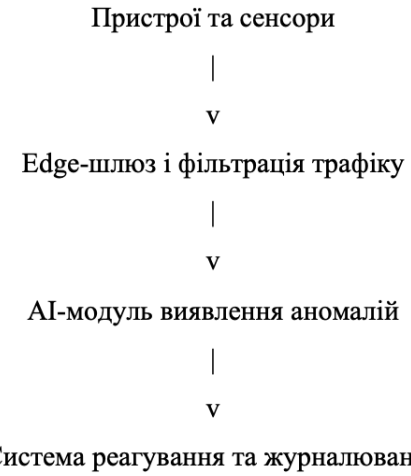

Рис. 1. Узагальнена схема AI-підсиленого захисту IoT-мережі

На практиці для IoT-безпеки застосовують як контрольоване, так і неконтрольоване навчання. Перший підхід доцільний у випадках, коли є розмічені набори даних щодо відомих атак. Другий ефективний для виявлення невідомих або рідкісних відхилень. Окрему увагу привертають федеративне навчання та гібридні моделі, які дозволяють навчати алгоритми на розподілених вузлах без централізованого накопичення чутливих даних. Це особливо важливо для розумних міст, промислових систем і освітніх кампусів, де одночасно працюють тисячі пристроїв із різним рівнем критичності [1], [6].

У табл. 1 наведено порівняння підходів до виявлення загроз в IoT-мережах.

Табл. 1

Порівняння підходів до виявлення загроз в IoT-мережах

Підхід	**Переваги**	**Обмеження**	**Доцільність у IoT**
Сигнатурний IDS	Швидко виявляє відомі сценарії атак	Майже не розпізнає нові патерни загроз	Стабільні середовища з передбачуваним трафіком
Правила та пороги	Простий для впровадження на шлюзах	Дає багато хибних спрацювань у динамічних мережах	Базовий моніторинг сенсорних мереж
ML / DL-аналітика	Виявляє аномалії та невідомі атаки	Потребує якісних даних і додаткових ресурсів	Розумні міста, промислові та кампусні системи
Федеративне / edge AI	Зменшує затримку та ризик витоку сирих даних	Складніше керувати моделями та оновленнями	Розподілені системи з вимогами приватності

Разом з тим впровадження AI-рішень у сфері IoT-безпеки не є безумовно простим. Ефективність моделей залежить від якості датасетів, репрезентативності сценаріїв атак, стійкості до дрейфу даних і рівня обчислювальних ресурсів на периферійних вузлах. Крім того, зростає ризик нових типів впливу, зокрема отруєння навчальних вибірок, adversarial-атак на моделі, помилок інтерпретації результатів і хибних спрацювань, які можуть спричинити небажані операційні наслідки [1], [6]. Саме тому штучний інтелект варто розглядати не як заміну базовим засобам кіберзахисту, а як інтелектуальний шар, що посилює сегментацію, автентифікацію, керування оновленнями та моніторинг.

Для українських організацій, що впроваджують IoT у міському господарстві, на виробництві або в освітньому середовищі, доцільно поєднувати стандартизовані вимоги до пристроїв із поетапним використанням аналітики на основі AI. На першому етапі потрібні інвентаризація всіх IoT-активів, сегментація мережі, заборона типовим обліковим записам, контроль оновлень і журналювання подій. На другому етапі доцільно додавати системи виявлення аномалій на рівні шлюзів і центрів моніторингу, а також оцінювати якість моделей за реальними інцидентами й операційними метриками [2], [3], [4], [5].

Отже, безпека IoT-мереж у сучасних умовах неможлива без поєднання нормативних вимог, захисту за проєктуванням і адаптивної аналітики. Штучний інтелект не усуває потребу у базових кібербезпекових механізмах, однак істотно підвищує здатність системи виявляти нові загрози, скорочувати час реакції на інциденти й підтримувати стійкість цифрової інфраструктури. Саме тому інтеграція AI у контури захисту IoT слід розглядати як важливий напрям подальшого розвитку розумних, безпечних і масштабованих систем [1], [6].

Список використаних джерел

1. Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., & Mahgoub, I. (2025). Machine learning-based security solutions for IoT networks: A comprehensive survey. Sensors, 25(11), Article 3341. https://doi.org/10.3390/s25113341

2. ENISA. (2020). Guidelines for securing the Internet of Things. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

3. ETSI. (2024). ETSI EN 303 645 V3.1.3 (2024-09): Cyber Security for Consumer Internet of Things: Baseline Requirements. European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

4. Fagan, M., Megas, K., Marron, J., Brady, K. G., Cuthill, B. B., Herold, R., Lemire, D., & Hoehn, N. (2021). IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements (NIST SP 800-213). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213

5. Megas, K. N., Fagan, M., Marron, J., Brady, K. G., Cuthill, B. B., Herold, R., Lemire, D., & Hoehn, N. (2021). IoT device cybersecurity guidance for the federal government: IoT device

cybersecurity requirement catalog (NIST SP 800-213A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213A

6. Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. Scientific Reports, 13, Article 21255. https://doi.org/10.1038/s41598-023-46640-9

Васильєв Сергій Олександрович
студент 5 курсу
спеціальності «Комп'ютерна інженерія»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
pro100proserga@gmail.com

Антоненко Артем Васильович
доцент, к.т.н., доцент
кафедри стандартизації та сертифікації сільськогосподарської продукції
Національного університету біоресурсів і природокористування України
artem.v.antonenko@gmail.com

ЗАСТОСУВАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

Стрімкий розвиток концепції Інтернету речей (IoT) охоплює все більше сфер: від концептів розумних міст до автоматизованих промислових систем. Разом зі збільшенням кількості підключених пристроїв експоненційно зростає і кількість потенційних вразливостей інфраструктури. Класична схема IoT-системи [1], що включає кінцеві вузли, мережеве обладнання та хмарні сервери, створює надзвичайно широку поверхню для кібератак (рис. 1).

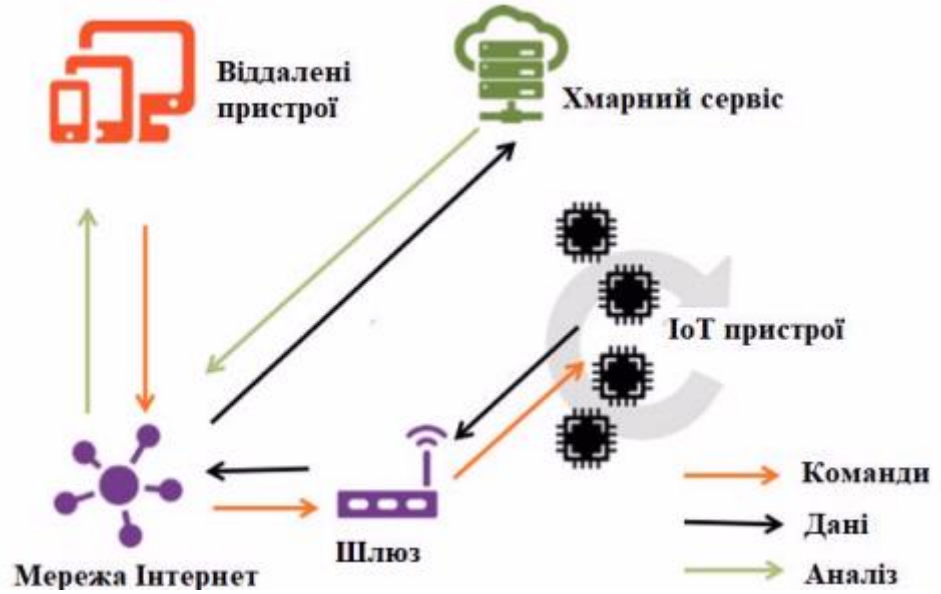

Рис. 1. Класична схема IoT-системи [1]

Традиційні методи забезпечення кібербезпеки, такі як статичні брандмауери та антивірусні програми на основі сигнатур, часто виявляються неефективними в середовищі IoT. Це зумовлено обмеженими обчислювально-енергетичними ресурсами кінцевих пристроїв, різноманітністю протоколів передачі даних та високою динамічністю топології мереж. З огляду на це, критично актуальним стає впровадження інтелектуальних систем виявлення вторгнень (IDS), що базуються на алгоритмах штучного інтелекту (ШІ) та машинного навчання (ML).

Використання моделей ШІ дозволяє аналізувати великі масиви мережевого трафіку (Big Data) в режимі реального часу. На відміну від жорстко заданих правил, нейронні мережі здатні адаптивно виявляти аномалії, які свідчать про несанкціонований доступ, підміну вузлів або розгортання DDoS-атак. Короткий порівняльний аналіз традиційних та інтелектуальних підходів до безпеки наведено в таблиці (табл. 1).

Табл. 1

Порівняльний аналіз методів захисту IoT-мереж

Критерій оцінки	Традиційні методи безпеки	ШІ та машинне навчання
Виявлення загроз	Засноване на відомих сигнатурах	Аналіз поведінки та виявлення аномалій
Адаптивність	Низька (потребує ручного оновлення)	Висока (моделі самонавчаються)
Zero-day атаки	Практично не виявляються	Висока ймовірність предиктивного виявлення
Навантаження	Високе для кінцевих пристроїв	Оптимізоване (обчислення на рівні Edge/Cloud)

Сучасні дослідження підтверджують, що використання ансамблевих алгоритмів класифікації та глибокого навчання (Deep Learning) дозволяє досягти точності виявлення мережевих загроз понад 95% [2]. Інтеграція штучного інтелекту в мережеву архітектуру дозволяє не лише реактивно блокувати відомі загрози, але й предиктивно виявляти нові вектори атак, аналізуючи нестандартні поведінкові патерни підключеної периферії.

Отже, імплементація алгоритмів штучного інтелекту в парадигму кіберзахисту IoT-мереж є не просто інновацією, а необхідним кроком для побудови надійних, відмовостійких систем, здатних превентивно протистояти сучасним викликам інформаційної безпеки.

Список використаних джерел

1. TajDini, M., & Sokolov, V. (2017). Internet of Things Security Problems. Zenodo. https://doi.org/10.5281/ZENODO.2528814

2. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37. URL: https://doi.org/10.1016/j.jnca.2016.10.027.

Тарасенко Мар'яна Романівна
студентка групи ІСДМ-51
Державного університету
інформаційно-комунікаційних технологій
+380501838348
Gunger117@gmail.com

ХАРАКТЕРИСТИКА МЕТОДІВ ДЕТЕКЦІЇ ФІШИНГОВИХ АТАК У ВЕБ-СЕРЕДОВИЩІ

Незважаючи на вдосконалення систем автентифікації та протоколів безпеки, фішинг залишається однією з найбільш поширених та економічно руйнівних загроз у кіберпросторі. Згідно з даними галузевих звітів, кількість фішингових атак щорічно зростає на десятки відсотків, а збитки від них обчислюються мільярдами доларів, що зумовлює високу актуальність досліджень у цій сфері. Складність протидії полягає у постійній адаптації зловмисників: вони використовують техніки соціальної інженерії, приховують шкідливі посилання за легітимними сервісами скорочення URL тощо. Об'єктом даного дослідження виступають сучасні системи виявлення фішингових ресурсів, а предметом - два фундаментальні підходи до детекції: метод блоклистів та метод евристичного аналізу. Метою роботи є порівняльна характеристика ефективності цих методів, виявлення їхніх сильних та слабких сторін, а також обґрунтування необхідності їх комплексного застосування.

Найпоширенішим методом захисту є використання репутаційних списків, які підтримуються такими сервісами, як Google Safe Browsing, VirusTotal або PhishTank. Принцип їхньої роботи полягає у порівнянні адреси веб-ресурсу, який відвідує користувач, із базою даних уже підтверджених фішингових сайтів. Основними перевагами цього підходу є висока швидкість перевірки та практично повна відсутність хибнопозитивних спрацьовувань, оскільки ресурси додаються до списку лише після верифікації експертами або автоматизованими системами. Однак цей метод має критичний недолік – він неефективний проти нових, щойно створених фішингових сайтів, які ще не встигли потрапити до жодного чорного списку. Тривалість такого «вікна вразливості» може становити від кількох хвилин до кількох діб, чого цілком достатньо для успішної атаки на сотні користувачів.

Альтернативою або доповненням до репутаційних списків виступають евристичні методи аналізу. Евристика базується на виявленні характерних ознак фішингу без звернення до зовнішніх баз даних. Алгоритм аналізує параметри веб-сторінки: вік домену, структуру URL-адреси, вміст сторінки, а також наявність та валідність SSL-сертифікатів. Оцінюючи ці фактори за певною шкалою, система ухвалює рішення про блокування ресурсу. Головна перевага евристики полягає у здатності до виявлення нульових загроз, які невідомі антивірусним лабораторіям. Проте цей підхід має й суттєві недоліки: він є ресурсозатратнішим, оскільки потребує часу на аналіз, та схильний до помилок першого роду таких як хибне блокування легітимних сайтів.

В результаті дослідження можна сказати, що жоден із розглянутих методів окремо не здатен забезпечити стовідсотковий захист від фішингових атак. Використання лише репутаційних списків робить систему вразливою до нових атак, тоді як використання лише на евристику може призвести до блокування легітимних ресурсів та збільшення навантаження на обчислювальні потужності. Таким чином, оптимальним підходом на сучасному етапі є комбінування обох методів у гібридні системи захисту. Первинна фільтрація за допомогою швидких репутаційних списків дозволяє відсіяти відомі загрози, після чого підозрілі, але не ідентифіковані ресурси передаються на поглиблений евристичний аналіз. Перспективи подальших досліджень вбачаються у вдосконаленні евристичних алгоритмів із застосуванням методів машинного навчання для зменшення кількості хибних спрацьовувань та підвищення точності виявлення складних, замаскованих фішингових сторінок.

Список використаних джерел

1. *VirusTotal. Режим електронного доступу до ресурсу - https://shorturl.at/kEACS*
2. *Semantic Scholar. Стаття «On the Effectiveness of Techniques to Detect Phishing Sites». Режим електронного доступу до ресурсу -https://shorturl.at/kN6lP.*
3. *Journal of Data Analysis and Information Processing. Стаття в журналі «Effectiveness of Deep Learning Algorithms in Phishing Attack Detection for Cybersecurity Frameworks» Режим електронного доступу до ресурсу - https://shorturl.at/WBrMR.*

Жуков Анатолій Олексійович
старший викладач кафедри
Кафедри інформаційних технологій та кібербезпеки
Житомирського військового інституту
імені С. П. Корольова, м. Житомир
anzhukov@ukr.net

ІНТЕЛЕКТУАЛЬНА СИСТЕМА МОНІТОРИНГУ КІБЕРЗАГРОЗ В IOT СЕРЕДОВИЩАХ

Стрімке впровадження IoT-рішень у критичну інфраструктуру створює нові виклики для кібербезпеки. Як зазначає Weber R. H., архітектура Інтернету речей характеризується фундаментальними проблемами конфіденційності та безпеки через відсутність єдиних стандартів захисту [2]. Обмежені обчислювальні ресурси IoT-пристроїв значно ускладнюють застосування класичних криптографічних і антивірусних механізмів, що зумовлює необхідність розробки нових підходів до захисту.

IoT-системи є привабливою ціллю для кіберзлочинців через велику кількість слабко захищених вузлів. Яскравим прикладом є ботнет Mirai, який продемонстрував можливість масового використання IoT-пристроїв для DDoS-атак [3].

Згідно з класифікацією Alaba F. A., загрози охоплюють рівні пристроїв, мережі, хмарних сервісів та додатків [5].

Особливу небезпеку становлять побутові IoT-пристрої, які часто мають слабкі паролі та застаріле програмне забезпечення, що робить їх “точками входу” для атак на локальні мережі.

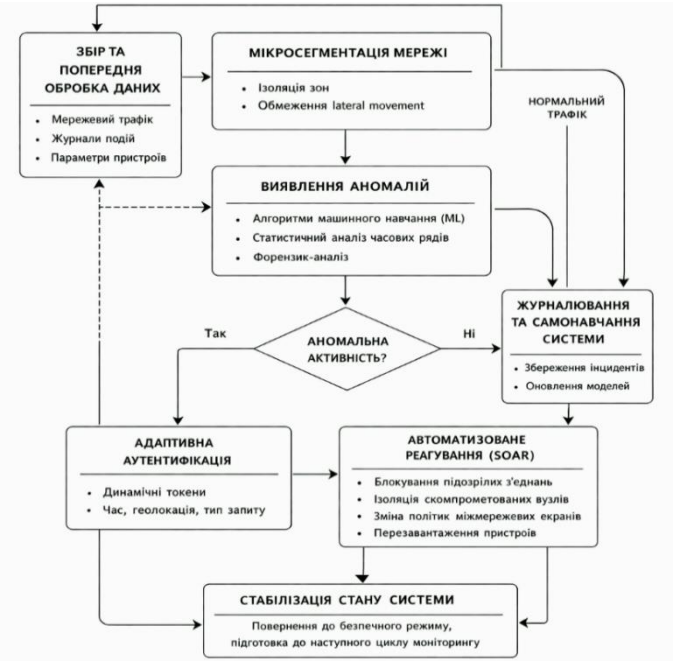

Рис. 1. Архітектура інтелектуальної системи попередження кіберзагроз у розподілених IoT-середовищах

З метою мінімізації часу реагування на інциденти та підвищення ефективності виявлення загроз у роботі запропоновано багаторівнева модель попередження кіберзагроз, що базується на поєднанні периферійних обчислень Edge Computing, інтелектуального аналізу трафіку та автоматизованого реагування (рис. 1).

Використання концепції Edge Computing дозволяє реалізувати механізми безпеки безпосередньо на периферії мережі, тобто ближче до джерела генерації даних. Це суттєво знижує затримки передачі інформації та забезпечує оперативне реагування на інциденти. Такий підхід є ключовим для формування так званого «ланцюжка довіри» у розподілених системах, оскільки централізований аналіз кожного пакета призводив би до критичних затримок у високонавантажених IoT-середовищах [1]. Водночас впровадження проміжного рівня туманних обчислень дозволяє вирішити специфічні проблеми масштабованості та конфіденційності, притаманні розподіленим системам [7].

Запропонований метод включає наступні етапи:

1. Збір та попередня обробка даних. На цьому етапі здійснюється агрегація телеметричних даних (мережевий трафік, журнали подій, параметри пристроїв). Первинна обробка виконується на Edge-вузлах, що дозволяє фільтрувати нерелевантні дані та зменшити навантаження на центральні компоненти системи.

2. Мікросегментація мережі. IoT-мережа розподіляється на ізольовані сегменти відповідно до функціональних ролей пристроїв. Такий підхід обмежує можливість горизонтального переміщення (lateral movement) зловмисника у разі компрометації одного з вузлів та локалізує інцидент у межах окремого сегмента.

3. Інтелектуальний аналіз та виявлення аномалій. Виявлення загроз у реальному часі базується на інтелектуальному аналізі мережевого трафіку та поведінкових характеристик системи [6]. Для цього застосовуються:

- статистичні методи аналізу часових рядів;
- алгоритми машинного навчання;
- поведінкові моделі (виявлення нетипових шаблонів активності).

У зв'язку з постійною еволюцією кіберзагроз особливого значення набуває форензик-аналіз IoT-середовищ, який дозволяє ідентифікувати приховані закономірності атак та підвищити точність моделей виявлення [4].

4. Адаптивна аутентифікація та контроль доступу. У разі виявлення підозрілої активності система переходить до механізмів адаптивної автентифікації. Доступ до ресурсів надається з урахуванням контексту (час доступу, геолокація, поведінкові характеристики пристрою, тип запиту). Використання динамічних токенів та політик доступу дозволяє значно знизити ризик несанкціонованого втручання.

5. Автоматизоване реагування (SOAR). На основі результатів аналізу система автоматично визначає рівень загрози та ініціює відповідні дії реагування.

6. Журналювання та самонавчання системи. Інформація про виявлені інциденти накопичується у централізованих або розподілених сховищах для подальшого аналізу. Отримані дані використовуються для до навчання моделей та підвищення ефективності виявлення нових типів атак.

Запропонований підхід є ефективним для захисту критичної інфраструктури, промислових середовищ, систем «розумного міста» та побутових мереж. Використання інтелектуального аналізу, алгоритмів машинного навчання та форензик-підходів дозволяє точно ідентифікувати складні та приховані загрози, включно з атаками zero-day, мінімізуючи при цьому кількість хибних спрацювань.

Гібридна архітектура забезпечує високу масштабованість і адаптивність до зростаючих обсягів трафіку. Додаткове впровадження мікросегментації дозволяє локалізувати інциденти в межах окремих сегментів, запобігаючи компрометації всієї інфраструктури, що критично важливо для стабільної роботи систем реального часу.

Список використаних джерел

1. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 2015.

2. Weber R. H. Internet of Things – New security and privacy challenges. Computer Law & Security Review, 2010.

3. Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and other botnets. IEEE Computer, 2017.

4. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 2018.

5. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications, 2017.

6. Mothukuri V., et al. A survey on security and privacy of federated learning. Future Generation Computer Systems, 2021, 115, pp. 619–640.

7. Alrawais A., et al. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 2017, 21(2), pp. 34–42.

Федоров Любомир Володимирович
студент групи ІСД- 42
Державного університету
інформаційно-комунікаційних технологій, м. Київ
(099)-339-10-52
lyubomir.fedorov@gmail.com

Козлов Дмитро Євгенович
PhD, доцент кафедри Інформаційних систем та технологій Державного університету
інформаційно-комунікаційних технологій, м. Київ

МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ IOT-МЕРЕЖ НА ОСНОВІ АРХІТЕКТУРИ ZERO TRUST

Інтернет речей - це широка сфера технологічного прогресу, яка активно розвивається останні 15 років. IoT являє собою систему взаємопов'язаних пристроїв, підключених до глобальної мережі, які збирають, обробляють та передають дані. Проте незважаючи на цей високий потенціал, невід'ємним супутником є значні виклики в кібербезпеці.

Стрімке зростання кількості взаємопов'язаних пристроїв викликає занепокоєння з приводу безпеки й конфіденційності переданих та отриманих даних, а також цілісності програмної складової самого пристрою IoT. Ця проблема виникає через те, що велика частка пристроїв IoT мають лімітовані ресурси та функціональність, що робить їх вразливішими до кібератак. На відміну від звичайних побутових приладів, вузли мережі Інтернету речей зазвичай опрацьовують конфіденційну інформацію маючи стандартні налаштування , що створює площину у якій кіберзловмисники можуть експлуатувати вразливості з метою отримати несанкціонований доступ до персональних даних чи встановити контроль над пристроями. Аналітика свідчить про те, що кількість девайсів, підключених до Інтернету речей, стрімко зростатиме в найближчі роки. Все більше галузей та бізнес сфер впроваджуватимуть IoT для підвищення ефективності та конкурентоспроможності. У 2022 році ринок безпеки Інтернету речей оцінювався в понад п'ять мільярдів доларів США, і, за прогнозами, до кінця 2027 року він зросте в чотири рази. Зростання кількості пристроїв Інтернету речей призвело до різкого збільшення кількості та різноманітності кібератак, оскільки вся мережа безпеки

компанії може бути значно ослаблена через відсутність заходів або неправильно впроваджені політики.

Постановка задачі

З огляду на вищезазначене, ключовий бар'єр у побудові безпечних IoT-середовищ полягає у застосуванні застарілих оборонних парадигм. Класичні стратегії здебільшого спираються на ідею “довіреного периметра”, де легітимність пристрою підтверджується виключно фактом його знаходження у локальній мережі. В епоху масового розгортання вразливих IoT-компонентів ця концепція зазнає краху. Після успішного злому навіть найпростішого крайового датчика зловмисник отримує можливість безперешкодно рухатися інфраструктурою по горизонталі , ставлячи під удар усю систему в цілому, попри захищеність зовнішнього контуру.

Мета дослідження

Головна мета роботи полягає у модернізації механізмів захисту IoT-інфраструктур за рахунок інтеграції адаптивного контролю доступу, що спирається на парадигму Zero Trust. Відповідно до поставленої мети, визначено наступні завдання:

дослідити критичні вразливості традиційних довірчих контурів у просторі Інтернету речей;

аргументувати необхідність використання архітектури нульової довіри , яка вимагає обов'язкової попередньої автентифікації будь-якого мережевого вузла в процесі мережевої взаємодії, ігноруючи його фізичну чи логічну топологію;

розробити підхід до динамічного регулювання прав доступу з метою ізоляції сегментів та безперервної верифікації смарт-пристроїв, враховуючи обмеженість енергетичних і обчислювальних ресурсів.

Результати дослідження

Основним здобутком роботи є концептуалізація нової безпекової моделі для IoT-систем, фундаментом якої слугує Zero Trust Architecture. Замість статичних правил застосовано атрибутивний метод контролю (ABAC), який спирається на перманентний моніторинг поведінки вузлів та постійну актуалізацію рівня довіри.

Запропонований фреймворк об'єднує п'ять базових інструментів. Прийняття ключових рішень щодо авторизації делеговано центральному модулю PDP (Policy Decision Point), який аналізує контекстні параметри, **зокрема** ризики, геолокацію та тип обладнання і може розгортатися у контейнеризованих середовищах типу Kubernetes. Виконавчою ланкою виступає спеціалізований шлюз PEP (Policy Enforcement Point), що реалізує команди центрального модуля на практиці, відповідаючи за шифрування, управління якістю обслуговування та ізоляцію підозрілих елементів. За ідентифікацію відповідає брокер IDP (Identity Provider), який оперує сучасними токенами і формує первинні атрибути. Водночас модуль телеметрії TM (Telemetry Monitor) агрегує статистику навантажень та API-звернень, передаючи її до аналітичного ядра TE (Trust Engine). Останнє в свою чергу , застосовуючи поведінкові патерни, генерує актуальний індекс довіри.

Функціонування системи є циклічним: після первинної валідації через постачальника ідентифікації, подальший доступ регулюється PDP з постійною

оглядкою на оцінки ТЕ. Будь-які аномалії в телеметрії призводять до знаження показника довіри, змушуючи мережевий шлюз миттєво обмежувати права пристрою або повністю блокувати скомпрометований вузол. Оцінка моделі доводить її здатність критично зменшити ймовірність горизонтальних атак завдяки динамічній валідації кожної сесії. Разом з тим, існують певні апаратні обмеження: концентрація перевірок на шлюзі PEP генерує ризик утворення єдиної точки відмови, а повноцінне виявлення складних атак вимагає додаткової синхронізації з платформами класу SIEM.

