ISSN 2786-5460 (Print)
ISSN 2786-5479 (Online)

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT

МАУП

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

Випуск 4 (15), 2024
Issue 4 (15), 2024

Видавничий дім
«Гельветика»
2024

Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 12 від 26 грудня 2024 року)

Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ : Міжрегіональна Академія управління персоналом, 2024. – Випуск 4 (15). – 130 с.

Журнал «Інформаційні технології та суспільство» є науковим рецензованим виданням, в якому здійснюється публікація матеріалів науковців різних рівнів у вигляді наукових статей з метою їх поширення як серед вітчизняних дослідників, так і за кордоном.

Редакційна колегія не обов'язково поділяє позицію, висловлену авторами у статтях, та не несе відповідальності за достовірність наведених даних і посилань.

Реєстрація суб'єкта у сфері друкованих медіа:
Рішення Національної ради України з питань телебачення і радіомовлення № 1173 від 11.04.2024 року.

Відповідно до Наказу МОН України № 1290 від 30 листопада 2021 року (додаток 3) журнал включено до Переліку наукових фахових видань України (категорія Б) зі спеціальностей 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 124 – Системний аналіз, 125 – Кібербезпека, 126 – Інформаційні системи та технології.

Усі електронні версії статей журналу оприлюднюються на офіційній сторінці видання
http://journals.maup.com.ua/index.php/it

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 12 dated 26 December 2024)

Information Technology and Society / [chief editor Oleksandr Popov]. – Kyiv : Interregional Academy of Personnel Management, 2024. – Issue 4 (15). – 130 p.

Journal «Information Technology and Society» is a peer-reviewed scientific edition, which publishes materials of scientists of various levels in the form of scientific articles for the purpose of their dissemination both among domestic researchers and abroad.

Editorial board do not necessarily reflect the position expressed by the authors of articles, and are not responsible for the accuracy of the data and references.

Registration of Print media entity:
Decision of the National Council of Television and Radio Broadcasting of Ukraine: Decision No. 1173 as of 11.04.2024.

According to the Decree of MES No. 1290 (Annex 3) dated November 30, 2021, the journal was included in the List of scientific professional publications of Ukraine (category B) in specialties 121 – Software engineering, 122 – Computer sciences, 123 – Computer engineering, 124 – Systems analysis, 125 – Cybersecurity, 126 – Information systems and technologies.

All electronic versions of articles in the collection are available on the official website edition
http://journals.maup.com.ua/index.php/it

The articles were checked for plagiarism using the software
StrikePlagiarism.com developed by the Polish company Plagiat.pl.

ЗМІСТ

CONTENTS

УДК 004.272.3:004.85
DOI https://doi.org/10.32689/maup.it.2024.4.1

Олег БОНДАРЧУК
магістр, Інженер Azure DevOps,
Stealthmail Ukraine LLC, iperaser@gmail.com
***ORCID:** 0009-0003-9626-1124*

Сергій ЗИБІН
доктор технічних наук, професор кафедри безпеки інформаціних технологій,
Національний авіаційний університет, zysv@ukr.net
***ORCID:** 0000-0002-2670-2823*

Світлана ВАСИЛЮК-ЗАЙЦЕВА
магістр, старший викладач кафедри комп'ютерних наук,
Національний університет біоресурсів і природокористування України, svetlanafvasylyuk@gmail.com
***ORCID:** 0000-0002-0875-462X*

ЕФЕКТИВНІСТЬ ВИКОРИСТАННЯ КВАНТОВИХ КОМП'ЮТЕРІВ У РОЗВ'ЯЗАННІ СКЛАДНИХ ЗАВДАНЬ

Анотація. *У статті з'ясовано, що квантові обчислення є одним із найважливіших досягнень сучасної науки, яке відкриває нові можливості для розв'язання завдань, недоступних для класичних обчислювальних систем. Актуальність дослідження зумовлена швидким розвитком квантових технологій, які мають потенціал для революційних змін у таких сферах, як фінанси, хімія, матеріалознавство та криптографія. Виявлено, що використання квантових комп'ютерів значно підвищує ефективність процесів оптимізації, аналізу великих обсягів даних і моделювання складних систем, що є критично важливим у сучасних умовах швидкого збільшення обсягів інформації.*

Метою *статті є дослідження ефективності квантових обчислень у розв'язанні складних завдань, аналіз основних проблем їх впровадження та розробка рекомендацій для інтеграції цих технологій у високопродуктивні обчислювальні інфраструктури.*

Методологія. *У статті проаналізовано ключові принципи квантових обчислень, такі як суперпозиція, квантова заплутаність та інтерференція, а також виконано оцінювання потенціалу квантових алгоритмів Шора та Гровера. Здійснено порівняльний аналіз теоретичних і практичних аспектів впровадження квантових комп'ютерів у різних галузях, таких як фінансова сфера, хімія, матеріалознавство і криптографія. Використано підхід системного аналізу для виявлення проблем і потенціалу впровадження квантових обчислювальних технологій.*

Наукова новизна. *Наукова новизна роботи полягає в комплексному аналізі прикладних аспектів використання квантових обчислень, виявленні основних технічних і інфраструктурних проблем їх впровадження та розробці рекомендацій щодо інтеграції квантових технологій у сучасні обчислювальні системи. Визначено перспективи використання квантових алгоритмів у нових галузях, таких як медична діагностика, прогнозування кліматичних змін і створення інтелектуальних систем управління.*

Висновок. *У результаті дослідження доведено, що квантові обчислення мають потенціал для значного підвищення ефективності розв'язання складних завдань, але їх широкомасштабне впровадження обмежено технічними та інфраструктурними викликами. Запропоновано рекомендації, які передбачають удосконалення апаратного забезпечення, розробку нових алгоритмів корекції помилок, створення стандартів для інтеграції квантових і класичних систем, а також розвиток хмарних сервісів для забезпечення доступності квантових обчислень. Окреслено перспективи подальших досліджень, які охоплюють розширення сфер застосування квантових технологій і підготовку фахівців, здатних працювати з цими інноваційними системами.*

Ключові слова: *обчислювальні технології, оптимізація процесів, квантові алгоритми, високопродуктивні системи, технічні інновації.*

Oleg BONDARCHUK, Serhii ZYBIN, Svitlana VASYLYUK-ZAITSEVA. EFFECTIVENESS OF QUANTUM COMPUTERS IN SOLVING COMPLEX PROBLEMS

Abstract. *The study establishes that quantum computing represents a significant advancement in modern science, providing new opportunities to solve problems that are unattainable for classical computing systems. The relevance of this research stems from the rapid development of quantum technologies, which hold the potential to revolutionize fields such as finance, chemistry, materials science, and cryptography. It has been revealed that quantum computers significantly enhance the efficiency of optimization processes, large-scale data analysis, and complex system modeling, which is critically important in the current era of rapidly growing information volumes.*

The purpose *of the article is to study the effectiveness of quantum computing in solving complex problems, analyze the main problems of its implementation, and develop recommendations for integrating these technologies into high-performance computing infrastructures.*

Methodology. *The study analyzes the key principles of quantum computing, including superposition, quantum entanglement, and interference, while assessing the potential of quantum algorithms such as Shor's and Grover's. A comparative analysis*

of theoretical and practical aspects of quantum computer implementation across various fields, such as finance, chemistry, materials science, and cryptography, has been conducted. A systematic analytical approach has been employed to identify challenges and potential applications of quantum computing technologies.

Scientific Novelty. *The scientific novelty lies in the comprehensive analysis of the applied aspects of quantum computing, the identification of major technical and infrastructural challenges in its implementation, and the development of recommendations for integrating quantum technologies into modern computing systems. Prospects for the use of quantum algorithms in emerging areas such as medical diagnostics, climate change forecasting, and intelligent management systems have also been identified.*

Conclusion. *The study concludes that quantum computing has the potential to significantly improve the efficiency of solving complex problems, however its large-scale implementation is constrained by technical and infrastructural challenges. Recommendations include improving hardware, developing new error-correction algorithms, creating standards for integrating quantum and classical systems, and advancing cloud-based services to make quantum computing more accessible. Prospects for further research include expanding the scope of quantum technologies and preparing specialists capable of working with these innovative systems.*

Key words: *computational technologies, process optimization, quantum algorithms, high-performance systems, technical innovations.*

Вступ. Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Квантові комп'ютери є одним із найважливіших досягнень сучасної науки, які відкривають нові можливості для розв'язання завдань, недоступних для традиційних обчислювальних систем. Основна проблема полягає у високій складності та обмеженій ефективності класичних алгоритмів при розв'язанні завдань, що вимагають обчислення великих обсягів даних, оптимізації процесів або моделювання систем із численними змінними. Квантові комп'ютери, завдяки використанню принципів суперпозиції та заплутаності, пропонують радикально нові підходи до обробки інформації, дозволяючи виконувати розрахунки значно швидше, ніж традиційні комп'ютери. Проблема впровадження цих технологій пов'язана не лише з технічними обмеженнями, такими як висока чутливість до помилок і потреба в унікальній інфраструктурі, але й зі складністю адаптації квантових алгоритмів до реальних завдань.

Наукова значущість дослідження квантових комп'ютерів полягає в їхньому потенціалі для розв'язання таких завдань, як факторизація чисел, оптимізація ресурсів у складних системах, моделювання хімічних процесів та аналіз великих даних, що має важливе значення для розвитку штучного інтелекту, матеріалознавства та фінансових технологій. Практичне значення полягає у створенні передумов для впровадження квантових обчислень у сфері високопродуктивних обчислювальних систем, що сприятиме збільшенню ефективності інноваційних процесів, покращенню управління складними системами та розробці нових технологій.

Аналіз останніх досліджень і публікацій. Ефективність квантових комп'ютерів у розв'язанні складних завдань досліджується з різних аспектів, включаючи їхній теоретичний потенціал, практичне застосування та виклики, що виникають у процесі інтеграції цієї технології.

Так, природу квантових обчислень досліджували Я. Кулешник та О. Сорокач. Автори розкривають базові принципи надпозиції й квантової заплутаності, що лежать в основі роботи кубітів. Ці явища дозволяють значно прискорити обчислювальні процеси порівняно з класичними алгоритмами, особливо в завданнях, що вимагають опрацювання великих масивів даних [8].

У дослідженні В. Корольова та О. Ходзінського акцентується на практичних аспектах використання алгоритмів Grover's і Shor's для розв'язання завдань комбінаторної оптимізації. Результати, отримані науковцями, свідчать про потенціал квантових алгоритмів у таких сферах, як фінансове прогнозування та аналіз великих обсягів даних [7].

Проблематика безпеки даних і вплив квантових комп'ютерів на криптографію є темою дослідження Ю. Горбенка та Р. Ганзі. У своїй роботі вчені аналізують, як квантові комп'ютери здатні зламувати традиційні системи шифрування, такі як RSA, водночас вказуючи на можливості впровадження постквантових алгоритмів для підвищення безпеки інформації [2]. На додаток до цього, Є. Каптьол та І. Горбенко зосереджуються на особливостях програмування криптографічних завдань на квантових комп'ютерах, підкреслюючи перспективи використання алгоритму QKD для забезпечення безпечної передачі даних [6].

Крім того, аналіз впливу квантових комп'ютерів на безпеку механізмів інкапсуляції ключів, розглянутий у праці Є. Каптьола, демонструє приклади застосування квантових обчислень для вдосконалення національних стандартів шифрування, таких як ДСТУ 8961:2019 «Скеля». У дослідженні підкреслюється важливість розвитку квантових механізмів для адаптації наявних криптографічних методів до нових загроз [5]. Тим часом Д. Ватолкін та Ю. Гусєва звертають увагу на можливості квантових обчислень у прогнозуванні кліматичних змін і моделюванні природних процесів, демонструючи практичне застосування квантових моделей для розв'язання глобальних екологічних проблем [1].

У контексті порівняння обчислювальних моделей робота В. Задіраки, А. Терещенка та І. Швидченко вивчають переваги квантової арифметики в завданнях високоточної оптимізації. Дослідження показує, що квантові системи значно перевершують традиційні методи в розв'язанні складних обчислювальних завдань [2]. W. Ming додає до цього аналізу глобальну перспективу, розглядаючи використання квантових комп'ютерів для розв'язання проблем управління ресурсами та моделювання великих систем [17].

Практичне застосування алгоритмів квантової оптимізації, таких як QAOA, висвітлює N. Njeri. Автор детально аналізує ефективність цих алгоритмів для покращення роботи транспортних і логістичних систем, водночас звертаючи увагу на виклики, пов'язані з нестабільністю квантових систем [18].

S. Hussain та співавтори в емпіричному дослідженні демонструють, як квантові обчислення застосовуються в таких галузях, як енергетика, логістика та медицина. Автори підкреслюють необхідність розв'язання технічних проблем, зокрема стабілізації кубітів, для ширшого впровадження технології [16].

Сучасні тренди в тестуванні програмного забезпечення, включаючи адаптацію квантових систем, досліджуються в праці I. Hunko. Авторка підкреслює, що оптимізація процесів тестування є ключовим викликом для інтеграції квантових обчислень у реальні бізнес-середовища [15].

На освітній аспект використання квантових технологій звертають увагу О. Трифонова та М. Садовий. Науковці підкреслюють важливість впровадження симуляторів квантових комп'ютерів у навчальні програми, що дозволяє готувати фахівців для роботи з новітніми технологіями [12].

Трансформаційний вплив квантових обчислень на наукові дослідження аналізується такими дослідниками, як S. Gill та R. Buyya. Автори описують, як квантові алгоритми змінюють підходи до моделювання складних систем, зокрема в хімії та фінансах [13].

В. Нестеров зосереджується на використанні квантових алгоритмів у бізнес-аналітиці. Дослідження вченого демонструє, як ця технологія дозволяє підвищити ефективність прийняття рішень, аналізуючи великі обсяги даних та прогнозуючи ринкові тенденції [9].

Цікавим також є дослідження С. Зибіна, присвячене оптимізації структур і трафіків передачі інформації в захищених корпоративних мережах [4]. Автор демонструє потенціал квантових обчислень у покращенні криптографічного захисту та управлінні інформаційними потоками, зокрема для підвищення кібербезпеки корпоративних середовищ. Це підкреслює практичну цінність квантових технологій у розв'язанны завдань оптимізації у сфері інформаційної безпеки.

Аналіз наукових праць свідчить про багатогранність застосування квантових комп'ютерів у різних галузях, охоплюючи як теоретичні дослідження, так і практичні реалізації. Ці роботи переконливо підтверджують високий потенціал квантових обчислень у розв'язанні актуальних проблем сьогодення та подоланні викликів майбутнього.

Попри значні досягнення в дослідженні квантових обчислень, залишаються нерозв'язаними кілька важливих аспектів. Насамперед недостатньо вивчено практичну реалізацію ключових принципів квантових обчислень, таких як суперпозиція, квантова заплутаність та інтерференція, що обмежує їхню адаптацію до складних обчислювальних завдань. Теоретичні моделі потребують удосконалення для врахування умов реального використання.

Потенціал квантових алгоритмів, зокрема Шора і Гровера, також залишається не повністю розкритим у прикладних завданнях. Основні обмеження полягають у технічних викликах, таких як стабільність апаратного забезпечення та адаптація алгоритмів до різних галузевих сценаріїв. Емпіричний аналіз їхньої ефективності в реальних умовах потребує подальшого розвитку.

Технічні й інфраструктурні виклики, зокрема проблеми корекції помилок, чутливості кубітів до зовнішніх впливів та відсутність уніфікованих стандартів інтеграції з класичними обчисленнями, залишаються бар'єрами для широкого впровадження квантових комп'ютерів. Це ускладнює їхню інтеграцію в сучасні високопродуктивні системи. Недостатньо досліджені й прикладні аспекти використання квантових технологій у фінансовій сфері, хімії, матеріалознавстві та криптографії, що обмежує їх ефективне впровадження у практичну діяльність. Такі прогалини впливають на швидкість розвитку технологій та їх адаптацію до нових викликів.

У статті запропоновано розв'язання зазначених проблем через детальний аналіз теоретичних основ, оцінювання алгоритмів, вивчення технічних викликів і розробку рекомендацій. Використання сучасних методів дослідження та розширення емпіричної бази сприятиме подоланню цих прогалин і вдосконаленню квантових обчислювальних систем.

Мета статті – дослідити ефективність використання квантових комп'ютерів для розв'язання складних обчислювальних завдань, визначити основні переваги квантових алгоритмів та оцінити їхню роль у розвитку високопродуктивних систем і технічних інновацій.

Завдання статті:

1. Проаналізувати теоретичні основи квантових обчислень, їхні ключові принципи та оцінити потенціал квантових алгоритмів для розв'язання складних завдань.

2. Вивчити технічні виклики впровадження квантових комп'ютерів та їхні прикладні аспекти в різних галузях.

3. Розробити рекомендації щодо розвитку квантових обчислювальних систем і їхньої інтеграції у високопродуктивні інфраструктури.

Виклад основного матеріалу. Квантові обчислення є новою технологією, яка базується на законах квантової механіки й пропонує революційні можливості для обробки інформації. На відміну від класичних комп'ютерів, які використовують біти для представлення інформації як 0 або 1, квантові комп'ютери працюють із кубітами, що можуть перебувати в станах 0, 1 або їхній суперпозиції одночасно. Завдяки цьому квантові комп'ютери здатні виконувати експоненціально більшу кількість операцій одночасно [11]. Основні принципи, такі як суперпозиція, квантова заплутаність та інтерференція, створюють умови для високої ефективності квантових алгоритмів. Вони дозволяють розв'язувати завдання, які потребують значних обчислювальних ресурсів, включаючи факторизацію, моделювання складних молекул і оптимізацію систем (табл. 1).

Таблиця 1

Ключові принципи квантових обчислень

Принцип	Опис	Приклади практичного застосування
Суперпозиція	Кубіт може одночасно перебувати в станах 0 і 1, що дає змогу паралельно обробляти дані.	Використовується у квантовій криптографії для створення стійких до зламу ключів.
Квантова заплутаність	Кубіти взаємопов'язані незалежно від відстані, що забезпечує синхронізацію обчислень.	Застосовується в телекомунікаціях для квантового розподілу ключів.
Інтерференція	Квантові хвилі складаються таким чином, щоб підсилювати правильні відповіді й зменшувати неправильні.	Оптимізує алгоритми пошуку у великих базах даних, наприклад, у медичній діагностиці.

Джерело: сформовано авторами на підставі [11, 18]

Сучасна практика демонструє широкий спектр можливостей для використання квантових обчислень у різних сферах. Наприклад, суперпозиція активно використовується у квантових алгоритмах для швидкої обробки великих обсягів інформації у фінансових технологіях, таких як аналіз ризиків і побудова прогнозів. Квантова заплутаність уже довела свою ефективність у забезпеченні безпечного зв'язку в телекомунікаційних мережах. В умовах сучасних кіберзагроз ця технологія стає вирішальним фактором для захисту інформації. Інтерференція, своєю чергою, ефективно працює в медичній галузі, наприклад, для прискорення аналізу геномів і пошуку мутацій, що дозволяє вдосконалити персоналізовану медицину. У реальних умовах квантові обчислення ще знаходяться на ранній стадії розвитку, однак низка провідних компаній, таких як IBM, Google та D-Wave, уже створили прототипи квантових комп'ютерів, які здатні розв'язувати спеціалізовані завдання з високою точністю [14].

Квантові алгоритми є основою ефективності квантових обчислень, оскільки вони дозволяють розв'язувати завдання, які є складними або навіть неможливими для класичних алгоритмів [8]. Серед найбільш відомих квантових алгоритмів виокремлюються алгоритми Шора та Гровера, які демонструють значний потенціал у різних прикладних сферах. Алгоритм Шора призначений для факторизації цілих чисел і є революційним у контексті криптографії, оскільки він може зламати широко використовувані системи шифрування, що базуються на складності факторизації великих чисел. Алгоритм Гровера, своєю чергою, ефективно розв'язує завдання в пошуку елементів у невпорядкованих базах даних, забезпечуючи квадратичне прискорення порівняно з класичними методами (табл. 2).

Таблиця 2

Порівняльна характеристика квантових алгоритмів Шора й Гровера та їх практичне застосування

Алгоритм	Призначення	Переваги	Приклади застосування
Алгоритм Шора	Факторизація цілих чисел на прості множники.	Експоненціальне скорочення часу обчислень порівняно з класичними алгоритмами.	Розшифровка RSA-кодів, моделювання складних хімічних молекул.
Алгоритм Гровера	Пошук у невпорядкованих базах даних.	Квадратичне прискорення порівняно з класичними методами пошуку.	Пошук потрібних даних у великих базах, оптимізація логістичних процесів.

Джерело: сформовано авторами на підставі [6]

На практиці алгоритми Шора та Гровера демонструють унікальні переваги в розв'язанні завдань, які раніше вважалися нерозв'язними за допомогою класичних обчислювальних систем. Алгоритм Шора, завдяки своїй здатності факторизувати великі числа, є каталізатором для перегляду глобальних стандартів криптографії. Його ефективність підкреслює важливість розробки квантово-стійких рішень, які могли б забезпечити безпеку сучасних систем передачі даних. Це створює нові наукові виклики, зокрема в напрямі пошуку альтернативних методів шифрування, таких як використання еліптичних кривих або гомоморфного шифрування. Крім того, алгоритм Шора відкриває можливості для фундаментальних досліджень у теорії чисел, що може вплинути на розвиток нових напрямів у математиці та комп'ютерних науках.

Алгоритм Гровера, своєю чергою, демонструє потенціал не лише в прискоренні пошуку в базах даних, а й у застосуванні до завдань оптимізації в мультидисциплінарних контекстах [18]. Його ефективність базується на зменшенні кількості ітерацій, необхідних для знаходження рішення, що робить його особливо корисним у завданнях із великою кількістю можливих комбінацій. Це створює нові перспективи для розробки квантових гібридних систем, які поєднують класичні й квантові обчислення, що дозволяє використовувати сильні сторони обох підходів для розв'язання складних проблем.

Загалом обидва алгоритми формують базу для майбутніх розробок у сфері квантових обчислень і сприяють поширенню їх у нових галузях, таких як моделювання складних систем, розробка інноваційних матеріалів або навіть прогнозування природних катаклізмів. Важливість цих алгоритмів виходить за межі їхніх практичних застосувань, оскільки вони стимулюють інтерес до квантової науки, сприяючи залученню інвестицій та міждисциплінарній співпраці на глобальному рівні. У цьому контексті розвиток відповідних досліджень є не лише технічним викликом, а й стратегічним напрямом для підготовки до нової епохи квантових технологій.