Висновки та преспективи

Підсумовуючи результати, варто зазначити, що міграція на стандарти Zero Trust є безальтернативним вектором розвитку для подолання безпекової кризи в сучасних різнорідних IoT-мережах. Інтеграція механізмів ABAC та гнучкого індикатора Trust Score остаточно руйнує застарілу концепцію безпечного периметра, замінюючи її принципом перманентної недовіри. Завдяки взаємодії центрів прийняття та виконання рішень кожен сеанс зв'язку трактується як потенційна загроза. Це позбавляє зловмисника простору для маневру та блокує переміщення зловмисника між вузлами всередині мережі навіть за умови успішного захоплення одиничного сенсора, що особливо корисно у промисловості, де злам одного датчика не повинен приводити до звупинки цілої виробничої лінії.

Попри отримані переваги, архітектура стикається з проблемою перевантаження контролюючих шлюзів та складністю впровадження зовнішнього моніторингу. У подальших наукових роботах доцільно сфокусуватися на застосуванні нейромереж для предиктивного виявлення поведінкових аномалій, а також на створенні оптимізованих криптографічних протоколів, здатних функціонувати на ультрабюджетних контролерах у парадигмі нульової довіри.

Список використаних джерел

1. *Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень / Ю. Костюк та ін. Кібербезпека: освіта, наука, техніка. 2025. Т. 4, № 28. С. 633–655.*
2. *Коваленко О. В., Мельник А. О. Аналіз сучасних загроз та методів забезпечення кібербезпеки в системах Інтернету речей (IoT). Захист інформації. 2023. Т. 25, № 2. С. 112–120.*
3. *Zero Trust Architecture / S. Rose et al. National Institute of Standards and Technology, 2020. 59 p. URL: https://doi.org/10.6028/NIST.SP.800-207.*

Поперешняк Тимофій Дмитрович
ліцеїст взводу 10.21
Волинського обласного ліцею з посиленою військово-фізичною підготовкою
імені Героїв Небесної Сотні, м. Ковель
t.popereshniak@gmail.com

Папіровий Дмитро Валентинович
студент 4 курсу, групи ТСД-42
Державного університету інформаційно-комунікаційних технологій, м. Київ
papirivii@gmail.com

МЕТОДИ ПІДВИЩЕННЯ ЯКОСТІ БЕЗПЕКИ В ІОТ-МЕРЕЖАХ

У сучасних умовах стрімкого розвитку Internet of Things питання забезпечення безпеки мереж набуває особливої актуальності, що зумовлено зростанням кількості підключених пристроїв, їх гетерогенністю та підвищеною вразливістю до кіберзагроз. Особливістю IoT-інфраструктур є обмежені обчислювальні ресурси кінцевих вузлів, що ускладнює застосування традиційних засобів захисту та потребує використання адаптивних і легковагових механізмів контролю безпеки. У цьому контексті перспективним напрямом є впровадження систем виявлення вторгнень, зокрема безпроводових, які забезпечують моніторинг мережевої активності в реальному часі та дозволяють виявляти як відомі, так і нові типи атак.

У запропонованому підході розглядається архітектура безпроводової системи виявлення вторгнень, що базується на інтеграції розподілених сенсорних елементів, точок доступу та централізованих засобів обробки інформації (рис. 1). Сенсори та клієнтські пристрої здійснюють збір первинних даних про мережеву активність, включаючи параметри трафіку, частоту запитів та поведінкові характеристики вузлів. Точки доступу виступають як проміжні вузли агрегації, забезпечуючи передачу даних до центрального сервера управління системою виявлення вторгнень.

На рівні сервера реалізується аналітичний модуль, який здійснює обробку отриманої інформації з використанням методів статистичного аналізу та алгоритмів машинного навчання. Це дозволяє формувати поведінкові моделі нормального функціонування мережі та виявляти відхилення, що можуть свідчити про наявність загроз. Консоль управління забезпечує візуалізацію результатів аналізу, підтримує процес прийняття рішень та дозволяє оперативно реагувати на інциденти безпеки.

Запропонована архітектура характеризується модульністю та масштабованістю, що дозволяє адаптувати її до мереж різного розміру та складності. Розподілений характер збору даних сприяє зменшенню навантаження на окремі вузли та підвищує надійність системи в цілому. Водночас централізований аналіз забезпечує узгодженість прийняття рішень і підвищує точність виявлення аномалій.

Рис. 1. Архітектура безпроводової системи виявлення вторгнень

Використання безпроводових систем виявлення вторгнень дозволяє підвищити рівень захищеності мереж за рахунок своєчасного виявлення підозрілої активності, зниження часу реагування на інциденти та можливості інтеграції з іншими компонентами систем кібербезпеки. Таким чином, запропонований підхід є ефективним інструментом забезпечення інформаційної безпеки в умовах зростаючої складності та динамічності сучасних мережевих середовищ.

Перспективи подальших досліджень пов’язані з удосконаленням методів аналізу аномалій шляхом застосування більш складних моделей машинного навчання, зокрема глибоких нейронних мереж, а також із розробкою розподілених архітектур обробки даних безпосередньо на рівні IoT-пристроїв (edge computing). Важливим напрямом є підвищення точності виявлення загроз при одночасному зменшенні кількості хибних спрацювань, а також тестування запропонованих підходів на реальних мережевих даних. Окрему увагу доцільно приділити інтеграції систем виявлення вторгнень із комплексними платформами кібербезпеки та адаптації їх до умов високодинамічних мережевих середовищ.

Список використаних джерел

1. Alsoufi M. A., Siraj M. M., Ghaleb F. A., Al-Razgan M., Al-Asaly M. S. et al. Anomaly-Based Intrusion Detection Model Using Deep Learning for IoT Networks // Computer Modeling in Engineering & Sciences. – 2024. – Vol. 141, No. 1. – P. 823–845. – DOI: 10.32604/cmes.2024.052112. techscience.com

2. Nguyen T. M., Vo H. H.-P., Yoo M. Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach // Sensors. – 2024. – Vol. 24, No. 11. – Art. 3339. – DOI: 10.3390/s24113339.

Бачков Володимир Андрійович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
vladimir.bachkov@gmail.com

ПІДВИЩЕННЯ СТІЙКОСТІ КОРПОРАТИВНИХ МЕРЕЖ ДО ТЕРМІЧНИХ ЗАГРОЗ ЗА ДОПОМОГОЮ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ МОНІТОРИНГУ НА БАЗІ IOT

Сучасна корпоративна мережа критично залежить від стабільного функціонування серверного обладнання, де термічні аномалії становлять серйозну загрозу доступності даних та цілісності інфраструктури. Дослідження Villegas-Ch та співавторів присвячене розробці системи інтелектуального моніторингу на базі IoT, що поєднує збір даних у реальному часі з предиктивною аналітикою [1]. Вимірюваним результатом роботи стала точність виявлення температурних аномалій на рівні 98,7%, що дозволило системі ідентифікувати потенційні проблеми задовго до виникнення критичних відмов. Значення цього дослідження полягає у переході від реактивного до проактивного управління, що забезпечує стабільність промислових та IT-середовищ через механізми постійного навчання алгоритмів на основі зворотного зв'язку.

Еволюція безпеки в IoT-мережах станом на 2025 рік характеризується зміщенням фокусу з автоматизації процесів на розвиток предиктивних спроможностей захисту. Суть цього підходу полягає у використанні штучного інтелекту як фундаменту для стратегії Zero Trust, де моніторинг фізичних параметрів середовища стає інструментом верифікації безпечного стану критичної інфраструктури. Вимірюваним результатом є підвищення стійкості мереж до інцидентів через завчасне передбачення загроз, що дозволяє розглядати термічний контроль як невід'ємну частину загальної архітектури кібербезпеки.

Комплексний аналіз рішень на базі машинного навчання (ML), проведений Alfahaid та колегами, демонструє ефективність використання рекурентних нейронних мереж (RNN) та алгоритмів GRU для аналізу часових рядів у IoT-середовищах. Дослідники наводять результати, згідно з якими ансамблеві моделі досягають точності у 99,7% при виявленні аномалій та загроз доступності, спричинених перевантаженням вузлів. Значення даного огляду полягає у систематизації методів глибокого навчання (DL) для забезпечення стійкості розподілених мереж та класифікації термічних загроз як векторів атак на відмову в обслуговуванні.

Критичний аналіз наведених джерел дозволяє виявити ряд невирішених питань. По-перше, незважаючи на високу точність прогнозування, залишається відкритим питання інтеграції предиктивних моделей із локальними механізмами

адаптивного точкового охолодження в умовах динамічного навантаження. По-друге, в існуючих роботах недостатньо уваги приділено захисту самої системи моніторингу від ін'єкцій хибних термічних даних, що може бути використано зловмисниками для навмисного вимкнення охолодження. Основними об'єктивними причинами такого стану є висока обчислювальна складність інтелектуальних алгоритмів для виконання на периферійних (Edge) пристроях та обмеженість ресурсів IoT-вузлів. Суб'єктивним чинником є традиційний поділ досліджень на галузь системного адміністрування (моніторинг працездатності) та інформаційну безпеку (захист від атак), що перешкоджає створенню єдиних стійких архітектур. Систематизація цих локальних проблем вказує на відсутність цілісного підходу, який би поєднував предиктивний тепловий контроль із захищеною передачею даних та автоматизованим керуванням охолодженням. Отже, загальною невирішеною проблемою є відсутність архітектурних рішень для підвищення теплової стійкості корпоративних мереж, які б інтегрували інтелектуальне прогнозування станів із захищеними механізмами оперативного реагування на термічні загрози.

Архітектурна концепція пропонованої системи базується на інтеграції мережі IoT-датчиків із предиктивною моделлю обробки часових рядів для динамічного керування мікрокліматом серверних приміщень. Функціонування рішення реалізується через багаторівневу модель, де фізичний рівень представлений розподіленими вузлами сенсорів, що фіксують термічні показники в реальному часі.

Центральним елементом аналітичного блоку є рекурентна нейронна мережа з архітектурою Gated Recurrent Unit (GRU), що спеціалізується на виявленні довгострокових залежностей у послідовностях даних. На відміну від традиційних порогових систем, інтелектуальний алгоритм здійснює екстраполяцію значень температури на заданий горизонт планування. Це дозволяє реалізувати стратегію випереджального (проактивного) впливу: у разі виявлення тенденції до перевищення допустимих значень, система ініціює локальне посилення охолодження окремих зон до моменту фактичного настання критичного перегріву.

Програмна реалізація, виконана з використанням інструментарію Python, передбачає візуалізацію процесів у вигляді динамічних теплових карт (heatmaps). Такий підхід забезпечує точкову адаптацію потужностей охолодження до конкретних стійок з високою щільністю обладнання, мінімізуючи надмірне використання енергоресурсів у зонах з низьким навантаженням. Порівняльний аналіз функціонування інфраструктури за участю штучного інтелекту та без нього демонструє суттєве згладжування амплітуди температурних коливань та запобігання тепловому стресу серверного парку.

Список використаних джерел

1. Villegas-Ch, W., García-Ortiz, J., & Sánchez-Viteri, S. (2024). Towards Intelligent Monitoring in IoT: AI Applications for Real-Time Analysis and Prediction. IEEE Access, 1. https://doi.org/10.1109/access.2024.3376707

2. AI IoT Security: How AI Changed Automation in 2025 - Device Authority. Device Authority. https://deviceauthority.com/ai-iot-security-how-ai-changed-automation-in-2025/

3. Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., & Mahgoub, I. (2025). Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey. Sensors, 25(11), 3341. https://doi.org/10.3390/s25113341

Фесенко Андрій Олегович
студент групи ТЦР-41
Державного університету інформаційно-комунікаційних технологій,м. Київ
st7988269@stud.duikt.edu.ua

Поперешняк Світлана Володимирівна
доцент кафедри Інформатики та програмної інженерії
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського", м. Київ
spopereshnyak@gmail.com

ПРИКЛАДНІ АСПЕКТИ БЕЗПЕКИ IoT-МЕРЕЖ

На даний момент відомо, що кількість підключених IoT-пристроїв на сьогодні перевищують 75 мілярдів. Швидке розповсюдження технологій Інтернету речей супроводжується появою нових уразливостей та кіберзагроз, які потребують комплексного аналізу та розробки ефективних методів захисту. На сучасному етапі IoT активно впроваджується у системах «розумного дому», транспорті, медицині, логістиці, промисловості, енергетиці та міській інфраструктурі. Водночас розширення сфер застосування IoT супроводжується зростанням кількості кіберризиків, що робить проблему безпеки IoT-мереж надзвичайно актуальною [1].

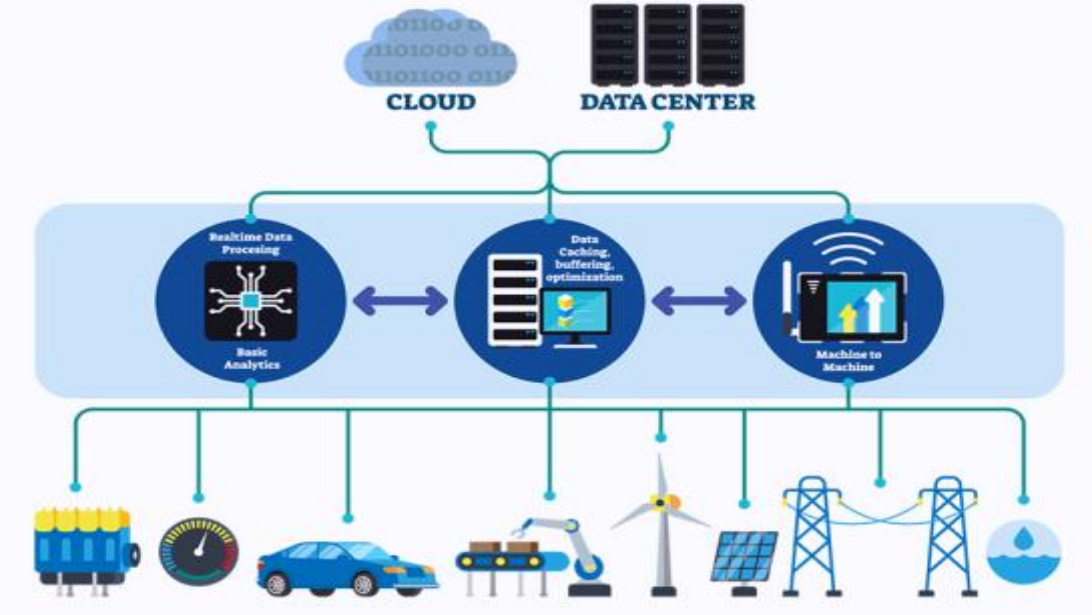

Рис. 1. Сфери застосування IoT

Актуальність дослідження зумовлена тим, що IoT-мережі поєднують велику кількість різнорідних пристроїв, які часто мають обмежені апаратні ресурси, спрощені механізми захисту та недостатній рівень програмної підтримки. Унаслідок цього вони стають потенційно вразливими до несанкціонованого доступу, перехоплення даних, шкідливого програмного впливу та мережевих атак. Як показують сучасні дослідження, питання захисту IoT-систем потребує комплексного підходу, який охоплює як технічні, так і організаційні засоби кібербезпеки [2]. Однією з головних особливостей IoT-мереж є їх багаторівнева структура. Типова IoT-система включає рівень сенсорів і виконавчих пристроїв, мережевий рівень передавання даних та прикладний рівень, де здійснюється обробка й використання інформації. Кожен із цих рівнів має власні вразливості. Наприклад, на рівні пристроїв можливі фізичне втручання, підміна вузлів або зчитування конфіденційної інформації. На мережевому рівні виникають ризики перехоплення трафіку, атак типу «людина посередині» та відмови в обслуговуванні. На прикладному рівні небезпеку становлять помилки автентифікації, порушення конфіденційності даних і вразливості програмного забезпечення [3].

Табл. 1.

Основні загрози IoT-мереж

Загроза	**Спосіб захисту**
Несанкціонований доступ	Надійна автентифікація, складні паролі
Перехоплення данних	Шифрування інформації
Ботнет-атаки	Оновлення пз, моніторинг активності
Уразливості firmware	Регулярне оновлення та перевірка пристроїв

Важливу небезпеку становить також використання IoT-пристроїв у ботнет-мережах. Через слабкий рівень захисту та відсутність регулярних оновлень велика кількість пристроїв може бути заражена шкідливим програмним забезпеченням і використана для DDoS-атак, розсилання шкідливого трафіку або несанкціонованого сканування інших систем. Такі інциденти підтверджують, що IoT-пристрої можуть виступати не лише об'єктами атак, а й інструментами для їх реалізації [4].

Безпека IoT-мереж є критично важливою умовою надійного функціонування сучасних цифрових систем. Основними загрозами для IoT-середовища є несанкціонований доступ до пристроїв, перехоплення даних, ботнет-атаки та вразливості програмного забезпечення. Ефективний захист IoT-мереж можливий лише за умови реалізації комплексного підходу, що включає надійну автентифікацію, криптографічний захист, оновлення програмного забезпечення, сегментацію мережі та моніторинг активності тощо.

Список використаних джерел

1. Гайдур Г. І., Шулімова Д. Д., Бойко А. О., Постніков Є. І. Модель забезпечення кібербезпеки Інтернету речей. Телекомунікаційні та інформаційні технології. 2024. № 2. https://tit.dut.edu.ua/index.php/telecommunication/article/view/2524

2. Руденко Н. В., Луцюк І. В., Сутик А. П. Дослідження безпеки та приватності систем Інтернету речей у мережах мобільного зв'язку. Зв'язок. 2023.https://con.dut.edu.ua/index.php/communication/article/view/2728

3. Лісовий І. В., Войтович О. П., Волинець О. Ю. Рекомендації забезпечення безпеки бездротових з'єднань Інтернету речей. 2024. https://ir.lib.vntu.edu.ua/handle/123456789/41938

4. Жидка О. В., Андрійченко Т. Р. Інформаційна безпека систем IoT. Зв'язок. 2024. https://con.dut.edu.ua/index.php/communication/article/view/2794

Степура Владислав Олегович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
st7936235@stud.duikt.edu.ua

ІНТЕЛЕКТУАЛЬНИЙ МОНІТОРИНГ МЕРЕЖЕВИХ АНОМАЛІЙ ЯК БАЗОВИЙ ЕЛЕМЕНТ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Стрімкий розвиток Інтернету речей (IoT) призводить до того, що нас оточує дедалі більше підключених пристроїв. Оскільки всі вони дуже різні за своїм типом і призначенням, мережі стають складнішими, а їх захист – важчим. Чим

більше в мережі гаджетів, тим більше потенційних лазівок з'являється для зловмисників [1].

Головна проблема полягає в тому, що більшість IoT-пристроїв мають слабкі процесори та мало пам'яті. Через це на них неможливо встановити повноцінний антивірус чи локальну систему захисту [2]. Тому найдієвішим рішенням стає централізований аналіз усього мережевого трафіку.

Найкраще з цим завданням справляються розумні системи моніторингу. Вони вивчають, як пристрої поводяться у звичайному режимі, і створюють так звану модель нормальної поведінки. Оскільки IoT-гаджети зазвичай передають дані за чітким розкладом, будь-які відхилення – наприклад, різкі стрибки трафіку чи звернення до невідомих серверів – одразу викликають підозру.

На відміну від класичних антивірусів, які шукають лише відомі загрози, системи виявлення аномалій здатні знаходити абсолютно нові атаки. Завдяки алгоритмам машинного навчання вони підлаштовуються під зміни в мережі та помічають приховані небезпеки [1].

Якщо система бачить щось підозріле, вона може миттєво згенерувати сповіщення або автоматично заблокувати скомпрометований пристрій. Це допомагає зупинити атаку на ранньому етапі та мінімізувати шкоду.

Висновки. Інтелектуальний моніторинг трафіку – це необхідна основа для безпеки IoT. Поєднання централізованого контролю та машинного навчання дає змогу захищати мережу проактивно, виявляючи загрози до того, як вони завдадуть реальної шкоди. У майбутньому такі системи варто вдосконалювати та інтегрувати з технологіями периферійних обчислень (edge computing).

Список використаних джерел

1. Al-Garadi, M. A., et al. A survey of machine and deep learning methods for Internet of Things (IoT) security. – Режим доступу: https://ieeexplore.ieee.org/document/9072101

2. Zarpelão, B. B., et al. A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S1084804517300802

Бережний Сергій Володимирович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
sirojaberejny@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

СИСТЕМА ВІДДАЛЕНОГО ДОСТУПУ ДО ПРИВАТНОЇ ІНФРАСТРУКТУРИ НА БАЗІ WIREGUARD ДЛЯ EDGE ТА IoT-СЕРЕДОВИЩ

Цифровізація бізнес-процесів, розвиток розподілених сервісів та поширення пристроїв Інтернету речей формують потребу у безпечному віддаленому доступі до приватної інфраструктури. Особливо актуальним це є для сценаріїв, де мережеві вузли розміщені поза межами центрального офісу: домашні мережі, мобільні об'єкти, польові комплекси, виробничі майданчики або сенсорні системи збору даних. Традиційні VPN-рішення часто характеризуються складністю налаштування, високими накладними витратами та залежністю від централізованої серверної моделі. У зв'язку з цим зростає інтерес до використання протоколу WireGuard як основи сучасної системи захищеного доступу [1].

Постановка задачі.

Основною проблемою побудови систем віддаленого доступу є необхідність одночасного забезпечення високого рівня безпеки, стабільності з'єднання, простоти адміністрування та можливості масштабування. У випадку IoT- та edge-середовищ додатковими вимогами виступають обмежені апаратні ресурси пристроїв, нестабільні канали зв'язку, потреба автономної роботи та швидкого розгортання без складної серверної інфраструктури. Класичні VPN-платформи не завжди ефективно відповідають таким умовам через складні механізми конфігурації та значні витрати на підтримку [2].

Мета дослідження.

Метою дослідження є аналіз можливостей побудови системи віддаленого доступу до приватної інфраструктури на базі WireGuard із використанням edge-підходу, дослідження архітектури взаємодії вузлів, оцінка практичних переваг використання вбудованих маршрутизаторів під керуванням OpenWRT, а також визначення перспектив інтеграції такого рішення у IoT-мережі.

Результати дослідження.

Протокол WireGuard базується на сучасних криптографічних алгоритмах та використовує мінімалістичну модель обміну ключами. Ідентифікація вузлів виконується за допомогою пар приватного та публічного ключів, що зменшує залежність від традиційних механізмів логінів і паролів. Такий підхід підвищує безпеку системи та знижує ризик помилок конфігурації. Окремою перевагою є швидкий handshake-механізм, що дозволяє оперативно відновлювати тунель навіть при зміні мережевого середовища або переході між каналами зв'язку [1].

Практична реалізація системи може базуватися на маршрутизаторах класу GL.iNet із підтримкою OpenWRT. У такій архітектурі VPN-шлюз переноситься безпосередньо на граничний мережевий пристрій, що скорочує кількість проміжних вузлів, зменшує затримки та спрощує логіку маршрутизації. Налаштування можуть виконуватись як через web-інтерфейс, так і через SSH-консоль із використанням утиліт wg, що забезпечує повний контроль над параметрами тунелю, ключами та правилами доступу.

Важливим елементом WireGuard є механізм Cryptokey Routing, де параметр AllowedIPs одночасно визначає дозволені адреси клієнта та маршрути проходження трафіку. Це дозволяє поєднати функції контролю доступу та маршрутизації без використання великої кількості додаткових ACL-правил чи складних таблиць маршрутизації. У результаті адміністрування системи спрощується, а ризик помилок конфігурації знижується.

Для IoT-середовищ така модель є особливо корисною, оскільки польові пристрої або шлюзи можуть передавати телеметрію до центральної інфраструктури через захищений тунель із використанням мобільного зв'язку 4G/5G. Це дозволяє швидко розгортати сенсорні мережі у віддалених місцях без потреби у стаціонарному провайдері чи відкритті зовнішніх портів. Одночасно забезпечується ізоляція трафіку та захист службових даних (рис. 1) [3].

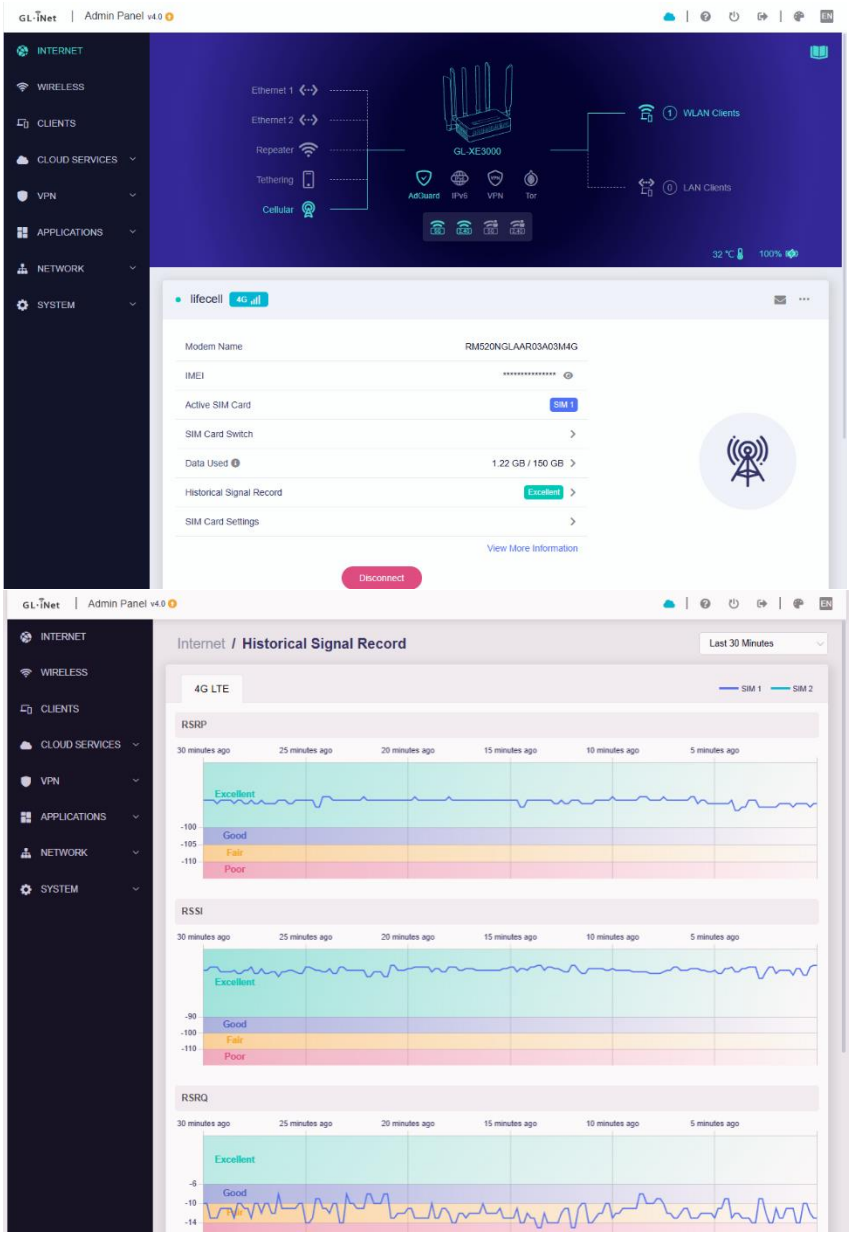

Рис. 1. Забезпечення роботи VPN через резервний інтернет-канал

Економічний аспект також є суттєвою перевагою. Використання OpenWRT і WireGuard не потребує ліцензійних платежів, а масштабування системи не супроводжується витратами на додаткові користувацькі ліцензії. Основні витрати зводяться до придбання апаратної платформи та базового адміністрування, що робить таке рішення привабливим як для малого бізнесу, так і для корпоративного сектору [4].

Висновки та перспективи.

У результаті дослідження встановлено, що побудова системи віддаленого доступу на базі WireGuard є ефективним підходом для захисту приватної інфраструктури, особливо в edge- та IoT-сценаріях. Рішення поєднує високий

рівень безпеки, швидке встановлення з'єднання, просте адміністрування та низьку вартість володіння.

Перспективними напрямами подальших досліджень є інтеграція системи з overlay-мережами, автоматизованим моніторингом стану тунелів, централізованим керуванням великою кількістю вузлів, а також використанням технологій штучного інтелекту для прогнозування відмов каналів зв'язку та оптимізації маршрутизації.

Список використаних джерел

1. *WireGuard Official Documentation. WireGuard. URL: https://www.wireguard.com/ (дата звернення: 12.04.2026).*
2. *OpenWrt Project Documentation. OpenWrt. URL: https://openwrt.org/ (дата звернення: 12.04.2026).*
3. *GL.iNet Product Documentation. GL.iNet. URL: https://docs.gl-inet.com/ (дата звернення: 12.04.2026).*
4. *Network World. VPN Cost and Infrastructure Analysis. URL: https://www.networkworld.com/ (дата звернення: 13.04.2026).*

Охріменко Назарій Олександрович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
nazarrr956@gmail.com

Бученко Ігор Анатолійович
старший викладач кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

СИСТЕМА БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ДОСТУПУ ДО ПРИВАТНОЇ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ КОНТЕЙНЕРИЗОВАНОГО СЕРВІСУ

У сучасних умовах цифровізації та зростання кількості кіберзагроз питання захисту доступу до приватної серверної інфраструктури набуває критичного значення. Традиційні методи автентифікації, зокрема використання логіну та пароля, вже не забезпечують належного рівня безпеки через вразливість до атак типу brute force, phishing та витоку облікових даних. Особливо це актуально для розподілених середовищ, де сервіси можуть функціонувати незалежно або бути частиною складної мікросервісної архітектури [1].

Постановка задачі.

Однією з ключових проблем є відсутність універсального механізму впровадження багатофакторної автентифікації (MFA) для вже існуючих сервісів, які не підтримують її на рівні реалізації. Це створює потребу у створенні незалежного рішення, яке можна інтегрувати у будь-яку інфраструктуру без суттєвого втручання в існуючі сервіси [2].

Мета дослідження.

Метою дослідження є розробка концептуальної моделі системи багатофакторної автентифікації у вигляді контейнеризованого сервісу, який може бути інтегрований у приватну серверну інфраструктуру для забезпечення додаткового рівня захисту доступу до ресурсів.

Результати дослідження.

Запропонована система базується на використанні контейнеризованого сервісу автентифікації (далі – Auth-сервіс), який розгортається у середовищі Docker та функціонує як проксі-рівень між користувачем і цільовими сервісами інфраструктури.

Основна ідея полягає у тому, що доступ до будь-якого ресурсу (вебсайту, API, внутрішнього сервісу) здійснюється не напряму, а через Auth-сервіс, який виконує перевірку багатофакторної автентифікації. Такий підхід дозволяє реалізувати MFA навіть для тих сервісів, які не мають вбудованої підтримки автентифікації [1].

Система підтримує такі фактори автентифікації:

- знання (пароль або PIN-код);
- володіння (одноразові коди OTP, мобільні додатки);
- біометричні або поведінкові фактори (опційно).
- Контейнерна реалізація забезпечує:
- ізольованість виконання;
- масштабованість;
- простоту інтеграції у різні середовища;
- можливість роботи у межах віртуальних мереж Docker або взаємодії з зовнішніми IP-адресами (рис. 1) [2].

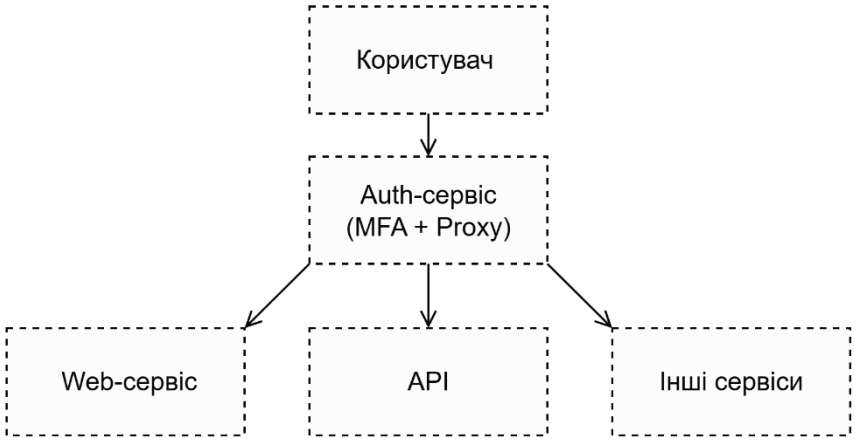

Рис. 1. Організації доступу через сервіс багатофакторної автентифікації

Auth-сервіс виступає як центральний вузол контролю доступу. Після проходження автентифікації користувач отримує тимчасовий токен доступу, який дозволяє взаємодіяти з внутрішніми сервісами без повторної перевірки протягом сесії.

Додатково система може інтегруватися з журналами подій та аналітичними платформами для відстеження підозрілої активності, що дозволяє підвищити рівень безпеки шляхом аналізу поведінкових патернів користувачів [3].

Важливою перевагою є можливість розгортання системи у вигляді окремого контейнера без необхідності модифікації існуючих сервісів, що значно спрощує впровадження у реальних умовах експлуатації [2].

Висновки та перспективи.

У результаті дослідження було розроблено концепцію системи багатофакторної автентифікації, яка реалізується у вигляді контейнеризованого сервісу та забезпечує універсальний механізм захисту доступу до приватної серверної інфраструктури.

Запропонований підхід дозволяє:

- підвищити рівень безпеки без зміни існуючих сервісів;
- забезпечити гнучкість масштабування;
- реалізувати централізований контроль доступу;
- інтегрувати систему у сучасні DevOps-процеси.

Перспективними напрямами подальших досліджень є:

- інтеграція з системами штучного інтелекту для адаптивної автентифікації;
- використання поведінкової біометрії;
- впровадження Zero Trust моделей безпеки;
- розширення функціоналу для роботи з IoT-пристроями та edge-середовищами.

Список використаних джерел

1. Multi-Factor Authentication (MFA) Basics. Microsoft Security. URL: https://learn.microsoft.com/en-us/security/zero-trust/develop/mfa (дата звернення: 13.04.2026)

2. Virtualization vs containerization. Scale Computing. URL: https://www.scalecomputing.com/resources/whats-the-difference-between-virtualization-vs-containerization (дата звернення: 13.04.2026)

3. What is User Behavior Analytics (UBA)? IBM. URL: https://www.ibm.com/topics/user-behavior-analytics (дата звернення: 13.04.2026)

НАПРЯМ 5. BIG DATA І АНАЛІЗ ДАНИХ

Стражніков Андрій Анатолійович
аспірант 3 року навчання
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
andrew.strazh@gmail.com

Пронькін Олександр Васильович
аспірант 3 року навчання
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
oleksandr.pronkin@gmail.com

ТРАНСФОРМАЦІЯ ЦЕНТРАЛІЗОВАНИХ ПЛАТФОРМ МІКРОЗАВДАНЬ У ДЕЦЕНТРАЛІЗОВАНІ ЕКОСИСТЕМИ

Економіка мікрозавдань (Human Intelligence Tasks – HITs) стала фундаментом для розвитку сучасного штучного інтелекту. Гіганти по прикладу MTurk або Appen роками забезпечували розмітку величезних масивів даних. Проте централізована модель вичерпала свій кредит довіри через високі комісії (до 45%), ризики DDoS-атак та непрозорі механізми виплат. Сьогодні ми спостерігаємо фундаментальний зсув у бік децентралізованих екосистем, де роль посередника бере на себе блокчейн. [1].

У класичних системах працівник і замовник перебувають у стані постійного конфлікту інтересів:

- Free-riding (Безкоштовний проїзд): Замовник може отримати дані, але відхилити оплату, посилаючись на нібито «низьку якість».
- False reporting (Фальшиві звіти): Працівники можуть надавати випадкові відповіді для швидкого заробітку або копіювати результати колег.

Централізовані платформи вирішують це суб'єктивно. Децентралізована ж трансформація пропонує математичний підхід до справедливості.

Сучасний ринок мікрозавдань (HITs) переживає трансформацію від закритих централізованих платформ, таких як Amazon Mechanical Turk, до прозорих децентралізованих екосистем. Традиційні сервіси дедалі частіше піддаються критиці через високі комісії (до 45%), ризики технічних збоїв та відсутність прозорості в оцінюванні роботи. Впровадження блокчейну дозволяє усунути посередника, замінивши його смарт-контрактом, який виступає незалежним арбітром. Це забезпечує незмінність умов завдання та гарантує, що жодна зі сторін не зможе маніпулювати результатами або виплатами в односторонньому порядку.

На рисунку нижче представлена концептуальна схема децентралізованої системи, яка вирішує ключовий парадокс блокчейну: як обробляти великі дані, не витрачаючи тисячі доларів на «газ» (комісії мережі).

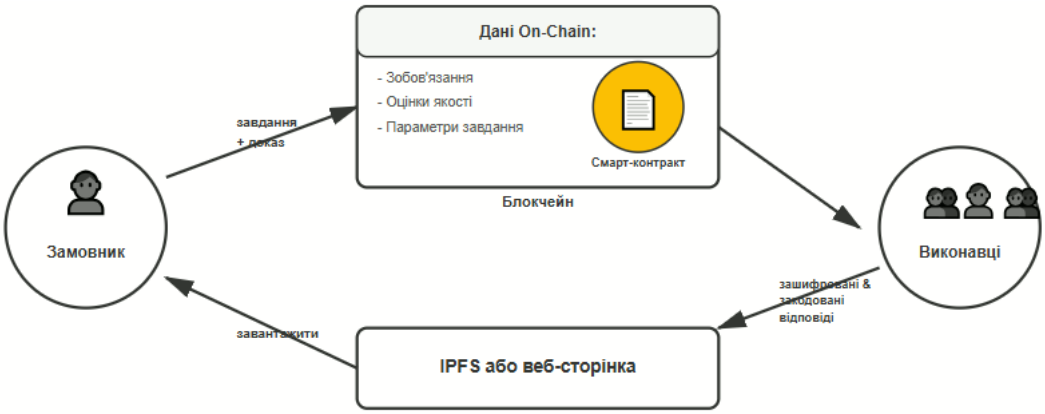

Рис. 1. Взаємодія замовника, виконавців, смарт-контракту та IPFS. [1]

Ключовим елементом трансформації краудсорсингу є гібридна архітектура, де великі обсяги даних зберігаються поза мережею (IPFS), а блокчейн фіксує лише компактні криптографічні докази, що розв'язує проблему масштабованості та дозволяє обробляти мільйони питань із мінімальними витратами на газ. Завдяки використанню смарт-контрактів та зашифрованих відповідей система запобігає отриманню даних без оплати й копіюванню результатів, реалізуючи механізм «подвійної справедливості» через автоматизоване виявлення істини на основі більшості голосів. Застосування математичних примітивів, зокрема білінійних акумуляторів, дозволяє підтверджувати якість роботи без попередньо відомих еталонів, перетворюючи децентралізований краудсорсинг на надійний та економічно ефективний інструмент для підготовки високоякісних наборів даних для штучного інтелекту.

Висновок

Трансформація ринку мікрозавдань – це не просто заміна сервера на блокчейн. Це створення саморегульованого середовища, де математика гарантує чесність. Завдяки оптимізації зберігання даних та новим методам криптографічної перевірки, децентралізовані платформи готові стати основним інструментом для підготовки даних наступного покоління ШІ.

Список використаних джерел

1. Liang, Y., Li, Y., & Shin, B. S. (2024). Blockchain-based crowdsourcing for human intelligence tasks with dual fairness. Blockchain: Research and Applications, 5(4), 100213. https://doi.org/10.1016/j.bcra.2024.100213

2. Yihuai Liang, Yan Li, Byeong-Seok Shin. Decentralized crowdsourcing for human intelligence tasks with efficient on-chain cost Proc. VLDB Endow., 15 (9) (2022), pp. 1875-1888, 10.14778/3538598.3538609

Бакал Інна Володимирівна
студентка групи САДМ-51
Державного університету
інформаційно-комунікаційних технологій
(067)-478-43-55
bakalinna2@gmail.com

РОЗРОБКА ТА СИСТЕМНИЙ АНАЛІЗ ГІБРИДНОЇ ІНТЕЛЕКТУАЛЬНОЇ МОДЕЛІ ДЛЯ ПРОГНОЗУВАННЯ ТА ОПТИМІЗАЦІЇ СТІЙКОСТІ РЕСУРСНОЇ СИСТЕМИ

Постановка задачі

Сучасні ресурсні системи функціонують у середовищі, що характеризується високим ступенем невизначеності та частими зовнішніми збуреннями. Традиційні підходи до управління такими системами часто орієнтовані на стабільні умови, що робить їх вразливими до раптових змін (криз, дефіциту чи технічних збоїв). Виникає наукова суперечність між необхідністю забезпечити безперебійне постачання ресурсів та обмеженістю інструментів, здатних одночасно аналізувати великі масиви даних і приймати гнучкі управлінські рішення. Основним завданням є створення інтелектуального механізму, який би дозволяв не лише передбачати критичні стани системи, а й автоматично розробляти стратегії адаптації для збереження її життєздатності.

Мета дослідження

Метою роботи є розробка та системне обґрунтування гібридної інтелектуальної моделі, що поєднує можливості глибокого машинного навчання та апарату нечіткої логіки. Така інтеграція спрямована на підвищення точності прогнозування динаміки ресурсних потоків та оптимізацію параметрів стійкості системи в умовах багатофакторних ризиків.

Результати дослідження

У ході дослідження було проведено системний аналіз архітектури ресурсної системи, що дозволило виділити ключові параметри її стійкості: здатність до поглинання шоків та швидкість відновлення. Запропонована гібридна модель базується на дворівневому підході. На першому рівні використовується рекурентна нейронна мережа з архітектурою довгої короткострокової пам'яті (LSTM). Вона спеціалізується на обробці часових рядів і дозволяє ідентифікувати приховані закономірності у споживанні ресурсів, враховуючи ретроспективні дані та циклічні коливання.

На другому рівні моделі інтегровано систему нечіткого логічного виводу. Її роль полягає в інтерпретації отриманих прогнозів та формуванні рекомендацій

щодо управління. Оскільки в реальних системах управління часто спирається на досвід експертів, використання нечітких лінгвістичних змінних (наприклад, «низький рівень запасу», «висока ймовірність збою») дозволяє формалізувати людські знання та забезпечити гнучке прийняття рішень там, де класичні алгоритми стають занадто жорсткими.

Системний аналіз розробленої моделі показав, що такий гібридний підхід компенсує недоліки окремих методів: нейронна мережа нівелює суб'єктивізм експертів у прогнозуванні, а нечітка логіка забезпечує прозорість та зрозумілість процесу прийняття рішень. Впровадження моделі дозволяє завчасно виявляти ознаки втрати стійкості та перерозподіляти навантаження між вузлами системи, що значно знижує ризик виникнення системного колапсу.

Висновки та перспективи

Розроблена гібридна інтелектуальна модель довела свою ефективність у задачах підтримки стійкості складних ресурсних систем. Поєднання прогнозної сили нейромереж із регуляторним потенціалом нечітких систем забезпечує якісно новий рівень адаптивності до зовнішніх загроз.

Перспективи подальших досліджень полягають у розширенні моделі шляхом додавання модулів адаптивного навчання, які дозволять системі самостійно оновлювати базу нечітких правил на основі накопиченого досвіду подолання кризових ситуацій. Це дозволить створити повністю автономні інтелектуальні системи управління критичною інфраструктурою.

Список використаних джерел

1. *Davenport, T. H., Harris, J. G. (2007). Competing on Analytics: The New Science of Winning. Harvard Business Press.*
2. *Provost, F., Fawcett, T. (2013). Data Science for Business. O'Reilly Media.*
3. *Witten, I. H., Frank, E., Hall, M. A., Pal, C. J. (2016). Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann.*
4. *Шостак, В. Є. (2010). Бізнес-процеси: побудова та оптимізація. Київ: КНЕУ.*

Шумик Сергій Васильович
студент 3 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
sergiy.shumyk@gmail.com

Суханевич Євген Іванович
студент 3 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ

ІНФОРМАЦІЙНА СИСТЕМА ПРОГНОЗУВАННЯ ЗАЛЕЖНОСТЕЙ МІЖ АКТИВАМИ ФОНДОВОГО РИНКУ З УРАХУВАННЯМ ЧАСОВИХ ЛАГІВ ТА НОВИННИХ ФАКТОРІВ

Вступ

Фондовий ринок характеризується складною нелінійною структурою взаємозв'язків між активами, що змінюється у часі під впливом внутрішніх ринкових процесів та зовнішніх інформаційних факторів. Традиційні підходи до прогнозування, такі як ARIMA або VAR, розглядають часові ряди ізольовано або з фіксованими залежностями, що обмежує їх здатність моделювати динамічну структуру ринку [2].

Сучасні методи машинного навчання, зокрема регуляризовані моделі та нейронні мережі, дозволяють враховувати складні взаємозв'язки між змінними [1], однак інтеграція структурних залежностей, часових лагів та текстових даних новин у межах єдиної інформаційної системи залишається відкритою проблемою. Особливої актуальності набуває врахування новин як джерела екзогенних факторів, що впливають на поведінку ринку [3], [4].

Запропонований підхід

Запропонований підхід базується на інтеграції трьох взаємопов'язаних компонентів, що формують єдину інформаційну систему прогнозування залежностей на фондовому ринку. На відміну від існуючих рішень, кожен із компонентів розширює класичні методи аналізу часових рядів та машинного навчання [1], [2] і адаптує їх до задачі моделювання динамічних ринкових взаємозв'язків із урахуванням інформаційного впливу [3].

1. Прогноз структури залежностей між активами

Наукова новизна полягає у переході від традиційного прогнозування окремих часових рядів до прогнозування динамічної структури взаємозалежностей між активами у вигляді графа.

У класичних підходах, таких як VAR-моделі, залежності між змінними вважаються фіксованими або задаються апріорно [2]. У сучасних підходах машинного навчання залежності часто є неявними та важко інтерпретованими. Використання регуляризованих методів, зокрема Lasso [1], дозволяє отримати розріджені моделі, проте вони зазвичай застосовуються для статичного аналізу.

У запропонованому підході:

- залежності явно представлені у вигляді графової структури;
- структура графа адаптивно оновлюється у часі;
- враховується розрідженість зв'язків відповідно до принципів регуляризації [1].

Це дозволяє не лише підвищити точність прогнозування, а й отримати інтерпретовану модель структури ринку.

2. Метод адаптивного визначення часових лагів впливу

Наукова новизна полягає у визначенні індивідуальних часових лагів між кожною парою активів з урахуванням їх динамічної взаємодії.

У класичних часових моделях, зокрема VAR, лаги задаються фіксовано для всіх змінних [2]. Подібне спрощення не дозволяє врахувати асинхронність реакції ринку та складні часові залежності.

Запропонований підхід передбачає:

- визначення лагів окремо для кожної пари активів;
- врахування зміни лагів у часі;
- інтеграцію лагів у структуру графа залежностей.

Такий підхід узгоджується з сучасними дослідженнями у сфері аналізу часових залежностей та кореляційних структур [2], проте розширює їх за рахунок поєднання з графовим представленням ринку.

У результаті досягається більш точне моделювання причинно-часових зв'язків між активами.

3. Інтеграція причинно-наслідкових залежностей із текстовими даними новин

Наукова новизна полягає у поєднанні структурної моделі залежностей ринку з семантичним аналізом новин, що дозволяє враховувати зовнішні інформаційні фактори як джерело змін у структурі ринку.

Існуючі дослідження показують, що новини впливають на динаміку фінансових ринків [3], однак зазвичай вони використовуються як окремі ознаки без інтеграції у структурні моделі. Використання трансформерних моделей, таких як BERT [4], дозволяє ефективно кодувати текстову інформацію, проте питання інтеграції цих представлень у моделі залежностей залишається відкритим.

У запропонованому підході:

- текст новин перетворюється у векторні представлення за допомогою моделей глибинного навчання [4];
- враховується часовий зв’язок між новинами та реакцією ринку;
- вплив новин інтегрується у процес побудови графа залежностей.

Це дозволяє створити єдину модель, що поєднує кількісні та якісні фактори, і підвищує адаптивність системи до змін ринкового середовища.

Висновки

Запропоновано підхід до прогнозування на фондовому ринку, що поєднує моделювання структури залежностей, адаптивні часові лаги та інтеграцію новинних факторів. На відміну від традиційних моделей, запропонована інформаційна система дозволяє враховувати динамічну природу ринку та вплив інформаційного середовища.

Очікується, що застосування даного підходу дозволить підвищити точність прогнозування та забезпечити кращу інтерпретованість результатів.

Список використаних джерел

1. Tibshirani, R. (1996). Regression shrinkage and selection via the Lasso. Journal of the Royal Statistical Society: Series B, 58(1), 267–288. https://doi.org/10.1111/j.2517-6161.1996.tb02080.x

2. Hamilton, J. D. (1994). Time series analysis. Princeton University Press.

3. Tetlock, P. C. (2007). Giving content to investor sentiment: The role of media in the stock market. The Journal of Finance, 62(3), 1139–1168. https://doi.org/10.1111/j.1540-6261.2007.01232.x

4. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. In Proceedings of NAACL-HLT (pp. 4171–4186). https://doi.org/10.18653/v1/N19-1423

Ткаленко Оксана Миколаївна
доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
tkalenko-oksana888@ukr.net

Ковальчук Олександр Володимирович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.kovalchuk@gmail.com

СПЕЦИФІКА ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ У ЗАДАЧАХ ПРОГНОЗУВАННЯ ЧАСОВИХ РЯДІВ

Прогнозування часових рядів є однією з ключових задач у сучасних інформаційних системах. Воно широко використовується у багатьох галузях, основними з яких є фінанси, енергетика, телекомунікації, медицина. З розвитком обчислювальних технологій та накопиченням великих обсягів даних особливого значення набувають методи машинного навчання, які дозволяють будувати більш точні та гнучкі прогностичні моделі.

Статистичні методи хоча й залишаються актуальними, мають обмеження щодо роботи із складними нелінійними залежностями. Саме тому все більшої популярності набувають алгоритми машинного навчання, які здатні враховувати складну структуру даних.

Часові ряди мають специфічні характеристики, які ускладнюють процес прогнозування, до яких належать: наявність тренду та сезонності; автокореляція значень; шум та випадкові коливання; можливість структурних змін у даних. Ці особливості потребують спеціальних підходів до попередньої обробки даних, зокрема нормалізації, видалення тренду та сезонних компонентів.

Серед найбільш поширених методів машинного навчання для роботи з часовими рядами доцільно виділити наступні:

- моделі регресії (лінійна регресія, Ridge, Lasso);
- дерева рішень та ансамблеві методи (Random Forest, Gradient Boosting), що забезпечують високу точність при роботі з нелінійними залежностями;
- метод опорних векторів (SVM);
- нейронні мережі, зокрема рекурентні нейронні мережі (RNN), LSTM та GRU, які спеціально розроблені для обробки послідовних даних.

Особливу увагу слід надати глибоким нейронним мережам, які здатні автоматично виділяти релевантні ознаки з даних без необхідності ручного конструювання.

Застосування методів машинного навчання у задачах прогнозування часових рядів має ряд переваг:

- здатність працювати з великими обсягами даних;
- можливість моделювання складних нелінійних залежностей;
- гнучкість у налаштуванні моделей;
- висока точність прогнозування за умови правильної підготовки даних.

У практичних задачах важливу роль відіграє правильний вибір моделі, а також якісна підготовка даних. Комбінування різних методів (гібридні моделі) дозволятиме досягати кращих результатів. Наприклад, поєднання статистичних методів з нейронними мережами надає змогу враховувати як лінійні, так і нелінійні компоненти часових рядів.

Методи машинного навчання відкривають нові можливості для прогнозування часових рядів, забезпечуючи високу точність та гнучкість моделей. Слід зазначити, що їх ефективність значною мірою залежить від якості даних, правильного вибору алгоритму та налаштування параметрів.

Специфіка використання машинного навчання у задачах прогнозування часових рядів полягає насамперед у необхідності врахування їх часової структури та залежності між послідовними спостереженнями. У часових рядах кожне значення залежить від попередніх, що потребує застосування спеціальних підходів до формування ознак, зокрема використання лагових змінних та вікон спостережень. Важливим аспектом є також наявність трендів, сезонних коливань і шуму, які необхідно коректно ідентифікувати та враховувати під час побудови моделей. Крім того, значну роль відіграє проблема нестаціонарності даних, коли статистичні властивості ряду змінюються з часом, що ускладнює навчання моделей та потребує їх адаптації. Ще однією особливістю є необхідність балансування між точністю прогнозу та здатністю моделі до узагальнення, оскільки складні алгоритми можуть бути схильні до перенавчання. Також важливим є вибір адекватної метрики оцінювання якості пронозу, яка повинна враховувати специфіку предметної області. У сукупності ці фактори визначають необхідність комплексного підходу до побудови моделей машинного навчання для часових рядів, що включає попередню обробку даних, вибір відповідних алгоритмів та їх налаштування.

Висновки та перспективи. Подальші дослідження доцільно спрямувати на розробку гібридних моделей та підвищення інтерпретованості результатів, що дозволить розширити сферу застосування машинного навчання у задачах прогнозування. Важливим напрямом є також удосконалення методів попередньої обробки часових рядів, зокрема виявлення та усунення шумів, сезонних і трендових компонентів. Крім того, перспективним є дослідження можливостей адаптивних моделей, здатних враховувати зміну структури даних у реальному часі. Це сприятиме підвищенню точності прогнозів та ефективності використання моделей у практичних задачах.