Квантові обчислення, завдяки своїм унікальним можливостям, відкривають нові перспективи для інновацій у фінансовій сфері, хімії, матеріалознавстві та криптографії. Їх інтеграція в практичну діяльність відображає сучасні глобальні тренди [13]. У фінансовому секторі квантові алгоритми, такі як алгоритм Гровера, дозволяють значно прискорити аналіз великих баз даних для виявлення аномалій та прогнозування ризиків. Наприклад, у світі вже тестуються квантові технології для виявлення шахрайських транзакцій у реальному часі. Провідні інвестиційні компанії, такі як BlackRock, розглядають можливості використання квантових обчислень для створення адаптивних портфелів, що враховують динаміку ринків у режимі реального часу. В Україні такі технології могли б застосовуватися для автоматизації процесів у системі податкового адміністрування, зокрема для виявлення фінансових злочинів або оптимізації державних витрат.

У хімії квантові обчислення вже змінюють підхід до дослідження складних молекулярних структур. Наприклад, IBM за допомогою свого квантового процесора моделює поведінку молекул, що може значно прискорити розробку нових ліків. У сучасних умовах це дає можливість не лише створювати препарати для лікування рідкісних захворювань, але й прогнозувати їхню взаємодію на клітинному рівні з мінімальними витратами. В Україні така технологія може знайти застосування у фармацевтичних стартапах, які спеціалізуються на розробці препаратів для лікування посттравматичних синдромів або інших медичних потреб, актуальних у воєнний час.

У матеріалознавстві квантові обчислення відкривають нові шляхи для створення надміцних матеріалів і надпровідників [10]. Наприклад, дослідження з використанням квантових комп'ютерів дозволили виявити нові структури для створення акумуляторів із тривалим терміном служби, що має вирішальне значення для розвитку електромобільної індустрії. В Україні такі технології могли б стати основою для розвитку оборонної промисловості, зокрема створення енергетично ефективних матеріалів для військової техніки або захисного обладнання.

У сфері криптографії квантові обчислення не лише створюють виклик для традиційних методів шифрування, але й пропонують нові рішення [2]. Квантовий розподіл ключів вже використовується для захисту урядових і фінансових комунікацій у Китаї та США, гарантуючи абсолютну безпеку даних. Для України, яка стикається з масштабними кіберзагрозами, інтеграція квантової криптографії могла б стати ключовим елементом національної безпеки, забезпечуючи захист критичних державних баз даних та енергетичних систем [1]. У поєднанні з інноваційними підходами до розробки квантово-стійких алгоритмів Україна може закласти фундамент для посилення кіберзахисту та участі в глобальній інноваційній екосистемі.

Впровадження квантових комп'ютерів у практичну діяльність стикається з низкою технічних та інфраструктурних викликів, які обмежують їх використання в реальних умовах. Однією з основних технічних проблем є висока чутливість кубітів до зовнішніх факторів. Кубіти, які є основою квантових обчислень, потребують надзвичайно стабільного середовища для функціонування [8]. Навіть незначні температурні

коливання, електромагнітні поля або шум можуть викликати їхню нестабільність, що призводить до обчислювальних помилок. Це вимагає створення складних кріогенних систем, які забезпечують роботу кубітів у надпровідному стані, що є технічно складним і фінансово витратним процесом.

Іншою суттєвою проблемою є квантові помилки, які виникають через нестабільність кубітів і квантовий шум. Наявні методи корекції таких помилок потребують значної кількості додаткових кубітів для збереження точності обчислень [17]. Це суттєво збільшує вимоги до апаратного забезпечення квантових комп'ютерів, що уповільнює їхній розвиток і комерціалізацію. Розробка нових методів корекції помилок, які потребують менше ресурсів, залишається одним із найважливіших напрямів досліджень.

Інфраструктурні виклики також створюють значні бар'єри для широкомасштабного впровадження квантових комп'ютерів. Їхня експлуатація вимагає спеціалізованих лабораторій із суворими умовами для збереження стабільності кубітів. Крім того, обслуговування таких систем потребує висококваліфікованих фахівців, кількість яких залишається обмеженою. Важливим питанням є також інтеграція квантових комп'ютерів у традиційні інформаційні системи. Відсутність уніфікованих стандартів і протоколів взаємодії між квантовими та класичними обчисленнями ускладнює їхнє спільне використання в реальних умовах.

Ще однією суттєвою проблемою є висока вартість квантових комп'ютерів. Процес розроблення, виробництва та технічного обслуговування таких систем вимагає суттєвих фінансових вкладень, що робить доступ до цих технологій привілеєм переважно провідних компаній та науково-дослідних установ. Це створює ситуацію, коли потенціал квантових обчислень залишається недоступним для широкого кола користувачів.

В Україні ці виклики мають свої особливості. По-перше, дефіцит висококваліфікованих спеціалістів у сфері квантових технологій є серйозною проблемою, яка обмежує можливості для розроблення та впровадження цих систем. По-друге, обмежені фінансові ресурси стримують створення необхідної інфраструктури для підтримки квантових обчислень. Крім того, інтеграція квантових комп'ютерів у державні інформаційні системи стикається з проблемою адаптації наявного програмного забезпечення та відсутністю квантово-стійких рішень у сфері кібербезпеки. Розв'язання цих проблем потребує активної державної підтримки, міжнародної співпраці та розвитку освітніх програм, орієнтованих на підготовку спеціалістів у сфері квантових технологій. Враховуючи потенціал квантових комп'ютерів для покращення інформаційної безпеки та ефективності управління державними ресурсами, їх впровадження в Україні може стати важливим елементом національної інноваційної політики.

Подальший розвиток квантових обчислювальних систем вимагає комплексного підходу, який охоплює технічні, інфраструктурні та науково-освітні аспекти. Одним із ключових напрямів є вдосконалення апаратного забезпечення квантових комп'ютерів, зокрема розробка стабільніших і менш чутливих до зовнішніх факторів кубітів. Це можливо завдяки розробці інноваційних підходів у сфері матеріалознавства, спрямованих на створення нових концепцій, зокрема топологічних кубітів. Паралельно з цим необхідно розвивати алгоритмічні рішення, що оптимізують використання доступних ресурсів і підвищують ефективність обчислень. Наприклад, створення алгоритмів із покращеною корекцією помилок здатне зменшити апаратні вимоги та зробити квантові системи більш доступними.

Інтеграція квантових технологій у високопродуктивні обчислювальні інфраструктури потребує створення стандартів для взаємодії між квантовими та класичними системами. Уніфіковані протоколи забезпечать плавну інтеграцію квантових обчислень у наявні обчислювальні платформи, дозволяючи використовувати переваги обох підходів. Важливим аспектом є розширення доступу до квантових обчислень через хмарні сервіси, що дозволить дослідникам і компаніям користуватися потужностями квантових комп'ютерів без необхідності володіти дорогим обладнанням. Такий підхід уже демонструє успіх завдяки ініціативам провідних компаній, таких як IBM і Google [16], які пропонують доступ до квантових платформ для тестування та розробки нових додатків.

Серед пріоритетів залишається розвиток квантово-стійких систем безпеки, оскільки впровадження квантових обчислень суттєво змінює ландшафт кіберзагроз. Це передбачає розроблення криптографічних рішень, стійких до атак, які можуть бути здійснені за допомогою квантових алгоритмів. Державна підтримка відіграє важливу роль у забезпеченні фінансування досліджень, створенні спеціалізованих лабораторій і навчальних програм, орієнтованих на підготовку кадрів у цій галузі. Освітні ініціативи мають бути спрямовані на формування нового покоління фахівців, здатних працювати з квантовими технологіями та інтегрувати їх у сучасні обчислювальні системи.

Особливе значення має міждисциплінарна співпраця між дослідниками, інженерами та представниками бізнесу. Це сприятиме швидкому переходу від лабораторних експериментів до комерційних застосувань квантових технологій, зокрема в галузях фінансів, охорони здоров'я та матеріалознавства. У довгостроковій перспективі необхідно створювати міжнародні партнерства для обміну досвідом та доступу до передових досліджень, що прискорить глобальне впровадження квантових обчислень у різні сфери.

Висновки. Дослідження, яке було виконано авторами, дозволило дійти висновків, згідно з якими квантові технології мають революційний потенціал для обчислювальних систем, особливо в галузі оптимізації процесів, аналізу даних і моделювання складних систем. Основними перевагами квантових обчислень є експоненціальне скорочення часу виконання завдань і можливість обробки великих обсягів інформації, що робить їх незамінними у фінансовій галузі, хімії, матеріалознавстві та криптографії.

Серед основних проблем впровадження квантових обчислювальних систем можна виокремити високу чутливість кубітів до зовнішніх впливів, потребу в складній кріогенній інфраструктурі, недостатню стійкість до квантових помилок та обмежену доступність через високу вартість технологій. Крім того, відсутність стандартів для інтеграції квантових обчислень із традиційними системами ускладнює їх практичне використання.

Для розв'язання зазначених проблем рекомендується зосередити зусилля на розробці стабільніших кубітів і нових алгоритмів корекції помилок, що зменшить вимоги до апаратного забезпечення. Важливим напрямом є створення уніфікованих протоколів взаємодії між класичними та квантовими системами, що забезпечить плавну інтеграцію цих технологій у наявні обчислювальні платформи. Необхідно також інвестувати в розвиток хмарних квантових сервісів, які зроблять технологію доступнішою для дослідників і бізнесу.

Перспективи подальших досліджень передбачають вивчення нових сфер застосування квантових обчислень, таких як медична діагностика, прогнозування кліматичних змін і розробка інтелектуальних систем керування. У контексті України варто акцентувати на підготовці фахівців у цій галузі, створенні дослідницької інфраструктури та інтеграції квантових технологій у державні системи управління. Це сприятиме не лише покращенню економічної ефективності, але й підвищенню рівня національної безпеки через впровадження квантово-стійких криптографічних рішень.

Список використаних джерел:

1. Ватолкін Д. П., Гусева Ю. І. Використання квантових обчислень у наукових дослідженнях. *Історія розвитку науки, техніки та освіти: збірник праць XXII Міжнародної молодіжної науково-практичної конференції, за темою високі технології та сучасні виклики* (м. Київ, 18 квітня 2024 р.). Київ, 2024. С. 158–163. URL: https://histeproc.kpi.ua/article/view/304530 (дата звернення: 16.11.2024).

2. Горбенко Ю. І., Ганзя Р. С. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів. *Вісник Національного університету Львівська політехніка. Комп'ютерні системи та мережі.* 2014. Вип. 806. С. 40–48. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/nov/6624/8-40-48.pdf (дата звернення: 16.11.2024).

3. Задірака В., Терещенко А., Швидченко І. Багаторозрядна арифметика у послідовній, паралельній та квантовій моделях обчислень. *Фізико-математичне моделювання та інформаційні технології.* 2023. Вип. 36. С. 87–91. URL: http://www.fmmit.lviv.ua/index.php/fmmit/article/view/282 (date of access: 16.11.2024).

4. Зибін С. Оптимізація розробки структур і трафіків передачі інформації в захищених корпоративних мережах. Кількісна оптимізація. *Кібербезпека: освіта, наука, техніка*. 2020. № 7 (Том 3). С. 103–114. DOI: 10.28925/2663-4023.2020.7.103114

5. Каптьол Є. Аналіз впливу квантових комп'ютерів на безпеку механізмів інкапсуляції ключів на прикладі ДСТУ 8961: 2019 «Скеля». *Фізико-математичне моделювання та інформаційні технології.* 2023. № 36. С. 106–110. URL: http://www.fmmit.lviv.ua/index.php/fmmit/article/view/286 (дата звернення: 16.11.2024).

6. Каптьол Є. Ю., Горбенко І. Д. Аналіз можливостей та особливості програмування завдань криптології на квантовому комп'ютері. *Radiotekhnika.* 2020. Вип. 202. С. 37–48. DOI: https://doi.org/10.30837/rt.2020.3.202.03 (дата звернення: 16.11.2024).

7. Корольов В. Ю., Ходзінський О. М. Розв'язування завдань комбінаторної оптимізації на квантових комп'ютерах. *Кібернетика та комп'ютерні технології.* 2020. № 2. С. 5–13. URL: https://icyb180.org.ua/wp-content/uploads/2020/07/rozvyazuvannya-zadach-kombinatornoyi-optimizatsiyi-na-kvantovih-komp-yuterah.pdf (дата звернення: 16.11.2024).

8. Кулешник Я. Ф., Сорокач О. В. Квантові комп'ютери та кубіти. *Інформаційні технології в освіті та практиці: матеріали Всеукраїнської науково-практичної конференції* (Львів, 17 грудня 2021 р.). Львів: ЛьвДУВС, 2021. С. 43–45. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4309/1/17_12_2021.pdf#page=43 (дата звернення: 16.11.2024).

9. Нестеров В. Дослідження впливу аналітики великих даних на ефективність бізнесу в цифрову епоху. *Інформаційні технології та суспільство.* 2024. Вип. 1 (12). С. 70–76. DOI: https://doi.org/10.32689/maup.it.2024.1.10

10. Ткачук А. Особливості розгляду питання «квантові комп'ютери» під час вивчення основ елементної бази сучасної комп'ютерної електроніки та ЕОМ. *Наукові записки. Серія: Педагогічні науки*. 2021. Вип. 198. С. 181–184. DOI: https://doi.org/10.36550/2415-7988-2021-1-198-181-184

11. Трифонова О. М., Садовий М. І. Сучасні інноваційні технології та методика професійного навчання квантових комп'ютерів. *Наукові записки. Серія: Педагогічні науки.* 2023. Вип. 209. С. 373–379. DOI: https://doi.org/10.36550/2415-7988-2022-1-209-373-379

12. Трифонова О. М., Садовий М. І. Сучасні інноваційні технології та методика професійного навчання квантових комп'ютерів. *Наукові записки. Серія: Педагогічні науки.* 2023. Вип. 209. С. 373–379. DOI: https://doi.org/10.36550/2415-7988-2022-1-209-373-379

13. Gill S. S., Buyya R. Transforming Research with Quantum Computing. *Journal of Economy and Technology.* 2024. URL: https://www.sciencedirect.com/science/article/pii/S2949948824000295?via%3Dihub (date of access: 16.11.2024).

14. Hassija V., Chamola V., Gupta V., Jain S., Guizani M. Present landscape of quantum computing. *IET Quantum Communication.* 2020. Vol. 1. № 2. P. 42–48. DOI: https://doi.org/10.1049/iet-qtc.2020.0027

15. Hunko I. Software Testing in 2023: New Trends and Challenges. *Herald of Kyiv Institute of Business and Technology.* 2023. Vol. 49. № 1–2. P. 25–36. DOI: https://doi.org/10.37203/kibit.2023.49.03

16. Hussain S., Neupane Y., Wang W. L., Ibrahim N., Khan S. U. R., Kareem A. Empirical Investigation of Quantum Computing on Solving Complex Problems. *In: Kruchten P., Gregory P. (eds) Agile Processes in Software Engineering and Extreme Programming – Workshops. XP XP 2022 2023. Lecture Notes in Business Information Processing.* Vol. 489. Springer, Cham, 2024. P. 150–163. DOI: https://doi.org/10.1007/978-3-031-48550-3_22

17. Ming W. S. The Role of Quantum Computing in Solving Complex Global Problems. *Hong Kong International Journal of Research Studies.* 2023. Vol. 1. № 1. P. 18–25. URL: https://octopuspublication.com/index.php/hkijrs/article/view/4 (date of access: 16.11.2024).

18. Njeri N. Quantum Computing Algorithms for Solving Complex Optimization Problems. *Journal of Advanced Technology and Systems.* 2023. Vol. 1. № 1. P. 24–34. URL: https://forthworthjournals.org/journals/index.php/JATS/article/view/13 (date of access: 16.11.2024).

УДК 004.67
DOI https://doi.org/10.32689/maup.it.2024.4.2

Олександр БОРИСОВ
магістр кафедри комп'ютерних систем і технологій,
Національний університет «Запорізька політехніка», enterprize.v2@gmail.com
***ORCID:** 0009-0009-6722-0423*

Марія ТЯГУНОВА
кандидат технічних наук, доцент кафедри комп'ютерних систем і технологій,
Національний університет «Запорізька політехніка», mary.tyagunova@gmail.com
***ORCID:** 0000-0002-9166-5897*

ПІДХІД ДО АВТОМАТИЗАЦІЇ ЗАМОВЛЕНЬ У РЕСТОРАНІ З ВИКОРИСТАННЯМ ІТ-ТЕХНОЛОГІЙ

***Анотація. Метою дослідження** є підвищення оперативності обслуговування клієнтів та оптимізація робочих процесів у ресторанному бізнесі шляхом розробки автоматизованої системи приймання та оброблення замовлень через Telegram-бот. У роботі представлено інноваційний підхід, що поєднує використання сучасних мовних моделей на базі архітектури Transformer із функціональністю месенджер-бота для створення інтерактивного та персоналізованого сервісу.*

***Методологія.** Для досягнення мети проведено аналіз існуючих підходів до автоматизації процесів у ресторанній галузі. На основі отриманих даних розроблено Telegram-бот для приймання замовлень, який інтегрується з мовною моделлю Llama 3.1 Instruct 8B. Для обробки замовлень створено програму-менеджер, що взаємодіє з базою даних PostgreSQL. У роботі також досліджено ефективність запропонованого рішення у реальних умовах, тестуючи систему на коректність виконання ключових функцій, таких як оформлення замовлень і бронювання столиків.*

***Наукова новизна.** Використання Telegram-бота в поєднанні з сучасними мовними моделями забезпечує можливість обробки неструктурованих запитів, що недоступно для традиційних POS-систем. Особливістю підходу є інтеграція персоналізованого обслуговування, що враховує індивідуальні потреби клієнтів, а також відсутність необхідності у дорогому обладнанні чи тривалому навчанні персоналу. Система пропонує гнучкість і доступність, знижуючи витрати на впровадження та обслуговування.*

***Висновки.** Результати дослідження підтвердили ефективність розробленої системи. Telegram-бот стабільно виконує основні функції, забезпечуючи точність і швидкість обробки замовлень, а також підтримку інтерактивної взаємодії з клієнтами. Інтеграція з мовною моделлю дозволила значно підвищити рівень персоналізації обслуговування, що позитивно вплинуло на клієнтський досвід. Система легко інтегрується з існуючими програмними рішеннями, що робить її доступною для широкого кола закладів. Таким чином, запропоноване рішення сприяє оптимізації внутрішніх процесів у ресторанному бізнесі, встановлюючи нові стандарти автоматизації та обслуговування клієнтів.*

***Ключові слова:** програмне запезпечення, автоматизація, ресторан, телеграм, чат-бот, python, штучний інтелект, llma, customtkinter, pytelegrambotapi.*

Oleksandr BORYSOV, Mariya TIAHUNOVA. AN APPROACH TO AUTOMATING RESTAURANT ORDERS USING IT TECHNOLOGIES

***Abstract. The objective of the study** is to enhance the efficiency of customer service and optimize workflow in the restaurant business by developing an automated system for order acceptance and processing through a Telegram bot. The study presents an innovative approach that combines the use of modern language models based on the Transformer architecture with the functionality of a messenger bot to create an interactive and personalized service.*

***Methodology.** To achieve the goal, an analysis of existing approaches to process automation in the restaurant industry was conducted. Based on the collected data, a Telegram bot was developed for order acceptance, which integrates with the Llama 3.1 Instruct 8B language model. A manager program was created for order processing, interacting with a PostgreSQL database. The study also examined the effectiveness of the proposed solution in real-world conditions by testing the system for the correctness of its core functions, such as order placement and table reservation.*

***Scientific novelty.** The use of a Telegram bot combined with modern language models enables the processing of unstructured queries, which is not feasible with traditional POS systems. A distinctive feature of the approach is the integration of personalized service that considers the individual needs of customers, as well as the absence of the need for expensive equipment or extensive staff training. The system offers flexibility and accessibility, reducing implementation and maintenance costs.*

***Conclusions.** The research findings confirmed the effectiveness of the developed system. The Telegram bot consistently performs essential functions, ensuring the accuracy and speed of order processing while supporting interactive customer interaction. Integration with the language model significantly enhanced the level of service personalization, positively impacting the customer experience. The system easily integrates with existing software solutions, making it accessible to a wide range of establishments. Thus, the proposed solution contributes to the optimization of internal processes in the restaurant business, setting new standards for automation and customer service.*

***Key words:** software, automation, restaurant, telegram, chatbot, python, artificial intelligence, llma, customtkinter, pytelegrambotapi.*

Вступ. В умовах стрімкого розвитку технологій сучасний ресторанний бізнес стикається з необхідністю підвищення ефективності обслуговування клієнтів та оптимізації внутрішніх процесів. Однією з ключових тенденцій останніх років є впровадження автоматизації на основі чат-ботів у месенджерах, що відкриває нові можливості для оперативного приймання замовлень та інтерактивної взаємодії з клієнтами.

Основною проблемою, яку вирішує ця стаття, є підвищення швидкості та якості обслуговування в ресторанах шляхом автоматизації процесів. У традиційних підходах до роботи з замовленнями виникають затримки через людський фактор, неефективну обробку запитів або відсутність належної інтеграції між різними компонентами ресторанної системи. Це не лише впливає на клієнтський досвід, але й знижує продуктивність закладу загалом.

Метою цього дослідження є розробка автоматизованої системи, яка поєднує функціональність Telegram-бота для приймання замовлень та програми-менеджера для їх обробки. Така система спрямована на забезпечення зручності для користувачів, покращення операційної діяльності ресторану та інтеграцію сучасних технологій у ресторанний бізнес.

Аналіз сучасних рішень. Автоматизація процесів у ресторанному бізнесі є важливим аспектом, що визначає ефективність, рентабельність і задоволеність клієнтів. Сучасні технології дозволяють оптимізувати численні аспекти діяльності ресторанів, забезпечуючи кращу взаємодію між закладом і його відвідувачами, а також підвищуючи точність і швидкість обслуговування. На ринку доступні численні рішення для автоматизації роботи ресторанів. До найбільш популярних відносяться POS-системи, мобільні додатки та спеціалізовані платформи для управління замовленнями, такими як OpenTable, Square POS і Toast POS. Ці рішення пропонують широкий спектр функцій, серед яких є обробка замовлень та управління меню; інтеграція з бухгалтерськими системами та інвентаризацією; збір аналітичних даних про продажі та вподобання клієнтів; зручна інтеграція з сервісами доставки та CRM-системами.

Такі системи дозволяють знижувати кількість помилок у замовленнях, пришвидшують обслуговування і сприяють підвищенню ефективності використання ресурсів [4, 8, 9, 10].

Однак традиційні системи мають і певні обмеження, зокрема потребу у дорогому обладнанні, складність у навчанні персоналу, обмеження у функціоналі для специфічних потреб закладу та відсутність інтерактивної взаємодії з клієнтами [5].