Список використаних джерел

1. Mienye I., Swart T., Obaido G., Jordan M., Ilono P. Deep Convolutional Neural Networks: A Comprehensive Review. Preprints, 2024, Article 202408.1288. https://doi.org/10.20944/preprints202408.1288.v1

2. Darban Z., Las-Heras I., G-Berdonces M., Valero M., Barambones O. Deep Learning for Time Series Anomaly Detection: A Survey. *ACM Computing Surveys, 57, 1–42, 2024. https://doi.org/10.48550/arXiv.2211.05244*

Капітон Марія Віталіївна
студентка 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kapitonmariia@gmail.com

Полоневич Ольга Володимирівна
к.т.н., доцент, доцент кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
o.polonevych@duikt.edu.ua

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕКРУТИНГУ ПЕРСОНАЛУ ШЛЯХОМ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасних реаліях розвитку мережевої економіки, питання належної організації пошуку кадрів набуває першочергового значення. Корпорації постають перед потребою оперативно укомплектовувати робочі місця, одночасно гарантуючи високу якість відібраних претендентів. Звичні підходи до рекрутингу, які значною мірою ґрунтуються на ручному опрацюванні відомостей, дедалі частіше не відповідають актуальним вимогам через повільність та високий ступінь суб'єктивності.

Інтеграція програмних комплексів дає змогу трансформувати всю парадигму організації найму, забезпечуючи механізацію ключових кроків – починаючи від збору первинних даних і до остаточного вердикту. Подібні рішення створюють уніфікований інформаційний простір, де консолідуються відомості про потенційних співробітників, відкриті позиції та підсумки оцінювання. Це не лише спрощує процедуру доступу до необхідних даних, але й мінімізує ризик їхньої втрати або надмірної дуплікації.

Вирішальною перевагою застосування інформаційних платформ є здатність до зв’язування із сучасними цифровими каналами залучення фахівців. Залучення претендентів через профільні ресурси та соціальні мережі для ділових

контактів дає можливість розширити коло потенційних кандидатів та миттєво реагувати на динаміку ринку зайнятості. Водночас, механізми автоматизованого пре-скринінгу дозволяють спрощено відкинути нерелевантні відгуки та сфокусувати зусилля на найбільш перспективних фахівцях.

Значущим аспектом є впровадження аналітичних інструментарію, що забезпечує обробку колосальних масивів даних. Аналіз кількісних показників ефективності, таких як терміни закриття вакансій або результативність тих чи інших джерел пошуку, дозволяє виявити "вузькі місця" у процесі рекрутингу та завчасно внести необхідні корективи. Таким шляхом формується більш обґрунтована стратегія управління людськими ресурсами.

Окрему роль виконує процес автоматизації взаємодії із самими кандидатами. Інформаційні інструменти забезпечують швидкий обмін повідомленнями, синхронізацію графіків інтерв'ю та моніторинг проходження етапів відбору. Це позитивно відображається на враженнях претендентів і сприяє формуванню привабливого образу роботодавця. Крім того, це знижує ймовірність втрати дійсно цінних кадрів через затягування комунікаційних процесів.

Слід також брати до уваги питання збереження конфіденційності особистих відомостей. Використання актуальних інформаційних систем дає можливість застосувати механізми контролю доступу, протоколювання дій та захисту інформації у відповідності до чинних стандартів безпеки. Це є критичною умовою для формування довіри до системи як з боку кандидатів, так і з боку самої організації.

Підсумовуючи, впровадження інформаційних систем у сферу найму персоналу забезпечує комплексне зростання результативності всієї процедури підбору. Автоматизація рутинних завдань, застосування аналізу даних та інтеграція із цифровими майданчиками дозволяють зменшити часові витрати на найм, підвищити якість відбору та оптимізувати функціонал відділів кадрів. У майбутньому подальший розвиток подібних платформ буде нерозривно пов'язаний із вбудовуванням інтелектуальних алгоритмів, що сприятиме ще точнішому прогнозуванню результатів кадрового забезпечення.

Список використаних джерел

1. Deloitte. Global Human Capital Trends 2024. – URL: https://www2.deloitte.com/global/en/insights/focus/human-capital-trends.html

2. LinkedIn Talent Solutions. Future of Recruiting Report 2023. – URL: https://business.linkedin.com/talent-solutions/resources/future-of-recruiting

3. McKinsey & Company. The state of AI in HR 2022–2024. – URL: https://www.mckinsey.com/capabilities/people-and-organizational-performance

4. IBM. AI and Automation in Talent Acquisition. – 2025. – URL: https://www.ibm.com/topics/talent-acquisition

Іваненко Сергій Євгенович
студент 4 курсу
спеціальності «Комп'ютерні науки»
Державного університету інформаційно-комунікаційних технологій, м. Київ
st6426569@stud.duikt.edu.ua

Катков Юрій Ігорович
професор, доктор технічних наук

АДАПТИВНА ІНТЕЛЕКТУАЛЬНА ВІЗУАЛІЗАЦІЯ ПОТОКОВИХ ДАНИХ В ЕКОЛОГІЧНИХ IoT-ПЛАТФОРМАХ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ

Стрімкий розвиток сенсорних мереж призвів до появи концепції "розумного довкілля", де тисячі датчиків генерують безперервні потоки відкритих даних про стан повітря, води та радіаційного фону. Актуальність теми зумовлена необхідністю оперативного прийняття рішень на основі Big Data. Традиційні методи статичної графіки не здатні відобразити динаміку екологічних процесів у реальному часі. Створення ефективних інструментів візуалізації дозволяє трансформувати сирі потокові дані у зрозумілі індикатори для екологів та громадськості, забезпечуючи прозорість моніторингу довкілля [1, 2].

*Методи візуалізації та їх сутність***.** Сучасні екологічні IoT-платформи використовують декілька основних методів обробки потоків [3, 4]:

- Теплові карти (Heat Maps) у реальному часі: Відображають інтенсивність забруднення на географічній площині, де колір змінюється динамічно залежно від нових надходжень з датчиків.
- Часові ряди з ковзним вікном (Rolling Time Series): Графіки, що оновлюються автоматично, відкидаючи застарілі дані та фокусуючись на останніх показниках.
- Інтерактивні приладові панелі (Dashboards): Агрегують дані через віджети (gauge charts, лінійні графіки), дозволяючи фільтрувати потоки за типом сенсора.
- Потокові графіки (Streamgraphs): Використовуються для візуалізації зміни часток різних типів забруднювачів у загальному обсязі викидів протягом певного часу.

Порівняння методів. Порівняння методів виявляє їхні функціональні межі. Теплові карти є найкращими для просторового орієнтування, проте вони мають високу обчислювальну складність при інтерполяції великої кількості точок у реальному часі. Часові ряди забезпечують найвищу точність аналізу трендів, але перевантажують інтерфейс при моніторингу понад 10 параметрів одночасно. Приладові панелі пропонують комплексну картину, проте часто мають затримку

(latency) через необхідність попередньої агрегації даних. Потокові графіки естетично демонструють складні екосистеми, але програють у чисельній точності. Ці методи нездатні вирішити проблему "інформаційного шуму" при одночасному відображенні сотень активних джерел даних. Тому в роботі запропоноване застосування гібридного підходу, де просторові дані поєднуються з деталізацією часових зрізів для критичних вузлів мережі [5].

Постановка завдання

При використанні лише просторових методів (наприклад, теплових карт) втрачається точна динаміка змін у конкретних точках, а при використанні лише часових зрізів (графіків) втрачається розуміння масштабів поширення забруднення. Це створює труднощі для оперативного аналізу Big Data в реальному часі. Звідси виникає завдання розробки гібридної візуалізації просторово-часових екологічних даних (Big Data) в екологічних IoT-мережах, що дозволить обробляти потокові відкриті дані з мінімальною затримкою. Такий підхід поєднає просторові дані теплових карт із деталізацією часових зрізів для критичних вузлів. Це забезпечить одночасний аналіз масштабів забруднення та динаміки змін показників у реальному часі.

Метою є підвищення ефективності екологічного моніторингу та створення інструментарію для підтримки прийняття управлінських рішень у концепції "розумного міста" (Smart City) шляхом розробки гібридного методу візуалізації Big Data в екологічних IoT-платформах

Основна частина:

Вирішення завдання полягає у інтеграції алгоритмів, що дозволяють виділяти аномальні значення (викиди) та автоматично акцентувати на них увагу користувача через адаптивні елементи інтерфейсу, мінімізуючи когнітивне навантаження на оператора екологічної служби. Це дозволить синхронно аналізувати масштаби поширення та швидкість змін показників у реальному часі. Це передбачає створення методів, які не просто відображають поточні показники, а й візуалізують прогнозні моделі та імовірнісні зони поширення забруднення шляхом:

1. Розробки моделі дворівневої фільтрації (створення алгоритму, який автоматично ідентифікує «критичні вузли» мережі (датчики з аномальними показниками або різким зростанням концентрації речовин) для їх пріоритетної деталізаці).

2. Синтезу гібридного інтерфейсу (проектування динамічного середовища, де загальна просторова карта (Macro-view) слугує контекстом, а часові зрізи (Micro-view) автоматично активуються як «спливаючі» або «вкладені» елементи для критичних точок).

3. Оптимізації потоків даних (для забезпечення мінімальної затримки візуалізації пропонується використовувати Edge-обчислення для детектування аномалій на рівні вузла, тоді як генерація предиктивних шарів забруднення

здійснюється в хмарному середовищі за допомогою потужних нейромережевих моделей).

4. Перехід від статичного відображення до адаптивної інтелектуальної візуалізації (AIV) (основна ідея полягає у впровадженні шару штучного інтелекту (AI) між потоком Big Data та графічним інтерфейсом користувача). Підхід адаптивної інтелектуальної візуалізації (AIV) включає:

1. Семантичної фільтрації на основі штучного інтелекту: Нейронна мережа в реальному часі аналізує вхідний потік і визначає ступінь важливості кожної події. Наприклад, якщо рівень PM2.5 (є одним із головних параметрів, що відстежуються в системах екологічного моніторингу та розумних міст, це дрібнодисперсні частинки пилу та аерозолю, діаметр яких становить 2,5 мікрометра або менше) знаходиться в межах норми, система використовує спрощену візуалізацію (крапкову), але при наближенні до критичного порогу AI автоматизує перехід: нейромережа аналізує потік PM2.5 і при загрозі сама розгортає Micro-view для вузла. Це усуває ручне перемикання, фокусуючи увагу лише на аномаліях.

2. Предиктивну візуалізацію «тіньових потоків»: Це використання рекурентних нейронних мереж (LSTM) для генерації "прогнозних шарів". На карті відображаються не лише фактичні дані датчиків, а й напівпрозорі зони очікуваного забруднення на наступні 2-4 години. Це дозволяє візуалізувати динаміку, якої ще не існує фізично.

3. Автоматичне кластерне групування: При надмірній кількості сенсорів штучний інтелект групує їх у "віртуальні мета-сенсори", візуалізуючи агрегований стан регіону. При натисканні кластер динамічне розпадається на окремі вузли за принципом декомпозиції, що базується на поточному стані аномалій.

Для кращого розуміння запропонованого методу AIV (Adaptive Intelligent Visualization) надане порівняння підходів у Таблиці 1.

Табл. 1.

Порівняння класичний та запропонованого підходу

Характеристика	Традиційні методи (Dashboards)	Запропонований метод (AIV)
Фільтрація даних	Ручна (фільтри користувача)	Семантична (на основі AI)
Реакція на аномалії	Візуальна ідентифікація оператором	Автоматичне розгортання деталей
Прогнозування	Зазвичай відсутнє (статичне)	Предиктивні "тіньові потоки" (LSTM)
Когнітивне навантаження	Високе (через надмірність датчиків)	Мінімальне (адаптивні елементи)

Такий підхід дозволяє реалізувати концепцію "Когнітивного резонансу візуалізації", де параметри графічного відображення (яскравість, частота оновлення, рівень деталізації) змінюються автоматично залежно від ступеня екологічної загрози, виявленої алгоритмами машинного навчання. На відміну від існуючих методів, де візуалізація є лише відображенням бази даних, запропонований підхід перетворює інтерфейс на активну аналітичну систему, що самостійно розставляє пріоритети уваги. Це мінімізує час реакції на екологічні катастрофи та дозволяє ефективно використовувати відкриті дані в умовах обмежених обчислювальних ресурсів IoT-пристроїв.

Висновки та перспективи

У ході роботи було проаналізовано існуючі методи візуалізації та доведено необхідність їх інтелектуалізації для екологічних IoT-платформ. Впровадження AI-алгоритмів у процеси графічної обробки Big Data дозволяє вирішити проблему перевантаження каналів зв'язку та когнітивного перевтомлення операторів. Запропоновані методи адаптивної візуалізації забезпечують вищу швидкість інтерпретації даних у порівнянні з класичними дашбордами.

Перспективи подальших розробок лежать у площині використання Інтернету Нано-речей (IoNT) для надтонкого моніторингу та інтеграції доповненої реальності (AR) для візуалізації екологічних даних безпосередньо на міських об'єктах. Це дозволить мешканцям "розумних міст" отримувати інформацію про якість повітря просто спрямувавши смартфон на вулицю, що стане новим етапом розвитку відкритого громадянського суспільства в Україні та світі.

Список використаних джерел

1. *Gartner Magic Quadrant for Analytics and Business Intelligence Platforms (2025). URL: https://www.gartner.com/en/documents/6576602*
2. *Zanella, A., et al. (2020) "Internet of Things for Smart Cities." IEEE Internet of Things Journal. URL: https://ieeexplore.ieee.org/abstract/document/6740844*
3. *Toddy Aditya, Rahmayati Rahmayanti (2022) IoT and Big Data Analytics for Smart Cities: A Global Perspective. URL: https://journals.sagepub.com/doi/full/ 10.1177/00420980231189394, https://doi.org/10.1177/00420980231189394*
4. *Wagner Junior Ladeira, Fernando de Oliveira (2024) Big data analytics and the use of artificial intelligence in the services industry: a meta-analysis. URL: https://www.tandfonline.com/doi/full/10.1080/02642069.2024.2374990, https://doi.org/10.1080/02642069.2024.2374990*
5. *Ana Stojanov, Ben Kei Daniel (2023) A decade of research into the application of big data and analytics in higher education: A systematic review of the literature. URL: https://dl.acm.org/doi/abs/10.1007/s10639-023-12033-8*

Ємельянова Дарія Юріївна
студентка 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
dariyduring@gmail.com

МЕТОДОЛОГІЯ АЛГОРИТМІЧНОГО УСУНЕННЯ АНОМАЛІЙ ДАНИХ У КОРПОРАТИВНИХ ERP-СИСТЕМАХ (НА ПРИКЛАДІ MICROSOFT DYNAMICS NAV)

Впровадження ERP-систем (Enterprise Resource Planning) спрямоване на уніфікацію бізнес-процесів, проте питання якості даних (Data Quality) часто залишається слабкою ланкою. Незважаючи на вбудовані модулі контролю, корпоративні бази даних накопичують значну кількість логічних помилок, що критично впливає на точність управлінської аналітики.

Постановка задачі та технічні обмеження архітектури ERP.

При налаштуванні ERP-системи для масштабної компанії розробники стикаються з трьома критичними обмеженнями:

1. Продуктивність транзакцій (The Performance Trade-off).

Dynamics NAV використовує подієву модель валідації (тригери OnValidate). Якщо до кожного поля додати складну логіку перевірки (наприклад, порівняння з даними з інших десяти таблиць), час запису нових даних зросте в геометричній прогресії. Для компанії з сотнями операцій на годину це неприпустимо, тому більшість логічних перевірок просто ігноруються на користь швидкодії.

2. Обмеження реляційної моделі NAV.

У NAV валідація часто працює на рівні окремого поля. Система не бачить суперечності між двома полями, якщо вони формально заповнені правильно. Наприклад, вона прийме значення mnetto=20 кг. і mbrutto=10 кг., оскільки обидва є позитивними числами, хоча фізично така ситуація неможлива.

3. Інертність розробки.

Будь-яка зміна внутрішньої логіки NAV потребує втручання в C/AL код, тривалого тестування та оновлення всієї системи [1]. Це робить ERP нездатною оперативно адаптуватися до змін бізнес-правил (наприклад, появи нової категорії товарів зі специфічними вимогами до заповнення).

Мета дослідження.

Дослідити та обґрунтувати методику багаторівневого аналізу даних через зовнішній SQL-контур, що дозволяє ідентифікувати приховані логічні аномалії в ERP-системах без втручання в їхнє програмне ядро.

Результати дослідження.

У ході аналізу архітектурних особливостей сучасних ERP-систем було обґрунтовано концепцію винесення валідації у зовнішній аналітичний шар [2]. Такий підхід дозволяє проводити глибокий аудит бази даних через прямі SQL-запити, не втручаючись у програмне ядро системи та не знижуючи її продуктивність.

На основі цієї концепції в межах дослідження було виділено та систематизовано наступні методи контролю якості даних:

1. Атрибутивна валідація (Data Profiling).

Метод полягає у кількісному аналізі пустих полів та оцінці повноти інформації. Через агреговані SQL-запити обчислюється індекс заповненості критичних полів (бренди, описи, технічні коди). Це дозволяє виявити аномалії в тих атрибутах, які ERP-система технічно дозволяє залишати порожніми, але які є критичними для коректної побудови аналітичної звітності [3].

2. Контроль фізико-логічних параметрів.

Використовує математичні предикати для виявлення не реальних значень.

Наприклад, перевірка умови WHERE [Net Weight] > [Gross Weight].

3. Валідація структурних зв'язків (Referential Integrity).

Аналіз коректності ієрархічних посилань. За допомогою операторів JOIN та EXISTS перевіряється відповідність товарних карток встановленим класифікаторам. Метод ідентифікує записи, що посилаються на неіснуючі або логічно несумісні рівні ієрархії, що часто трапляється при масовому імпорті даних.

4. Аналіз часової актуальності (Data Timeliness).

Метод оцінки старіння даних на основі аналізу часових міток останніх модифікацій. Це дозволяє виокремити сегменти бази, що потребують актуалізації, забезпечуючи життєвий цикл інформації відповідно до поточної ситуації [4].

Результати аналізу ефективності стандартних методів валідації від ERP-системи та запропонованих методів через зовнішній SQL-контур продемонстровані у Таблиці 1.

Табл. 1

Ефективність методів контролю якості даних

Параметр порівняння	Стандартна валідація ERP (C/AL)	Запропонований зовнішній SQL-контур
Об’єкт аналізу	Атомарний (окремі поля та типи даних)	Системний (взаємозв’язок параметрів та логіка)
Вплив на продуктивність	Високий (уповільнює транзакції користувачів)	Відсутній (виконується як фоновий аналітичний запит)
Гнучкість налаштувань	Низька (потребує зміни коду та рестарту системи)	Висока (миттєве впровадження нових бізнес-правил)

Висновки.

Дослідження підтверджує, що архітектурні обмеження великих ERP-систем унеможливлюють повну валідацію даних всередині системи. Застосування зовнішнього SQL-контуру, що базується на методах атрибутивного, фізико-логічного та структурного аналізу, є оптимальною стратегією для підтримки високої якості корпоративної інформації та створення надійного фундаменту для бізнес-аналітики.

Список використаних джерел

1. Architectural Evolution of Microsoft ERP Systems: From Monolithic Dynamics NAV to Event-Driven Business Central Extensions / A. L. S. Santos та ін. ResearchGate. 2024. URL: https://www.researchgate.net/publication/401975724_Architectural_Evolution_of_Microsoft_ERP_Systems_From_Monolithic_Dynamics_NAV_to_Event-Driven_Business_Central_Extensions (дата звернення: 07.04.2026).

2. Data governance & quality management–Innovation and breakthroughs across different fields / B. M. V. Bernardo та ін. Journal of Innovation & Knowledge. 2024. Т. 9, № 4. С. 100598. URL: https://doi.org/10.1016/j.jik.2024.100598 (дата звернення: 07.04.2026).

3. A Survey of Data Quality Measurement and Monitoring Tools / S. S. S. Shrivas та ін. ResearchGate. 2022. URL: https://www.researchgate.net/publication/359636546_A_Survey_of_Data_Quality_Measurement_and_Monitoring_Tools (дата звернення: 07.04.2026).

4. DAQUA-MASS: An ISO 8000-61 Based Data Quality Management Methodology for Sensor Data / R. Perez-Castillo та ін. Sensors. 2018. Т. 18, № 9. С. 3105. URL: https://doi.org/10.3390/s18093105 (дата звернення: 07.04.2026).

Прач Олег Олександрович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
olegprac0@gmail.com

Кузьміч Михайло Юрійович
доктор філософії, доцент кафедри
Інформаційних Систем та Технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

BIG DATA І АНАЛІЗ ДАНИХ У СИСТЕМАХ ІНТЕЛЕКТУАЛЬНОГО ПРОГНОЗУВАННЯ ПОПИТУ

На сьогодні успішне керування складськими запасами в логістиці та ритейлі критично залежить від того, наскільки безпомилково розраховується

майбутній попит. Звичні статистичні підходи добре працюють виключно на стабільних ринках з лінійною динамікою, тоді як в умовах турбулентності та стрімких змін вони демонструють низьку результативність. Залучення інструментарію великих даних (Big Data) дозволяє відмовитися від застарілого аналізу минулих періодів на користь побудови прогнозів у режимі реального часу, враховуючи при цьому багатовимірні зовнішні та внутрішні чинники.

Загалом, впровадження технологій Big Data відкриває величезні перспективи для багатьох економічних галузей. Цей інструментарій допомагає ефективно закривати такі ключові потреби:

- стимулювання маркетингових ініціатив та зростання обсягів збуту;
- передбачення змін ринкової кон'юнктури;
- якісна сегментація клієнтської бази;
- покращення характеристик товарів та сервісів;
- формування більш виважених управлінських рішень;
- ухвалення швидких операційних кроків завдяки аналітиці Big Data;
- підвищення показників продуктивності робочих процесів;
- побудова дієвих логістичних ланцюгів;
- контроль за станом основних засобів підприємства;
- раціоналізація інвестиційних портфелів [2].

В основу архітектури пропонованої системи закладено здатність до безперебійного опрацювання різнотипної інформації. Це охоплює транзакційні логи, інформацію про складські залишки, показники маркетингових кампаній, а також низку зовнішніх обставин: погодні умови, сезонні коливання та активність користувачів у соціальних мережах. Обчислювальне ядро системи доцільно розробляти із застосуванням інструментарію Apache Spark. Завдяки обробці даних безпосередньо в оперативній пам'яті, ця технологія суттєво пришвидшує ітеративний процес навчання моделей, якщо порівнювати з класичними підходами.

Загалом, Apache Spark являє собою комплексний рушій та набір бібліотек, оптимізований для паралельних обчислень на кластерах. Він підтримує такі популярні мови програмування, як Scala, R, Java та Python, має у своєму арсеналі інструменти для широкого спектра завдань (від SQL-запитів до обробки потоків і машинного навчання) та здатен працювати в будь-якому середовищі: від звичайного ноутбука до серверних кластерів на тисячі машин [3] (рис. 1).

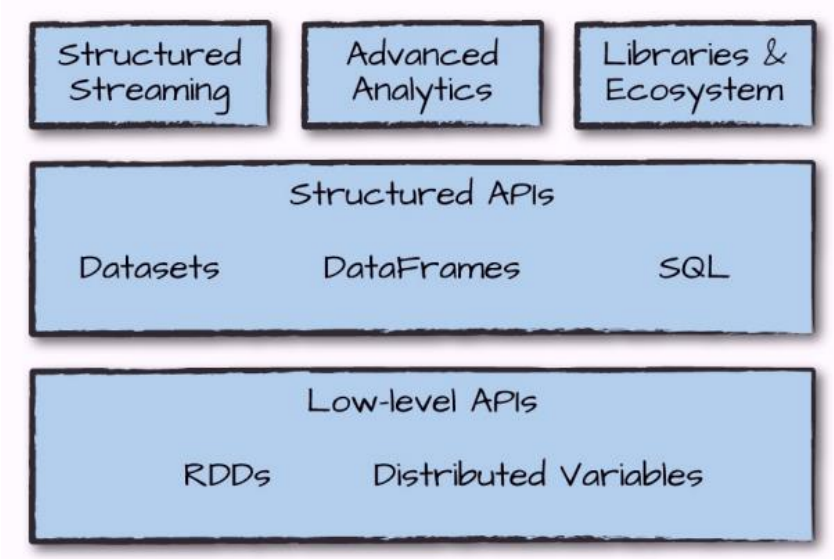

Рис. 1. Набір інструментів Spark

У розробленій архітектурі критично важливе місце відводиться крокам попередньої підготовки інформації (Data Preprocessing). Вони включають очищення масивів від інформаційного «шуму», заповнення порожніх значень та нормалізацію показників. Вибір конкретних алгоритмів зумовлений їхньою стійкістю до аномальних значень у статистиці продажів, а також здатністю виявляти нелінійні, складні залежності між рівнем попиту та маркетинговими чинниками, які його формують.

Етап Data Preprocessing передбачає процедури:

- очищення (фільтрацію несумісних даних та шумів),
- інтеграцію (об'єднання інформації з різних джерел), трансформацію (зведення до формату, зручного для агрегації або специфічних завдань);
- скорочення бази даних через виділення найрелевантніших ознак і прикладів [1].

Впровадження описаної архітектури дозволяє вивести автоматизацію управлінських рішень на новий якісний рівень. Як засвідчили результати моделювання, система відмінно справляється з великими масивами даних, виявляючи в них неочевидні закономірності. У підсумку це призводить до зниження показника середньоквадратичної похибки прогнозування (RMSE) на 15–20% у порівнянні з традиційними економетричними інструментами, що стає особливо помітним при зростанні обсягів вхідної інформації та кількості факторів впливу.

Список використаних джерел

1. *García, S., Luengo, J., & Herrera, F. (2015). Data preprocessing in data mining. Springer International Publishing. URL: https://doi.org/10.1007/978-3-319-10247-4*
2. *Scientific Bulletin of MSU. Series Economics Issue. (2019). p. 53.*
3. *Zaharia, M., & Chambers, B. (2018). Spark: The definitive guide. O'Reilly Media.*

Тищенко Данило Володимирович
студент 5 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kotyarishka@gmail.com

МОДЕЛЬ ОЦІНЮВАННЯ РЕПУТАЦІЇ КОРИСТУВАЧІВ У ЦИФРОВИХ СЕРВІСАХ ЯК СКЛАДОВА IoT-ЕКОСИСТЕМ

Інтернет речей (IoT) у стандартизаційному розумінні є глобальною інфраструктурою, що забезпечує надання розвинених сервісів шляхом взаємодії фізичних і віртуальних «речей» на основі інтероперабельних ІКТ, за умови виконання вимог безпеки та приватності [8]. Такий підхід підкреслює, що практичні IoT-рішення майже завжди мають сервісний характер і існують як частина ширших цифрових екосистем, де цінність створюється через координацію багатьох учасників та їхніх активів (даних, API, сервісів, виконавців, інфраструктури) [9], [2].

У сервісно-орієнтованих екосистемах центральними стають дві взаємопов'язані задачі: (1) управління «замовленнями» як формалізованими сервісними запитами (життєвий цикл, SLA/умови, артефакти, приймання результату) та (2) управління довірою між учасниками. Для онлайн-ринків довіра часто реалізується через репутаційні механізми: репутаційна система збирає, розподіляє та агрегує зворотний зв'язок про попередню поведінку учасників, допомагаючи іншим вирішувати, кому довіряти, і стимулюючи доброчесну поведінку [12]. Огляди сучасних платформ показують, що репутація та відгуки є суттєвим чинником ефективності онлайн-маркетплейсів, але водночас дизайн метрик може провокувати зміщення (bias) і потребує продуманих механізмів подолання спотворень [13].

Актуальність задачі довіри зростає в IoT-контексті, оскільки помилки або зловживання у наданні сервісу можуть впливати на кіберфізичні процеси. Дослідження платформ спільного споживання демонструють, що рейтингові механізми можуть виконувати роль інструмента «контролю/допуску» (gatekeeping) і підтримувати якість сервісу в умовах ризику та невизначеності [3]. Паралельно, для «соціального IoT» (SIoT) існують підходи trust management, які охоплюють обчислення/агрегацію/оновлення довіри, включно з event-driven оновленнями та аналізом атак на довіру [1].

Метою роботи є обґрунтування та проєктування інформаційної системи управління замовленнями й репутацією виконавців як компонента цифрової екосистеми сервісів у середовищі IoT. Об'єктом виступає цифрова екосистема сервісів, у якій замовники формують запити на виконання задач, а виконавці надають результат у рамках визначених умов. Предметом є моделі даних і

механізми, що забезпечують прозорий життєвий цикл замовлення та стійке до маніпуляцій формування репутації виконавців [12], [13]. Практичним кейсом для апробації підходів є маркетплейс фріланс-послуг у середовищі моддингу Garry's Mod, що дозволяє досліджувати поведінку учасників і механізми довіри в реальній цифровій спільноті.

Запропонований підхід передбачає модульну архітектуру компонента екосистеми: модуль управління замовленнями (створення, статуси, артефакти, приймання), модуль репутації (оцінки, відгуки, ваги сигналів, антифрод-правила), модуль аналітики (агрегація показників виконання, виявлення аномалій), модуль інтеграції (API/подієва взаємодія), а також модуль безпеки (ідентифікація, доступ, аудит, оновлення). Така архітектура узгоджується з підходами до «маркетплейсів» у IoT, де ресурси (дані/доступ/сервіси) мають публікуватися, знаходитися та обмінюватися між сторонами, а довіра підтримується рейтинговими механізмами [10]. Для подієвої інтеграції IoT-сервісів і реакції на телеметрію доцільні pub/sub-патерни; MQTT стандартизований як легковаговий publish/subscribe протокол, придатний для M2M та IoT-контекстів [11].

З позиції кібербезпеки компонент екосистеми повинен враховувати «мінімально необхідні» можливості та вимоги до IoT-вбудовуваності. NISTIR 8259A визначає базовий набір можливостей для «securable IoT devices», серед яких – унікальна ідентифікація, керування конфігурацією, захист даних, обмеження доступу до інтерфейсів, безпечні оновлення ПЗ та індикація кіберстану [5]. Рекомендації NIST SP 800-213 доповнюють це підходом до формування вимог і планування інтеграції IoT-пристроїв у систему з міркувань ризик-менеджменту [6]. ETSI EN 303 645 задає baseline-положення щодо безпеки та захисту даних для consumer IoT і підкреслює принципи security-by-design, орієнтуючись на найбільш поширені слабкості (зокрема легко вгадувані паролі) [4].

Очікуваним результатом є формалізована модель «замовлення–виконавець–оцінка/довіра» та набір метрик репутації, які спираються на (а) транзакційний фідбек (оцінки/відгуки) і (б) операційні показники якості виконання (терміни, дотримання вимог, стабільність взаємодії). Для IoT-орієнтованих сценаріїв доцільно розглядати trust-атрибути, що поєднують «соціальну довіру» та якість сервісу (QoS) – подібний поділ використовується в оглядах trust management для SIoT [1]. Додатково необхідно враховувати ризики упередженості та маніпуляцій у відгуках, які підкреслюються в оглядах репутаційних систем [13].

У підсумку, інформаційна система управління замовленнями та репутацією виконавців може розглядатися як критичний компонент цифрової екосистеми сервісів у IoT-середовищі, що підвищує керованість сервісних процесів і формує довіру між учасниками. У прикладних доменах (розумні міста, промислова

автоматизація) це потенційно знижує транзакційні витрати на відбір виконавців і підвищує надійність виконання сервісних робіт, а в дослідницькому вимірі дозволяє поєднати репутаційні підходи онлайн-маркетплейсів з trust-моделями IoT.

Список використаних джерел

1. *Trust Management in Social Internet of Things (SIoT): A Survey / S. Alam et al. IEEE Access. 2022. P. 1. URL: https://doi.org/10.1109/access.2022.3213699 (date of access: 12.04.2026).*
2. *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / A. Al-Fuqaha et al. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, no. 4. P. 2347–2376. URL: https://doi.org/10.1109/comst.2015.2444095 (date of access: 12.04.2026).*
3. *Basili M., Rossi M. A. Platform-mediated reputation systems in the sharing economy and incentives to provide service quality: The case of ridesharing services. Electronic Commerce Research and Applications. 2020. Vol. 39. P. 100835. URL: https://doi.org/10.1016/j.elerap.2019.100835 (date of access: 12.04.2026).*
4. *European Telecommunications Standards Institute. (2024). ETSI EN 303 645 V3.1.3 (2024-09): CYBER; Cyber Security for Consumer Internet of Things (Baseline Requirements). URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf (date of access: 12.04.2026).*
5. *IoT device cybersecurity capability core baseline / M. Fagan et al. Gaithersburg, MD : National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/nist.ir.8259a (date of access: 12.04.2026).*
6. *IoT Device Cybersecurity Guidance for the Federal Government / M. Fagan et al. Gaithersburg, MD : National Institute of Standards and Technology, 2021. URL: https://doi.org/10.6028/nist.sp.800-213 (date of access: 12.04.2026).*
7. *Gussek L., Wiesche M. Understanding the careers of freelancers on digital labor platforms: The case of IT work. Information Systems Journal. 2024. URL: https://doi.org/10.1111/isj.12509 (date of access: 12.04.2026).*
8. *Recommendation ITU-T Y.2060: Overview of the Internet of Things. ITU: Connecting the world and beyond. URL: https://www.itu.int/rec/dologin_pub.asp?id=T-REC-Y.2060-201206-I!!PDF-E&lang=e&type=items (date of access: 12.04.2026).*
9. *A matter of definition: Criteria for digital ecosystems / M. Koch et al. Digital Business. 2022. P. 100027. URL: https://doi.org/10.1016/j.digbus.2022.100027 (date of access: 12.04.2026).*
10. *IoT Marketplace: A data and API market for IoT devices / B. Krishnamachari et al. University of Southern California. URL: https://msbfile03.usc.edu/digitalmeasures/gerardpo/intellcont/USCIoTMarketplace_Jan152017-1.pdf (date of access: 12.04.2026).*
11. *MQTT v3.1.1. OASIS Open. URL: https://www.oasis-open.org/standard/mqttv3-1-1/ (date of access: 12.04.2026).*
12. *Reputation Systems / P. Resnick et al. Communications of the ACM. URL: https://cs.uwaterloo.ca/~klarson/teaching/F04-886/papers/p45-resnick.pdf (date of access: 12.04.2026).*
13. *Tadelis S. Reputation and Feedback Systems in Online Platform Markets. Haas School of Business. URL: https://faculty.haas.berkeley.edu/stadelis/Annual_Review_Tadelis.pdf (date of access: 12.04.2026).*

Поплавський Дмитро Іванович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
dimtrppl@gmail.com
st8095456@stud.duikt.edu.ua

Кузміч Михайло Юрійович
доктор філософії, доцент кафедри
Інформаціних Систем та Технологій Державного університету
інформаційно-комунікаційних технологій, м. Київ
m.kuzmich@duikt.edu.ua

СИСТЕМНИЙ АНАЛІЗ ТА ВЕЛИКІ ДАНІ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Стрімкий розвиток технологій Інтернету речей (IoT), розширення мережевої інфраструктури та глобальна цифровізація призвели до експоненційного зростання обсягів інформації. Корпоративні інформаційні системи (КІС) щоденно генерують та обробляють терабайти даних від різноманітних датчиків, користувацьких пристроїв та серверного обладнання. Проте наявність масивів «сирих» даних не гарантує підвищення ефективності. Ключовим викликом для організацій стає здатність швидко аналізувати цю інформацію, та використовувати її для дієвих управлінських рішення.

Традиційні реляційні бази даних та класичні інструменти бізнес-аналітики вже не здатні повною мірою впоратися зі швидкістю, обсягом та різноманітністю сучасних інформаційних потоків. Тому на перший план виходить системний аналіз великих даних, який дозволяє виявляти приховані закономірності та прогнозувати ринкові або внутрішньосистемні тенденції. Для повноцінного використання потенціалу Big Data необхідний продуманий підхід до інтеграції аналітичних інструментів у корпоративну архітектуру, що формує єдиний інформаційно-аналітичний контур підприємства чи освітньої установи.

Для технісної реалізації цього процессу необхідна через побудова багаторівневої інфраструктури: від безперервного збору телеметрії, та інших показників на базовому рівні до маршрутизації та виведення результатів на інтерактивні дашборди. Ефективність системи безпосередньо залежить від застосованих математичних та статистичних методів. Їх інструментарій автоматизує пошук аномалій, та забезпечує предиктивне обслуговування обладнання, і інформування персоналу. Водночас все ще важливим залишається забезпечення належного рівня інформаційної безпеки та відмовостійкості під час обробки корпоративних даних .

Головною перевагою впровадження системного аналізу Big Data є зміна парадигми управління мережами. Якщо класичні підходи базувалися на реактивному усуненні проблем, то сучасні системи забезпечують проактивне управління. Аналізуючи дані в режимі реального часу, КІС здатна автоматично перерозподіляти навантаження або блокувати підозрілі транзакції ще до настання критичних збоїв.

Підсумовуючи, системний аналіз великих даних є невід'ємним фундаментом сучасних корпоративних інформаційних систем. Він надає організаціям можливість ефективно використовувати накопичений інформаційний капітал для оптимізації процесів, зниження витрат та створення нових конкурентних переваг на ринку. Подальші дослідження у цій сфері доцільно спрямовувати на вдосконалення моделей потокової обробки даних та їх глибшу інтеграцію з IoT-рішеннями.

Список використаних джерел

1. Madugula, S., Pratapagiri, S., Phridviraj, M. S. B., Rao, V. C. S., Polala, N., & Kumaraswamy, P. (2023). Big data for the comprehensive data analysis of IT organizations. The Journal of High Technology Management Research, 34(2), 100465.

*2. Ranjan, J., & Foropon, C. (2021). Big data analytics in building the competitive intelligence of organizations. International Journal of Information Management, 56, 102231.**

3. Kopnova, O., Shaporeva, A., Iklassova, K., Kushumbayev, A., Tadzhigitov, A., & Aitymova, A. (2022). Building an information analysis system within a corporate information system for combining and structuring organization data (on the example of a university). Eastern-European Journal of Enterprise Technologies, 6(2(120)), 20–29.

4. Kushnir, O. K., & Chaplinskyi, V. R. (2023). Statistical methods for big data analysis. Modern Economics, 39, 75–81.

5. Матеріали досліджень щодо обробки великих даних. Електронний архів ТНТУ імені Івана Пулюя (ELARTU). URL: https://elartu.tntu.edu.ua/handle/lib/35835

Литвинець Богдан Вікторович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
zwerok0z@gmail.com

ІНТЕГРАЦІЯ ТА ОБРОБКА АЛЬТЕРНАТИВНИХ ДАНИХ ДЛЯ ОЦІНКИ КРЕДИТНОГО РИЗИКУ КЛІЄНТІВ З КОРОТКОЮ КРЕДИТНОЮ ІСТОРІЄЮ

Одним із найскладніших викликів для сучасної банківської системи є проблема фінансового виключення. Значна частина населення, зокрема молодь, самозайняті особи, трудові мігранти або цифрові кочівники, потрапляє до категорії «thin-file» або «no-file» клієнтів – осіб із відсутньою або мінімальною кредитною історією. Класичні моделі скорингу, що базуються на даних БКІ (бюро кредитних історій), часто присвоюють таким клієнтам низький бал або просто відмовляють у послугах через високий ризик. Це створює попит на розробку альтернативних методів оцінки ризиків.

Альтернативні дані (Alternative Data) – це нетрадиційна інформація, що може прямо або опосередковано характеризувати споживчу поведінку позичальника чи фінансову дисципліну. До основних джерел можна віднести:

• дані телеком-операторів: регулярність та обсяги поповнення рахунку, тривалість використання SIM-картки, а також іноді геолокаційні патерни;

• цифровий слід та метадані: поведінкові патерни під час заповнення анкет, метадані сесії, пристрій доступу, швидкість заповнення та копіювання даних;

• комунальні та орендні платежі: історія оплати рахунків за електроенергію, інтернет, оренду житла чи постачання газу тощо;

• соціальні мережі та їхні професійні варіанти: аналіз публічних профілів для визначення зайнятості та соціальних зв’язків.

Усі ці дані, на відміну від структурованих записів БКІ, часто є напівструктурованими (найчастіше у форматі JSON) або навіть зовсім неструктурованими, тому їхня інтеграція потребує складних процесів:

1. Збір та ETL-процес (Extract, Transform, Load): використання API для отримання даних від партнерів.

2. Парсинг та NLP (Natural Language Processing): застосування методів парсингу соціальних мереж та обробки природної мови для аналізу описів транзакцій або текстових метаданих.

3. Вилучення ознак (Feature Extraction): вилучення GPS-координат для оцінки стабільності способу життя клієнта.

Це також впливає на антифрод-захист. Шахраям простіше підробити довідки та записи в БКІ, ніж створити багаторічний цифровий слід, тому доволі

часто використовують моделі на основі альтернативних даних як коригувальні. Але, враховуючи роботу з чутливими даними, не слід забувати про регуляторні та етичні аспекти, які також своєю мірою впливають на створення таких систем: необхідність дотримання GDPR та Закону України «Про захист персональних даних», а також регулярність аудитів таких систем для запобігання дискримінації певних груп (Fairness AI).

Впровадження таких систем у секторі фінансових технологій дозволяє залучити нові сегменти клієнтів, які раніше були «невидимими» для банківських установ, та одночасно підвищити стійкість до фроду. Тому використання гібридних підходів беззаперечно ефективніше завдяки поєднанню фінансової точності традиційних джерел та динамічності альтернативних методів.

Список використаних джерел

1. Baesens B. Analytics in a Big Data World: The Essential Guide to Data Science and Its Applications. Wiley & Sons, Incorporated, John, 2014. https://www.oreilly.com/library/view/the-practitioners-guide/9780123737175/OEBPS/B9780123737175000117.htm

2. Loshin D. Practitioner's Guide to Data Quality Improvement. Elsevier Science & Technology Books, 2010.

https://cloudera2017.wordpress.com/wp-content/uploads/2019/01/bart-baesens-analytics-in-a-big-data-world.-the-essential-guide-to-data-science-and-its-applications-wiley-2014.pdf

3. Siddiqi N. Credit Risk Scorecards: Developing and Implementing Intelligent Credit Scoring. Wiley & Sons, Incorporated, John, 2012. 208 p. https://www.academia.edu/33357499/Credit_Risk_Scorecards_Developing_and_Implementing_Intelligent_Credit_Scoring

Литвинець Богдан Вікторович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
zwerok0z@gmail.com

ВЗАЄМОЗВ'ЯЗОК МІЖ ЯКІСТЮ ДАНИХ ТА СТІЙКІСТЮ СКОРИНГОВИХ МОДЕЛЕЙ. АВТОМАТИЗАЦІЯ КОНВЕЄРІВ ПІДГОТОВКИ ДАНИХ

В умовах тотальної цифровізації фінансових послуг і переходу банківського сектору на моделі прийняття рішень у реальному часі роль машинного навчання стає визначальною. Проте ефективність будь-якої системи обмежена фундаментальним принципом «Garbage in, Garbage out» (сміття на вході - сміття на виході). Для систем скорингу, де помилка може коштувати

фінансовій установі значних збитків або втраченого прибутку, якість даних перестає бути суто технічним аспектом і стає стратегічним активом.

Історичні дані, що використовуються для навчання скорингових моделей, зазвичай накопичуються з багатьох джерел: CRM-систем, логів транзакцій, запитів до бюро кредитних історій та зовнішніх API. У цьому процесі неминуче виникає «шум», який можна класифікувати за походженням:

• технічний: дублікати записів через збої в синхронізації, некоректні формати дат, пропуски значень (NaN) при невдалих запитах;

• людський: помилки при ручному введенні даних операторами або самими клієнтами у формах;

• навмисний (шахрайство): маніпуляції даними, приховування активних зобов'язань.

Наявність шуму призводить до деградації функції втрат під час навчання моделі. Наприклад, модель може завчити випадкові аномалії як стійкі закономірності (що називається перенавчанням або overfitting); це призведе до помилкових відмов надійним клієнтам або схвалення ризикових заявок. Щоб цьому запобігти, впроваджують метрики якості даних (табл. 1) за такими напрямками:

Табл. 1

Метрики якості даних

Метрика	Опис у контексті домену
Повнота (Completeness)	Відсоток заповнених критичних полів (дохід, стаж, контактні дані)
Точність (Accuracy)	Відповідність даних реальним фактам (валідація стажу через ПФУ)
Узгодженість (Consistency)	Відсутність суперечностей (вік клієнта збігається з датою народження в ІПН)
Актуальність (Timeliness)	Час, що минув із моменту останнього оновлення даних про заборгованість
Унікальність (Uniqueness)	Відсутність дубльованих профілів клієнтів (проблема дедуплікації)

Але все це потребує автоматизації та контролю даних на кожному етапі – так званих конвеєрів даних (Data Quality Pipelines), які складаються з кількох основних етапів (табл. 2).

Табл. 2

Ключові етапи конвеєра даних

Етап	Опис у контексті домену
Профайлінг даних (Profiling)	Аналіз структури даних: типи колонок, пропущені значення (NaN), мінімальні/максимальні значення.
Валідація (Validation)	Перевірка даних на відповідність правилам: чи заповнені обов'язкові поля (ID, сума кредиту, ім'я), валідація форматів даних, ранжування (чи входить, наприклад, сума кредиту в розумний діапазон).
Очищення (Cleaning)	Видалення дублікатів, заповнення пропусків, нормалізація форматів відповідно до стандартів ISO (для прикладу).
Збагачення (Enrichment)	Наприклад, додавання геоданих за IP-адресою чи зведення валют за актуальним курсом.
Моніторинг (Monitoring and Alerting)	Відсутність дубльованих профілів клієнтів (проблема дедуплікації)

Зважаючи на важливість управління даними в сучасному світі, створення стійкої скорингової моделі неможливе без системного управління ними. Автоматизація перевірки якості на кожному етапі – від збору до формування ознак – дозволяє не лише мінімізувати фінансові ризики, а й забезпечити довгострокову стабільність та інтерпретованість алгоритмів.

Список використаних джерел

1. Baesens B. Analytics in a Big Data World: The Essential Guide to Data Science and Its Applications. Wiley & Sons, Incorporated, John, 2014. https://www.oreilly.com/library/view/the-practitioners-guide/9780123737175/OEBPS/B9780123737175000117.htm

2. Loshin D. Practitioner's Guide to Data Quality Improvement. Elsevier Science & Technology Books, 2010.

https://cloudera2017.wordpress.com/wp-content/uploads/2019/01/bart-baesens-analytics-in-a-big-data-world.-the-essential-guide-to-data-science-and-its-applications-wiley-2014.pdf

3. Siddiqi N. Credit Risk Scorecards: Developing and Implementing Intelligent Credit Scoring. Wiley & Sons, Incorporated, John, 2012. 208 p.

https://www.academia.edu/33357499/Credit_Risk_Scorecards_Developing_and_Implementing_Intelligent_Credit_Scoring

Сокульський Олег Євгенович
доцент, к.т.н.
Військового інституту телекомунікацій та інформатизації імені Героїів Крут
mortimer@ukr.net

Топольськов Євгеній Олександрович
доцент, к.т.н.
Київського національного університету імені Тараса Шевченка
y.topolskov@knu.ua

Москаленко Наталія Володимирівна
асистент
Київського національного університету імені Тараса Шевченка
moskalenkonv@ukr.net

СУБД NOSQL В ТЕХНОЛОГІЯХ BIG DATA

Великі об’єми різнорідних даних та високі вимоги до їх збору, збереження та аналізу призвели до появи Big Data та розвитку технологій, які ефективно працюють з цими даними. Технології Big Data втілюють іноваційні концепції в не тільки медицину, бізнес, промисловість, науку, а також в побут людини.

Особливістю проектів IoT є збір, зберігання та аналіз великого потоку даних, які надходять від різнорідних датчиків , сенсорів та контролерів, кількість та якість яких постійно зростає, як і зростає різноманітність задач, які вирішуються з використанням IoT-технологій. Паралельно з технологічним розвитком відбувається розвиток програмного забезпечення для реалізації проектів IoT. Оскільки головною умовою проектів IoT є використання інтернету, для реалізації проектів з початку виникнення почали успішно застосовувати досвід розробки веб-сайтів, соціальних мереж та ін., де для збереження та обробки даних використовуються СУБД NoSQL. Як з’ясувалося, ці види СУБД максимально ефективно задовольняють вимогам работи зі слабоструктурованими та неструктурованими даними, які генеруються різними джерелами даних, зокрема датчиками та контролерами[1].

Сучасний ринок СУБД NoSQL доволі різноманітний. Вони реалізують як різні моделі збереження даних, так і різні можливості їх обробки та аналізу. СУБД NoSQL для IoT-проектів повинна забезпечувати високу швидкість збору даних від датчиків(зазвичай дані обробляються в реальному часі), маштабованість, гнучкість структури даних(датчики можуть змінювати формати даних) та надійність.

Найбільш популярні СУБД NoSQL для IoT:

- **Apache Cassandra (Колонкова):** Модель зберігання даних даних на базі сімейства стовпців (ColumnFamily), написана на мові Java, має високу стійкість до збоїв. Для взаємодії з БД використовується мова формування структурованих запитів CQL (Cassandra Query Language), Ефективна для обробки часових

рядів (Time-Series) та промислових IoT-проектів. Забезпечує високу швидкість запису, обробку даних та лінійне маштабування.

- **ScyllaDB (Колонкова):** Розглядається як альтернатива СУБД Cassandra, написана на C++ , що забезпечує в рази більшу пропускну спроможність та суттєво менші затримки (low latency) при роботі з великими даними. Автоматично адаптується до обладнання, що дозволяє максимально використовувати ресурси апаратури.
- **MongoDB (Документо-орієнтована):** Дані зберігаються в форматі BSON (бінарний JSON), що дозволяє зберігати дані в форматі дати та числовому форматі. Має потужну мову запитів, яка реалізує фільтрацію, сортування та агрегацію даних. Підтримує горизонтальне маштабування. Легко інтегрується.
- **Redis (Ключ-значення):** Розподілена СУБД, працює в оперативній пам'яті (in-memory), що забезпечує дуже швидке читання та запис. Має функції обробки структурованих даних, таких як списки, хеші таі множини. Підтримка транзакцій гарантує несуперечність та послідовність виконання команд. В разі виникнення проблем є можливість відкотити зміни. Має два режими збереження: періодична синхронізація даних на диск і ведення на диску логу змін. В режимі ведення змін гарантується повне їх збереження. Використовується для хешування та обробки даних в реальному часі.,
- **InfluxDB (Спеціалізована):**Написана на мові Go. Орієнтована на часові ряди (Time Series Data). Для обробки даних має спеціалізовану SQL-подобну мову. запитів з вбудованими функціями для роботи з часом і структурою даних що складається з, серій та точок даних. Кожна точка складається з кількох пар ключ-значення, які називаються множиною полів. Часто використовується для систем моніторінгу, метрик програмного забезпечення та даних сенсорів, оскільки автоматично видаляє старі дані.
- **Neo4j (Графова):** Призначена для работи з сильно взаємопов'язаними даними, забезпечує високую ефективність запитів, ACID-відповідність. Мова запитів Cypher. Використовуються для складних IoT-проектів, які потребують аналізу взаємозв'язків між пристроями.
- **ArangoDB (Мультимодельна):** Розроблена на мовіC++. Поєднує три моделі даних: документи (JSON), графи та пари «ключ-значення», завдяки чому можна використовувати одну базу для різних типів даних. Мова запитів AQL (ArangoDB Query Language) дозволяє робити складні вибірки.

Вдалий вибір СУБД NoSQ є важливим для успішної реалізації IoT-проекту та ефективного його функціонування[2].

Список використаних джерел

1. М.А. Демиденко Введення в сучасні бази даних: навч. посіб. /; НТУ «Дніпровська політехніка». – Д.:2020. – 38с. URL: https://shorturl.at/q72Xu

2. Н.В. Ситник, І.С. Зіов'єва – Організація баз даних NoSQL URL: https://shorturl.at/I5VWy

Лейбюк Володимир Володимирович
студент 4 курсу
спеціальності «Системний аналіз»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
lvvua2004@gmail.com
st8072954@stud.duikt.edu.ua

Головченко Артем Васильович
викладач кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ

АНАЛІЗ ВЕЛИКИХ ДАНИХ У СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ МЕТОДИ ТА ІНСТРУМЕНТИ

Стрімкий розвиток технологій Інтернету речей (IoT) зумовив лавиноподібне зростання обсягів даних, що генеруються мільярдами підключених пристроїв по всьому світу. За прогнозами аналітиків, до 2027 року кількість IoT-пристроїв перевищить 29 мільярдів одиниць, а щорічний обсяг даних, що продукуються ними, сягатиме сотень зетабайт [1]. Опрацювання таких масивів інформації потребує принципово нових підходів, що виходять за межі традиційних систем управління базами даних.

Поняття "великі дані" (Big Data) охоплює набори інформації, що характеризуються трьома ключовими властивостями - так званою моделлю "3V": великий обсяг (Volume), висока швидкість надходження (Velocity) та різноманітність форматів (Variety) [2]. Стосовно IoT-систем до цих характеристик додаються ще дві: достовірність (Veracity) та цінність (Value), що разом формують розширену модель "5V". Відповідно, ефективний аналіз IoT-даних вимагає комплексного підходу, що враховує всі п'ять вимірів.