Описаний у статті розроблений підхід до автоматизації передбачає використання чат-боту на платформі Telegram у поєднанні з мовними моделями, на архітектурі decoder-only Transformer на 8 мільярдів параметрів. Це рішення значно відрізняється від традиційних систем, пропонуючи безліч переваг [1].

Чат-боти не потребують складного обладнання чи тривалого навчання, що знижує вартість впровадження [2]. Інтеграція з сучасними мовними моделями дозволяє сприймати і обробляти неструктуровані або складні запити від клієнтів.

Система легко налаштовується під специфічні потреби закладу, забезпечуючи ефективну інтеграцію з існуючими інфраструктурами, включаючи бази даних та програми-менеджери [7, 9]. Використання месенджерів дозволяє автоматизувати процес прийому замовлень, розширюючи можливості зворотного зв'язку та комунікації.

Особливістю використання Telegram-боту є акцент на персоналізації обслуговування. Завдяки інтеграції з мовними моделями, такі рішення перевершують традиційні POS-системи, дозволяючи адаптувати відповіді під конкретні запити клієнтів, що робить сервіс більш гнучким і зручним.

Технологічний підхід до створення системи. Розроблена система автоматизації обробки замовлень ґрунтується на інтеграції трьох ключових компонентів: Telegram-бота, програми-менеджера та реляційної бази даних, загальна схема системи представлена на рис. 1.

Кожен із цих елементів має власну функціональну роль, і їх злагоджена взаємодія створює комплексну екосистему для обробки замовлень ресторану. Telegram-бот є користувацьким інтерфейсом, що дозволяє клієнтам оформлювати замовлення, бронювати столики, переглядати меню та отримувати інформацію про доступні послуги. Ця частина системи реалізує можливість взаємодії в зручній текстовій формі через команди та інтерактивні кнопки. Програма-менеджер виступає центральним модулем управління, забезпечуючи обробку даних, синхронізацію з базою даних (БД) та інтеграцію із внутрішніми системами ресторану, такими як кухня чи каса. Реляційна БД PostgreSQL служить сховищем інформації, де зберігаються дані для коректної діяльності автоматизацій обробки замовлень, схема БД представлена на рис. 2.

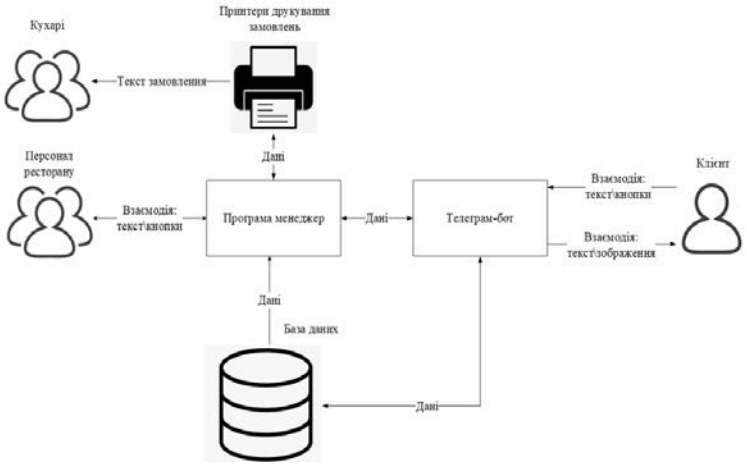


Рис. 1. Загальна схема системи

База даних системи спроєктована таким чином, щоб забезпечувати структурований і послідовний облік інформації. Основні таблиці включають клієнтів, замовлення, склад замовлень, меню, статуси столиків і таблиці для довідкових даних, таких як статуси замовлень.

Telegram-бот функціонує як точка входу для клієнтів, які надсилають свої запити. Отримані дані передаються в програму-менеджер, що аналізує інформацію і взаємодіє з базою даних для виконання необхідних операцій. БД зберігає всі ключові дані та забезпечує доступ до них у режимі реального часу. Такий підхід забезпечив гнучкість, масштабованість та стійкість системи.

Вибір технологій для реалізації системи обґрунтовано їхньою функціональністю та відповідністю завданням. Telegram-бот розроблено з використанням бібліотеки PyTelegramBotAPI, ця бібліотека надає легкий доступ до API Telegram і підтримує широкий спектр функцій, необхідних для реалізації інтерактивного інтерфейсу. Програма-менеджер створена на основі бібліотеки CustomTkinter, яка дозволяє розробляти сучасний графічний інтерфейс користувача.

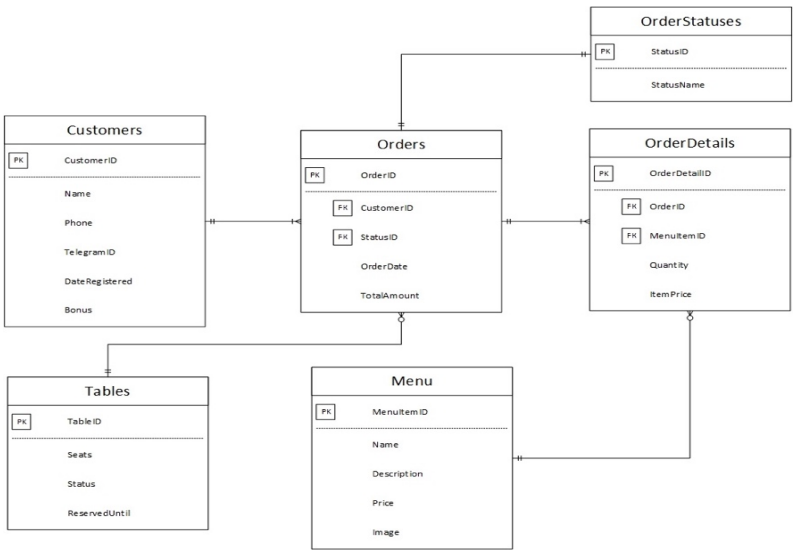


Рис. 2. Схема бази даних системи

Загальний алгоритм роботи системи можна побачити на рис. 3, в ньому відображена синхронізації всіх її компонентів.

Першим етапом є ініціалізація бази даних, яка готується до прийому запитів і зберігання інформації. Далі запускається програма-менеджер, яка забезпечує виконання логіки системи, включно з обробкою запитів від Telegram-бота і користувачів, які взаємодіють через касовий інтерфейс. Важливим аспектом стабільної роботи представленої системи є інтеграція Telegram-боту з великою мовною моделлю (LLM) Llama 3.1 Instruct 8B. Як вже було зазначено Telegram-бот виступає одним з інтерфейсів взаємодії між

клієнтами і системою. Крім можливості оформлення замовлень через касу або особистого звернення до ресторану, бот являє собою зручний інструмент для дистанційної взаємодії з системою. Інтеграція Telegram-бота з LLM дозволяє йому аналізувати складні текстові запити, навіть якщо вони не відповідають заздалегідь запрограмованим командам. Це дає змогу системі адаптивно реагувати на потреби клієнтів, пропонуючи їм релевантні рішення та спрощуючи процес взаємодії.

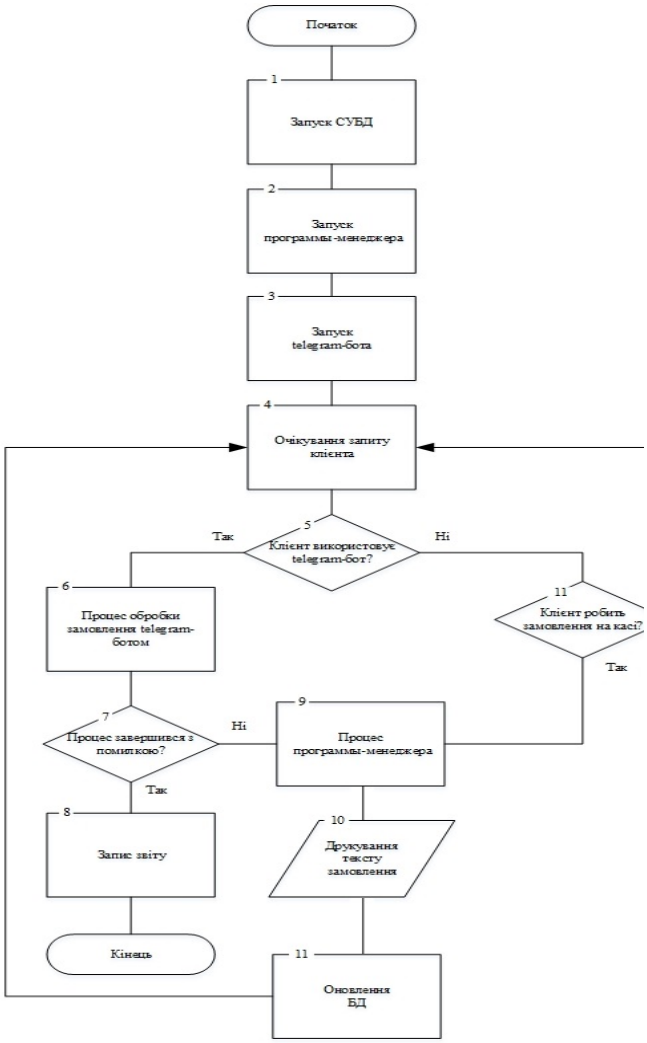


Рис. 3. Загальний алгоритм роботи системи

Якщо користувач надсилає складний текстовий запит, який не відповідає заздалегідь заданим командам, бот передає повідомлення в мовну модель для аналізу. Інтеграція з LLM забезпечує аналіз таких запитів, формуючи структуровані відповіді, які потім використовуються для автоматичної обробки в програмі-менеджері. Такий підхід дозвоив Telegram-боту у потрібному вигляді обробляти запити клієнтів, навіть якщо вони подані в неструктурованій або складній формі.

Результати реалізації. Розроблена система автоматизації ресторанного обслуговування об'єднує Telegram-бота, програму-менеджер і базу даних PostgreSQL у єдину інтегровану екосистему, яка забезпечує ефективну взаємодію між клієнтами, персоналом і внутрішніми процесами ресторану. У цьому розділі детально представлено функціональні можливості створеного програмного комплексу, особливості його архітектури та результати тестування.

Telegram-бот виконує функцію користувацького інтерфейсу, забезпечуючи клієнтів можливістю зручно взаємодіяти з рестораном. Основні функції бота включають перегляд меню, оформлення замовлень, бронювання столиків і отримання актуальної інформації. Бот підтримує текстові команди, інтерактивні кнопки, а також динамічну адаптацію інтерфейсу до потреб користувачів. Інтеграція з мовною моделлю Llama 3.1 Instruct 8B дозволяє обробляти складні текстові запити клієнтів, навіть якщо вони не відповідають заздалегідь запрограмованим сценаріям. Наприклад, бот здатен зрозуміти

запит типу: «хочу вафлі, стейк і соду через годину з собою», розпізнати його структуру і автоматично сформувати замовлення в базі даних.

Програма-менеджер забезпечує управління внутрішніми процесами ресторану. Її інтерфейс, створений за допомогою бібліотеки CustomTkinter, дозволяє персоналу обробляти замовлення, оновлювати меню, відстежувати статус столиків і керувати взаємодією з клієнтами. Основні елементи інтерфейсу, такі як картки замовлень і блоки управління меню, оптимізовані для швидкого доступу до інформації та зручної роботи з великими обсягами даних. Програма також інтегрує функції друку замовлень для кухарів, автоматичного оновлення статусів і звітності.

Архітектура системи побудована з урахуванням принципів модульності та масштабованості. БД PostgreSQL зберігає всю необхідну інформацію, включаючи дані про клієнтів, замовлення, меню, статуси столиків і склад замовлень. Схема бази даних передбачає зв'язки між основними сутностями, що дозволяє швидко виконувати запити і забезпечувати актуальність даних у реальному часі. Для забезпечення ефективності роботи система використовує SQL-запити, які динамічно формуються на основі введених користувачами даних.

Для забезпечення надійної роботи розробленої системи автоматизації ресторанного обслуговування було впроваджено детальний процес тестування, який охоплював усі аспекти її функціонування. Основою цього підходу стала концептуальна ідея створення інтегрованої екосистеми, яка забезпечує взаємодію між клієнтами, персоналом та внутрішніми процесами закладу. Тестування включало кілька ключових етапів, спрямованих на перевірку коректності роботи кожного компонента системи, інтеграції між ними та їхньої здатності адаптуватися до реальних умов.

Тестування системи базувалося на заздалегідь підготовлених сценаріях, які відображали різні аспекти її використання. Наприклад, під час запиту про перегляд меню, після активації функції «Показати меню», бот надавав користувачу зображення меню у високій якості (рис. 4). Подальші дії включали можливість оформлення замовлення через інтерактивні кнопки або вручну. У разі текстового запиту модель Llama 3.1 Instruct 8B аналізувала отриману інформацію, інтерпретувала її та передавала структурований вихідний результат для подальшої обробки.

Також проводилось тестування оформлення замовлень, під час якого перевірялася здатність Telegram-бота обробляти складні текстові запити, наприклад: «замовити піцу, салат і лимонад через годину» (рис. 5). Модель на 8 мільярдів параметрів без fine-tuning успішно інтерпретувала контекст запиту за допомогою спеціально складеного промпту і формувала структуровані дані (наприклад, <Pizza><Salad><Lemonade>[3][timer:60]), які передавалися до програми-менеджера. Ці дані використовувалися для формування SQL-запитів.

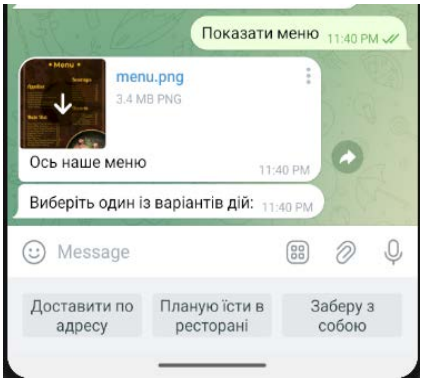


Рис. 4. Інтерактивні кнопки з готовими відповідями та можливістю вводити власні запити

Рис. 5. Процес вибору оформлення текстовим запитом

Окрему увагу приділено тестуванню взаємодії з функцією бронювання столиків. Telegram-бот надавав користувачу схему ресторану (зображення у високій якості) із позначенням доступних столиків (рис. 6). На основі даних з бази даних PostgreSQL [6] користувач міг обрати конкретний столик, зазначити час прибуття та додаткові побажання. Цей процес забезпечував швидке та точне резервування місць із синхронізацією з іншими елементами системи.

Рис. 6. Схема вільних столиків

На рис. 7 приведено результати запису даних у БД після тестування, оброблення системою складного текстового запиту від клієнта. Тестування підтвердило функціональність і відповідність поставленим вимогам. Telegram-бот успішно виконує роль клієнтського інтерфейсу, обробляючи як прості, так і складні запити. Запит на оформлення замовлення з тексту «замовити піцу та чай на 18:00» був правильно оброблений системою, сформовано замовлення, оновлено статус столика і відправлено підтвердження клієнту. Програма-менеджер показала стабільну роботу, забезпечуючи коректну синхронізацію з базою даних і ефективну обробку великого обсягу інформації.

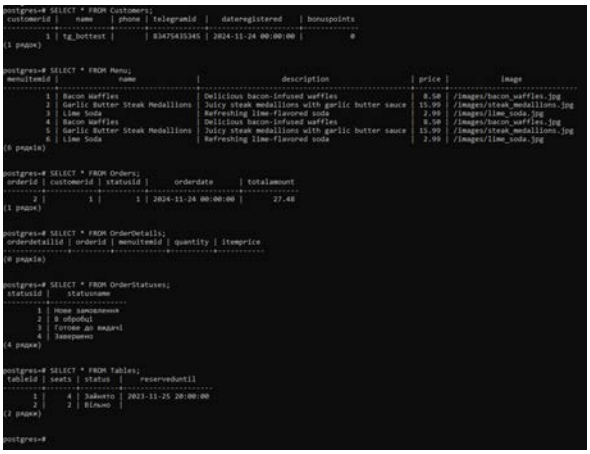


Рис. 7. Результат виконання SQL-запитів, сформованих Telegram-ботом на основі даних мовної моделі

Одним із ключових елементів тестування було перевірка інтеграції Telegram-бота з мовною моделлю. Навіть за умов некоректно сформульованих запитів система демонструвала високу точність розуміння контексту, що забезпечує адаптивність до різних сценаріїв використання. Наприклад, запит типу «замовити щось із десертів і лимонад» був інтерпретований моделлю з уточненням деталей і успішно переданий у програму-менеджер.

Таким чином, розроблений програмний комплекс забезпечує високу ефективність автоматизації ресторанного обслуговування. Telegram-бот спрощує взаємодію з клієнтами, програма-менеджер оптимізує внутрішні процеси, а база даних гарантує надійне зберігання інформації. Система успішно впоралася з тестовими сценаріями, демонструючи високу надійність і функціональність у реальних умовах роботи.

Висновки. Розробка автоматизованої системи для ресторанного обслуговування, що об'єднує Telegram-бота, програму-менеджер та базу даних PostgreSQL, є прогресивним рішенням у галузі автоматизації ресторанних процесів. Система створює комплексну екосистему, яка сприяє значному підвищенню ефективності роботи ресторану, забезпечуючи оперативність і точність обробки замовлень, покращуючи взаємодію з клієнтами та оптимізуючи внутрішні процеси.

Використання Telegram-бота у поєднанні з мовною моделлю Llama 3.1 Instruct 8B дозволяє обробляти навіть складні текстові запити, які не відповідають жорстко запрограмованим сценаріям. Це є значною перевагою перед традиційними POS-системами, які часто обмежені стандартними функціями.

Використання сучасних мовних моделей у ресторанному бізнесі є новим підходом, що дозволяє значно підвищити рівень персоналізації обслуговування. Telegram-бот інтегрується з мовною моделлю для створення адаптованих відповідей, враховуючи індивідуальні запити клієнтів. Це забезпечує унікальну конкурентну перевагу для закладів, які впроваджують таку систему.

Проведене тестування підтвердило передбачуваність формування відповідей системою та її надійність у реальних умовах роботи. Telegram-бот продемонстрував стабільність у виконанні ключових функцій, таких як оформлення замовлень, бронювання столиків і надання інформації про доступність меню. Інтеграція з мовною моделлю забезпечила можливість обробки некоректно сформульованих запитів і адаптацію до широкого спектру сценаріїв використання. Розроблене рішення має низку переваг, які роблять його ефективним і практичним для ресторанного бізнесу. По-перше, система значно підвищує ефективність, скорочуючи час обробки замовлень і знижуючи ймовірність помилок, викликаних людським фактором. По-друге, завдяки використанню Telegram-бота, впровадження не потребує додаткових фінансових витрат на обладнання та інфраструктуру, що робить її доступною для широкого кола закладів. Крім того, персоналізація сервісу сприяє покращенню клієнтського досвіду, підвищуючи задоволеність відвідувачів. Важливо зазначити, що система також відзначається легкою інтеграцією з уже існуючими програмними рішеннями, що забезпечує її зручне використання та ефективність у щоденній роботі.

Виходячи з цього можна ствердити, що розроблена система демонструє значний крок вперед у напрямку автоматизації ресторанного бізнесу. Пропонований підхід, заснований на використанні Telegram-бота та сучасної мовної моделі, створює нові можливості для оптимізації внутрішніх процесів закладу та забезпечення високого рівня обслуговування клієнтів. Цей підхід може стати основою для подальшого розвитку автоматизації у ресторанній сфері, створюючи нові стандарти обслуговування.

Список використаних джерел:

1. Chui M. Four fundamentals of workplace automation. McKinsey & Company. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/four-fundamentals-of-workplace-automation (date of access: 08.12.2024).

2. Hartati R., Manullang E. B. Implementation of Telegram Chatbot AI with Natural Language Processing (NLP) in Learning Creative Entrepreneurship to Develop Students' Creative and Innovative Competence. *In Talenta Conference Series: Local Wisdom, Social, and Arts (LWSA),* 2024, Vol. 7, No. 2, pp. 72–79.

3. Limna P., Kraiwanit T., Jangjarat K., Klayklung P., Chocksathaporn P. The use of ChatGPT in the digital era: Perspectives on chatbot implementation. *Journal of Applied Learning and Teaching*, 2023, 6(1), 64–74.

4. Restaurant operations management system vs traditional methods. Simplex Technology Solutions. URL: https://simplexts.net/restaurant-operations-management-system-vs-traditional-methods/ (date of access: 08.12.2024).

5. Sawyer K. The pros and cons of running an automated restaurant. Deputy Blog. URL: https://www.deputy.com/blog/the-pros-and-cons-of-running-an-automated-restaurant (date of access: 08.12.2024).

6. SCHÖNIG, Hans-Jürgen. Mastering PostgreSQL 15: Advanced techniques to build and manage scalable, reliable, and fault-tolerant database applications. *Packt Publishing Ltd*, 2023.

7. Solohubov I., Moroz A., Tiahunova M., Kyrychek H., Skrupsky S. Accelerating software development with AI: exploring the impact of ChatGPT and GitHub Copilot. – *The 11th Workshop on Cloud Technologies in Education (CTE 2023)* – Kryvyi Rih, December 22, 2023. P. 76–86

8. Автоматизація ресторану. Proriat Franchise. URL: https://proriat-franchise.com/uk/listing/avtomatizacya-restoranu/ (дата звернення: 07.12.2024).

9. POS-система для ресторану. Poster. URL: https://joinposter.com/ua/post/pos-systema-dlya-restoranu (дата звернення: 07.12.2024).

10. Технології в ресторанному бізнесі: як автоматизувати кол-центр для прийому замовлень та доставки. Wezom. URL: https://wezom.com.ua/ua/blog/tehnologiyi-v-restorannomu-biznesi (дата звернення: 07.12.2024).

УДК 004.432
DOI https://doi.org/10.32689/maup.it.2024.4.3

Тетяна ВАВРИК
асистент кафедри інженерії програмного забезпечення,
Івано-Франківський національний технічний університет нафти і газу, vavruk1060@gmail.com
***ORCID:** 0000-0002-0612-0084*

Ліда ГОБИР
асистент кафедри інженерії програмного забезпечення,
Івано-Франківський національний технічний університет нафти і газу,
lidagobyr@gmail.com

ОПТИМІЗАЦІЯ ЗАХИСТУ ДАНИХ: ПРЕВЕНТИВНІ ТА РЕАКТИВНІ СТРАТЕГІЇ

Анотація. *У статті досліджуються ключові аспекти оптимізації захисту даних в умовах постійно зростаючих кіберзагроз. Автори виокремлюють дві основні категорії стратегій: превентивні, які спрямовані на запобігання інцидентам, та реактивні, що акцентують увагу на реагуванні на вже виниклі загрози.*

Мета роботи *дослідження основних підходів до забезпечення безпеки даних у сучасних інформаційних системах. Стаття розглядає ефективні превентивні стратегії для попередження витоків або несанкціонованого доступу до інформації, а також реактивні стратегії для відновлення систем та мінімізації наслідків кіберінцидентів.*

Методологія. *Огляд наукових публікацій, що стосуються стратегій захисту даних. Вивчення нормативних документів щодо захисту інформації.*

Це дозволить встановити сучасний стан проблеми та визначити найбільш ефективні превентивні і реактивні методи захисту. Аналіз превентивних стратегій використання методу порівняння різних підходів до захисту даних. Оцінка реактивних стратегій захисту таких як, відновлення після інцидентів, моніторинг атак та реагування на інциденти.

Наукова новизна. *Розробка методології оптимізації витрат на заходи з кібербезпеки. Це дозволяє визначити оптимальний баланс між проактивними і реактивними заходами безпеки. Введення комплексної оцінки, яка враховує не тільки витрати на реалізацію технологій, але й економічний ефект від зниження ризику безпеки та оперативного відновлення після атак.*

Висновки *дослідження підкреслюють важливість комплексного підходу до захисту даних, який поєднує превентивні та реактивні заходи, забезпечуючи більш надійний рівень інформаційної безпеки, а також зменшити ризики в умовах швидко змінюваного кіберпростору Це може бути корисними для фахівців у галузі інформаційних технологій, безпеки даних і стратегічного управління.*

Ключові слова: *захист даних, оптимізація, превентивні стратегії, реактивні стратегії, кібербезпека, політики безпеки.*

Tetiana VAVRYK, Lida HOBYR. OPTIMIZING DATA PROTECTION: PREVENTIVE AND REACTIVE STRATEGIES

Abstract. *The article examines key aspects of optimizing data protection in the face of ever-increasing cyber threats. The authors identify two main categories of strategies: preventive, which are aimed at preventing incidents, and reactive, which focus on responding to threats that have already occurred.*

The purpose of the work *is to study the main approaches to ensuring data security in modern information systems. The article considers effective preventive strategies to prevent leaks or unauthorized access to information, as well as reactive strategies to restore systems and minimize the consequences of cyber incidents.*

Methodology. *Review of scientific publications related to data protection strategies. Study of regulatory documents on information protection.*

This will allow to establish the current state of the problem and determine the most effective preventive and reactive protection methods. Analysis of preventive strategies using the method of comparing different approaches to data protection. Evaluation of reactive protection strategies such as, incident recovery, attack monitoring and incident response.

Scientific novelty*. Development of a methodology for optimizing costs for cybersecurity measures. This allows determining the optimal balance between proactive and reactive security measures. Introduction of a comprehensive assessment that takes into account not only the costs of implementing technologies, but also the economic effect of reducing security risk and rapid recovery after attacks.*

Conclusions. *The study's findings highlight the importance of a comprehensive approach to data protection that combines preventive and reactive measures, ensuring a more robust level of information security, as well as reducing risks in a rapidly changing cyberspace. This may be useful for professionals in the fields of information technology, data security, and strategic management.*

Key words: *data protection, optimization, preventive strategies, reactive strategies, cybersecurity, security policies.*

Вступ. Постановка проблеми. В сучасному цифровому світі, де обмін і зберігання інформації відбуваються в онлайн-режимі, захист конфіденційності, цілісності та доступності даних стає надзвичайно важливою задачею як для окремих користувачів так і для підприємств. Кіберзагрози стають все більш складними і руйнівними, змушуючи користувачів зосередитися на розробці та впровадженні ефективних стратегій захисту інформації. Розробка політики захисту даних дає змогу визначати межі ризику для кожної категорії інформації та забезпечити дотримання нормативно-правових вимог. Також ця

політика допомагає налаштувати автентифікацію й авторизацію, які визначають, кому потрібно надати доступ, до якої інформації та чому.

Важливим аспектом дослідження є порівняння ефективності превентивних та реактивних стратегій у мінімізації загроз і забезпеченні стійкості інформаційних систем. Превентивні стратегії спрямовані на попередження можливих загроз і запобігання інцидентам безпеки заздалегідь. З іншого боку, реактивні стратегії орієнтовані на виявлення інцидентів та реагування після їх виникнення.

Аналіз останніх досліджень і публікацій. Захист даних є одним із найважливіших аспектів у сучасному інформаційному суспільстві. Дослідження в цій сфері зосереджуються на розвитку стратегій, які можуть забезпечити безпеку інформаційних систем. Інтернет дав потужний поштовх для розвитку масової комунікації, торгівлі та обміну інформацією. Разом з тим сьогодні він є тією сферою, де здійснюється чимало правопорушень. Суттєве зростання кількості інцидентів у кіберпросторі обумовлює необхідність системного аналізу джерел виникнення загроз [1–3], на перше місце серед яких виходить фішинг. У роботі [2] отримано класифікатор та розглядаються можливості його використання для подальшого створення програмних рішень для розпізнавання фішингових сайтів [2].

Користувачі зараз використовують стратегію даних для покращення кібербезпеки за допомогою систем автоматичного реагування на наслідки (AMR), особливо в контексті боротьби зі складними загрозами. Дослідницька стаття [2] містить ретельний аналіз цього явища, вивчення його наслідків для операцій, розподілу ресурсів і довіри до автоматизації. Крім того, автори пропонує зрозуміти складності, пов'язані з управління хибними спрацьовуваннями, підкреслюючи необхідність ефективних механізмів перевірки [2].

Штучний інтелект і машинне навчання нещодавно зробили видатний внесок у продуктивність інформаційних систем і безпеку кібер-фізичних систем. У цій галузі було проведено безліч досліджень, що призвело до спалаху публікацій за останні два роки. Вибір правильного алгоритму для вирішення складної проблеми безпеки в дуже точному промисловому контексті є складним завданням. Автори статті [4] пропонують структуру рекомендацій щодо алгоритму навчання, яка для чітко визначеної ситуації керує вибором алгоритму навчання та наукової дисципліни (наприклад, RNN, GAN, RL, CNN тощо). Ця структура має перевагу в тому, що вона була створена на основі обширного аналізу літератури, як показано в цій статті для рекурентних нейронних мереж та їх варіацій [4].

У роботах [5–6] запропоновано інформаційну технологію моніторингу безпеки даних програмного забезпечення. Передбачається, що розроблена інформаційна технологія моніторингу безпеки даних програмного забезпечення набуде широкого використання не лише в комерційній розробці програмного забезпечення, але і в навчальному та науковому застосуванн [5, 7].

У роботах [8–10] виділені два дуже різні підходи до надання IT-підтримки. Неправильна стратегія може негативно вплинути на здатність служби підтримки оперативно вирішувати проблеми. Це може призвести до тривалих відключень і тривалого часу очікування вирішення проблеми . Реактивний підхід може змусити команду підтримки виправляти проблеми з наслідками, які впливають на загальне IT-середовище. Проактивні стратегії передбачають більш обережний і ефективний підхід до надання IT-підтримки. Проактивна стратегія передбачає розробку планів вирішення різних проблем ще до їх виникнення [10].

Метою статті є аналіз та оптимізація стратегій захисту даних в інформаційних системах, зокрема визначення ефективності превентивних і реактивних заходів у контексті запобігання і реагування на загрози безпеці. Дослідження також спрямоване на розробку рекомендацій щодо впровадження комплексного підходу до захисту даних, що дозволить підвищити стійкість до кібератак і забезпечити безпечнішу обробку інформації.

Виклад основного матеріалу дослідження

Превентивні стратегії захисту інформації. Превентивні стратегії захисту інформації спрямовані на запобігання потенційним загрозам та атакам заздалегідь. Їх основною метою є мінімізація ризиків та зменшення ймовірності виникнення вразливостей у системах та даних. Однією з основних переваг превентивних стратегій є їх здатність передбачити та попередити можливі загрози, що дозволяє організаціям підготуватися та вжити заходів у відповідь на них заздалегідь.

Превентивні стратегії захисту інформації включають широкий спектр заходів, спрямованих на запобігання можливим загрозам та атакам до їх виникнення. Ось деякі з основних компонентів превентивних стратегій:

1. Політика безпеки: Розробка чітких політик і стандартів безпеки для організації, що встановлюють правила щодо управління доступом, шифрування даних, регулярного оновлення програмного забезпечення тощо.

2. Шифрування даних: Застосування шифрування для захисту конфіденційної інформації від несанкціонованого доступу, забезпечуючи безпеку даних навіть у випадку втрати контролю над ними.

3. Управління доступом: Встановлення строгих прав доступу згідно принципу найменших привілеїв, що дозволяє обмежити доступ до даних лише для необхідних користувачів.

4. Регулярне оновлення програмного забезпечення: Вчасне встановлення патчів безпеки і оновлень програмного забезпечення для усунення вразливостей і запобігання атак.

5. Безпечне зберігання паролів: Використання безпечних методів зберігання паролів, таких як хешування та сіль.

6. Фізичний захист: Захист фізичного доступу до приміщень, серверних кімнат та інших просторів, де зберігається інформація.

7. Антивірусне програмне забезпечення та брандмауери: Використання програмних засобів для виявлення та запобігання вторгнень, включаючи віруси, шкідливі програми та несанкціонований доступ.

8. Захист мережі: Використання технічних засобів, таких як брандмауери та веб-фільтри, для моніторингу та блокування небажаного мережевого трафіку.

9. Резервне копіювання даних: Регулярне створення резервних копій даних і зберігання їх в безпечному місці для відновлення в разі втрати або пошкодження.

Реактивні стратегії захисту.

Реактивні стратегії, спрямовані на виявлення і реагування на загрози після їх виникнення. Ці стратегії спрямовані на реагування на інциденти безпеки, коли вони вже сталися, і їх мета – мінімізувати наслідки атак або порушень безпеки. Наприклад, регулярні аудити безпеки, моніторинг активності користувачів та вжиття заходів у разі виявлення атаки.

Моніторинг та виявлення загроз: Реактивні стратегії починаються з ефективного виявлення загроз. Для цього використовуються системи моніторингу і виявлення вторгнень (IDS), програми для аналізу аномалій в мережевому трафіку або на комп'ютерах, а також засоби для моніторингу безпеки. Чим раніше інцидент буде виявлений, тим швидше можна почати реагувати на нього. Постійний моніторинг систем та мереж для виявлення незвичайної або підозрілої активності, яка може вказувати на потенційні загрози.

Інцидентний відгук: Реагування на виявлені або підтверджені загрози шляхом запуску планів реагування на інциденти. Це може включати блокування атак, відключення компрометованих систем або зупинку небезпечних процесів. Також створення плану дій для команд безпеки, щоб оперативно і ефективно вирішувати проблему.

Відновлення після інциденту: Одна з основних цілей реактивної стратегії– швидке відновлення нормальної роботи після інциденту. Це може включати відновлення втрачених або пошкоджених даних з резервних копій, відновлення доступу до систем або перегляд безпекових налаштувань для запобігання повторним інцидентам.

Аналіз інциденту: Після того, як інцидент було ліквідовано, дуже важливо проаналізувати його і прийняти заходи для підвищення рівня безпеки в майбутньому. Це може включати коригування політик безпеки, оновлення програмного забезпечення, навчання персоналу щодо нових загроз або поліпшення методів моніторингу. Також аналіз слабких місць в системі, які дозволили інциденту статися, та внесення відповідних покращень.

Навчання та підвищення свідомості: Після інциденту проводиться навчання персоналу та вдосконалення політик безпеки для підвищення стійкості до майбутніх атак. Інформування персоналу про інциденти та навчання їх, як уникати подібних ситуацій у майбутньому.

Політики та процедури відновлення: Визначення чітких політик та процедур для відновлення після інцидентів, включаючи регулярні аудити та оцінку ефективності.

Превентивні та реактивні стратегії захисту інформації мають різний підхід до забезпечення безпеки системи, і кожна з них має свої особливості, переваги та недоліки. Порівняємо ці підходи (табл. 1).

Тепер розглянемо недоліки кожної стратегії (рис. 1).

Пропонуємо наступну формулу, яка дозволить оцінити, наскільки ефективною є кожна стратегія захисту в контексті конкретного випадку, враховуючи як вигоди, так і витрати, пов'язані з її впровадженням та використанням.

$$E = \frac{(P_k \cdot P_b \cdot V_r \cdot T_c) - (P_l \cdot P_b \cdot V_c \cdot T_r)}{C_i \cdot C_P} \cdot F_r \cdot F_v \cdot F_a \cdot F_t$$

Де E – ефективність стратегії захисту інформації; P_k – потенційний ризик загрози; P_b – ймовірність виявлення загрози; V_r – вартість відновлення після загрози; T_c – тривалість кризового періоду; P_l – потенційний втрати від загрози; V_r – вартість відновлення після загрози; T_r – тривалість реагування на загрозу; C_i – вартість інвестицій у стратегію захисту; C_p – вартість захисту інформації; F_r – фактор ризику; F_v – фактор вразливості; F_a – фактор адаптивності; F_t – фактор часу;

Таблиця 1

Порівняльний аналіз кожної стратегії

Критерій	Превентивні стратегії	Реактивні стратегії
Основна мета	Запобігати виникненню загроз і атак	Виявлення та реагування на загрози та атаки після їх виникнення
Характер заходів	Попередні заходи, які призначені для мінімізації ризиків та запобігання атакам	Заходи, які вживаються після виникнення загрози або атаки для нейтралізації їх впливу та відновлення безпеки
Вартість	Зазвичай вимагає менших витрат, оскільки передбачається витрачання ресурсів перед подією	Може вимагати більших витрат, оскільки включає в себе відновлення після виникнення події
Ефективність	Може бути ефективнішою у запобіганні атак та мінімізації ризиків	Може бути менш ефективною у виявленні та нейтралізації загроз, але важлива для відновлення безпеки після події
Прогнозованість	Дозволяє заздалегідь приготуватися до можливих загроз та реагувати на них	Може бути менш передбачуваною, оскільки вимагає виявлення та реагування на непередбачені події
Превентивність	Запобігає загрозам до їх виникнення	Реагує на загрози після їх виникнення
Технічні засоби	Включає в себе використання технологічних засобів, таких як програмне та апаратне забезпечення	Може включати аудити безпеки та вирішення виявлених проблем
Організаційні аспекти	Включає в себе розроблення політик, процедур та навчання персоналу	Включає в себе впровадження політик безпеки та навчання персоналу з питань кібербезпеки
Орієнтація	Спрямована на передбачення майбутніх загроз та запобігання їм	Спрямована на виявлення та вирішення проблем після їх виникнення
Час	Вимагає часу на виявлення, відгук та відновлення після інциденту	Вимагає часу на встановлення та підтримку запобіжних заходів, але може заощадити час у майбутньому

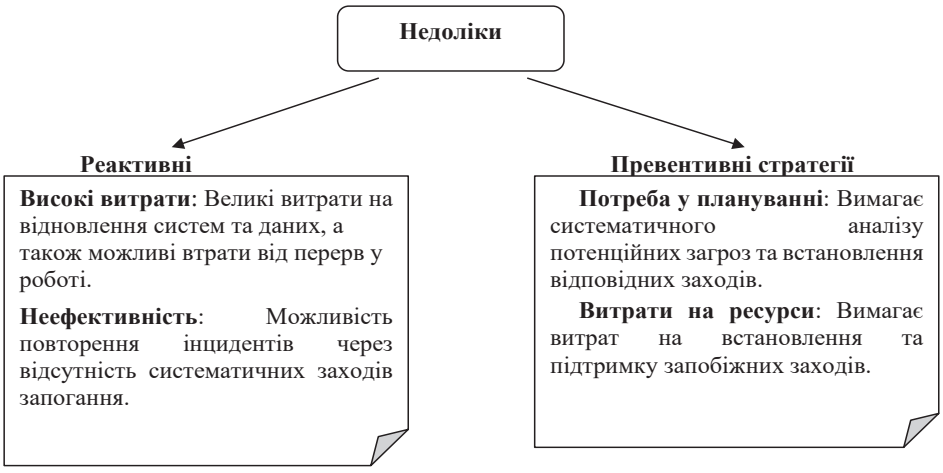


Рис. 1. Недоліки превентивної та реактивної стратегії захисту

Ця формула дозволяє врахувати різноманітні аспекти, такі як ризики, втрати, вартість та інші фактори, що впливають на ефективність стратегії захисту інформації у складних інформаційних середовищах.

Висновки даного дослідження і перспективи подальших розвідок у даному напрямку. Захист даних вимагає комплексного підходу, який включає як превентивні, так і реактивні стратегії. Порівняльний аналіз надає загальний огляд переваг та обмежень превентивних та реактивних стратегій захисту інформації. Порівнюючи превентивні та реактивні стратегії захисту інформації, можна зазначити, що обидва підходи мають свої переваги та обмеження. Успішний захист інформації вимагає поєднання як превентивних, так і реактивних стратегій. Комбінування цих стратегій дозволяє створювати комплексну систему захисту інформації, яка ефективно впорається з сучасними кіберзагрозами. Перспективи подальших досліджень можуть бути зосереджені на вдосконаленні існуючих методів та розробці нових, зокрема в контексті розвитку технологій, таких як штучний інтелект та машинне навчання. Використання сучасних методів аналізу та штучного інтелекту для виявлення аномалій і прогнозування загроз може значно підвищити ефективність реактивних стратегій.

Список використаних джерел:

1. Куперштейн Л., Луцишин Г., Кренцін М. Інформаційна технологія моніторингу безпеки даних програмного забезпечення. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. 3(23), 71–84. URL: https://doi.org/10.28925/2663-4023.2024.23.7184

2. Штонда Р., Черниш Ю., Терещенко Т., Терещенко К., Цикало Ю., Поліщук С. Класифікація та методи виявлення фішингових атак. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. 4(24), 69–80. URL: https://doi.org/10.28925/2663-4023.2024.24.6980

3. Alam, Mohammad Nazmul, et al. Phishing attacks detection using machine learning approach. In: *2020 third international conference on smart systems and inventive technology (ICSSIT)*. IEEE, 2020. 1173–1179.

4. Barreto C., Koutsoukos X. Design of Load Forecast Systems Resilient Against Cyber-Attacks. In Lecture Notes in Computer Science 2019. (pp. 1–20). *Springer International Publishing*. URL: https://doi.org/10.1007/978-3-030-32430-8_1

5. CHANTI S., CHITHRALEKHA T. A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, 2022, 9.89: 446–476.

6. Christophe Feltus. Optimizing Data Strategy for Automated Mitigation Response Security – Ransoware Case Study URL: https://www.researchgate.net/publication/380464686_Optimizing_Data_Strategy_for_Automated_Mitigation_Response_Security_-_Ransoware_Case_Study

7. Detecting Phishing Emails URL: https://meu.edu.jo/uploads/1/590422b4d5dd81.pdf Detecting Phishing Emails Using Machine Learning Techniques

8. Feltus C. Learning algorithm recommendation framework for IS and CPS security: Analysis of the RNN, LSTM, and GRU contributions. *International Journal of Systems andSoftware Security and Protection (IJSSSP)* 13, no. 1 (2022): 1–23.

9. Holmes D., Papathanasaki M., Maglaras L., Ferrag M. A., Nepal S., Janicke H. (2021, September). Digital twins and cyber security – solution or challenge? 2021 *6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Preveza, Greece. URL: https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566277

10. Optimizing IT Support: Proactive vs. Reactive Strategies. URL: https://vastitservices.com/blog/optimizing-it-support-proactive-vs-reactive-strategies/

УДК 004.42, 005.8
DOI https://doi.org/10.32689/maup.it.2024.4.4

Олександр ГОРДІЄНКО
кандидат технічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», oleksandr.m.hordiienko@gmail.com
***ORCID:** 0009-0002-7764-8668*

Аліна КОВАЛЬ
викладач кафедри комп'ютерних інформаційних систем та технологій
Інститут комп'ютерно-інформаційних технологій та дизайну,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», copa9393@gmail.com
***ORCID:** 0009-0001-7379-5065*

ПРОБЛЕМИ КОНФІДЕНЦІЙНОСТІ ТА ЕТИКИ У ВИКОРИСТАННІ ВІДКРИТИХ ДАНИХ ДЛЯ РОЗРОБКИ ДОДАТКІВ

Анотація. *У сучасну епоху цифрових технологій відкриті дані стали потужним ресурсом для розробки інноваційних додатків. Вони забезпечують розробників доступом до цінної інформації, яка сприяє створенню рішень для різноманітних сфер – від медицини до транспорту, від освіти до урбаністики. Проте використання відкритих даних викликає низку питань, пов'язаних із конфіденційністю та етикою. Як балансувати між необхідністю вільного доступу до інформації та захистом приватності? Як забезпечити етичне використання даних у додатках, що впливають на життя мільйонів людей? У цій статті ми розглянемо ключові проблеми конфіденційності та етики у контексті використання відкритих даних для розробки додатків.*

Мета статті. *Проаналізувати етичні та конфіденційні аспекти використання відкритих даних у процесі розробки програмних додатків, визначити ключові проблеми, пов'язані з захистом приватності користувачів, та запропонувати рекомендації для дотримання етичних принципів при роботі з відкритими даними.*

Методологія. *Проведено аналіз нормативно-правових актів, які регулюють використання відкритих даних. Використано кейс-аналіз реальних прикладів, коли використання відкритих даних викликало етичні або конфіденційні суперечності. Проведено опитування та інтерв'ю з розробниками додатків і експертами в галузі даних, щоб виявити їхні підходи та труднощі у роботі з відкритими даними. Систематизовано ризики через порівняння теоретичних концепцій конфіденційності з практичними викликами.*

Наукова новизна. *Представлено новий підхід до класифікації етичних викликів при використанні відкритих даних у розробці додатків, враховуючи їхній вплив на різні стейкхолдери. Описано механізми виявлення прихованих ризиків для конфіденційності користувачів при інтеграції відкритих даних у програмні продукти. Розроблено рекомендації щодо впровадження етичних стандартів у життєвий цикл розробки додатків, включаючи етапи збору, аналізу та інтеграції відкритих даних.*

Висновок. *Використання відкритих даних у розробці додатків створює значні етичні та конфіденційні ризики, які можуть порушувати права користувачів та знижувати довіру до програмних продуктів. Для мінімізації цих ризиків необхідно впроваджувати етичні стандарти на всіх етапах розробки, розробляти механізми захисту даних, дотримуватись правових норм і створювати прозорі політики щодо використання інформації. Ефективне управління конфіденційністю сприятиме гармонізації інтересів розробників, користувачів і суспільства.*

Ключові слова: *відкриті дані, деанонімізація, диференційна приватність, штучний інтелект.*

Oleksandr HORDIIENKO, Alina KOVAL. PRIVACY AND ETHICAL ISSUES IN THE USE OF OPEN DATA FOR APPLICATION DEVELOPMENT

Abstract. *In the modern era of digital technologies, open data has become a powerful resource for developing innovative applications. It provides developers with access to valuable information that helps create solutions for various fields – from medicine to transportation, from education to urban planning. However, the use of open data raises a number of questions related to privacy and ethics. How to balance the need for free access to information with the protection of privacy? How to ensure the ethical use of data in applications that affect the lives of millions of people? In this article, we will consider key privacy and ethics issues in the context of using open data for application development.*

The purpose of the article. *To analyze the ethical and confidential aspects of using open data in the process of developing software applications, to identify key issues related to the protection of user privacy, and to offer recommendations for adhering to ethical principles when working with open data.*

Methodology*. An analysis of regulatory and legal acts that regulate the use of open data was conducted. Case studies of real examples were used when the use of open data caused ethical or confidential conflicts. Surveys and interviews were conducted with application developers and data experts to identify their approaches and difficulties in working with open data. Risks were systematized by comparing theoretical concepts of privacy with practical challenges.*

Scientific novelty. *A new approach to classifying ethical challenges when using open data in application development is presented, taking into account their impact on various stakeholders. Mechanisms for identifying hidden risks to user privacy when integrating open data into software products are described. Recommendations have been developed for implementing ethical standards in the application development lifecycle, including the stages of collecting, analyzing, and integrating open data.*

Conclusion: *The use of open data in application development poses significant ethical and privacy risks that can violate user rights and reduce trust in software products. To minimize these risks, it is necessary to implement ethical standards at all stages of development, develop data protection mechanisms, comply with legal regulations, and create transparent policies for the use of information. Effective privacy management will help harmonize the interests of developers, users, and society.*

Key words: *open data, deanonymization, differential privacy, artificial intelligence.*

Вступ. Поняття відкритих даних. Відкриті дані – це інформація, яка доступна для загального використання, її можна вільно використовувати, аналізувати та поширювати. Зазвичай такі дані публікуються урядами, організаціями та науковими установами [17]. Наприклад, відкриті дані можуть включати статистику населення, метеорологічні показники, фінансові звіти державних установ, а також геопросторові дані [12]. Головна мета – зробити інформацію доступною для широкої аудиторії, сприяючи прозорості, інноваціям та економічному розвитку [3].