Серед сучасних методів аналізу великих даних у контексті IoT найширшого застосування набули потокова обробка даних (stream processing), пакетна обробка (batch processing) та гібридні архітектури. Потокова обробка, реалізована, зокрема, у платформах Apache Kafka та Apache Flink, дозволяє аналізувати дані в режимі реального часу безпосередньо в процесі їх надходження від сенсорів і пристроїв [3]. Це особливо критично для застосувань, де затримка відповіді вимірюється мілісекундами, - наприклад, у системах промислової автоматизації або медичного моніторингу.

Пакетна обробка, натомість, оптимально підходить для виявлення довгострокових трендів та глибокого аналізу накопичених даних. Фреймворк Apache Hadoop із його розподіленою файловою системою HDFS залишається базовою технологією для зберігання і MapReduce-обробки петабайтних масивів IoT-даних [2]. Водночас Apache Spark, завдяки обчисленням у пам'яті (in-memory

computing), демонструє у 10-100 разів вищу продуктивність порівняно з класичним Hadoop при виконанні ітеративних алгоритмів машинного навчання.

Гібридна λ-архітектура (Lambda Architecture) поєднує переваги обох підходів: "швидкий шар" (speed layer) забезпечує оперативну обробку з невеликими затримками, тоді як "пакетний шар" (batch layer) формує точні агрегати на повних наборах даних [1]. Результати обох шарів об'єднуються у "шарі обслуговування" (serving layer) для відповіді на запити. Хоча λ-архітектура ускладнює розробку через необхідність підтримки двох кодових баз, вона залишається стандартом де-факто для корпоративних IoT-платформ.

Окремої уваги заслуговує застосування методів машинного навчання для аналізу IoT-даних. Алгоритми виявлення аномалій (anomaly detection) - зокрема, ізоляційні ліси (Isolation Forest) та автоенкодери на основі нейронних мереж - дозволяють автоматично виявляти несправності обладнання або кібератаки в режимі, близькому до реального часу [3]. Рекурентні нейронні мережі (RNN) та архітектура LSTM показують високу ефективність при прогнозуванні часових рядів IoT-даних - наприклад, у задачах передбачуваного технічного обслуговування (predictive maintenance).

Проведений аналіз дозволяє зробити такі висновки. По-перше, вибір методу обробки великих даних у IoT-системах визначається насамперед вимогами до затримки відповіді та обсягом оброблюваної інформації. По-друге, інтеграція методів машинного навчання з традиційними підходами Big Data відкриває нові можливості для інтелектуального аналізу IoT-потоків. По-третє, гібридні архітектури залишаються найбільш збалансованим рішенням для промислових застосувань, де критичні як оперативність, так і точність аналізу [2].

Список використаних джерел

1. Buyya, R., & Dastjerdi, A. V. (2016). Internet of Things: Principles and paradigms. Elsevier.

2. Marz, N., & Warren, J. (2015). Big data: Principles and best practices of scalable real-time data systems. Manning Publications.

3. Zaharia, M., Xin, R. S., Wendell, P., Das, T., Armbrust, M., Dave, A., Meng, X., Rosen, J., Venkataraman, S., Franklin, M. J., Ghodsi, A., Gonzalez, J., Shenker, S., & Stoica, I. (2016). Apache Spark: A unified engine for big data processing. Communications of the ACM, 59(11), 56–65. https://doi.org/10.1145/2934664

Федоренко Дмитро Олександрович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
fedorenko.dmitro05@gmail.com

Торошанко Ярослав Іванович
кандидат технічних наук, старший науковий співробітник,
доцент кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС СИНХРОНІЗАЦІЇ ДАНИХ У ГІБРИДНІЙ ЛОКАЛЬНО-ХМАРНІЙ ІНФРАСТРУКТУРІ

У сучасних інформаційних системах активно використовується підхід гібридної інфраструктури, який поєднує локальні сервери та хмарні сервіси для зберігання і обробки даних. Одним із найбільш поширених сценаріїв є резервування, дублювання та синхронізація файлів між локальним середовищем та хмарним сховищем Amazon S3. Такий підхід дозволяє підвищити надійність зберігання, забезпечити відмовостійкість та доступність даних, а також оптимізувати витрати на інфраструктуру [1].

Постановка задачі.

Основною задачею є забезпечення ефективної, надійної та ресурсоощадної синхронізації даних між локальним сервером і хмарним S3-сховищем. Проблематика полягає у великому обсязі даних, необхідності регулярного оновлення, обмеженнях пропускної здатності мережі та ризиках дублювання або втрати інформації. Стандартні підходи до копіювання (наприклад, повне дублювання) є неефективними, оскільки створюють надмірне навантаження на мережу та систему зберігання [2].

Мета дослідження.

Метою дослідження є оптимізація процесу синхронізації даних між локальним сервером та хмарним сховищем Amazon S3 за рахунок використання інкрементальних методів передачі даних та інструментів локальної синхронізації.

Результати дослідження.

У роботі розглянуто практичну модель організації синхронізації даних, яка базується на використанні інструментів командного рядка, таких як rsync, AWS CLI та rclone, що дозволяють ефективно працювати з файловими структурами та хмарними сховищами.

Основні підходи до синхронізації включають:

1. Інкрементальна синхронізація (rsync-подібний підхід) – передача лише змінених частин файлів, що значно зменшує обсяг трафіку.

2. Об’єктна синхронізація через AWS CLI (aws s3 sync) – порівняння локальної та віддаленої структури та передача лише відмінностей.

3. Універсальна синхронізація через rclone – підтримка різних хмарних сервісів та гнучка конфігурація процесу.

4. Планувальники задач (cron) – автоматизація процесу синхронізації у визначені інтервали часу [3].

Запропоновано узагальнену модель взаємодії, у якій локальний сервер виступає джерелом даних, а S3 – цільовим сховищем (рис. 1)

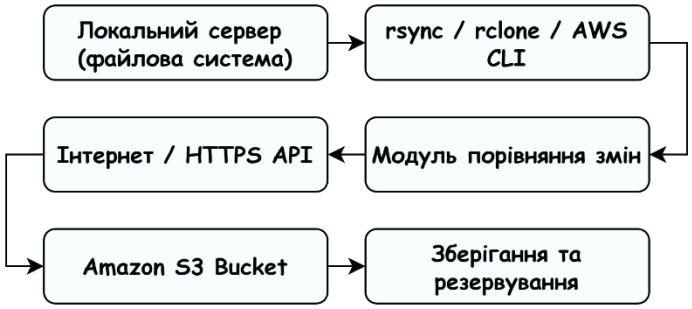

Рис. 1. Схема взаємодії системи синхронізації

У процесі синхронізації ключовими є такі механізми:

1. Порівняння контрольних сум або часу модифікації файлів для визначення змін.

2. Передача тільки змінених файлів або їх частин, що зменшує навантаження на мережу.

3. Підтримка двосторонньої синхронізації (за потреби).

4. Обробка помилок та повторні спроби передачі для забезпечення надійності.

Практичне застосування показує, що використання aws s3 sync є доцільним для базових сценаріїв, тоді як rclone забезпечує більшу гнучкість, а rsync – ефективність при роботі з локальними або змонтованими файловими системами [3].

Запропонований підхід дозволяє значно зменшити обсяг переданих даних, підвищити швидкість синхронізації та забезпечити стабільність роботи системи навіть при обмежених мережевих ресурсах [2].

Висновки та перспективи.

У результаті дослідження встановлено, що використання інкрементальних методів синхронізації у поєднанні з інструментами типу rsync, AWS CLI та rclone є ефективним рішенням для організації обміну даними між локальним сервером та Amazon S3.

Запропонована модель дозволяє мінімізувати мережеве навантаження, зменшити час передачі даних та забезпечити високу надійність процесу

синхронізації. Вона є практично застосовною та легко масштабованою у реальних умовах.

У подальшому доцільним є дослідження автоматизованих механізмів моніторингу синхронізації, інтеграції з системами контейнеризації, а також впровадження механізмів шифрування та контролю доступу для підвищення безпеки даних [4].

Список використаних джерел

1. AWS S3 Overview and Best Practices. Amazon Web Services. URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html (дата звернення: 12.04.2026)

2. Efficient Data Transfer and Synchronization Techniques. Google Cloud Blog. URL: https://cloud.google.com/blog/products/storage-data-transfer (дата звернення: 12.04.2026)

3. Rclone Documentation: Sync Command. Rclone.org. URL: https://rclone.org/commands/rclone_sync/ (дата звернення: 12.04.2026)

4. Data Security in Cloud Storage. IBM Cloud. URL: https://www.ibm.com/cloud/learn/cloud-storage-security (дата звернення: 13.04.2026)

Іващенко Роман Миколайович
студент групи КІД-41
Державного університету
інформаційно-комунікаційних технологій, м. Київ
r.ivashchenko2004@gmail.com

Лащевська Наталія Олександрівна
кандидат технічних наук, доцент,
завідувач кафедри Комп'ютерної інженерії
Державного університету
інформаційно комунікаційних технологій, м. Київ

СИСТЕМА АВТОМАТИЗОВАНОГО РОЗГОРТАННЯ ТА БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОНТЕЙНЕРИЗОВАНИХ ЗАСТОСУНКІВ ІЗ ВИКОРИСТАННЯМ DOCKER COMPOSE ТА GITHUB ACTIONS

Цифровізація сучасних інформаційних систем зумовлює необхідність автоматизації процесів розгортання програмного забезпечення та підвищення рівня безпеки доступу до серверної інфраструктури. Одним із ефективних підходів є використання контейнеризації разом із CI/CD-процесами, що дозволяє забезпечити швидке розгортання, масштабованість і контроль версій. Водночас, зростання кількості кіберзагроз актуалізує впровадження багатофакторної автентифікації (MFA) для захисту доступу до критичних ресурсів. Поєднання цих

підходів формує основу для створення сучасних автоматизованих інфраструктур [1].

Постановка задачі.

Основною проблемою є забезпечення безпечного та автоматизованого розгортання контейнеризованих застосунків у приватній серверній інфраструктурі. Традиційні методи розгортання часто потребують ручного втручання, що підвищує ризик помилок і знижує ефективність. Крім того, відсутність багаторівневого контролю доступу створює потенційні вразливості для несанкціонованого доступу.

Мета дослідження.

Метою дослідження є розробка та аналіз архітектури системи автоматизованого розгортання контейнеризованих застосунків із використанням Docker Compose та GitHub Actions, інтегрованої із системою багатофакторної автентифікації для доступу до приватної серверної інфраструктури.

Результати дослідження.

Запропонована система базується на використанні контейнерної технології Docker, яка дозволяє ізолювати застосунки та їх залежності. Для оркестрації контейнерів використовується Docker Compose, що забезпечує декларативний опис сервісів та їх взаємодії. Автоматизація процесу розгортання реалізується за допомогою GitHub Actions, який виконує збірку, тестування та деплой після внесення змін у репозиторій [1].

Система багатофакторної автентифікації включає:

- пароль як базовий фактор;
- одноразовий код (OTP);
- апаратний або програмний токен (наприклад, мобільний додаток).

Це дозволяє значно підвищити рівень захисту серверної інфраструктури та мінімізувати ризики компрометації облікових записів (рис. 1) [3].

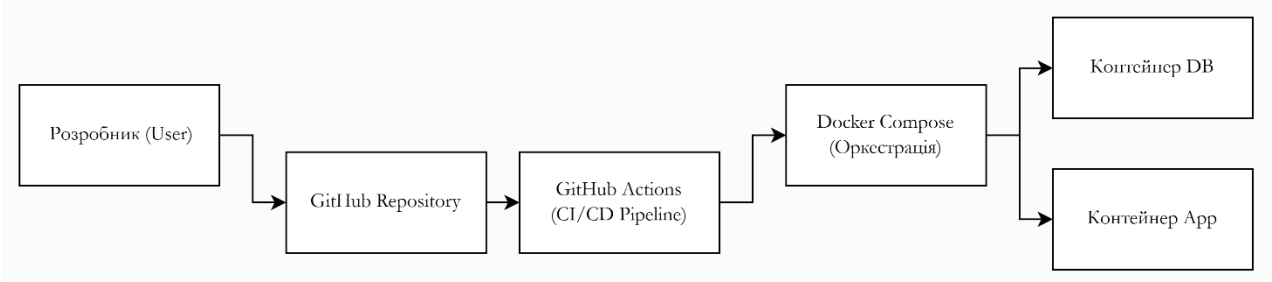

Рис. 1. Інтеграція GitHub Actions, Docker Compose та MFA у серверній інфраструктурі

У запропонованій моделі:

- GitHub виступає як система контролю версій;
- GitHub Actions автоматизує процес CI/CD;
- Docker Compose забезпечує запуск багатоконтейнерних застосунків;

- MFA контролює доступ до серверної інфраструктури.

Застосування такого підходу дозволяє:

- скоротити час розгортання;
- забезпечити відтворюваність середовища;
- підвищити рівень безпеки доступу;
- автоматизувати процеси адміністрування [2].

Крім того, система може бути розгорнута як на локальному обладнанні (наприклад, сервер або персональний комп'ютер із Docker Desktop), так і на хмарних платформах. Це забезпечує гнучкість та масштабованість рішення [3].

Висновки та перспективи.

У результаті дослідження встановлено, що поєднання контейнеризації, CI/CD та багатофакторної автентифікації є ефективним підходом до створення сучасних безпечних IT-систем. Запропонована архітектура дозволяє автоматизувати процеси розгортання, підвищити надійність інфраструктури та забезпечити захист доступу до серверних ресурсів.

Перспективними напрямами подальших досліджень є:

- інтеграція з системами оркестрації Kubernetes;
- використання штучного інтелекту для виявлення аномалій доступу;
- впровадження Zero Trust моделей безпеки;
- розширення функціональності MFA за рахунок біометричних методів автентифікації [4].

Список використаних джерел

1. Virtualization vs containerization. Scale Computing. URL: https://www.scalecomputing.com/resources/whats-the-difference-between-virtualization-vs-containerization (дата звернення: 13.04.2026)

2. CI/CD Pipelines Explained. Red Hat. URL: https://www.redhat.com/en/topics/devops/what-is-ci-cd (дата звернення: 13.04.2026)

3. Multi-Factor Authentication (MFA) Basics. Microsoft Security. URL: https://learn.microsoft.com/en-us/security/identity-protection/mfa-overview (дата звернення: 13.04.2026)

4. Zero Trust Security Model. IBM. URL: https://www.ibm.com/topics/zero-trust (дата звернення: 13.04.2026)

Дячук Назар Ігорович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
n.diachuk333@gmail.com

Шахматов Іван Олександрович
викладач кафедри
Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
i.shahmatov@duikt.edu.ua

ОЗНАКИ РИНКОВИХ МАНІПУЛЯЦІЙ ЧЕРЕЗ ПРИЗМУ АНАЛІЗУ ВЕЛИКИХ ТРАНЗАКЦІЙ У БЛОКЧЕЙНІ

Постановка задачі.

Криптовалютний ринок, попри технологічну відкритість блокчейну, залишається вразливим до цілеспрямованих маніпуляцій з боку великих учасників. Концентрація значних обсягів активів у відносно невеликої кількості власників – так званих «китів» – у поєднанні з низьким рівнем регуляторного нагляду та асиметрією інформації створює умови, за яких цінові сигнали можуть штучно спотворюватися. Це зумовлює потребу у систематичному дослідженні поведінкових патернів великих власників криптовалют з метою виявлення ознак маніпулятивної активності.

Попри публічність блокчейн-реєстрів, комплексний аналіз великих транзакцій для ідентифікації маніпуляцій залишається недостатньо дослідженим напрямом. Більшість наявних підходів зосереджені або на технічному моніторингу транзакцій без глибокої інтерпретації поведінкових патернів, або на статистичному аналізі цінових рядів без урахування on-chain даних. Відсутність системного підходу до поєднання цих двох аспектів ускладнює своєчасне виявлення маніпулятивної активності та формування аналітичних висновків.

Мета дослідження.

Метою дослідження є своєчасне виявлення ознак ринкових маніпуляцій на криптовалютному ринку на основі аналізу великих транзакцій у блокчейні та вдосконалення засобів моніторингу підозрілої активності шляхом розробки системи оперативного on-chain спостереження.

Результати дослідження.

В ході дослідження виявлено три основні схеми маніпулятивної поведінки, характерні для криптовалютного ринку, та розроблено практичну систему їх моніторингу.

Pump-and-dump – схема, при якій група пов'язаних адрес поступово акумулює низьколіквідний актив, після чого штучно піднімає його ціну через скоординовані купівлі та масово скидає на піку. On-chain ознаками є одночасна активація «сплячих» гаманців, різке зростання переказів на централізовані біржі перед ціновим піком та кластеризація активності навколо пов'язаних адрес.

Wash trading – штучне накручування торгового обсягу шляхом циклічних переказів між власними адресами без реального переходу активу. Виявляється через повторювані перекази між двома-трьома адресами, аномально рівномірний розподіл обсягів у часі та відсутність зростання кількості унікальних учасників при зростанні обсягів.

Координована акумуляція та дистрибуція – тривале накопичення активу групою пов'язаних адрес з наступним різким розподілом через вторинні гаманці. Діагностується через систематичний відтік коштів з бірж у холодні гаманці з подальшим різким збільшенням депозитів на торгових платформах.

На основі виявлених патернів розроблено систему Whale Tracker – платформу моніторингу великих транзакцій мережі Ethereum у реальному часі.

Система включає: веб-дашборд (Рис. 1) з відображенням live-транзакцій, графіками ETH-обсягів, тепловою картою активності, мережею адрес китів (Рис. 2) та кореляцією ціни ETH з обсягами whale-транзакцій; а також Telegram-бот (Рис. 3), що надсилає миттєві сповіщення при виявленні аномально великих транзакцій із зазначенням адрес відправника, отримувача та суми переказу.

Рис. 1. Веб-дашборд системи Whale Tracker

Рис. 2. Мережа адрес китів

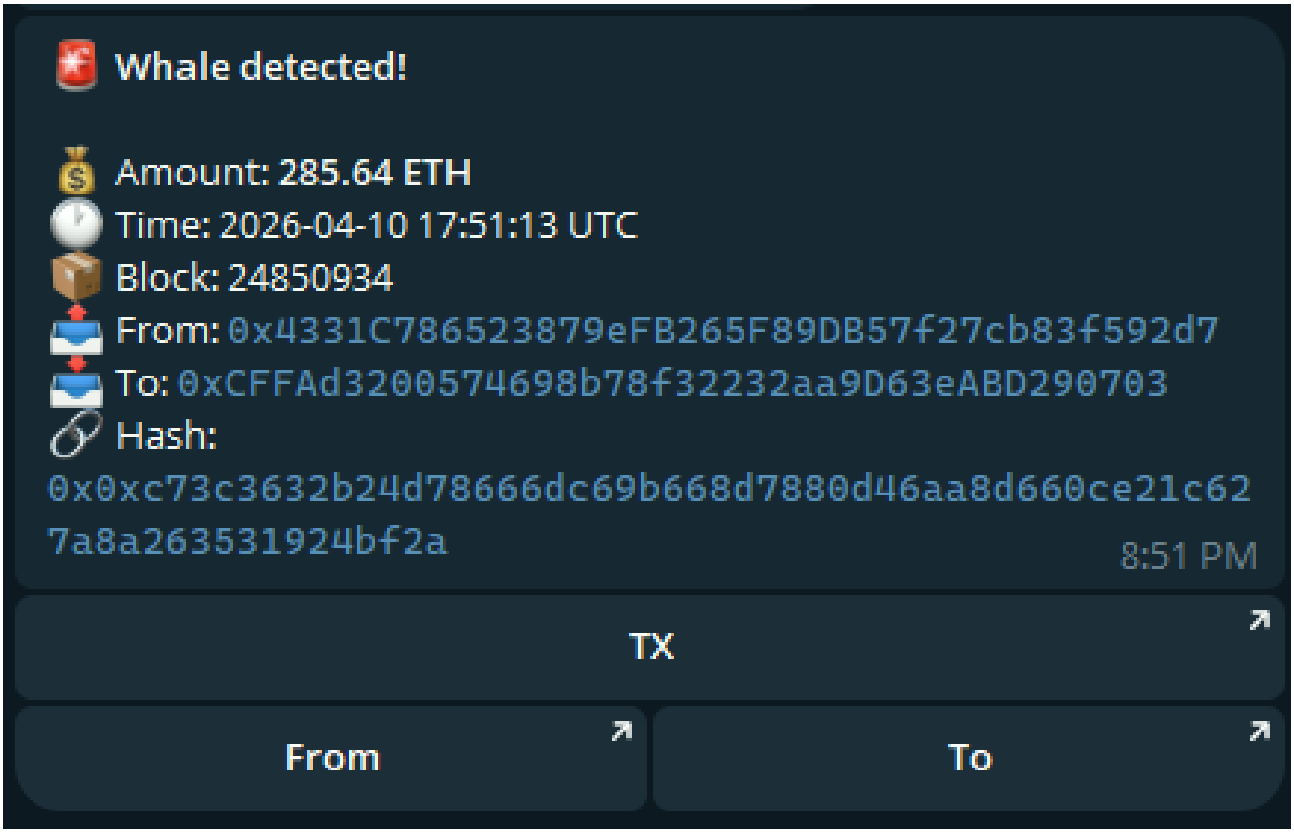

Рис. 3. Telegram-бот для сповіщень про великі транзакції

Висновки та перспективи.

Розроблена система підтвердила практичну можливість виявлення ознак маніпулятивної активності через аналіз on-chain даних у режимі реального часу. Характерні патерни – координована акумуляція, циклічні перекази, різкі зміни потоків між біржами та холодними гаманцями – утворюють «цифровий слід», доступний для автоматизованого аналізу завдяки відкритості блокчейн-реєстрів. Перспективи розвитку пов'язані з інтеграцією методів машинного навчання для

автоматичної класифікації підозрілих патернів та розширенням системи на інші блокчейн-мережі.

Список використаних джерел

1. Gandal N., Hamrick J. T., Moore T., Oberman T. Price Manipulation in the Bitcoin Ecosystem. Journal of Monetary Economics, 2018, Vol. 95, pp. 86–96.

2. Li T., Shin D., Wang B. Cryptocurrency Pump-and-Dump Schemes. SSRN Electronic Journal, 2019.

3. Cong L. W., Li X., Tang K., Yang Y. Crypto Wash Trading. Management Science, 2023, Vol. 69, No. 11.

4. Chainalysis. Crypto Crime Report 2024.

5. Glassnode. On-Chain Data Insights.

6. Binance Research. Market Behavior and On-Chain Analysis Reports.

7. Elliptic. Cryptoasset Risk & Compliance Reports.

НАПРЯМ 6. ІНТЕРНЕТ НАНО-РЕЧЕЙ (IONT)

Максимук Оксана Олексіївна
студентка 4 курсу
спеціальності «Проектування і програмування інтелектуальних систем та пристроїв»,
кафедри САП,
Інституту комп'ютерних наук та інформаційних технологій,
Національного університету "Львівська Політехніка", м.Львів
oksana.maksymuk.pp.2022@lpnu.ua

Зільник Марта Василівна
студентка 4 курсу
спеціальності «Проектування і програмування інтелектуальних систем та пристроїв»,
кафедри САП,
Інституту комп'ютерних наук та інформаційних технологій,
Національного університету "Львівська Політехніка", м.Львів
marta.zilnyk.pp.2022@lpnu.ua

Головацький Руслан Іванович
старший викладач кафедри САП,
Інституту комп'ютерних наук та інформаційних технологій,
Національного університету "Львівська Політехніка", м.Львів
ruslan.i.holovatskyi@lpnu.ua

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПІДТРИМКИ РІШЕНЬ В АГРОНОМІЇ НА ОСНОВІ IONT З ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ ДЛЯ АНАЛІЗУ ПАРАМЕТРІВ ҐРУНТУ ТА ПОГОДНИХ УМОВ

Сучасний розвиток сільського господарства передбачає активне впровадження цифрових технологій, зокрема концепції Internet of Nano-Things, яка забезпечує збір та передачу даних із використанням мікро- та наносенсорів. Застосування таких технологій дозволяє отримувати детальну інформацію про стан ґрунту та навколишнього середовища в реальному часі.

Одним із ключових завдань агрономії є визначення оптимального часу посіву, що залежить від комплексу факторів, зокрема вологості ґрунту, температури, кислотності та погодних умов [2], [3]. Традиційні методи прийняття рішень базуються на досвіді агрономів і не завжди враховують всі змінні, що може призводити до зниження врожайності.

У роботі запропоновано інтелектуальну систему підтримки прийняття рішень, що поєднує можливості Artificial Intelligence та Internet of Things / IoNT. Система передбачає використання сенсорної мережі для збору даних про параметри ґрунту (вологість, pH, температура) та інтеграцію з метеорологічними сервісами для отримання прогнозу погоди [5].

Архітектура системи включає такі основні компоненти:

- сенсорний рівень (датчики ґрунту);

- комунікаційний модуль (наприклад, Wi-Fi або LoRa);
- сервер обробки даних;
- інтелектуальний модуль аналізу на основі нейронної мережі.

Запропонована архітектура має багаторівневу структуру та включає такі компоненти (рис.1):

1. Сенсорний рівень (IoNT-рівень).

Забезпечує збір первинних даних із середовища за допомогою датчиків вологості ґрунту (VWC), температури, кислотності (pH), вмісту макроелементів (NPK), а також метеорологічних параметрів [2], [3]. Сенсори формують потік даних у реальному часі:

2. Комунікаційний рівень.

Передача даних здійснюється за допомогою бездротових технологій (Wi-Fi, LoRa), що дозволяє інтегрувати розподілені вузли в єдину мережу IoNT. На цьому етапі забезпечується агрегація та попередня передача даних до серверної частини.

3. Рівень обробки даних.

Виконує попередню обробку інформації, включаючи нормалізацію, фільтрацію шуму та перетворення даних до формату, придатного для аналізу. Також здійснюється інтеграція з зовнішніми джерелами, зокрема метеорологічними API [5].

4. Інтелектуальний аналітичний рівень.

На цьому рівні здійснюється аналіз даних за допомогою моделей машинного навчання.

Задача визначення оптимального часу посіву формалізується як задача регресії, де вхідний вектор включає параметри ґрунту та погодні умови: вологість ґрунту (VWC), тиск ґрунтової вологи (SWT), вміст макроелементів (NPK), кислотність ґрунту (pH), індекс сонячної радіації (SRI), температуру повітря, вологість та швидкість вітру.

Для врахування експертних знань використано елементи нечіткої логіки. Для кожного параметра визначено трапецієподібні функції належності, що дозволяють оцінювати ступінь відповідності умов оптимальним.