Однак, незважаючи на переваги, відкриті дані можуть містити інформацію, яка прямо або опосередковано пов'язана з особистими даними громадян [20]. Це створює ризики для конфіденційності, особливо якщо такі дані неправильно обробляються чи використовуються [1].

Проблеми конфіденційності

1. *Деанонімізація даних.* Однією з головних загроз для конфіденційності у використанні відкритих даних є можливість деанонімізації. Навіть якщо дані публікуються у знеособленому вигляді, за допомогою сучасних методів аналізу їх можна пов'язати з конкретними особами [9]. Наприклад, поєднання інформації з різних наборів даних – таких як медичні записи, транспортні маршрути та дані про покупки – може дозволити ідентифікувати особу, навіть якщо ці дані були знеособлені [13]. Протягом останніх п’яти років відкриття даних в Україні стало одним із показників трансформації, яка наразі відбувається у сфері державного управління. Доступ до раніше закритої інформації дозволив створити цілу низку можливостей, які вже зараз використовуються для посилення громадського контролю над бюджетними витратами, оптимізації витрат через прозорість тендерних процедур та покращення рівня і швидкості надання послуг населенню [8]. Подальший розвиток у цій сфері відкриває значні перспективи не тільки для прозорості державних процедур та обґрунтованості політичних рішень, а й для досягнення економічного ефекту практично у всіх секторах [19]. Відкриті дані наразі визначаються українським законодавством як «публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання» [2]. У такому вигляді відкриті дані відкривають такі можливості:

– формування більш прозорих, підзвітних, ефективних органів влади;

– покращення співпраці держави і суспільства у царині ключових соціальних викликів та створення результативної політики;

– забезпечення громадського контролю над діяльністю органів влади, боротьба з корупцією;

– створення і посилення нових ринків, сервісів, підприємств та робочих місць;

– підтримка інновацій, у тому числі – розвиток штучного інтелекту, для якого відкриті дані є ключовим ресурсом.

Для використання цих можливостей важливо не тільки зафіксувати визначення, а й створити законодавче та регуляторне поле, яке б дозволило їх реалізувати та скоординувало зусилля громадських організацій, державних служб та бізнесу [2]. Це дослідження підготовлено експертами сектору IT і Телеком Офісу ефективного регулювання (BRDO) для Державного агентства з питань електронного урядування України в межах проєкту USAID/UK aid «Прозорість та підзвітність у державному управлінні та послугах/TAPAS». Виконання цього дослідження стало можливим завдяки підтримці Фонду Євразія, що фінансується урядом США через Агентство США з міжнародного розвитку (USAID), та урядом Великої Британії через UK aid. Зміст цієї публікації є винятковою відповідальністю Офісу ефективного регулювання (BRDO) і не обов’язково відображає погляди Агентства USAID, уряду США, уряду Великої Британії або Фонду Євразія. Метою дослідження є аналіз чинного національного законодавства у сфері відкритих даних та його відповідності європейському законодавству у сфері вторинного використання публічної ін формації. Також передбачається підготовка відповідних рекомендацій щодо вдосконалення чинних нормативно-правових актів з метою їх наближення до європейських норм.

2. *Недостатній захист даних.* Багато організацій, які публікують відкриті дані, не забезпечують належного рівня захисту інформації. Відсутність чітких стандартів анонімізації та шифрування може призводити до витоків даних або їх неправильного використання. Крім того, розробники, які працюють із такими даними, не завжди дотримуються принципів конфіденційності [15].

3. *Ризики для вразливих груп населення***.** Використання відкритих даних може завдати шкоди вразливим групам населення, наприклад, людям із обмеженими можливостями, національним меншинам або економічно незахищеним верствам. Дані можуть бути використані для дискримінації або маніпуляцій, якщо вони потраплять до рук недобросовісних користувачів.

Етичні виклики

1. *Етичність збору даних*. Хоча відкриті дані часто збираються на законних підставах, процес їх збору не завжди є етичним. Наприклад, дані можуть бути зібрані без інформованої згоди людей або без чіткого розуміння того, як вони будуть використовуватися [18]. Це створює конфлікт між законністю та етичністю використання таких даних.

Крім того, важливо враховувати культурні та соціальні аспекти. Наприклад, у деяких спільнотах інформація, яка здається безпечною або нейтральною, може вважатися конфіденційною [4]. Процес збору даних має бути прозорим, а особи або групи, чиї дані збираються, повинні бути повністю поінформовані про мету та можливі ризики використання цих даних. Недотримання цих принципів може підривати довіру суспільства до проектів, які базуються на відкритих даних [10].

Важливим є також питання справедливості у зборі даних. Наприклад, чи враховуються всі групи населення, чи лише певні категорії, що може викликати нерівномірність у представлених даних. Це особливо важливо для додатків, які впливають на соціальну політику, охорону здоров'я або доступ до публічних послуг [5].

2. *Проблема упередженості.* Дані, які використовуються для розробки додатків, часто відображають упередження, закладені на етапі їх збору або обробки. Наприклад, якщо дані про злочинність збиралися в основному в районах із низьким рівнем доходу, це може призвести до створення додатків, які несправедливо маркують ці райони як небезпечні. Упереджені дані можуть посилювати соціальну нерівність замість її зменшення [6].

3. *Відповідальність розробників.* Розробники, які працюють із відкритими даними, несуть відповідальність за те, як ці дані використовуються. Проте у багатьох випадках вони не мають достатньої підготовки або знань для оцінки етичних аспектів своїх дій. Це може призвести до створення додатків, які порушують права людей або мають негативні соціальні наслідки. Розробники, які працюють із відкритими даними, відіграють ключову роль у забезпеченні етичності їх використання. Ця відповідальність включає кілька важливих аспектів [5]:

– *Оцінка ризиків і впливу*. Розробники повинні проактивно оцінювати можливі ризики використання даних, такі як порушення конфіденційності, дискримінація або неочікувані соціальні наслідки. Це вимагає впровадження процедур для аналізу впливу їх додатків на суспільство.

– *Прозорість процесів*. Програмісти повинні пояснювати користувачам, як їхні дані використовуються у створюваних додатках. Це включає опис мети збору даних, механізмів їх захисту та можливостей контролю над власною інформацією.

– *Дотримання етичних стандартів*. Використання відкритих даних має відповідати етичним принципам, таким як справедливість, прозорість і повага до приватності. Для цього розробники повинні слідувати відповідним кодексам етики, які встановлюють правила використання даних.

– *Навчання та професійний розвиток*. Оскільки технології та підходи до аналізу даних швидко змінюються, розробники мають постійно оновлювати свої знання. Зокрема, це стосується принципів анонімізації даних, методів виявлення упередженості та впровадження сучасних стандартів конфіденційності.

– *Уникнення маніпуляцій*. Програмісти повинні уникати створення додатків, які можуть сприяти маніпуляції громадською думкою, дезінформації або зловживанням даними. Це особливо важливо для продуктів, які стосуються чутливих тем, таких як охорона здоров'я чи виборчі процеси.

Розробники мають усвідомлювати, що їхні рішення можуть мати значний вплив на життя людей і довіру суспільства до цифрових продуктів. Недбале або недобросовісне використання даних може не лише завдати шкоди окремим особам, а й підривати довіру до технологій у цілому.

Стратегії вирішення проблем

1. *Підвищення прозорості.* Організації, які публікують відкриті дані, повинні забезпечити прозорість процесу їх збору, обробки та використання. Це включає надання докладної інформації про джерела даних, методи їх анонімізації та потенційні ризики [17].

2. *Етичні кодекси та стандарти.* Розробка та впровадження етичних кодексів і стандартів для роботи з відкритими даними можуть допомогти мінімізувати ризики. Такі стандарти повинні враховувати права людини, питання конфіденційності та уникнення упередженості в даних [6].

3. *Навчання розробників.* Освіта та тренінги для розробників додатків є ключовими для вирішення етичних проблем. Вони повинні включати курси з питань конфіденційності, етики та відповідального використання даних [14].

– Розширення освітніх програм. Університети та навчальні заклади повинні включати курси з етики роботи з даними до програм з інформаційних технологій. Це сприятиме формуванню у розробників усвідомлення важливості етичних стандартів.

– Практичні семінари та тренінги. Організації та компанії можуть проводити спеціалізовані тренінги для своїх співробітників, фокусуючись на реальних кейсах порушення конфіденційності та шляхах їх уникнення.

– Професійні сертифікації. Введення сертифікаційних програм з етики та захисту даних може стати важливим кроком до підвищення професійного рівня розробників.

Технологічні рішення

Сучасні технології пропонують низку інструментів для вирішення проблем конфіденційності та етики у використанні відкритих даних:

1. *Диференційна приватність*. Цей метод дозволяє аналізувати дані, забезпечуючи захист від деанонімізації. Суть диференційної приватності полягає в додаванні контрольованого «шуму» до даних, що дозволяє отримувати статистичні інсайти без ризику розкриття персональної інформації [16].

2. *Блокчейн-технології*. Використання блокчейну забезпечує прозорість і безпеку у роботі з даними. Блокчейн може допомогти відслідковувати, хто має доступ до даних, як вони використовуються, та гарантувати, що вони не були змінені [11].

3. *Штучний інтелект і машинне навчання*. Використання AI для автоматичного виявлення упередженості в даних або аналізу потенційних ризиків для конфіденційності. Наприклад, алгоритми можуть перевіряти, чи відповідають дані встановленим стандартам етичності [7].

4. *Інструменти анонімізації*. Сучасні платформи надають можливості автоматичного видалення або приховування чутливої інформації з даних. Це особливо корисно для роботи з великими масивами даних [7].

5. *Контроль доступу до даних*. Розробка систем, які забезпечують гнучке управління доступом до даних. Це включає в себе використання ролей, обмежень і протоколів аутентифікації, щоб запобігти несанкціонованому використанню даних [5].

Висновки. Використання відкритих даних для розробки додатків є потужним інструментом для інновацій, але воно супроводжується серйозними проблемами конфіденційності та етики. Щоб мінімізувати ризики, необхідно впроваджувати прозорі процеси, етичні стандарти та новітні технології. Розробники, уряди та організації повинні спільно працювати над створенням відповідального підходу до використання відкритих даних, забезпечуючи баланс між інноваціями та захистом прав людини.

Список використаних джерел:

1. Anderson C., Patel N. Barriers to Effective Use of Open Data in Research and Development. *Research and Innovation Journal*, 2020. 7(3), 120–135.
2. BRDO. Analysis of Ukrainian Open Data Legislation and Recommendations for Improvement. Kyiv: BRDO. 2020.
3. Brown K., Green D. Privacy Concerns in Open Government Data. *Data Privacy Review*, 2020. 5(1), 20–32.
4. Brown P. L., Green M. A. Ethical Considerations in Data Collection and Usage. *Data Ethics Quarterly*, 2020. 8(1), 22–34.
5. Carter L. J., Adams T. Bridging the Gap: Cultural Sensitivities in Open Data Practices. *International Journal of Data Ethics*, 2020. 9(2), 56–67.
6. Carter L. J., Adams T. The Ethics of Open Data Utilization. *International Journal of Data Ethics*, 2021. 10(1), 34–48.
7. Davis P., Clark S. AI in Ethical Data Analysis. Ethics in Artificial Intelligence Review, 2022. 8(3), 45–67.
8. Domínguez-Mayo F. J., et al. "Framework for Open Data Impact Assessment: Case Study in Public Administration." *Government Information Quarterly*, 2020. 37(4), 101494.
9. Gonen H., Elazari A. "De-anonymization Risks in Open Data Sharing: A Legal and Technical Perspective." *Journal of Information Technology & Politics*, 2020. 17(3), 222–239.
10. 10Johnson K. Transparency and Privacy in the Digital Age: A Cross-Cultural Analysis. *Social Data Journal*, 2020. 15(4), 78–91.
11. Johnson M., Lee T. Blockchain for Open Data Security. *International Journal of Digital Ethics*, 2021. 10(1), 89–103.
12. Johnson P., Lee A. The Role of Open Data in Smart City Development. *International Journal of Smart Cities*, 2020. 8(2), 101–113.
13. Knight M. B., Torra V. "Differential Privacy and Open Data: Balancing Transparency and Confidentiality." *Information Sciences*, 2020. 522, 1–15.
14. Nguyen A., Lee S., Kim H. Training Developers for Ethical Data Use. *Journal of Information Ethics*, 2021. 15(2), 78–92.
15. Rolik O., Telenyk S., Zharikov E. IoT and Cloud Computing: The Architecture of Microcloud-Based IoT Infrastructure Management System. У Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications. 2020. (Chapter 52, pp. 1157–1185). Hershey, PA, USA: IGI Global.
16. Smith J., Brown L. Differential Privacy in Big Data: Challenges and Solutions. Journal of Data Security, 2021. 12(4), 233–250.
17. Smith J., Taylor R. Open Data Policies and Their Impact on Government Transparency. *Journal of Open Data and Governance*, 2020. 12(3), 45–56.
18. Smith J., Taylor R. Open Data Policies and Their Impact on Government Transparency. *Journal of Open Data and Governance*, 2020. 12(3), 45–56.
19. Taddeo M., Floridi L. "Artificial Intelligence, Governance, and Public Policy: Understanding Open Data Challenges." *Philosophy & Technology*, 2020. 33(4), 541–559.
20. Williams H., Davis M. Open Data Analytics for Public Policy Improvements. *Policy & Data Analysis Quarterly*, 2020. 14(4), 200–215.

УДК 004.8:004.42
DOI https://doi.org/10.32689/maup.it.2024.4.5

Олександр ГОРДІЄНКО
кандидат технічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», oleksandr.m.hordiienko@gmail.com
***ORCID:** 0009-0002-7764-8668*

Аліна КОВАЛЬ
викладач кафедри комп'ютерних інформаційних систем та технологій,
Інститут комп'ютерно-інформаційних технологій та дизайну
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», copa9393@gmail.com
***ORCID:** 0009-0001-7379-5065*

КОНЦЕПЦІЯ ПІДКЛЮЧЕННЯ ФІЗИЧНИХ ОБ'ЄКТІВ У РОЗУМНОМУ БУДИНКУ: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МОНІТОРИНГУ ТА ПОКРАЩЕННЯ ЯКОСТІ ПОВІТРЯ

***Анотація. Мета роботи**. Стаття присвячена концепції підключення фізичних об'єктів у розумному будинку для моніторингу та покращення якості повітря за допомогою штучного інтелекту. Вона досліджує інтеграцію різноманітних сенсорів і пристроїв, таких як датчики якості повітря, системи вентиляції та фільтрації, з розумними будинками для створення комфортних та здорових умов для життя і впливу на організм людини. Особливу увагу приділено використанню ШІ для аналізу даних, отриманих від сенсорів, для автоматичного коригування параметрів повітря, таких як рівень CO_2, вологість і температура, з метою підтримки оптимального мікроклімату., як штучний інтелект може покращити енергетичну ефективність розумних будинків, зменшуючи енергоспоживання та знижуючи витрати на опалення, охолодження і вентиляцію, одночасно підтримуючи здоров'я мешканців. **Наукова новизна**. Стаття також оцінює потенційні виклики та майбутні перспективи впровадження таких технологій, враховуючи як технічні, так і етичні аспекти. Метою роботи є продемонструвати, як інноваційні рішення на основі IoT та ШІ можуть змінити підхід до управління навколишнім середовищем у будинках, покращуючи якість повітря та комфорт проживання.*

***Висновок.** Загалом, концепція підключення фізичних об'єктів та використання ШІ для покращення якості повітря в розумному будинку є важливим кроком до створення безпечніших, здоровіших та енергоефективніших умов для життя, що має потенціал для значних змін у сфері житлового комфорту та інженерних технологій у майбутньому.*

***Ключові слова:** фізичні обєкти, IoT, термостати, освітлення, охоронні системи, CO_2, PM2.5 та PM10, Sharp, сенсор, штучний інтелект.*

Oleksandr HORDIIENKO, Alina KOVAL. THE FUTURE OF PROGRAMMING: HOW ARTIFICIAL INTELLIGENCE IS TRANSFORMING SOFTWARE DEVELOPMENT

***Abstract. The purpose of the work.** The article is devoted to the concept of connecting physical objects in a smart home to monitor and improve air quality using artificial intelligence. It explores the integration of various sensors and devices, such as air quality sensors, ventilation and filtration systems, with smart homes to create comfortable and healthy living conditions and impact on the human body. Special attention is paid to the use of AI to analyze data obtained from sensors to automatically adjust air parameters, such as CO_2 levels, humidity and temperature, in order to maintain an optimal microclimate., how artificial intelligence can improve the energy efficiency of smart homes, reducing energy consumption and lowering heating, cooling and ventilation costs, while supporting the health of residents.*

***Scientific novelty.** The article also assesses the potential challenges and future prospects for the implementation of such technologies, taking into account both technical and ethical aspects. The aim of the work is to demonstrate how innovative IoT and AI-based solutions can change the approach to environmental management in homes, improving air quality and living comfort.*

***Conclusion.** Overall, the concept of connecting physical objects and using AI to improve air quality in a smart home is an important step towards creating safer, healthier, and more energy-efficient living environments, which has the potential to significantly change the field of residential comfort and engineering technologies in the future.*

***Key words:** IoT, thermostats, lighting, security systems, CO_2, PM2.5 and PM10, Sharp, sensor, Artificial Intelligence.*

Вступ. ***IoT (Internet of Things)*** – це концепція підключення фізичних об'єктів, пристроїв і сенсорів до Інтернету, що дозволяє їм збирати, обмінюватися і обробляти даними без прямої участі людини [8]. Наприклад:

– У будинках: термостати, освітлення, охоронні системи, які можна контролювати через смартфон.

– Годинники та фітнес-трекери, які моніторять стан здоров'я.

– Автомобілі, що збирають дані про стан, швидкість, навіть мають можливість відправляти їх на сервери для аналізу чи віддаленого контролю.

– У сільському господарстві: датчики в ґрунті, які вимірюють вологу або температуру для оптимізації поливу.

Моніторинг якості повітря є важливим для підтримки здоров'я людини, оскільки повітря може містити різноманітні забруднювачі, які можуть негативно впливати на дихальну систему та загальний стан здоров'я. Основними факторами, що впливають на якість повітря в приміщеннях, є рівень вуглекислого газу (CO_2), пил, вологість, температура, а також наявність хімічних сполук, таких як летючі органічні сполуки (ЛОС), формальдегід, діоксиди азоту (NO_2) тощо.

Показники якості повітря. Вуглекислий газ (CO_2). Високі рівні CO_2 можуть свідчити про погану вентиляцію та недостатній приплив свіжого повітря. Підвищена концентрація CO_2 може спричиняти втому, головні болі, зниження концентрації та навіть нудоту. Нормальний рівень CO_2 у приміщеннях зазвичай не перевищує 1000 ppm (частин на мільйон). Рівень понад 1000 ppm може вказувати на необхідність покращення вентиляції [14].

Пил (PM2.5 та PM10). Пил складається з дрібних часток, які можуть потрапляти в дихальні шляхи, погіршуючи стан здоров'я, особливо у людей із респіраторними захворюваннями (астма, алергії). PM2.5 (частки менші за 2.5 мікрометра) можуть проникати в глибокі частини легень і навіть потрапляти в кровообіг, що може призвести до серйозних проблем зі здоров'ям. PM10 – це частки діаметром менше 10 мікрометрів, які також можуть бути небезпечними для дихальної системи [14].

Датчики для вимірюваннярівня пилу:

– Sharp GP2Y1010AU0F (PM2.5). Сенсор використовує метод розсіювання світла для визначення часток у повітрі. Лазерне світло направляється на частки, які розсіюють світло, і фотодіод фіксує це розсіяння, перетворюючи його на електричний сигнал.

– Plantower PMS5003. Цей сенсор використовує лазер для розсіювання світла на частках у повітрі. Інтенсивність і кут розсіювання світла дозволяють визначити концентрацію часток. Сенсор може відрізняти PM1.0, PM2.5 та PM10.

– Honeywell HPMA115S0. Використовує лазер для розсіювання світла на частках, надаючи оцінку концентрації PM2.5. Сенсор має високу чутливість до дрібних часток у повітрі.

Температура та вологість. Занадто висока або низька температура, а також непідконтрольний рівень вологості (вища за 60% або нижча за 30%) можуть сприяти розвитку грибка, плісняви та бактерій, а також створювати дискомфорт. Оптимальні параметри для здоров'я – температура в межах 18–22°C і вологість 40–60% [14].

Датчики, що вимірюють температуру та вологість:

– DHT22. Вимірює температуру у діапазоні від -40°C до +80°C з точністю ±0.5°C. Вологість від 0% до 100% (точність ±2-5% в межах 20–80% вологості).

– BME280. Діапазон вимірювання температури від -40°C до +85°C з точністю ±1.0°C (в межах -10°C до +65°C). Діапазон вимірювання вологості від 0% до 100% RH (відносна вологість) з точністю ±3% в діапазоні від 20% до 80% вологості.

– DS18B20. Температурний діапазон від -55°C до +125°C з точністю ±0.5°C в діапазоні від -10°C до +85°C.

Летючі органічні сполуки (ЛОС) [15]. ЛОС – це хімічні речовини, які випаровуються в атмосферу при кімнатній температурі. До них належать формальдегід, бензол, толуол та інші, які можуть бути присутні в матеріалах для ремонту, меблях, засобах для чищення, косметиці, побутових хімікатах. Підвищені рівні ЛОС можуть викликати головний біль, запаморочення, подразнення очей та дихальних шляхів, а також сприяти розвитку хронічних захворювань.

Діоксид азоту (NO_2). В основному виникають в результаті діяльності газових плит, обігрівачів, камінів. Вони можуть погіршувати стан дихальних шляхів, спричиняти астму та інші проблеми з диханням.

Датчики, що вимірюють якість повітря:

– MH-Z19 (CO_2). Інфрачервоний сенсор (NDIR) для вимірювання CO_2. Діапазон вимірювання від 0 до 5000 ppm CO_2 (проте, можливе розширення до 2000 ppm або 10000 ppm в залежності від версії) з точністю ±50 ppm ±3% від виміряної величини.

– MiCS-5524 (CO, NO_2, NH3, O3). Мультигазовий сенсор, що вимірює CO (0–1000 ppm), NO_2 (0–50 ppm), NH3 (0–100 ppm), O3 (0–1000 ppb) з точністю ±3% для кожного газу в межах діапазону.

– CCS811 (CO_2, TVOC). Цифровий сенсор для вимірювання CO_2 та TVOC (загальні летючі органічні сполуки). Діапазон вимірювання CO_2 від 400 до 8192 ppm з точністю ±30% та TVOC від 0 до 1187 ppb з точністю ±10%.

– Figaro TGS Series (VOC). Сенсор для вимірювання VOC (летючі органічні сполуки). В залежності від конкретної моделі серії TGS, вони можуть вимірювати VOC в різних концентраціях (зазвичай від 1 до кількох тисяч ppm).

Забезпечення комфортного і здорового середовища [2, 4, 15].

Управління вентиляцією – один з основних способів контролю за якістю повітря. Важливо регулярно провітрювати приміщення, використовувати витяжки, зокрема в кухнях і санвузлах. Встановити рекуператори тепла або системи припливно-витяжної вентиляції, щоб зберегти тепло та водночас, покращити циркуляцію повітря. Щоб знизити рівень пилу, ЛОС і навіть бактерій в повітрі можна використовувати очищувачі повітря з HEPA-фільтрами та вуглецевими фільтрами. Така вентиляція особливо корисна для людей із алергіями чи астмою.

Неправильний рівень температури (менше 18°C та більше 24–25°C) може викликати фізичний дискомфорт і погіршити самопочуття. Висока температура може спричиняти відчуття втоми, головний біль, знижувати концентрацію і продуктивність. Низька температура може викликати переохолодження, особливо в нічний час, і сприяти розвитку простудних захворювань.

Занадто низька вологість (менше 30%) сприяє сухості шкіри, слизових оболонок, подразненню дихальних шляхів, сухості в очах, а також може погіршити стан бронхіальних шляхів, що особливо небезпечно для людей з алергіями або астмою. Занадто висока вологість (понад 60%) може призвести до розвитку плісняви, грибків і бактерій, що є джерелом алергенів і сприяє розвитку респіраторних захворювань.

Температура та вологість можуть впливати на меблі, дерев'яні підлоги та інші будівельні елементи. Дерево розсихається та тріскатися при низькій вологості, а при високій – набухає та деформується. Надмірна вологість шкодить фарбованим поверхням, шпалерам і викликає корозію металевих конструкцій.

Правильна температура та вологість у спальні можуть значно вплинути на якість сну. Температура в межах 18–22°C вважається оптимальною для сну. Вологість на рівні 40–60% також є ідеальною для підтримки комфортного сну, оскільки знижує ризик пересушування повітря та покращує дихання [15].

Необхідно використовувати осушувачі повітря для зниження вологості в приміщенні, особливо в місцях з підвищеною вологістю (ванна кімната, кухня). Для збільшення вологості в сухих умовах можна використовувати зволожувачі.

Екологічна оселя – це не лише питання збереження природи. Необхідно виключити матеріали, що виділяють токсичні хімікати (фарби, клеї, лакофарбові матеріали, пластикові меблі з високим вмістом ЛОС). Значно покращить якість повітря в приміщенні використання природних, нетоксичних матеріалів при ремонті або декоруванні.

Управління температурою [2, 4].

Конвектори. Конвекційні обігрівачі працюють за принципом природного руху повітря: нагріте повітря піднімається, а холодне опускається, тим самим створюючи потік повітря, який рівномірно прогріває кімнату. Такі обігрівачі швидко прогрівають приміщення, компактні та безшумність. Вони легко управляються, тому їх можна підключити у систему розумного будинку. Недоліками такого обладнання є велике споживання електроенергії та вони висушують повітря.

Інфрачервоні обігрівачі. Ці пристрої нагрівають не повітря, а об'єкти та поверхні в кімнаті, які, в свою чергу, віддають тепло навколишньому середовищу. Інфрачервоний обігрів схожий на тепло від сонця. Легко керується системою розумного будинку. Такий пристрій економить енергію, бо не гріє повітря, яке вилітає у вентиляцію, швидко обігріває та не висушує повітря. Однак їх можна використовувати лише на коротких відстанях та можуть бути небезпечні при неправильному використанні [2].

Масляні обігрівачі працюють за принципом нагріву масла, яке рівномірно передає тепло в навколишнє середовище. Легко керується системою розумного будинку. Це найбільш популярний тип обігрівачів. Вони тривалий час зберігають тепло після вимкнення, безшумні, не висушують повітря. Але вони повільно прогрівають приміщення та займають багато місця.

Теплові насоси – це сучасний енергозберігаючий метод обігріву, який використовує природні ресурси, такі як повітря, грунт чи вода, для отримання тепла. Вони можуть також працювати як кондиціонери влітку. Теплові насоси високо-ефективні та екологічні. Їх можна інтегрувати у систему розумного будинку, проте є певні умови для ефективної роботи. Недоліками такої системи є висока вартість установки та обладнання. Потребує регулярного обслуговування ,яке може бути досить дорогим [4].

Печі та каміни є одним із найстаріших типом обігріву, але досі дуже популярним у приватних будинках. Вони можуть працювати на дровах, пелетах або інших видах палива. Каміни та печі дають приємне природне тепло, мають декоративний ефект та атмосферність. Основною перевагою є незалежніть від електрики. Такі обігрівачі потребують регулярного догляду, запасу палива та вентиляції. Печі та каміни, особливо ті, що працюють на дровах чи вугіллі, мають велику кількість потенційно небезпечних факторів, таких як відкритий вогонь, перегрівання та ризик пожежі. У поєднанні з автоматичними системами це може призвести до неконтрольованого вогню чи перегріву, що створює серйозну небезпеку.

У разі несправності вентиляції, чадний газ може накопичуватись у приміщенні, що є небезпечним для здоров'я [4].

Системи теплої підлоги можуть бути електричними або водяними. Вони прогрівають підлогу, яка, у свою чергу, нагріває та рівномірно розподіляє тепло у приміщенні. Така система зручна та економить місце. Її легко інтегрувати у систему розумного будинку. Тепла підлога має бути зпроектована на момент будівництва та має високу вартість встановлення.

Штучний інтелект (ШІ) в моніторингу [1, 3, 5, 6, 12, 13].

Завдяки IoT, можна автоматизувати різні процеси, збирати великі обсяги даних для подальшого аналізу, знизити витрати на енергію, значно покращити комфорт у приміщенні, забезпечити віддалений мобільний моніторинг.

Штучний інтелект використовується для обробки великих обсягів даних, що надходять від сенсорів IoT. Алгоритми ШІ можуть аналізувати дані та інші фактори (наприклад, погодні умови, час доби, активність у приміщенні) для передбачення рівня забруднення повітря в майбутньому. На основі даних від сенсорів та моделей ШІ можна автоматично вживати заходів, наприклад, регулювати рівень вентиляції, активувати систему очистки повітря або повідомляти про забруднення користувача.

У статті було розглянуто концепцію підключення фізичних об'єктів у розумному будинку, зокрема використання штучного інтелекту для моніторингу та покращення якості повітря. Інтеграція сенсорних технологій і систем, таких як датчики якості повітря, фільтрація, вентиляція та системи кондиціонування, створює основу для побудови ефективних, здорових і комфортних умов для мешканців розумного будинку.

Основною перевагою використання штучного інтелекту в цьому контексті є можливість автоматичного аналізу та обробки даних, що дозволяє своєчасно виявляти аномалії та коригувати умови повітря, такі як рівень CO_2, температура, вологість та інші важливі параметри, з огляду на специфічні потреби мешканців. Автоматизація цього процесу забезпечує не лише покращення якості життя, але й значно підвищує енергоефективність розумного будинку, що знижує витрати на енергоресурси [1].

Важливою складовою цього підходу є також забезпечення здоров'я мешканців. Врахування якості повітря в житлових приміщеннях має безпосередній вплив на фізичне та психологічне здоров'я людей. Автоматизовані системи, які контролюють рівень токсичних речовин, пилу та вологи, можуть значно знизити ризики для здоров'я, покращуючи дихальну функцію та загальний комфорт. Завдяки інтеграції з іншими системами розумного будинку, такими як освітлення, опалення та охолодження, можна створювати індивідуалізовані та адаптивні умови для кожного користувача [5, 6, 12, 13].

Проте, разом із можливостями, впровадження таких технологій також стикається з кількома викликами. Серед них – необхідність забезпечення високого рівня безпеки даних, захисту від кібератак, а також етичні питання, що стосуються збору та використання персональних даних мешканців. Крім того, важливим аспектом є доступність технологій для різних соціальних груп і забезпечення їх адаптації до різних кліматичних умов.

Майбутнє розумних будинків, оснащених ШІ, виглядає дуже перспективно. Очікується, що технології автоматизації та моніторингу стануть ще більш точними і доступними, дозволяючи зменшити витрати енергії, покращити екологічні умови та знизити витрати на обслуговування будинків. Технології штучного інтелекту стануть не лише частиною побутових процесів, але й активно сприятимуть розвитку нових форм взаємодії між людьми та навколишнім середовищем, надаючи можливості для адаптації до змінних умов у реальному часі.

Список використаних джерел:

1. "Internet of Things – An action plan for Europe". ec.europa.eu. Commission of the European Communities. 18 June 2009. COM(2009) 278 final.
2. "Lighting control saves money and makes sense" (PDF). Daintree Networks. Retrieved 2009-06-19.
3. "The Computer for the 21st Century". Scientific American. 265 (3), 94–04. Bibcode:1991SciAm.265c..94W. doi:10.1038/scientificamerican0991-94.
4. Bahga, Arshdeep; Madisetti, Vijay (2014-08-09). Internet of Things: A Hands-On Approach. VPT. p. 50. ISBN 978-0-9960255-1-5.
5. Catalin Cimpanu (23 вересня 2016). Akamai Boots Krebs from Their Network After Never-Ending DDoS Attack. Softpedia.
6. Catalin Cimpanu (5 жовтня 2016). Akamai Post-Mortem Report Confirms Mirai as Source of Krebs DDoS Attacks. Softpedia.
7. Dan Goodin (20 березня 2013). Guerilla researcher created epic botnet to scan billions of IP addresses. Risk Assessment. Ars Technica.
8. Gillis, Alexander (2021). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2021.

9. Hendricks, Drew (10 August 2015). "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
10. Muhammad Junaid Bohio (19 march 2015). Analyzing a Backdoor/Bot for the MIPS Platform. SANS Institute. Архів оригіналу за 2 вересня 2016. Процитовано 9 листопада 2016.
11. Shafiq, Muhammad; Gu, Zhaoquan; Cheikhrouhou, Omar; Alhakami, Wajdi; Hamam, Habib (3 August 2022). "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks". Wireless Communications and Mobile Computing. 2022: e8669348. doi:10.1155/2022/8669348. ISSN 1530-8669.
12. Steve Ragan. Here are the 61 passwords that powered the Mirai IoT botnet. CSO Online.
13. Zach Wikholm. When Vulnerabilities Travel Downstream. Flashpoint.
14. Брайчевський, С. М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право.* 2019. 4 (31). doi:10.37750/2616-6798.2019.4(31).194348.
15. Головна Smart Home: Одомашнювання Інтернет речей
16. Інтернет речей: друг чи ворог?. Архів оригіналу за 16 січня 2014. Процитовано 15 січня 2014.

УДК 004.8:004.42
DOI https://doi.org/10.32689/maup.it.2024.4.6

Олександр ГОРДІЄНКО
кандидат технічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», oleksandr.m.hordiienko@gmail.com
***ORCID:** 0009-0002-7764-8668*

Аліна КОВАЛЬ
викладач кафедри комп'ютерних інформаційних систем та технологій
Інститут комп'ютерно-інформаційних технологій та дизайну
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», cora9393@gmail.com
***ORCID:** 0009-0001-7379-5065*

ВИКОРИСТАННЯ КРИПТОГРАФІЇ ЯК СЕРВІСУ У ВЕБ ПРОГРАМУВАННІ

Анотація. *Стаття присвячена дослідженню використання криптографії як сервісу (Cryptography as a Service, CaaS) у веб-програмуванні, що є важливою складовою сучасних підходів до забезпечення безпеки веб-додатків. Зважаючи на постійний ріст кількості онлайн-сервісів і зростаючу важливість захисту персональних даних, необхідність у надійних методах криптографії є незаперечною. Веб-розробники часто стикаються з проблемою інтеграції криптографічних функцій у свої додатки, що потребує значних витрат часу, зусиль та ресурсів. Криптографія як сервіс надає зручну і ефективну альтернативу, дозволяючи швидко інтегрувати захист даних через API, без необхідності глибоких знань у сфері криптографії.*

Мета статті. *Дослідити концепцію використання криптографії як сервісу CaaS, Cryptography у веб-програмуванні, визначити її переваги, обмеження та перспективи для забезпечення безпеки веб-додатків, а також розробити рекомендації щодо інтеграції CaaS у сучасні веб-розробницькі процеси.*

Методологія. *Проведено огляд існуючих сервісів CaaS (наприклад, AWS Key Management Service, Azure Key Vault). Проаналізовано технічні аспекти інтеграції криптографічних сервісів у веб-додатки на прикладах популярних мов програмування (JavaScript, Python, Java). Виконано порівняльний аналіз ефективності та безпеки CaaS у порівнянні з традиційними методами реалізації криптографії в веб-програмуванні. Проведено тестування практичного використання CaaS у моделюванні сценаріїв для шифрування даних, управління ключами та автентифікації.*

Наукова новизна. *Представлено систематизований аналіз можливостей CaaS у веб-програмуванні, зокрема для шифрування даних, цифрового підпису, автентифікації та управління ключами. Описано нові підходи до зниження навантаження на розробників шляхом делегування складних криптографічних операцій хмарним сервісам. Запропоновано рекомендації щодо вибору та інтеграції CaaS з урахуванням специфіки веб-додатків.*

Висновок. *Криптографія як сервіс пропонує розробникам ефективні інструменти для підвищення безпеки веб-додатків, дозволяючи делегувати складні криптографічні завдання спеціалізованим платформам. Це спрощує впровадження надійних механізмів шифрування, автентифікації та управління ключами, що є критично важливими для сучасних веб-систем. Однак для ефективного використання CaaS необхідно враховувати специфіку додатків, забезпечувати відповідність нормативним вимогам і мінімізувати залежність від зовнішніх сервісів шляхом впровадження резервних механізмів.*

Загалом, стаття пропонує комплексний огляд криптографії як сервісу в контексті веб-програмування та демонструє, як цей підхід може значно полегшити розробку безпечних веб-додатків, зберігаючи при цьому високу ефективність і надійність системи.

Ключові слова: *Цифровий підпис, PKI (Public Key Infrastructure), Digital Certificates, CA, Certification Authority, (RA, Registration Authority), (DB, Database), (CMS, Certificate Management System), (CRL, Certificate Revocation List), (Public and Private Keys), ECDSA, RSA, SHA-2.*

Oleksandr HORDIIENKO, Alina KOVAL. USING CRYPTOGRAPHY AS A SERVICE IN WEB PROGRAMMING

Abstract. *The article is devoted to the study of the use of Cryptography as a Service (CaaS) in web programming, which is an important component of modern approaches to ensuring the security of web applications. Given the constant growth of the number of online services and the growing importance of protecting personal data, the need for reliable cryptography methods is undeniable. Web developers often face the problem of integrating cryptographic functions into their applications, which requires significant expenditure of time, effort and resources. Cryptography as a service provides a convenient and effective alternative, allowing you to quickly integrate data protection via API, without the need for in-depth knowledge in the field of cryptography.*

The purpose of the article. *To investigate the concept of using cryptography as a CaaS service, Cryptography in web programming, to determine its advantages, limitations and prospects for ensuring the security of web applications, as well as to develop recommendations for integrating CaaS into modern web development processes.*

Methodology. *A review of existing CaaS services (for example, AWS Key Management Service, Azure Key Vault) was conducted. The technical aspects of integrating cryptographic services into web applications were analyzed using examples of popular programming languages (JavaScript, Python, Java). A comparative analysis of the effectiveness and security of CaaS was performed in comparison with traditional methods of implementing cryptography in web programming. The practical use of CaaS was tested in modeling scenarios for data encryption, key management and authentication.*

Scientific novelty. *A systematic analysis of the capabilities of CaaS in web programming, in particular for data encryption, digital signature, authentication and key management, is presented. New approaches to reducing the burden on developers by delegating complex cryptographic operations to cloud services are described. Recommendations for the selection and integration of CaaS are proposed, taking into account the specifics of web applications.*

Conclusion. *Cryptography as a service offers developers effective tools for improving the security of web applications, allowing them to delegate complex cryptographic tasks to specialized platforms. This simplifies the implementation of reliable encryption, authentication, and key management mechanisms, which are critical for modern web systems. However, for effective use of CaaS, it is necessary to take into account the specifics of applications, ensure compliance with regulatory requirements, and minimize dependence on external services by implementing backup mechanisms.*

Overall, the article offers a comprehensive overview of cryptography as a service in the context of web programming and demonstrates how this approach can significantly facilitate the development of secure web applications, while maintaining high system performance and reliability.

Key words: *Digital Signature, PKI (Public Key Infrastructure), Digital Certificates, CA, Certification Authority, (RA, Registration Authority), (DB, Database), (CMS, Certificate Management System), (CRL, Certificate Revocation List), (Public and Private Keys), ECDSA, RSA, SHA-2.*

Вступ. Цифровий підпис – це електронний аналог власноручного підпису, який використовується для автентифікації та забезпечення цілісності електронних документів. Він дозволяє підтвердити, що документ не було змінено після підписання, а також, що підписант є автором цього документа.

Цифровий підпис базується на криптографії з відкритим ключем і використовує пару ключів: приватний і публічний [1-3, 7, 12, 13].

Криптографія з відкритим ключем.

PKI (Public Key Infrastructure) – це система, яка використовує криптографію з відкритим ключем для забезпечення безпеки в електронному середовищі, а також для управління та обміну електронними підписами, сертифікатами та іншими безпечними елементами. PKI дозволяє здійснювати аутентифікацію, шифрування та забезпечення цілісності даних, використовуючи пару ключів: публічний і приватний [1, 2].

Основні компоненти PKI:

1. *Сертифікати (Digital Certificates)* – це електронні документи, які містять публічний ключ і інформацію про власника цього ключа (наприклад, ім'я, організація, термін дії тощо). Сертифікати підписуються центром сертифікації (CA), що гарантує їх достовірність. Вони використовуються для підтвердження ідентичності суб'єктів і для забезпечення довіри до публічного ключа.

2. *Центр сертифікації (CA, Certification Authority)* – це організація або служба, яка видає сертифікати та перевіряє особу або організацію перед видачею сертифікату. CA підписує сертифікати, підтверджуючи їх дійсність і зв'язок з певною особою чи організацією. Прикладом CA може бути компанія, що надає послуги цифрових підписів (наприклад, VeriSign, DigiCert або Національний центр сертифікації ключів в Україні).

3. *Реєстраційний орган (RA, Registration Authority)*. RA працює в тісній взаємодії з центром сертифікації. Це орган або служба, яка відповідає за прийом запитів на сертифікати, перевірку особи та передачу запитів в CA для видачі сертифікатів. RA може здійснювати перевірку особи за допомогою документів, особистої перевірки тощо.

4. *Реєстраційна база даних (DB, Database)* – це база даних, де зберігаються сертифікати, статуси сертифікатів, ключі та інша важлива інформація для підтримки PKI-системи.

5. *Система управління сертифікатами (CMS, Certificate Management System).* CMS використовує сертифікати та допомагає у їх створенні, обміні, оновленні, відкликанні тощо.

6. *Система відкликання сертифікатів (CRL, Certificate Revocation List)* –це список сертифікатів, які були відкликані до завершення терміну їх дії. Відкликання сертифікатів може відбутися з різних причин: наприклад, якщо приватний ключ був скомпрометований, чи користувач припинив свою діяльність. CRL допомагає визначити, чи є сертифікат недійсним.

7. *Пара публічного і приватного ключів (Public and Private Keys)*. Приватний ключ використовується для підписання документів і повинен бути захищений. Лише підписант має доступ до свого приватного ключа. Публічний ключ використовується для перевірки підпису. Він може бути доступний будь-кому, хто хоче перевірити достовірність підписаного документа.

Функцій PKI для безпеки даних у цифровому середовищі [1].

1. *Аутентифікація*. Завдяки використанню сертифікатів, PKI дозволяє перевіряти, що обидві сторони (наприклад, підписувач та отримувач) є тими, за кого вони себе видають. Це важливо для онлайн-транзакцій, електронних підписів та інших операцій, що вимагають верифікації особи.

2. *Шифрування*. Для шифрування даних використовується публічний ключ: будь-хто може зашифрувати інформацію за допомогою публічного ключа, але тільки власник відповідного приватного ключа може її дешифрувати.