Фінальний індекс придатності обчислюється як зважена сума оцінок параметрів, де найбільшу вагу мають температура (0,20) та вологість ґрунту (0,15), що узгоджується з практичними агрономічними вимогами [2], [3].

Для прогнозування використано модель Neural Network типу багатошарового персептрона [1]. Архітектура моделі включає три приховані шари (128, 64, 32 нейрони) з функцією активації ReLU та шарами Dropout для запобігання перенавчанню. Навчання моделі здійснюється з використанням оптимізатора Adam та функції втрат MSE [4].

5. Рівень підтримки прийняття рішень.

На основі отриманого індексу система формує рекомендації щодо доцільності посіву та класифікує умови як сприятливі, ризиковані або критичні.

Важливою складовою системи є модуль візуалізації результатів. Зокрема, реалізовано:

• криві навчання, що демонструють зменшення помилки на тренувальній і валідаційній вибірках;

• діаграму розсіювання, яка показує високу кореляцію між прогнозованими та фактичними значеннями;

• гістограму помилок, що свідчить про концентрацію похибки біля нуля;

• радарну діаграму для візуального порівняння поточних умов із оптимальними профілями культур.

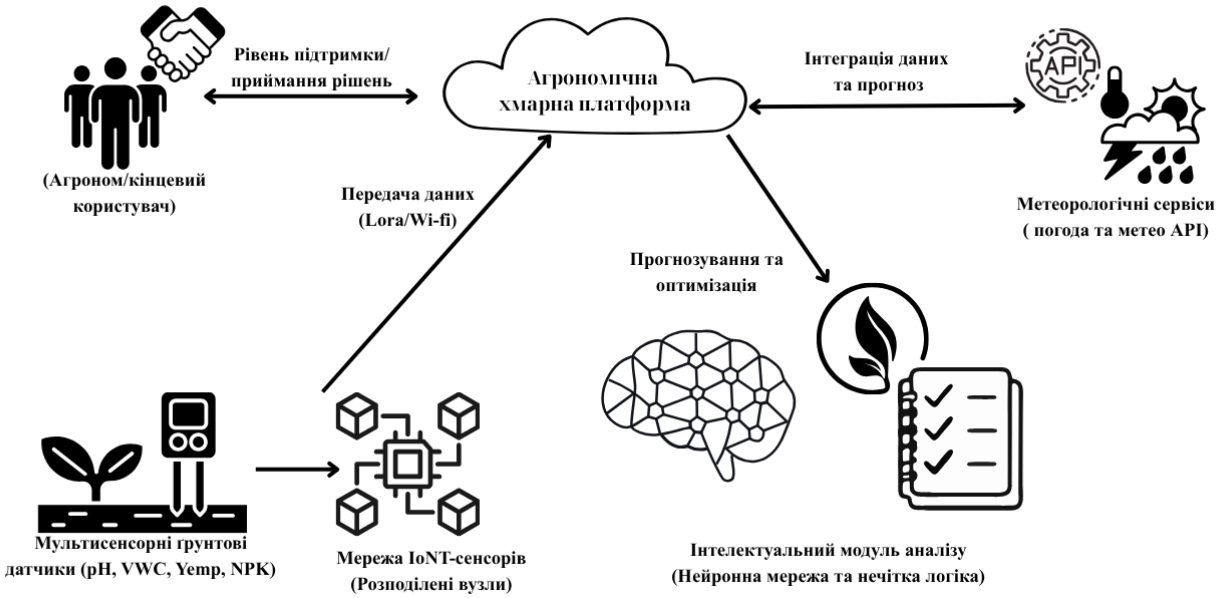

Рис. 1. Загальна архітектура системи

Аналіз результатів

Оцінка ефективності розробленої системи здійснюється за допомогою комплексу графічних візуалізацій (рис. 2–3).

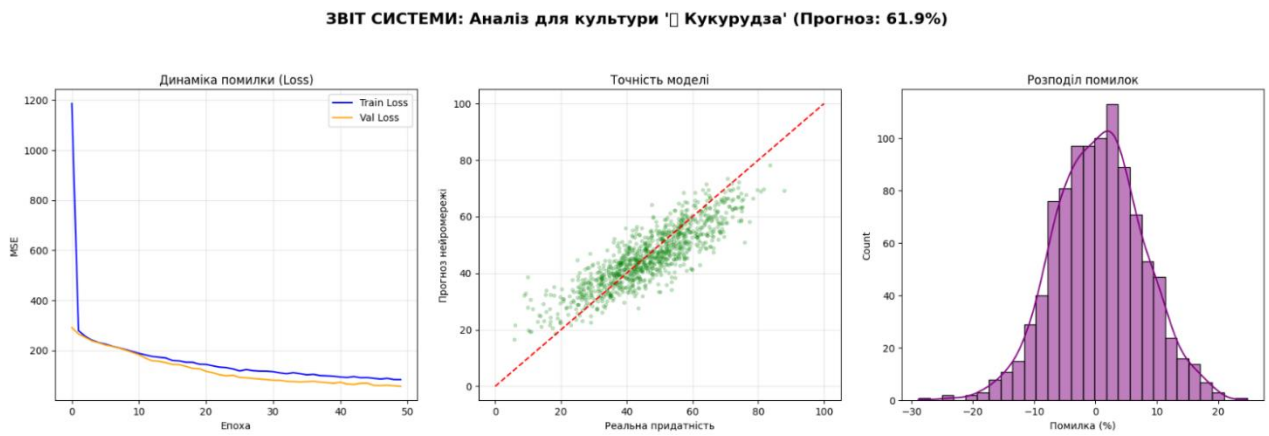

Рис. 2. Оцінка якості навчання нейронної мережі: динаміка функції втрат (ліворуч), порівняння реальних та прогнозних значень (центр) та гістограма розподілу помилок (праворуч)

Криві навчання моделі (рис. 2, зліва) демонструють стабільне зменшення функції втрат на тренувальній та валідаційній вибірках, що свідчить про коректне навчання моделі та відсутність перенавчання. **Діаграма розсіювання** (рис. 2, центр) підтверджує високу точність прогнозування, оскільки більшість точок розташована поблизу діагональної лінії ідеального прогнозу. **Гістограма помилок** (рис. 2, справа) показує концентрацію похибок біля нуля, що вказує на низький рівень відхилення прогнозів.

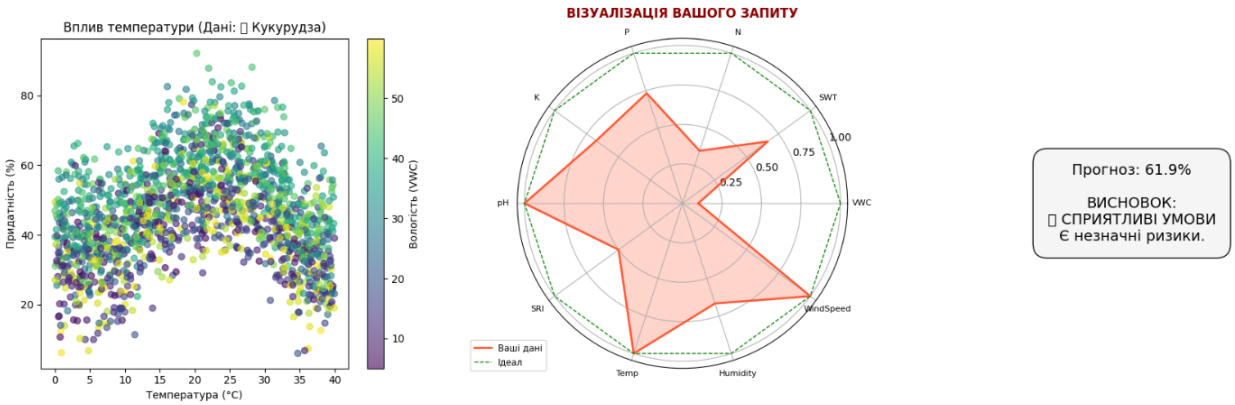

Рис.3. Аналіз прогнозування системи: залежність придатності від температури та вологості (ліворуч), порівняння поточних параметрів з оптимальними на радарній діаграмі та фінальний висновок (праворуч)

Додатковий **аналіз залежності індексу придатності від температури** (рис. 3, зліва) підтверджує наявність оптимального діапазону умов, характерного для агрономічних процесів. **Радарна діаграма** (рис. 3, справа) дозволяє порівняти поточні параметри середовища з оптимальними значеннями для конкретної культури, забезпечуючи наочну інтерпретацію результатів. Отримані результати підтверджують ефективність застосування нейронної мережі для

задачі прогнозування та доцільність використання системи у рамках технологій точного землеробства.

Запропонована система відповідає концепції Precision Agriculture та може бути використана для створення інтелектуальних агроінформаційних систем нового покоління.

Список використаних джерел

1. *IT Wiki. (n.d.). Багатошаровий перцептрон (Multilayer Perceptron). Отримано з https://itwiki.dev/data-science/ml-reference/ml-glossary/multilayer-perceptron*

2. *EOS Data Analytics. (2023). Вологість ґрунту: як вимірювати, зберігати та управляти. Отримано з https://eos.com/uk/blog/volohist-gruntu/*

3. *Агроексперт-Трейд. (n.d.). Аналіз ґрунту перед посівною: навіщо робити?. Отримано з https://agroexp.com.ua/uk/analiz-pochvy-pered-posevnoy-zachem-delat*

4. *Keras. (n.d.). Keras documentation: The Python deep learning library. Отримано з https://keras.io/api/*

5. *Open-Meteo. (n.d.). Open-Meteo weather API documentation. Отримано з https://open-meteo.com/en/docs*

НАПРЯМ 7. ІОТ В ОСВІТІ

Бойко Анастасія Юріївна
студентка 3 курсу
спеціальності «Комп'ютерні науки та інформаційні технології»
Харківського національного університету радіоелектроніки, м. Харків
anastasiia.boiko@nure.ua

Петрова Роксана Вадимівна
доцент, кандидат технічних наук
Комп'ютерного моделювання та інтелектуальних технологій
Харківського національного університету радіоелектроніки, м. Харків
roksana.petrova@nure.ua

ІНТЕЛЕКТУАЛЬНА IOT-СИСТЕМА НАГАДУВАНЬ ДЛЯ СТУДЕНТІВ

Сьогодні освітній процес активно трансформується під впливом цифрових технологій. Зокрема, застосування Інтернету речей (IoT) дозволяє автоматизувати частину щоденних задач студентів, пов'язаних із навчанням. Однією з таких задач є контроль розкладу та термінів виконання завдань [1]. У практиці навчання досить часто виникають ситуації, коли через перевантаження студенти пропускають важливі події або не встигають виконати завдання вчасно. Це свідчить про необхідність використання додаткових інструментів підтримки.

Метою цієї роботи є розробка концепції IoT-системи нагадувань, яка враховує індивідуальні особливості студента та допомагає більш ефективно планувати навчальну діяльність.

Запропонована система складається з кількох взаємопов'язаних компонентів: IoT-пристроїв, серверної частини та мобільного застосунку. Як IoT-пристрої можуть використовуватись смартфони, смарт-годинники або інші сенсори, які фіксують активність користувача, його місцезнаходження та повсякденні дії. Далі ці дані передаються на сервер, де відбувається їх обробка та аналіз із використанням відповідних алгоритмів [2].

Важливою характеристикою запропонованої системи є здатність підлаштовуватись під користувача. На відміну від стандартних календарів, вона не просто нагадує про події, а враховує поведінку користувача. Наприклад, система може аналізувати, коли студент найчастіше виконує завдання, та підлаштовувати нагадування під ці часові проміжки. Завдяки цьому повідомлення стають більш доречними та не ігноруються користувачем.

На нашу думку, впровадження таких систем може позитивно вплинути на організацію навчального процесу та допомогти студентам краще контролювати власний час.

Наукова новизна роботи полягає у використанні підходу, при якому нагадування формуються з урахуванням контексту та поведінки користувача. Це

дозволяє системі змінювати свою поведінку залежно від ситуації, що відрізняє її від традиційних рішень.

Для оцінювання ефективності системи може бути використана функціональна залежність:

$$E = f(A, T, C)$$

де:

A - активність користувача;

T - час доби;

C - контекст (місцезнаходження, розклад).

На рис. 1 представлено загальну структуру роботи системи.

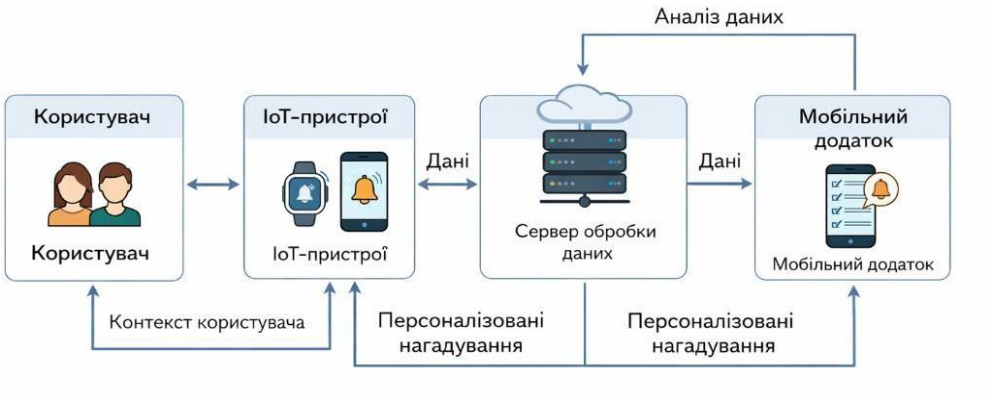

Рис. 1. Структура інтелектуальної IoT-системи нагадувань

Принцип функціонування полягає в тому, що після отримання даних від IoT-пристроїв система аналізує поточний стан користувача та формує відповідне нагадування. Наприклад, перебуваючи в університеті, студент отримує інформацію про найближчі заняття, тоді як вдома - про необхідність виконання завдань.

До основних переваг запропонованого підходу можна віднести:

- адаптацію до користувача;
- підвищення ефективності навчання;
- автоматизацію планування;
- можливість інтеграції з іншими цифровими сервісами.

У табл. 1 наведено порівняння звичайних систем нагадувань та запропонованої IoT-системи.

Табл. 1.

Порівняння систем нагадування

Характеристика	Звичайні системи	IoT-система
Тип нагадувань	Фіксований	Адаптивний
Урахування поведінки	Відсутнє	Присутнє
Контекст користувача	Не враховується	Враховується
Ефективність	Середня	Висока

Отже, запропоноване рішення спрямоване на покращення організації навчальної діяльності за рахунок врахування індивідуальних особливостей користувача. Такий підхід дозволяє більш гнучко формувати нагадування та підвищує ефективність використання часу. Подальший розвиток системи може бути пов’язаний із застосуванням методів штучного інтелекту для більш точного аналізу поведінки користувача [3].

Окремо варто зазначити, що подібні рішення можуть бути корисними не лише для студентів, а й для викладачів.

Список використаних джерел

1. *Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.*

2. *Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805.*

3. *Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.*

Олексюк Ганна Олексіївна
студентка групи ІСД-41
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
(050)-151-90-42
anna.oleksuk2004@gmail.com

Полоневич Ольга Володимирівна
кандидат технічних наук, доцент,
доцент кафедри Інформаційних систем
та технологій ДУІКТ, м. Київ
o.polonevych@duikt.edu.ua

ІНТЕРАКТИВНА СИСТЕМА ДЛЯ ВИВЧЕННЯ КИТАЙСЬКОЇ ІЄРОГЛІФІКИ ЧЕРЕЗ ВІЗУАЛІЗАЦІЮ ЛОГІЧНИХ ЗВ'ЯЗКІВ: ТЕХНОЛОГІЧНІ АСПЕКТИ ТА МОЖЛИВОСТІ IoT-ІНТЕГРАЦІЇ

Актуальність дослідження. Сучасний освітній простір зазнає суттєвої трансформації під впливом цифрових технологій. Концепція "Internet of Things" (IoT) – мережевої взаємодії інтелектуальних об'єктів – все активніше проникає в освітнє середовище, формуючи так звані "розумні" навчальні екосистеми, де дані про поведінку та прогрес користувача автоматично опрацьовуються та

адаптуються під індивідуальні потреби [2]. Саме в цьому контексті розробка інтерактивних навчальних систем з елементами збору й аналізу даних набуває особливої значущості.

Вивчення китайської мови є особливо показовим прикладом: складність ієрогліфічної писемності вимагає принципово нових підходів до організації навчального процесу, які ґрунтуються на принципах когнітивної психології та сучасної веб-архітектури. Більшість наявних цифрових інструментів зосереджені виключно на механічному запам'ятовуванні, нехтуючи асоціативними зв'язками між символами, і практично не мають україномовного інтерфейсу.

Мета та завдання. Метою роботи є проектування та реалізація інтерактивної веб-системи для вивчення китайської ієрогліфіки, яка поєднує візуалізацію семантичних і графічних зв'язків між символами у формі динамічних ментальних карт із забезпеченням повноцінної україномовної підтримки. Система розроблена на принципах клієнт-серверної архітектури з REST API [5], що дозволяє інтегрувати її у більш широку IoT-екосистему розумного навчального середовища.

Архітектура системи та технічні рішення. Розроблена система побудована за багатошаровою архітектурою. Серверна частина реалізована як REST API на базі фреймворку Spring Boot (Java) [5], що забезпечує стабільну обробку запитів, масштабованість і зручну інтеграцію з зовнішніми сервісами перекладу. Клієнтська частина розроблена засобами React.js [4] – сучасного фреймворку для побудови реактивних односторінкових застосунків. Особливу увагу приділено розробці інтерфейсу за принципами Bento Grid та стилістики Glassmorphism, що дозволяє знизити когнітивне навантаження при роботі з великими масивами графічних даних.

Ключовим елементом системи є модуль графової візуалізації, реалізований за допомогою силових алгоритмів (Force-directed graph), що забезпечує динамічну адаптацію структури графа при зміні фокусу навчання користувачем. Ієрогліфи відображаються як інтерактивні вузли, з'єднані ребрами відповідно до типу зв'язку: спільний радикал, семантична схожість, тематична належність або похідна структура. Наприклад, ієрогліф 木 ("дерево") пов'язується з 林 ("ліс", два дерева) та 森 ("гущавина", три дерева), ілюструючи принцип композиційного нарощення значення. Такий підхід активує механізми асоціативного мислення та сприяє якісному довготривалому запам'ятовуванню відповідно до теорії подвійного кодування [3].

Інформаційне забезпечення системи базується на інтеграції даних словника CC-CEDICT [1] з розробленою графовою моделлю семантичних зв'язків. Кожен ієрогліф у базі містить: написання, транскрипцію піньїнь, українські та англійські значення, список радикалів, тематичні теги та приклади вживання у словах і реченнях.

Можливості IoT-інтеграції та перспективи розвитку. Розроблена система спроектована з можливістю інтеграції в IoT-орієнтоване освітнє середовище [2]. REST API забезпечує підключення програмних модулів моніторингу навчального прогресу: трекінг дій користувача, частота помилок, маршрути навігації по графу. Ці дані формують базу для learning analytics – підходу до адаптивного навчання, що є невід'ємною складовою концепції smart learning environment. Таким чином, система може функціонувати як інтелектуальний вузол більш широкої освітньої екосистеми, передаючи аналітичні дані про навчальну активність користувача через стандартизований REST-інтерфейс.

У подальшому планується розширення функціоналу системи за рахунок: модуля розпізнавання ієрогліфів із рукописного вводу; рекомендаційного двигуна на основі алгоритмів машинного навчання для автоматичного формування персоналізованих карт знань; мобільного клієнта та елементів гейміфікації. Реалізація цих компонентів дозволить повноцінно інтегрувати систему в IoT-орієнтовану навчальну екосистему з адаптивним навчальним маршрутом для кожного користувача.

Висновки. Розроблена система є прикладом міждисциплінарного поєднання лінгвістики, когнітивної психології та сучасних веб-технологій. Вона забезпечує якісно новий рівень вивчення китайської мови для україномовних користувачів: замість механічного заучування символів – побудову живих асоціативних мереж знань. Відкрита архітектура системи та відповідність принципам IoT-освіти роблять її перспективним компонентом розумного навчального середовища, що підтверджує доцільність використання візуально-орієнтованих підходів у вивченні складних мовних систем.

Список використаних джерел

1. CC-CEDICT. CC-CEDICT: Chinese-English dictionary project. URL: https://cc-cedict.org/wiki/.

2. Systems C. IoT in education: Smart learning environments. URL: https://www.cisco.com/c/en/us/solutions/industries/education/iot.html.

3. Ковряга О. О., Нагорна Н. В. Ментальні карти у вивченні мов. Наукові записки Одеського національного університету імені І. І. Мечникова. Серія: Філологічні науки. 2021. С. 206–210. URL: https://dspace.onu.edu.ua/bitstream/123456789/36485/1/206-210.pdf.

4. Source M. O. React developer guide. URL: https://react.dev/.

5. VMware. Spring Boot: Spring framework project overview. URL: https://spring.io/projects/spring-boot.

Дмитрієва Анастасія Анатоліївна
студентка 5 курсу,
спеціальності «Комп'ютерні науки»,
Державного університету інформаційно-комунікаційних технологій, м. Київ
st01243796@stud.duikt.edu.ua

Катков Юрій Ігорович
професор, доктор технічних наук

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ВЕЛИКИХ ДАНИХ В ЕКОСИСТЕМІ ІОТ З МЕТОЮ ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ

Вступ

Успіх сучасних цифрових екосистем безпосередньо залежить від здатності компаній оперативно реагувати на динамічні зміни в поведінці аудиторії. Стрімкий розвиток концепції Internet of Things (IoT) дозволяє збирати колосальні обсяги телеметрії безпосередньо з пристроїв та сенсорів, що фіксують активність користувача в режимі реального часу. Зокрема, у сфері цифрової освіти впровадження методів машинного навчання для аналізу великих даних в екосистемі IoT дозволяє трансформувати бізнес-процеси навчальних закладів шляхом переходу до персоналізованих траєкторій навчання [1]. Використання інтелектуальних сенсорів для моніторингу залученості студентів та аналізу паттернів взаємодії з навчальним контентом дає змогу автоматично ідентифікувати прогалини в знаннях та оптимізувати адміністративне управління ресурсами закладу. Це створює адаптивне освітнє середовище, де прогнозування успішності та запобігання відтоку здобувачів освіти базується на об'єктивній телеметрії, а не лише на періодичному оцінюванні.

Однією з найгостріших проблем залишається відтік клієнтів (churn), оскільки витрати на утримання існуючого користувача є значно нижчими за вартість залучення нового. Традиційні методи аналізу не забезпечують необхідної адаптивності в умовах безперервного потоку даних, що потребує впровадження інтелектуальних систем прогнозування [2, 3] (рис. 1).

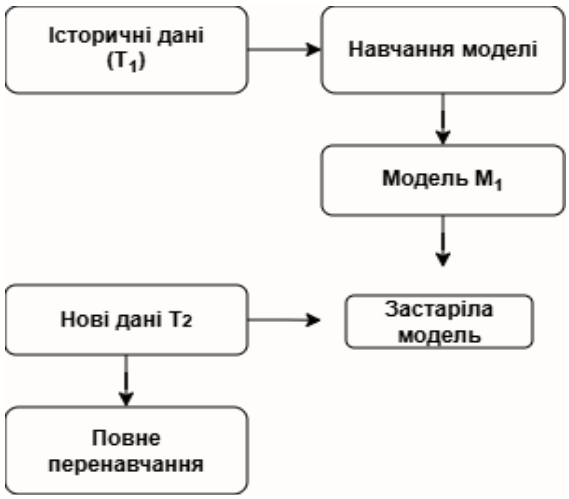

Рис. 1. Традиційний (статичний) підхід

Аналіз переваг та недоліків існуючих розробок. Сучасні системи прогнозування базуються переважно на статичних моделях навчання. Їхньою перевагою є висока точність на фіксованих історичних даних, проте вони мають суттєві недоліки: швидка втрата актуальності при зміні поведінкових патернів та висока вартість повного перенавчання (retraining). Дослідження [4, 5, 6] вказують на те, що в IoT-середовищах обробка сигналів супроводжується високим рівнем «шуму», що вимагає складніших архітектурних рішень для фільтрації та стабілізації прогнозів.

Мета роботи. Підвищення ефективності управління бізнес-процесами шляхом обґрунтування адаптивної архітектури для прогнозування відтоку користувачів у IoT-середовищі на основі інкрементального навчання.

Постановка завдання.

Необхідно розробити п’ятирівневу модель обробки даних, яка б інтегрувала сигнали від мережі сенсорів, забезпечувала їх інтелектуальну оптимізацію та дозволяла моделі адаптуватися до нових патернів у режимі реального часу без втрати раніше здобутих знань.

Результати дослідження.

Запропонована п’ятирівнева архітектура розроблена для роботи в умовах високої інтенсивності даних, що характерно для сучасних екосистем Internet of Things (IoT). Вона забезпечує стабільність прогнозів у динамічному бізнес-середовищі за наступною логікою (рис. 2):

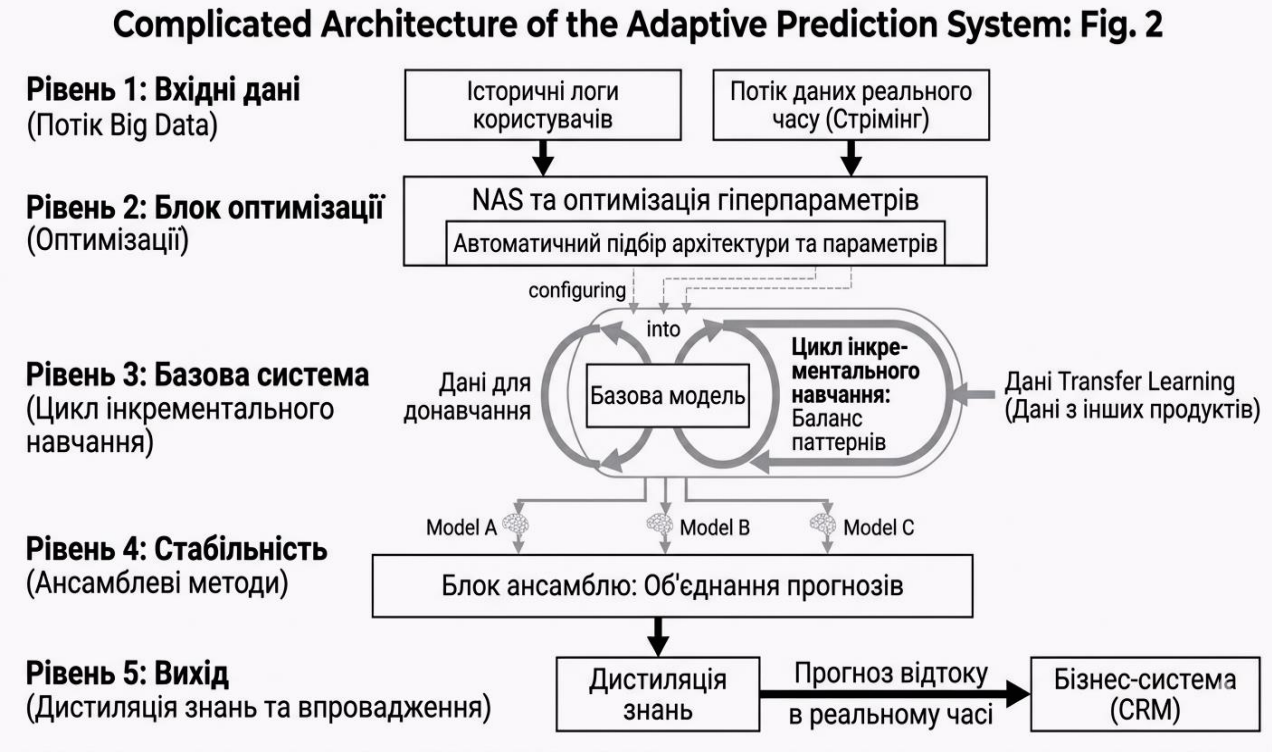

Рис. 2. Комплексна архітектура адаптивної системи прогнозування відтоку на основі інкрементального навчання та методів оптимізації

На рис. 2 показано:

Рівень 1: Вхідні дані та сенсорна мережа. На відміну від класичних систем, що базуються лише на транзакційних логах, дане рішення орієнтоване на обробку сигналів від мережі IoT-пристроїв та інтелектуальних сенсорів, які безпосередньо фіксують фізичну та цифрову активність користувача. Система одночасно опрацьовує два типи інформаційних потоків:

- Глибокі історичні бази даних, що накопичують телеметрію та показники активності за тривалі періоди для виявлення фундаментальних трендів поведінки.
- Стрімінгові дані реального часу, які надходять безпосередньо від сенсорів (наприклад, розумних гаджетів, датчиків присутності або терміналів самообслуговування). Це дозволяє фіксувати миттєві зміни у патернах використання продукту та ідентифікувати аномалії, що передують відтоку, ще на етапі їх зародження.

Рівень 2: Блок інтелектуальної оптимізації. Отримані з IoT-пристроїв дані характеризуються високим рівнем «шуму» та неоднорідністю. Для їх ефективної обробки використовуються технології Neural Architecture Search (NAS) та автоматичне налаштування гіперпараметрів. Це дозволяє системі автоматично конфігурувати модель під конкретний тип сенсорних даних, мінімізуючи потребу в ручному втручанні та адаптуючи аналітичний апарат до специфіки конкретного бізнес-процесу.

Рівень 3: Базова система та цикл інкрементального навчання. Це ядро системи, де реалізовано механізм Incremental Learning. Оскільки потік даних від IoT-пристроїв є безперервним, повне перенавчання моделей є ресурсозатратним. Тому на початковому етапі застосовується Transfer Learning для ініціалізації базової моделі знаннями, отриманими з суміжних екосистем або аналогічних продуктів. Це створює надійну стартову точку (pre-trained model), що особливо важливо в умовах дефіциту цільових даних на старті. Надалі, оскільки потік телеметрії від IoT-пристроїв є безперервним , базова модель проходить через постійний цикл донавчання (fine-tuning). Використання інкрементального підходу дозволяє моделі проходити через постійний цикл донавчання, інтегруючи нові поведінкові патерни в режимі «on-the-fly» та зберігаючи при цьому накопичений досвід про попередні стани системи та уникаючи катастрофічного забування [5, 6].

Рівень 4: Стабільність (Ансамблеві методи). Для мінімізації помилок окремих алгоритмів та підвищення стійкості до «шуму» в IoT-даних результати декількох моделей (Model A, B, C) об'єднуються у блок ансамблю. Це забезпечує високу точність прогнозування навіть при наявності «шуму» у даних сенсорної мережі. До складу ансамблю включено різнорідні алгоритми інкрементального навчання, зокрема: Online Random Forest для обробки нелінійних залежностей, Incremental SVM для стабільної класифікації в умовах концептуального зсуву (concept drift) та адаптивні дерева рішень Hoeffding Trees. Такий підхід забезпечує високу точність прогнозування навіть при аномальних сплесках активності в сенсорній мережі.

Рівень 5: Вихід (Дистиляція знань та впровадження). На цьому рівні складна ансамблева модель (модель-вчитель) проходить через офлайн-процес дистиляції знань. Це дозволяє перенести інтелектуальний потенціал ансамблю в компактну та архітектурно простішу модель-учня (student model). Отримана в результаті дистиляції модель потребує значно менше обчислювальних ресурсів, що дозволяє вже на етапі експлуатації (inference) генерувати прогнози відтоку в режимі реального часу з мінімальною затримкою (low latency) для миттєвої передачі результатів у CRM-систему.

Оцінювання ефективності запропонованої архітектури здійснюється не лише за технічними метриками точності (Accuracy, F1-score), а й за ключовими бізнес-показниками:

1. Churn Rate (Коефіцієнт відтоку клієнтів). Це відсоток користувачів, які перестали користуватися продуктом або послугою за певний період. П'ятирівнева архітектура спрямована на прогнозування цього показника в реальному часі.

2. LTV (Lifetime Value – Довічна вартість клієнта). Сукупний чистий прибуток, який компанія отримує від одного клієнта за весь час співпраці з ним. Використання інкрементального навчання дозволяє утримувати клієнта довше,

адаптуючи сервіс під його потреби, що безпосередньо подовжує «життєвий цикл» користувача та збільшує його LTV.

3. CAC (Customer Acquisition Cost – Вартість залучення клієнта). Сума всіх витрат на маркетинг та продаж, необхідних для залучення одного нового клієнта. Утримання існуючого клієнта є значно дешевшим за залучення нового, система оптимізації дозволяє бізнесу зменшити залежність від високих витрат на CAC, фокусуючись на збереженні поточної бази.

4. Time-to-Response (Час реагування на ризик). Це метрика швидкості, що визначає проміжок часу між виявленням аномалії в поведінці користувача та моментом прийняття управлінського рішення. Завдяки дистиляції знань (Рівень 5) та обробці стрімінгових даних (Рівень 1), така система забезпечує мінімальний час реагування, що дозволяє автоматично надсилати персоніфіковані пропозиції в CRM ще до того, як клієнт остаточно піде.

5. ROI (Return on Investment – Рентабельність інвестицій). Показник прибутковості, що відображає відношення отриманого ефекту до витрат на розробку та підтримку системи. Використання інкрементального підходу замість повного перенавчання моделей знижує витрати на обчислювальну інфраструктуру, що підвищує загальний ROI впроваджуваного рішення.

Отже, використання інкрементального підходу дозволяє мінімізувати Churn Rate завдяки превентивному реагуванню на зміни в поведінці користувачів. Це безпосередньо впливає на зростання LTV сукупного прибутку від клієнта за весь час співпраці, та зниження CAC, оскільки витрати на утримання стають прогнозованими та автоматизованими. Таким чином, система забезпечує вимірюваний економічний ефект для бізнес-екосистеми.

Висновки та перспективи

Запропонований підхід забезпечує високу адаптивність системи прогнозування в умовах безперервного потоку IoT-даних. Основні результати підтверджують, що поєднання інкрементального навчання та ансамблевих методів дозволяє знизити витрати на обчислювальну інфраструктуру та підвищити точність ідентифікації ризиків відтоку.

Перспективи подальших досліджень полягають у впровадженні механізмів Federated Learning (федеративного навчання). Це дозволить тренувати моделі безпосередньо на edge-пристроях користувачів, не передаючи сирі сенсорні дані на центральний сервер, що розв'яже питання конфіденційності. Також доцільним є дослідження стійкості ансамблю до навмисних спотворень сигналів (adversarial attacks) у відкритих IoT-мережах

Список використаних джерел

1. Катков Ю. Нечипорук А. (2025). «Жива траєкторія навчання» на основі редукованих моделей першого наближення в адаптивній платформі вивчення англійської мови/ International Science Journal of Engineering & Agriculture2025; 4(6): 28-46/ ISSN: 2720-6319/ URL: https://isg-journal.com/isjea/issue/view/89/ DOI: https://doi.org/10.46299/j.isjea.20250406

2. ОЛЕКСІВ, Т. І. (2025) Застосування машинного навчання для автоматизованого оцінювання управління бізнес-процесами в IT-підприємствах. Актуальні питання економічних наук, 2025, 9. URL: https://a-economics.com.ua/index.php/home/article/view/374

3. Zheng, H., et al. (2023) Incremental Learning-Based Framework for Churn Prediction in Complex Networks. IEEE Access. 2023. Vol. 11. URL: https://ieeexplore.ieee.org/document/10078274

3. Smith, J., Lee, K. (2024) Neural Architecture Search for Time-Series Sensor Data. Sensors (Basel). 2024. Vol. 24, No. 1. URL: https://www.mdpi.com/1424-8220/24/1/123

4. Mahajan, S., et al. (2022) Design and development of an open-source framework for citizen-centric IoT. Scientific Reports. 2022. Vol. 12. DOI: 10.1038/s41598-022-18700-z. URL: https://www.nature.com/articles/s41598-022-18700-z

5. Mokrani, H., et al. (2024) Smart Environmental Monitoring: Architecture and Protocols. Sensors. 2024. Vol. 24. URL: https://doi.org/10.3390/s24010123

6. Laha, S. R., et al. (2022) Advancement of Environmental Monitoring System Using IoT and Sensor: A Comprehensive Analysis. AIMS Environmental Science. 2022. Vol. 9, No. 6. DOI: 10.3934/environsci.2022044. URL: https://www.aimspress.com/article/doi/10.3934/environsci.2022044

Ахмедов Амір Фарідович
студент 2 курсу
спеціальності «Кібербезпека та захист інформації»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
infoforamir@gmail.com

Рашидов Сейфулла Фейзуллайович
доктор педагогічних наук, кандидат філософських наук,
професор кафедри Загальної педагогіки та спеціальної освіти
Ізмаїльського державного гуманітарного університету, м. Ізмаїл
seifulla.rashydov@gmail.com

ТРАНСФОРМАЦІЯ ІНТЕРНЕТУ РЕЧЕЙ В ОСВІТІ ВНАСЛІДОК ВПРОВАДЖЕННЯ ДЕЦЕНТРАЛІЗОВАНИХ ІДЕНТИФІКАТОРІВ

Сучасна концепція «розумного кампусу» (Smart Campus) нерозривно пов'язана з розгортанням мереж Інтернету речей (IoT). IoT-пристрої стали невід'ємною частиною освітнього процесу від автоматизованих систем контролю доступу до складних лабораторних стендів. Проте існуюча архітектура цих систем здебільшого базується на централізованих моделях ідентифікації: сервери Active Directory, хмарні логіни (OAuth через Azure AD), RFID-картки або паролі. Зазначена архітектура породжує системні недоліки, на кшталт неможливості використовувати єдині облікові дані в різних університетах, високий ризик витоку персональних даних при зламі центральної бази, а також повну залежність

від адміністратора кожної окремої системи. У разі недоступності сервера внаслідок кібератаки або відключення інтернету IoT-інфраструктура «розумного кампусу» може повністю паралізуватися [2].

Альтернативою є концепція децентралізованих ідентифікаторів (Decentralized Identifiers, DID) та самосуверенної ідентичності (Self-Sovereign Identity, SSI), що стандартизована консорціумом W3C та реалізована у технологічних протоколах Hyperledger Indy від Linux Foundation й ION від Microsoft [4].

Концептуальні основи DID та SSI

DID (Decentralized Identifier) - це унікальний цифровий ідентифікатор, який створюється та контролюється безпосередньо його власником без необхідності звернення до централізованого реєстратора. Згідно зі стандартами W3C, DID вказує на документ DID (DID Document), що містить публічні ключі та сервісні точки, необхідні для автентифікації без розкриття персональної інформації [5]. На відміну від традиційного логіну або email, DID не прив'язаний до конкретної організації.

SSI (Self-Sovereign Identity) - це парадигма, за якою людина самостійно зберігає свої ідентифікаційні дані у цифровому гаманці (наприклад, на смартфоні) та надає до них доступ виключно на власний розсуд. Важливо зазначити, що організація (університет) не контролює сам ідентифікатор користувача, але може видавати та відкликати верифіковані облікові дані (Verifiable Credentials, VC). Таким чином, забезпечується розподіл контролю, коли користувач володіє ідентичністю, а організація здійснює підтвердження певних атрибутів.

Проблематика централізованого IoT у закладах освіти

Відсутність відмовостійкості У разі недоступності центрального серверу автентифікації через аварію, кібератаку або відключення інтернету, вся периферія (розумні замки, принтери, лабораторні термінали) блокується.

Низький рівень інтероперабельності Кожен навчальний заклад використовує власну систему ідентифікації. У межах програм академічної мобільності (наприклад, Erasmus+) студенти стикаються з бюрократичною складністю отримання доступу до локальних ресурсів іншого вишу, оскільки їхня ідентичність «замкнена» в базі домашнього університету.

Приватність та безпека Централізоване зберігання персональних даних створює так звані «honeypots» (медові пастки) - пріоритетні цілі для кібератак. Для банального відкриття дверей у лабораторію система часто вимагає повний доступ до профілю студента, хоча для виконання дії достатньо знати лише факт наявності права доступу.

Трансформація IoT внаслідок впровадження DID/SSI

Впровадження децентралізованих протоколів радикально змінює архітектуру взаємодії «людина - пристрій». Ключова ідея підходу полягає в тому,

що студент зі своїм DID-гаманцем у смартфоні може миттєво авторизуватися на будь-якому IoT-пристрої у будь-якому університеті світу, якщо вони підтримують спільний протокол. Це забезпечується тим, що DID не потребує звернення до «рідного» сервера, бо він верифікується через розподілений реєстр (ledger) або через прямі peer-to-peer канали (DIDComm).

Децентралізована автентифікація на периферії IoT-пристрій завдяки використанню DID перетворюється на самостійний верифікатор, який використовуючи легкі криптографічні бібліотеки (наприклад, did-esp32 для мікроконтролерів) може самостійно перевірити цифровий підпис студента через NFC/Bluetooth-з'єднання зі смартфоном. Це забезпечує автономність, адже система залишається працездатною навіть за повного відключення інтернету в кампусі.

Застосування доказів з нульовим розголошенням (ZKP) SSI дозволяє використовувати технологію Zero-Knowledge Proofs. У освітньому середовищі це означає, що пристрій може отримати відповідь на запит «Чи має цей користувач право доступу до лабораторії?» не знаючи імені, прізвища, номера групи чи історії попередніх дій студента. Так реалізується принцип «вбудована приватність» (privacy by design), мінімізуючи обсяг даних, що передаються мережею.

Глобальна інтероперабельність та єдина ідентичність Оскільки DID базуються на відкритих стандартах W3C, студент із Києва, приїжджаючи до університету в Берліні, може використовувати той самий цифровий гаманець. IoT-система німецького вишу перевіряє верифіковані дані (VC), видані українським університетом, через глобальну «мережу довіри» (Trust Framework), таку як European Blockchain Services Infrastructure (EBSI) або Gaia-X [1, 3]. Жодної попередньої реєстрації в локальній базі даних не потрібно, що фактично формує передумови для створення глобальної освітньої екосистеми з єдиним простором довіри.

Захист від атак на центральну базу Оскільки персональні дані студентів не зберігаються на сервері університету (вони знаходяться лише в DID-гаманці самого студента), компрометація сервера суттєво знижує ризик витоку конфіденційної інформації. Навіть якщо дані DID-ідентифікаторів потраплять до зловмисника, особиста інформація залишиться в безпеці, оскільки доступ до неї неможливий без приватних ключів.

Перешкоди та перспективи впровадження

Незважаючи на значний потенціал, впровадження DID/SSI в IoT-інфраструктуру освіти супроводжується низкою викликів. Головною перешкодою є не технічна складність рішення, а відсутність масової підтримки DID у комерційних IoT-пристроях та освітніх інформаційних системах. Більшість виробників досі інтегрують лише централізовані протоколи (MQTT з паролями, OAuth через Azure AD тощо).

Іншими викликами є складність управління криптографічними ключами для кінцевих користувачів (втрата смартфона з DID-гаманцем може призвести до втрати доступу), недостатня стандартизація протоколів взаємодії між різними системами, а також питання масштабованості розподілених реєстрів.

Водночас стрімкий розвиток децентралізованих ідентифікаторів у Європі (проекти Gaia-X та EBSI) та поява легких DID-бібліотек для мікроконтролерів свідчить про реалістичність повноцінного впровадження DID/SSI в IoT-інфраструктуру освіти протягом 5-7 років [1, 3].

Висновки

Впровадження DID/SSI трансформує IoT-інфраструктуру освітнього закладу з централізованої, вразливої та замкненої екосистеми на відкриту, безпечну та інтероперабельну. Це не просто заміна одного способу логіну на інший, а повноцінний перехід до моделі «доказу замість довіри» (proof-based trust). Студент отримує можливість користуватися будь-яким сумісним IoT-пристроєм у будь-якому університеті світу без попередньої реєстрації. Одночасно заклад вищої освіти звільняється від відповідальності за зберігання чутливих персональних даних та тягаря адміністрування складних централізованих баз доступу.

Список використаних джерел

1. European Commission (2023). European Blockchain Services Infrastructure (EBSI). https://ec.europa.eu/digital-building-blocks/ebsi

2. Fedrecheski, G., De Luca, R. D., Zaina, L. M., & Cunha, F. D. (2022). Self-sovereign identity for IoT environments: A perspective. IEEE Access, 10, 45678-45695. https://doi.org/10.1109/ACCESS.2022.3145678

3. Gaia-X AISBL (2023). Gaia-X Architecture Document. https://docs.gaia-x.eu/

4. Sporny, M., Longley, D., & Sabadello, M. (2023). DID Specification Registries. W3C Working Group Note. https://www.w3.org/TR/did-spec-registries/

5. W3C DID Working Group (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation. https://www.w3.org/TR/did-core/

Закройщиков Ростислав Олександрович
студент 4 курсу
спеціальності «Інформаційні системи та технології»
Державного університету
інформаційно-комунікаційних технологій, м. Київ
rosstindev@gmail.com

Сторчак Каміла Павлівна
доктор технічних наук, професор,
завідувач кафедри Інформаційних систем та технологій
Державного університету
інформаційно-комунікаційних технологій, м. Київ
kafedraist2049@gmail.com

СИСТЕМИ МОНІТОРИНГУ НАВКОЛИШНЬОГО СЕРЕДОВИЩА НА ОСНОВІ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Сучасний стан довкілля потребує постійного та оперативного контролю якості атмосферного повітря, води, ґрунтів та інших компонентів навколишнього середовища. Урбанізація, індустріалізація та зростання антропогенного навантаження на природні екосистеми створюють необхідність у системах спостереження, здатних забезпечувати безперервний моніторинг у режимі, наближеному до реального часу [1].

Традиційні методи екологічного моніторингу, засновані на стаціонарних постах спостереження та періодичних лабораторних аналізах, мають суттєві обмеження: високу вартість обладнання та обслуговування, обмежену кількість точок вимірювання, часову дискретність даних та неможливість оперативного реагування на зміни стану довкілля. Це створює «сліпі зони» у просторовому та часовому покритті, що унеможливлює своєчасне виявлення та попередження екологічних загроз.

Інтеграція технологій Інтернету речей (IoT) у сферу екологічного моніторингу відкриває нові можливості для створення масштабованих, енергоефективних та економічно доступних систем спостереження. IoT-підхід передбачає об'єднання сенсорних вузлів, бездротових каналів зв'язку, хмарних платформ обробки даних та інтерфейсів візуалізації в єдиний інформаційний простір, що забезпечує високу просторову роздільну здатність при порівняно низькій вартості кожного вимірювального вузла [2].

Актуальність дослідження зумовлена зростанням антропогенного навантаження на довкілля, посиленням екологічних нормативів та необхідністю переходу від епізодичного контролю до безперервного інтелектуального спостереження. Системи моніторингу на основі IoT дозволяють оперативно виявляти перевищення екологічних норм, прогнозувати небезпечні ситуації та

формувати обґрунтовані управлінські рішення у сфері природокористування та охорони довкілля.

Метою роботи є дослідження принципів побудови, функціональних можливостей та особливостей реалізації систем моніторингу навколишнього середовища на основі технологій Інтернету речей. Для досягнення мети вирішено такі завдання: проаналізовано сучасний стан екологічного моніторингу та обмеження традиційних підходів; досліджено основні параметри довкілля та засоби їх вимірювання; розглянуто архітектурні рішення IoT-систем; визначено вимоги до проєктування; проаналізовано проблеми реалізації та перспективи розвитку.

Об'єктом дослідження є процеси моніторингу стану навколишнього середовища із застосуванням сучасних інформаційно-комунікаційних технологій. Предметом дослідження є методи, засоби, архітектурні рішення та програмно-апаратні компоненти систем моніторингу навколишнього середовища, побудованих на основі технологій Інтернету речей.

У роботі використано методи аналізу наукової та технічної літератури, порівняльного оцінювання апаратних платформ і технологій зв'язку, системного підходу до побудови архітектури IoT-систем, а також узагальнення практичного досвіду реалізації подібних рішень.

У першому розділі проаналізовано теоретичні основи екологічного моніторингу. Визначено, що екологічний моніторинг є систематичним процесом спостереження, контролю, оцінювання та прогнозування стану компонентів навколишнього середовища. Розглянуто класифікацію моніторингу за масштабом (глобальний, національний, регіональний, локальний) та об'єктом спостереження (атмосферний, гідрологічний, ґрунтовий, біологічний, комплексний). Комплексний підхід є найбільш перспективним, оскільки реальні екологічні процеси мають взаємопов'язаний характер [1].

Досліджено основні параметри довкілля, що підлягають моніторингу. Для атмосферного повітря ключовими є концентрації CO_2, CO, NO_2, SO_2, озону, летких органічних сполук та твердих частинок PM2.5 і PM10. Вимірювання газових параметрів здійснюється електрохімічними сенсорами, а контроль частинок – лазерними оптичними сенсорами розсіювання світла. Для водного середовища контролюються температура, pH, електропровідність, вміст розчиненого кисню та каламутність. Ґрунтовий моніторинг охоплює вологість, температуру, електропровідність та кислотність ґрунту [2, 3].

Типова архітектура IoT-системи екологічного моніторингу складається з чотирьох основних рівнів. На сенсорному рівні розташовуються датчики (DHT22, MQ-135, PM2.5) та мікроконтролерні платформи (ESP32). Комунікаційний рівень забезпечує передавання даних через Wi-Fi, LoRaWAN або NB-IoT з використанням протоколів MQTT та CoAP. Серверний рівень відповідає за зберігання даних у базах часових рядів, аналітичну обробку та

виявлення аномалій. Рівень користувача забезпечує візуалізацію через вебпанель або мобільний застосунок (рис. 1).

Рис. 1. Рівень користувача забезпечує візуалізацію через вебпанель або мобільний застосунок

У другому розділі сформульовано вимоги до системи моніторингу та розроблено її архітектуру. Функціональні вимоги включають: періодичне зчитування даних із сенсорів з налаштованим інтервалом, передавання до центрального сервера з буферизацією при втраті зв'язку, централізоване зберігання з можливістю пошуку та агрегації, візуалізацію у вигляді графіків, карт та дашбордів, а також адміністрування вузлів. Нефункціональні вимоги охоплюють надійність, масштабованість, енергоефективність, точність вимірювань та інформаційну безпеку (табл. 1).

Табл. 1

Порівняльна характеристика технологій зв'язку для IoT-моніторингу

Технологія	**Дальність**	**Споживання енергії**	**Пропускна здатність**	**Область застосування**
Wi-Fi	до 100 м	середнє	до 600 Мбіт/с	Локальні мережі
LoRaWAN	до 15 км	низьке	до 50 кбіт/с	Широкомасштабні мережі
NB-IoT	до 10 км	низьке	до 250 кбіт/с	Міський моніторинг
Bluetooth BLE	до 100 м	дуже низьке	до 2 Мбіт/с	Персональні пристрої
GSM/4G	до 35 км	високе	до 150 Мбіт/с	Віддалені об'єкти

У третьому розділі розглянуто практичні аспекти функціонування системи. Описано алгоритм роботи, що включає такі етапи: ініціалізація вузла та перевірка працездатності датчиків → збір вимірювань із заданою періодичністю → локальна попередня обробка (усереднення, фільтрація аномалій) → передавання даних каналами зв'язку → серверна валідація та запис до бази → аналітична обробка (ковзні середні, індекси якості повітря, виявлення аномалій) → візуалізація результатів через вебпанель.

Визначено п'ять основних сценаріїв використання системи: постійний фоновий моніторинг якості повітря у міському середовищі поблизу магістралей, шкіл і лікарень; локальний контроль поблизу промислових підприємств та потенційно небезпечних об'єктів; застосування в аграрному секторі для моніторингу мікроклімату та стану ґрунтів; освітні та наукові цілі у закладах вищої освіти; інформування населення в межах концепції «розумного міста» [4].

Проаналізовано основні проблеми реалізації IoT-систем моніторингу. Найбільш суттєвою є проблема достовірності даних: низьковартісні сенсори можуть мати підвищену похибку, нестабільність характеристик та залежність від зовнішніх умов. Для її мінімізації необхідне регулярне калібрування та верифікація даних референсними вимірюваннями. Проблема енергоспоживання вирішується застосуванням режимів глибокого сну, оптимізацією частоти передавання та використанням сонячних панелей. Надійність зв'язку забезпечується буферизацією даних локально та механізмами повторного підключення [3, 5].

Проведене дослідження підтвердило, що інтеграція технологій Інтернету речей у системи екологічного моніторингу дозволяє створювати масштабовані, оперативні та економічно доступні системи спостереження за станом довкілля. Перспективи подальшого розвитку пов'язані з підвищенням точності сенсорів, застосуванням алгоритмів машинного навчання для прогнозування екологічних змін, інтеграцією з геоінформаційними системами, розвитком енергонезалежних вузлів та формуванням єдиних платформ відкритих екологічних даних.

Список використаних джерел

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey // Computer Networks. – 2010. – Vol. 54, No. 15. – P. 2787–2805.

2. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions // Future Generation Computer Systems. – 2013. – Vol. 29, No. 7. – P. 1645–1660.

3. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, No. 4. – P. 2347–2376.

4. Borgia E. The Internet of Things Vision: Key Features, Applications and Open Issues // Computer Communications. – 2014. – Vol. 54. – P. 1–31.

5. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // IEEE Internet of Things Journal. – 2014. – Vol. 1, No. 1. – P. 22–32.

ЗМІСТ

АВТОРИ ПУБЛІКАЦІЙ