3. *Цілісність і підписання*. За допомогою криптографічних підписів з використанням приватного ключа можна гарантувати цілісність документа (що документ не був змінений після підписання) та підтвердження, що підпис стався від конкретної особи.

4. *Відкликання сертифікатів.* Якщо приватний ключ стає скомпрометованим або з іншої причини сертифікат більше не є дійсним, то він може бути відкликаний через CRL, що дає змогу уникнути зловживань.

Генерація ключів:

Спочатку підписант створює пару ключів: приватний ключ та публічний ключ. Приватний ключ зберігається в безпечному місці (наприклад, на токені або смарт-карті), тоді як публічний ключ може бути наданий для перевірки підписів.

Пара ключів генерується за допомогою криптографічних алгоритмів, таких як RSA або ECDSA (Elliptic Curve Digital Signature Algorithm).

Процес підписання:

1. Підписант створює хеш (унікальне цифрове представлення) документа:

– Для підписання документа спочатку обчислюється його хеш – це цифровий відбиток документа, що дозволяє зменшити його розмір. Зазвичай використовуються хеш-алгоритми, такі як SHA-256 або SHA-3.

– Хеш є унікальним для кожного документа, і будь-які зміни в документі призведуть до зміни хешу.

2. Цей хеш шифрується приватним ключем підписанта, створюючи цифровий підпис:

– Після того, як хеш обчислений, він шифрується за допомогою приватного ключа підписанта. Цей процес створює цифровий підпис, який додається до документа.

– Шифрування хешу гарантує, що підпис може бути перевірений тільки за допомогою відповідного публічного ключа.

Перевірка підписаного документу:

1. Для перевірки підпису отримувач документу використовує публічний ключ підписанта, який можна отримати через сертифікат (наприклад, X.509).

2. Спочатку обчислюється хеш документа, який перевіряється з хешем, що знаходиться в цифровому підписі.

3. Якщо хеші збігаються і підпис можна правильно розшифрувати за допомогою публічного ключа, це підтверджує автентичність підпису і те, що документ не був змінений після підписання.

Хешування має кілька важливих властивостей:

1. *Детермінованість*. Для однакових вхідних даних хеш-функція завжди генерує однакове хеш-значення.

2. *Неможливість відновлення (односторонність)*. З хеш-значення неможливо відновити оригінальні вхідні дані. Це робить хешування корисним для зберігання паролів, оскільки навіть якщо хеш буде вкрадений, не можна безпосередньо дізнатися сам пароль.

3. *Маленька зміна вхідних даних викликає великі зміни в хеші*. Якщо навіть одна літера у вхідних даних зміниться, хеш-значення зміниться кардинально.

4. *Унікальність*. Добре спроектовані хеш-функції повинні мінімізувати ймовірність того, що два різних набори даних дадуть однакові хеші. Такий випадок називається колізією.

Найпоширеніші криптографічні алгоритми [17]:

RSA (Rivest–Shamir–Adleman). Один з найпоширеніших алгоритмів для підписів і шифрування, використовується з хеш-функцією (наприклад, SHA-256) для створення цифрових підписів.

ECDSA (Elliptic Curve Digital Signature Algorithm). Використовується в рамках алгоритмів на основі еліптичних кривих. Він надає більшу безпеку при меншому розмірі ключа в порівнянні з RSA.

SHA-2 (Secure Hash Algorithm 2). Використовується для обчислення хешу документів. SHA-256 є однією з найбільш поширених функцій хешування для підписів.

Цифрові підписи використовуються в багатьох сферах:

– Юридичні документи: Контракти, угоди, та інші юридичні документи.

– Фінансові транзакції: Банківські та фінансові звіти, податкові декларації.

– Урядові послуги: Подача заявок на отримання ліцензій або взаємодія з урядовими установами.

– Медицина: Електронні медичні записи та рецепти.

– В Україні для використання цифрових підписів є державні сертифікаційні центри, які надають послуги:

– Видача сертифікатів електронного підпису.

– Перевірка дійсності підпису.

– Використання ключів для криптографічних операцій.

– Сервіси для зберігання і управління ключами.

Кваліфікований електронний підпис (КЕП) – це електронний підпис, який має юридичну силу, що прирівнюється до власноручного підпису, відповідно до законодавства. Для того, щоб підпис був кваліфікованим, він повинен відповідати певним вимогам, встановленим національними або міжнародними стандартами (зокрема, Регламентом ЄС № 910/2014, який визначає принципи використання електронних підписів в ЄС). У більшості країн, зокрема в Україні, цей підпис регулюється законодавством, яке забезпечує його юридичну значимість.

Генерація ключів в Україні:

– Для кожного користувача сертифікаційний центр генерує пару криптографічних ключів – публічний і приватний.

– Приватний ключ залишається в безпеці на сервері сертифікаційного центру або в апаратних засобах (токенах, смарт-картах).

– Публічний ключ надається у вигляді сертифіката користувача, який може бути використаний для перевірки підписів.

Використання електронного підпису на веб-сайті.

В Україні, приватний ключ недоступний для передачі на сервер – це правильна і безпечна практика. Приватний ключ не повинен залишати клієнтську сторону, де він зберігається. Це важливо для забезпечення конфіденційності та цілісності електронного підпису. В такому випадку, підписування виконується на клієнтській стороні, а сервер тільки перевіряє підпис та зберігає [14, 15].

Створення документу, який буде збережений на веб сервері разом із підписом та статусом перевірки підпису:

1. Створимо HTML-форму, шаблон документа, яку клієнт буде заповнювати. Кожне поле відповідає певному полю в базі даних для конкретного шаблону документа.

2. Після заповнення форма зберігається у базі даних. Кожен шаблон документа має свою таблицю, а кожен запис в таблиці – це дані з конкретної форми.

3. Клієнт завантажує документ із сервера. Перетворимо документ, який розташований у базі даних, у формат JSON, та повернемо клієнту.

4. Отриманий документ підписується клієнтом. Отриманий підпис клієнт завантажує назад на сервер.

5. Підпис зберігається на сервері в базі даних, і створюється зв'язок між документом і підписом.

6. Сервер перевіряє підписаний документ та встановлює мітку-результат до підпису.

Автоматизація підписання документа.

Щоб спростити алгоритм підписання документа можна використати систему вебхуків. Вебхук – спосіб інтеграції, де один сервіс або система може автоматично сповіщати іншу систему про події (наприклад, про запит на підписання документа), щоб виконати певні дії [14, 15]. Щоб реалізувати таку систему необхідно:

1. Сервер, який містить документ, генерує JSON файл та надсилає запит на сторонній сервіс (наприклад, сервіс для електронного підпису або іншу зовнішню систему), щоб підписати цей документ. В запиті є реквізити отримувача та реквізити сервера, якому необхідно повернути підпис.

2. Клієнт, користуючись стороннім сервісом, підписує документ. Сервіс повертає підпис назад на сервер, який вказаний у реквізитах.

3. Отримавши сповіщення, сервер збереже підпис у базі даних та виконає перевірку підписаного документа.

Висновки. У результаті дослідження використання криптографії як сервісу у веб-програмуванні можна зробити висновок, що цей підхід є перспективним інструментом для забезпечення високого рівня безпеки веб-додатків. Завдяки PKI розробники можуть інтегрувати складні криптографічні алгоритми без необхідності глибоких знань у цій галузі, що дозволяє зменшити час на розробку та підвищити надійність систем. Використання хмарних криптографічних сервісів дозволяє оптимізувати процеси обробки даних, зменшити навантаження на сервери та забезпечити більшу гнучкість у масштабуванні веб-додатків. Проте важливо враховувати можливі ризики, такі як безпека зберігання ключів та залежність від постачальника PKI. Для максимізації ефективності необхідно ретельно обирати постачальників послуг, враховуючи їх репутацію, рівень захисту даних і відповідність стандартам безпеки.

Список використаних джерел:

1. "Secure Electronic Signature Regulations SOR/2005-30". Justice Laws Website. 10 March 2011. Archived from the original on 28 February 2020. Retrieved 19 May 2020.

2. "US ESIGN Act of 2000" (PDF). Archived (PDF) from the original on 2011-05-22. Retrieved 2006-05-10.

3. Bellare, Mihir; Goldwasser, Shafi (July 2008). "Chapter 10: Digital signatures". Lecture Notes on Cryptography (PDF). p. 168. Archived (PDF) from the original on 2022-04-20. Retrieved 2023-06-11.

4. Ellis, James H. (January 1970). "The Possibility of Secure Non-Secret Digital Encryption" (PDF). Archived from the original (PDF) on 2014-10-
5. Hash_RC6 – Variable length Hash algorithm using RC6 https://ieeexplore.ieee.org/document/7164747 https://wiki.court.gov.ua/w/Що_таке_КЕП_та_ЕЦП%3F
6. JSON – Introduction https://www.w3schools.com/js/js_json_intro.asp
7. Katz Jonathan, Lindell Yehuda. "Chapter 12: Digital Signature Schemes". Introduction to Modern Cryptography. 2007. p. 399.
8. RSA Security's Official Guide to Cryptography by Steve Burnett, Stephen Paine, ISBN-13:978-0072131390, April 19, 2001.
9. Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar, ISBN-13: 978-3642041006, November 27, 2009.
10. Webhooks https://developer.atlassian.com/server/jira/platform/webhooks/.
11. What is PKI? https://www.digicert.com/what-is-pki.
12. Winn, Jane K. Wright, Benjamin "Digital Signatures: A Survey of Law and Practice in Global Perspective". Journal of Information Technology Law, 2021. Volume 25, Issue 3, pp. 45–60.
13. Головій Л. В., Янчук Ю. В. Правове регулювання інформаційних відносин у сфері електронної комерції. *Право. Людина. Довкілля*. 2020 Том 11, №2. С. 150–157.
14. ЗАКОН УКРАЇНИ Про електронну ідентифікацію та електронні довірчі послуги https://zakon.rada.gov.ua/laws/show/2155-19#Text.
15. Роз'яснення законодавства у сфері ЕДП https://czo.gov.ua/edp-legislation-clarification.
16. Що таке КЕП та ЕЦП?. 17Якими бувають електронні підписи? https://ca.diia.gov.ua/faq17

УДК 004.8:004.42
DOI https://doi.org/10.32689/maup.it.2024.4.7

Олександр ГОРДІЄНКО
кандидат технічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»,
oleksandr.m.hordiienko@gmail.com
***ORCID:** 0009-0002-7764-8668*

Аліна КОВАЛЬ
викладач кафедри комп'ютерних інформаційних систем та технологій,
Інститут комп'ютерно-інформаційних технологій та дизайну
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», cora9393@gmail.com
***ORCID:** 0009-0001-7379-5065*

МАЙБУТНЄ ПРОГРАМУВАННЯ: ЯК ШТУЧНИЙ ІНТЕЛЕКТ ЗМІНЮЄ РОЗРОБКУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Анотація. Мета роботи. *Дослідити вплив штучного інтелекту (ШІ) на процеси розробки програмного забезпечення, виявити основні напрямки змін, які спричиняє інтеграція ШІ у програмування, а також оцінити перспективи використання ШІ для оптимізації та автоматизації розробницьких процесів.*

Методологія. *Програмування вже давно стало основою сучасного світу, визначаючи розвиток технологій, бізнесу та суспільства. Однак із появою штучного інтелекту (ШІ) ця галузь переживає революційні зміни. ШІ не лише полегшує роботу розробників, автоматизуючи рутинні задачі, але й відкриває нові горизонти для творчості та інновацій. Від генерації коду до прогнозування поведінки систем, інструменти на основі ШІ змінюють саму суть програмування. Завдяки таким технологіям, як GitHub Copilot, TabNine чи ChatGPT, розробники отримали можливість працювати швидше, якісніше та ефективніше. ШІ вже зараз допомагає виявляти помилки, покращувати код і навіть створювати нові програмні рішення. Але як ці зміни вплинуть на майбутнє професії? Чи залишиться місце для людської творчості? І які виклики стоять перед програмістами в умовах стрімкого розвитку ШІ?*

Наукова новизна. *Вперше систематизовано основні підходи до застосування ШІ у розробці програмного забезпечення, такі як автоматизація кодування, виявлення помилок, оптимізація продуктивності програм та створення моделей генеративного дизайну. Представлено аналіз впливу генеративних мовних моделей (GPT, Codex тощо) на спрощення розробки та зміну ролі програмістів. Запропоновано новий погляд на майбутню співпрацю між розробниками і ШІ як «інтерактивну симбіотичну систему», де обидва учасники доповнюють сильні сторони один одного.*

Висновок. *Штучний інтелект уже змінює парадигму програмування, скорочуючи час на розробку, зменшуючи кількість помилок та підвищуючи продуктивність команд. У майбутньому роль розробників трансформується з написання коду на більш стратегічну та аналітичну діяльність, спрямовану на розв'язання складних задач, що потребують творчого підходу та критичного мислення. Програмування стає більш доступним для широкого кола людей, відкриваючи нові можливості для інновацій у різних галузях.*

Ця стаття досліджує, як штучний інтелект трансформує процес розробки програмного забезпечення, які переваги він пропонує, і з якими ризиками доведеться стикнутися в майбутньому.

Ключові слова: *штучний інтелект, обробка природної мови, машинне навчання, розробка програмного забезпечення, автоматична генерація коду.*

Oleksandr HORDIIENKO, Alina KOVAL. THE FUTURE OF PROGRAMMING: HOW ARTIFICIAL INTELLIGENCE IS TRANSFORMING SOFTWARE DEVELOPMENT

Abstract. Purpose of the work: *To investigate the impact of artificial intelligence (AI) on software development processes, to identify the main areas of change caused by the integration of AI into programming, and to assess the prospects for using AI to optimize and automate development processes.*

Methodology. *Programming has long been a cornerstone of the modern world, shaping the development of technology, business, and society. However, with the advent of artificial intelligence (AI), this industry is undergoing revolutionary changes. AI not only makes developers' work easier by automating routine tasks, but also opens up new horizons for creativity and innovation. From code generation to predicting system behavior, AI-based tools are changing the very essence of programming.*

Thanks to technologies such as GitHub Copilot, TabNine, and ChatGPT, developers have the opportunity to work faster, better, and more efficiently. AI is already helping to detect errors, improve code, and even create new software solutions. But how will these changes affect the future of the profession? Will there be room for human creativity? And what challenges do programmers face in the face of the rapid development of AI?

This article explores how artificial intelligence is transforming the software development process, what benefits it offers, and what risks it will face in the future.

Scientific novelty*. For the first time, the main approaches to the application of AI in software development, such as coding automation, error detection, program performance optimization and the creation of generative design models, are systematized. An analysis of the impact of generative language models (GPT, Codex, etc.) on simplifying development and changing the role of programmers is presented. A new view of the future cooperation between developers and AI is proposed as an «interactive symbiotic system», where both participants complement each other's strengths.*

Conclusion. *Artificial intelligence is already changing the programming paradigm, reducing development time, reducing the number of errors and increasing team productivity. In the future, the role of developers will transform from writing code to a more strategic and analytical activity aimed at solving complex problems that require a creative approach and critical thinking. Programming is becoming more accessible to a wide range of people, opening up new opportunities for innovation in various industries.*

This article explores how artificial intelligence is transforming the software development process, what benefits it offers, and what risks it will face in the future.

Key words: *artificial intelligence, natural language processing, machine learning, software development, automatic code generation.*

Вступ. Один із найважливіших аспектів впливу ШІ – можливість автоматичної генерації коду. Завдяки алгоритмам обробки природної мови (NLP), розробники можуть описувати бажаний функціонал у текстовій формі, а ШІ-системи генерують код на основі цих описів [5]. Це відкриває двері до більш інклюзивного програмування, де навіть користувачі без глибоких технічних знань можуть створювати прості додатки.

Генерація коду – це процес автоматичного створення програмного коду на основі заданих умов, специфікацій або вхідних даних [1]. Це може включати генерацію простих скриптів, функцій, класів або навіть складних програм, що виконують певні завдання.

Зазвичай, процес генерації коду включає кілька етапів:

1. *Визначення вимог.* Перед початком генерації коду необхідно чітко визначити, які функції, логіка або алгоритми мають бути реалізовані. Це можуть бути, наприклад, специфікації для роботи з базою даних, веб-сервером чи обробки даних.

2. *Перетворення вимог у структуровану модель.* На цьому етапі створюється модель, яка відображає архітектуру програми чи структуру даних. Це можуть бути діаграми класів, алгоритмічні блок-схеми або UML-діаграми.

3. *Генерація коду.* Використовуються інструменти або програми для створення коду. Це може бути спеціалізоване ПЗ або скрипти, які беруть на вхід структуру або шаблон і генерують код на певній мові програмування. Наприклад, генератори коду можуть створювати API клієнтів або сервіси за заданими параметрами.

4. *Автоматичні шаблони.* Генерація може базуватися на заздалегідь заданих шаблонах, що дозволяє швидко генерувати частини коду (наприклад, шаблони для роботи з базою даних, REST API тощо).

5. *Постобробка коду*. Після генерації код може потребувати додаткової обробки або оптимізації, щоб відповідати вимогам або специфікаціям проекту. Це може включати очищення коду, рефакторинг або інтеграцію з іншими частинами програми.

6. *Тестування згенерованого коду*. Важливий етап перевірки, щоб переконатися, що згенерований код працює правильно і відповідає вимогам. Для цього можуть використовуватись автоматичні тести чи інші методи перевірки.

Важливо зазначити, що генерація коду може бути частиною більш широкого процесу автоматизації розробки програмного забезпечення, зокрема в контексті таких інструментів, як IDE (Integrated Development Environment) або CI/CD (Continuous Integration/Continuous Delivery) [8].

Виявлення та виправлення помилок. ШІ-системи також досягли успіху у виявленні помилок у коді та їх виправленні. Наприклад, інструменти на основі машинного навчання аналізують великі обсяги коду, ідентифікуючи проблеми, які можуть бути неочевидними для людини. Вони також пропонують способи оптимізації та підвищення продуктивності коду.

Виявлення та виправлення помилок у програмному забезпеченні є важливими етапами в процесі розробки програм. У контексті ШІ-систем ці процеси можуть бути значно складнішими [15], оскільки помилки можуть бути неочевидними, і їх складно передбачити за допомогою традиційних методів тестування. Однак штучний інтелект може значно покращити ці етапи [3], надаючи нові підходи до виявлення та виправлення помилок.

1. *Виявлення помилок в ШІ-системах*. Існує кілька способів виявлення помилок в програмному коді та в самих моделях ШІ:

– Традиційні методи (дебагінг) – основний інструмент дебагінгу, дозволяють розробникам відстежувати виконання коду, крок за кроком, перевіряти змінні та стани програми. Дебагінг може допомогти виявити логічні помилки або невірну взаємодію між компонентами системи.

– Юніт-тести – тести які пишуться для кожної частини коду, що дозволяє перевіряти правильність роботи маленьких модулів програми. Цей метод може бути адаптований для перевірки окремих компонентів ШІ-моделей.

2. *Методи для ШІ та машинного навчання:*

– Логічне тестування моделей – виявлення помилок в ШІ-моделях може включати перевірку на логічні або статистичні аномалії, такі як невірна категоризація, класифікація або прогноз [10].

– Перевірка якості даних – ШІ-моделі дуже залежні від даних, на яких вони тренуються. Помилки можуть бути пов'язані з відсутніми, неповними або некоректними даними [2].

– Контроль перенавчання (overfitting) – виявлення того, чи модель надто пристосована до тренувальних даних, що може призвести до поганої роботи на нових або невідомих даних [14].

– Аналіз впливу параметрів (sensitivity analysis) – це дозволяє перевірити, як зміна вхідних даних або параметрів моделі впливає на результат, допомагаючи виявити потенційні помилки [6].

3. *Інструменти на основі ШІ для виявлення помилок:*

– Автоматичне тестування на основі ШІ – використання нейронних мереж або інших методів машинного навчання для аналізу великих обсягів коду або логів та автоматичного виявлення аномалій.

– Системи на основі ШІ для статичного аналізу коду – ШІ може вивчати структуру коду, знаходити непотрібні або недоопрацьовані частини, а також пропонувати виправлення на основі патернів помилок.

4. *Виправлення помилок в ШІ-системах* [4, 11]. Виправлення помилок в ШІ-системах може вимагати спеціальних підходів через складність моделей і залежність від великої кількості параметрів та даних.

– Адаптивне навчання – якщо помилка виникає через некоректні прогнози або рішення моделі, можна використати техніки адаптивного навчання, щоб модель змогла «навчитися» на нових, коректних даних або відкоригувати свої рішення.

– Техніки перенавчання (fine-tuning) – це може допомогти усунути помилки, які виникають при перенавченні моделі або неправильній генералізації. Для цього модель може бути додатково натренована на іншому наборі даних.

– Генерація контрприкладів – один із підходів для виправлення помилок в ШІ – це створення контрприкладів, які є спеціально сконструйованими прикладами, що демонструють, як модель може помилитися. Це допомагає моделі навчитися краще справлятися з різними варіантами ситуацій.

– Регуляризація та оптимізація – помилки в моделі можуть бути пов'язані з переоснащенням або недооснащенням. Використання технік регуляризації (наприклад, L1/L2 регуляризація) дозволяє модель краще узагальнювати та уникати помилок.

- Оптимізація гіперпараметрів – пошук кращих параметрів для моделі за допомогою методів, таких як Grid Search, Random Search або баєсівська оптимізація.

5. *Автоматичне виправлення коду за допомогою ШІ.* ШІ може також допомогти в автоматичному виправленні помилок у коді. Наприклад, GitHub Copilot використовує GPT для генерування коду і виправлення помилок у програмному коді.

Використання ШІ для покращення процесів тестування та виявлення помилок. ШІ-системи можуть значно покращити процес тестування, оскільки вони можуть:

– автоматично генерувати тести для різних сценаріїв.

– визначати ненавмисні помилки на основі статистичних методів та аномалій.

– аналізувати великі набори даних, щоб знайти рідкісні або складні для виявлення помилки.

В цілому, ШІ може не тільки допомогти виявити та виправити помилки в програмному забезпеченні, а й значно покращити ефективність тестування та адаптації моделей в реальних умовах.

Як ШІ змінює підхід до розробки програмного забезпечення [7, 9, 16]

1. *Прискорення циклу розробки.* Інтеграція ШІ в процеси розробки дозволяє значно скоротити час, необхідний для створення програмного забезпечення [13]. Завдяки автоматизації та швидшій генерації коду, команди можуть зосередитися на вирішенні складних задач та впровадженні нових функцій, замість витрачання часу на рутинні завдання.

2. *Підвищення якості продукту.* Алгоритми ШІ здатні аналізувати велику кількість даних і знаходити закономірності, які складно виявити людині. Це допомагає у створенні більш стабільних і якісних продуктів, мінімізуючи ризик появи критичних помилок.

3. *Інтеграція самонавчаючих систем.* Завдяки ШІ можливим стало впровадження самонавчаючих систем у програмне забезпечення. Наприклад, програми можуть автоматично адаптуватися до потреб користувачів або змінювати свій функціонал залежно від змін у середовищі використання.

4. *Демократизація програмування.* Із розвитком ШІ програмування стає доступним для ширшої аудиторії. Люди, які не володіють глибокими технічними знаннями, тепер можуть створювати прості програми або навіть складні системи за допомогою інтуїтивно зрозумілих інструментів. Це стимулює інновації в різних сферах – від бізнесу до освіти.

Виклики та ризики використання ШІ в програмуванні.

1. *Етичні питання.* Зростання залежності від ШІ ставить нові етичні виклики. Наприклад, як забезпечити, щоб автоматично згенерований код не містив упереджень чи неетичних рішень? Крім того, автоматизація може призвести до втрати робочих місць серед програмістів початкового рівня.

2. *Надмірна залежність від технологій.* Залежність від ШІ може створити ризики, коли розробники покладаються на автоматизацію настільки, що втрачають здатність до самостійного вирішення проблем. Це може призвести до втрати критичного мислення та професійних навичок.

3. *Безпека та конфіденційність.* Алгоритми ШІ часто базуються на великих обсягах даних, що можуть включати конфіденційну інформацію. Захист цих даних є критично важливим, оскільки витоки або зловживання можуть завдати значної шкоди.

4. *Якість та контроль.* Хоча ШІ може автоматизувати велику частину процесу розробки, зберігається ризик генерації коду, який важко перевірити або оптимізувати вручну. Розробники мають бути готовими до ретельного аналізу автоматично створених рішень.

5. *Перспективи розвитку, нові інструменти та платформи.* Очікується, що у майбутньому з'являться ще більш потужні інструменти, які будуть поєднувати можливості ШІ з традиційними підходами до розробки. Вони надаватимуть більш гнучкі можливості для команд будь-якого рівня кваліфікації.

6. *Співпраця людини та ШІ.* Майбутнє програмування полягає у тісній співпраці між людиною та ШІ. Люди забезпечуватимуть творчий і стратегічний підхід, тоді як ШІ автоматизуватиме рутинні процеси та пропонуватиме оптимальні рішення.

7. *Підготовка нових поколінь розробників*. Системи освіти мають адаптуватися до змін, які вносять ШІ в програмування. Навчання повинно зосереджуватися не лише на традиційних методах кодування, але й на використанні інструментів ШІ, управлінні їхніми ризиками та створенні етичних рішень.

Висновки. Штучний інтелект уже змінює програмування, роблячи його більш доступним, ефективним і якісним. Попри численні виклики, які супроводжують ці зміни, можливості, які відкриває ШІ, значно переважають ризики. Майбутнє програмування буде визначатися синергією між людськими навичками та потужністю ШІ, що дозволить створювати інноваційні продукти, які змінюють світ.

Список використаних джерел:

1. Ahmad W., Chakraborty S., Ray B., Chang K. W. Unified Pre-training for Program Understanding and Generation. Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 2021. 2655–2668. https://doi.org/10.18653/v1/2021.naacl-main.210

2. Chen H., Li Z. "Data Quality in Machine Learning: Challenges and Methods for Error Detection." *International Journal of Data Science and Analytics*, 2020. 9(2), 121–137.

3. Chen M., Tworek J., Jun H., Yuan Q., de Oliveira Pinto H. P., Kaplan J., Schulman J. Evaluating Large Language Models Trained on Code. arXiv preprint arXiv:2107.03374. 2021.

4. Davis K., Lee R. Fine-tuning models: Techniques and challenges in AI error correction. *International Journal of AI and Software Engineering*, 2020. 12(2), 101–115.

5. Feng Y., Guo D., Tang D., Duan N., Wei Z., Zhou M., Yin J. CodeBERT: A Pre-Trained Model for Programming and Natural Languages. Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), 2020. 1536–1547. https://doi.org/10.18653/v1/2020.emnlp-main.154

6. Jiang Z., Sun D. "Sensitivity Analysis in AI Models: Evaluating the Impact of Parameter Changes." *Artificial Intelligence Review*, 2020. 53(3), 159–179.

7. Kumar R., Singh P. "Enhancing Software Quality with AI-Based Data Analytics." Software Engineering Review, 2020. 8(1), 45–59. https://doi.org/10.1109/ser.2020.015007.

8. Li C., Li H., Sun J. Deep Learning for Automatic Code Generation and Completion: A Survey. ACM Computing Surveys (CSUR), 2021. 54(6), 1–29. https://doi.org/10.1145/3469023.

9. Li Z., Chen L. "AI-Powered Tools for Code Generation and Testing Automation." *International Journal of Computer Science and Information Technology*, 2020. 12(2), 187–202. https://doi.org/10.1093/ijcsit/ijcsit.2020.012030.

10. Liu Z., Zhang C., Wang Z. "Logical Testing of Machine Learning Models: A Comprehensive Review." Journal of Machine Learning Research, 2021. 22(4), 153–172.

11. Smith J., Brown A. Adaptive learning techniques for error correction in AI systems. *Journal of Machine Learning and Artificial Intelligence*, 2020. 18(4), 234–249.

12. Tiwari S., Chaturvedi A., Mishra R. Artificial Intelligence in Software Engineering: Benefits, Challenges, and Future Prospects. *International Journal of Advanced Research in Computer Science*, 2021. 12(2), 45–51. https://doi.org/10.26483/ijarcs.v12i2.

13. Vaithilingam P., Chen J., Alvarado C. Expectations vs. Reality: How Software Developers Use Generative AI Tools for Code. Proceedings of the 2022 ACM CHI Conference on Human Factors in Computing Systems, 2022. 1–15. https://doi.org/10.1145/3491102.3517489.

14. Wang Y., Xu L. "Overfitting in Machine Learning Models: Approaches to Detection and Mitigation." *Journal of Artificial Intelligence Research*, 2022. 68(1), 45–63.

15. Zaremba W., Sutskever I. Recurrent Neural Network Models for Code Generation. Advances in Neural Information Processing Systems (NeurIPS), 2020. 201–213.

16. Zhang Y., Wang X. "Artificial Intelligence and Its Impact on Software Development." *Journal of Software Engineering and Applications*, 2020. 13(4), 233–245. https://doi.org/10.4236/jsea.2020.134014.

УДК 004.94
DOI https://doi.org/10.32689/maup.it.2024.4.8

Андрій ДУДНІК
доктор технічних наук, доцент,
професор кафедри комп'ютерних інформаційних систем і технологій,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», a.s.dudnik@gmail.com
***ORCID:** 0000-0001-5725-5942*

Олег ТИЩЕНКО
аспірант кафедри комп'ютерно-інформаційних систем і технологій,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», 0987651234um@gmail.com
***ORCID:** 0009-0001-2763-579X*

Дарина ЯРЕМЕНКО
аспірант кафедри комп'ютерно-інформаційних систем і технологій,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»
dashayaremenko17@gmail.com
***ORCID:** 0000-0002-6294-9698*

ОГЛЯД СУЧАСНИХ ТЕХНІЧНИХ ТА ПРОГРАМНИХ РІШЕННЬ ДЛЯ УПРАВЛІННЯ БПЛА

Анотація. *Швидкий розвиток безпілотних літальних апаратів (БПЛА) ставить нові виклики перед інженерами та розробниками систем управління. БПЛА знайшли широке застосування в різних сферах, включаючи сільське господарство, логістику, моніторинг навколишнього середовища, пошуково-рятувальні операції та військові потреби. Ефективність цих систем значною мірою залежить від поєднання апаратних і програмних рішень, які забезпечують точне позиціювання, автономність, стабільність польоту та безпечне виконання завдань.*

У статті зосереджено увагу на ключових технічних компонентах, таких як контролери польотів, сенсори та системи зв'язку, а також на програмних платформах, які дозволяють автоматизувати процес управління польотами. Окрім того, розглянуто інноваційні підходи до інтеграції даних із різних джерел і використання алгоритмів машинного навчання для оптимізації роботи БПЛА.

***Метою статті** є висвітлення сучасних технічних і програмних рішень, які сприяють підвищенню ефективності, надійності та автономності безпілотних літальних апаратів, а також аналіз їхнього впливу на подальший розвиток галузі.*

***Методологія**, викладена в цій статті, базується на огляді сучасних технічних та програмних рішень для управління безпілотними літальними апаратами (БПЛА), зосереджуючи увагу на апаратних платформах, сенсорах, комунікаційних системах і програмному забезпеченні. Порівняльному аналізі апаратних платформ (FPGA, ARM, Atmel, Raspberry Pi) за ключовими параметрами: продуктивність, гнучкість, енергоспоживання, складність та вартість. Оцінці програмного забезпечення, яке включає відкриті платформи (ArduPilot, PX4, LibrePilot) та високорівневі системи управління (Aerostack2, GAAS). Інтеграції сенсорних даних із застосуванням алгоритмів машинного навчання, наприклад, фільтра Калмана, для підвищення точності навігації та стабільності польотів. Моделюванні енергоспоживання БПЛА з урахуванням ваги вантажу, довжини маршруту і квадратичного зростання через аеродинамічний опір. Аналізі багатоагентних систем для координації груп дронів, включаючи моделювання траєкторій та синхронізацію руху. Графічному поданні даних, яке демонструє порівняння платформ, траєкторій руху та моделі енергоспоживання.*

***Наукова новизна.** Запропоновано підхід до інтеграції сенсорних даних із використанням алгоритмів машинного навчання, зокрема фільтра Калмана, для підвищення точності навігації та стабільності польотів у складних умовах.*

***Висновки.** Проаналізовано сучасні апаратні і програмні платформи для управління безпілотними літальними апаратами (БПЛА) з урахуванням їх продуктивності, енергоспоживання, гнучкості та складності.*

Проаналізовано багатоагентні системи та їх потенціал для синхронізації дій груп БПЛА у різних завданнях, включаючи моніторинг і пошуково-рятувальні операції. Деталізовано енергетичні моделі БПЛА, що враховують вагу вантажу, маршрут і вплив аеродинамічного опору на загальне споживання енергії, що дозволяє оптимізувати тривалі місії.

Оцінено перспективи інтеграції хмарних технологій із апаратними платформами, що спрямовані на обробку великих масивів даних у реальному часі, що покращує автономність та адаптивність систем.

Визначено переваги і недоліки сучасних високорівневих систем управління, таких як Aerostack2, GAAS, і їх придатності для розробки інноваційних рішень у сфері управління БПЛА.

***Ключові слова:** безпілотні літальні апарати (БПЛА), технічні засоби, програмні платформи, контролери польоту, автопілот, системи стабілізації, сенсори, комунікаційні системи, багаторівневі системи управління, автономний політ, інтеграція даних, багатоагентність.*

Andrii DUDNIK, Oleh TYSHCHENKO, Daryna YAREMENKO. OVERVIEW OF MODERN TECHNICAL AND SOFTWARE SOLUTIONS FOR UAV CONTROL

Abstract. *The rapid development of unmanned aerial vehicles (UAVs) poses new challenges for engineers and developers of control systems. UAVs have found wide application in various fields, including agriculture, logistics, environmental monitoring, search and rescue operations and military needs. The effectiveness of these systems largely depends on a combination of hardware and software solutions that ensure accurate positioning, autonomy, flight stability and safe task performance.*

The article focuses on key technical components, such as flight controllers, sensors and communication systems, as well as on software platforms that allow for the automation of the flight control process. In addition, innovative approaches to integrating data from various sources and using machine learning algorithms to optimize UAV operation are considered.

The aim *of the article is to highlight modern technical and software solutions that contribute to increasing the efficiency, reliability and autonomy of unmanned aerial vehicles, as well as to analyze their impact on the further development of the industry.*

The methodology *presented in this article is based on a review of current technical and software solutions for controlling unmanned aerial vehicles (UAVs), focusing on hardware platforms, sensors, communication systems and software. Comparative analysis of hardware platforms (FPGA, ARM, Atmel, Raspberry Pi) on key parameters: performance, flexibility, power consumption, complexity and cost. Evaluation of software, which includes open platforms (ArduPilot, PX4, LibrePilot) and high-level control systems (Aerostack2, GAAS). Integration of sensor data using machine learning algorithms, such as the Kalman filter, to improve navigation accuracy and flight stability. Modeling of UAV energy consumption taking into account cargo weight, route length and quadratic growth due to aerodynamic drag. Analysis of multi-agent systems for coordinating drone groups, including trajectory modeling and motion synchronization. A graphical representation of data that demonstrates a comparison of platforms, trajectories, and energy consumption models.*

Scientific novelty. *An approach to integrating sensor data using machine learning algorithms, in particular the Kalman filter, is proposed to improve navigation accuracy and flight stability in difficult conditions.*

Conclusions. *Modern hardware and software platforms for controlling unmanned aerial vehicles (UAVs) are analyzed, taking into account their performance, energy consumption, flexibility, and complexity.*

Multi-agent systems and their potential for synchronizing the actions of UAV groups in various tasks, including monitoring and search and rescue operations, are analyzed. UAV energy models are detailed, taking into account the weight of the cargo, the route, and the impact of aerodynamic drag on the total energy consumption, which allows optimizing long missions.

The prospects for integrating cloud technologies with hardware platforms aimed at processing large data sets in real time, which improves the autonomy and adaptability of systems, are assessed.

The advantages and disadvantages of modern high-level control systems, such as Aerostack2, GAAS, and their suitability for developing innovative solutions in the field of UAV control are identified.

Key words: *unmanned aerial vehicles (UAVs), hardware, software platforms, flight controllers, autopilot, stabilization systems, sensors, communication systems, multi-level control systems, autonomous flight, data integration, multi-agency.*

Вступ. Постановка проблеми. Сучасний розвиток безпілотних літальних апаратів обумовлює необхідність впровадження ефективних систем керування, які забезпечують автономність, точність і надійність виконання завдань у різних умовах експлуатації. Різноманітність сфер застосування БПЛА, таких як аерофотозйомка, моніторинг, агрономія та пошуково-рятувальні операції, вимагає адаптації технічних і програмних засобів до специфічних завдань. Основними викликами залишаються відсутність універсальних рішень, що поєднують апаратні та програмні компоненти для задоволення потреб різних галузей, високі вимоги до точності навігації та стабільності польотів, а також недостатня уніфікація програмних платформ, яка ускладнює їх сумісність із різними контролерами польоту. Крім того, недостатня кількість досліджень щодо енергоспоживання та оптимізації програмно-апаратних платформ, а також потреба в інтеграції сучасних технологій, таких як штучний інтелект, комп'ютерний зір і хмарні обчислення, є суттєвими перешкодами для подальшого розвитку цієї галузі. Усе це створює актуальну потребу у вдосконаленні існуючих систем керування БПЛА, що дозволить не лише подолати зазначені виклики, але й забезпечити ефективність та функціональність цих систем у різних секторах економіки.

Аналіз останніх досліджень і публікацій. Останні дослідження в галузі керування безпілотними літальними апаратами (БПЛА) зосереджені на розробці та вдосконаленні технічних і програмних засобів, що забезпечують ефективне та автономне функціонування цих систем. Зокрема, значна увага приділяється створенню універсальних рішень, які поєднують апаратні та програмні компоненти для задоволення потреб різних галузей. У статті [5] проаналізовано існуючі методи керування БПЛА, включаючи пілотажні, навігаційні та автоматичні підходи. Автори підкреслюють важливість стандартизації методів контролю для наземних комплексів та літальних апаратів, що сприяє підвищенню надійності та безпеки експлуатації БПЛА. Дослідження [10] акцентує увагу на необхідності впровадження нових методів автономної навігації та утворення групових мереж для БПЛА. Автори зазначають, що збільшення кількості літальних апаратів вимагає пошуку ефективних рішень для забезпечення координації та безпеки польотів.

Виклад основного матеріалу. Система керування безпілотними літальними апаратами (БПЛА) складається з апаратних і програмних компонентів, які забезпечують навігацію, стабільність польоту, обробку даних та виконання конкретних завдань. Основними елементами є контролери польоту,

сенсори, комунікаційні системи, а також програмне забезпечення, яке дозволяє інтегрувати ці компоненти в єдину функціональну систему.

Контролери польоту виконують ключову роль у забезпеченні стабільності та навігації БПЛА. Для їх побудови використовуються мікроконтролери на базі архітектур FPGA, ARM, Atmel і Raspberry Pi [4]. Наприклад, контролер Pixhawk підтримує багатоплатформенність і використовується для різноманітних завдань, від аерофотозйомки до сільського господарства. Navio2, створений на основі Raspberry Pi, інтегрує вбудований GPS і сенсори, що забезпечують високу точність позиціювання [6].

Для оцінки платформ використовувалися параметри: продуктивність, гнучкість, енергоспоживання, складність. Кожен параметр нормалізується за шкалою 0–10.

Модель оцінки:

$$S=\{P,F,E,C\}$$

де P – продуктивність, F – гнучкість, E=10 – енергоспоживання, C=10 – складність.

Таблиця1

Порівняльна характеристика технічних платформ для керування БПЛА

Платформа	Продуктивність	Гнучкість	Енергоспоживання	Вартість	Складність
FPGA	Висока	Дуже висока	Низька	Висока	Висока
ARM	Середня	Висока	Низька	Середня	Низька
Atmel	Низька	Середня	Дуже низька	Низька	Низька
Raspberry Pi	Висока	Висока	Висока	Середня	Середня

Графік, що порівнює технічні платформи (FPGA, ARM, Atmel, Raspberry Pi) за чотирма основними параметрами: продуктивність, гнучкість, енергоспоживання (у вигляді енергоефективності) та складність використання (легкість), представлено на рис. 1.

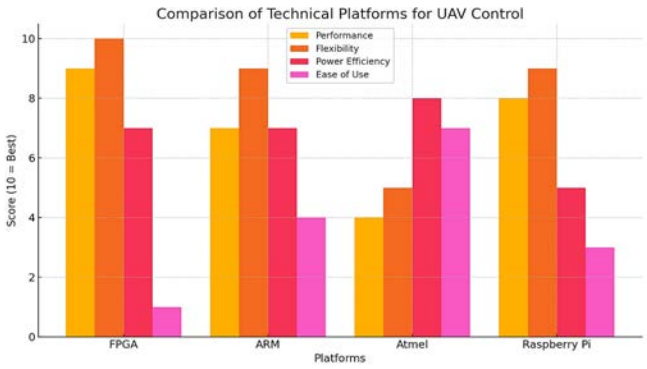


Рис. 1. Порівняльна характеристика технічних платформ для керування БПЛА

Сенсори є невід'ємною частиною системи керування БПЛА. Вони забезпечують збір даних про навколишнє середовище та дозволяють апарату адаптуватися до умов польоту. До найпоширеніших сенсорів належать інерційні вимірювальні блоки (IMU), барометри та GPS-модулі. Комбінація цих сенсорів дозволяє забезпечити точність навігації навіть у складних умовах.

Комунікаційні системи забезпечують зв'язок між БПЛА та наземними станціями управління або іншими безпілотними апаратами. Наприклад, протокол MAVLink, який підтримується програмними платформами ArduPilot та QGroundControl, забезпечує передачу телеметрії та команд управління в реальному часі [1].

Програмне забезпечення є ключовим елементом для інтеграції та управління всіма компонентами системи. Сучасні платформи, такі як ArduPilot, LibrePilot, Multiwii, забезпечують як базове управління польотом, так і можливість реалізації автономних місій [7]. Високорівневі системи, такі як Aerostack2 та GAAS, дозволяють розробникам створювати власні додатки та інтегрувати додаткові функції, наприклад, машинний зір або групове управління апаратами.

Відкриті програмні платформи. ArduPilot – одна з найбільш популярних платформ з відкритим кодом, яка підтримує мультикоптери, літаки з фіксованим крилом, наземні та навіть підводні апарати.

ArduPilot пропонує широку функціональність для автономного управління, включаючи побудову маршрутів, уникнення перешкод та взаємодію з іншими апаратами. Переваги: гнучкість, велика спільнота розробників, підтримка різних типів апаратів. Недоліки: висока вимога до обчислювальних ресурсів.

Платформа PX4 створена для високопродуктивних систем і забезпечує підтримку великих обсягів даних з сенсорів. PX4 інтегрується з протоколами MAVLink та підтримує платформи Pixhawk і Raspberry Pi [2]. Переваги**:** стабільність, гнучкість у налаштуванні, сумісність з сучасними апаратними платформами. Недоліки: складність конфігурації для новачків.

Платформа LibrePilot розроблена для стабілізації та керування польотами. Вона має простий інтерфейс і орієнтована на користувачів із базовими знаннями. Переваги: простота у використанні, ідеальна для початківців. Недоліки: обмежена функціональність порівняно з іншими платформами.

Спільнота Dronecode створює відкриті програмні рішення для БПЛА, включаючи інтеграцію з хмарними платформами, що дозволяє керувати великими обсягами даних у реальному часі. Переваги: підтримка інновацій, адаптація до нових умов, багатоплатформенність. Недоліки: залежність від якості хмарного зв'язку.

Високорівневі системи управління. Aerostack2 – система з модульною архітектурою, яка підтримує багатоагентність, планування польотів і інтеграцію з ROS2 [8]. Вона забезпечує високий рівень автономності та адаптації для виконання складних завдань. Переваги: модульність, підтримка групового управління, відкритий код. Недоліки: потреба у значних обчислювальних ресурсах.

GAAS спрямована на створення повністю автономних систем, які інтегрують лідар, HD-карти та траєкторне планування для складних польотів. Переваги: висока автономність, інтеграція сучасних технологій. Недоліки: складність реалізації у практичних умовах.

Agilicious – платформа, яка підтримує керування на основі моделей і нейронних мереж, що забезпечує маневреність і швидкість реагування. Переваги: гнучкість, використання штучного інтелекту. Недоліки: висока складність налаштування, потреба у спеціалізованому обладнанні.

Апаратні платформи також активно інтегруються з хмарними технологіями для обробки великих обсягів даних. Наприклад, платформи AuterionOS та Dronecode Community забезпечують синхронізацію з хмарними обчисленнями для аналізу даних у реальному часі, що дозволяє підвищити автономність і ефективність БПЛА [9].

Приклади використання систем

1. Аерофотозйомка та геодезія: використання GPS та фотограмметричних сенсорів для створення високоточної карти місцевості.

2. Сільське господарство: мультиспектральні сенсори для аналізу стану рослинності та прогнозування врожайності.

3. Пошуково-рятувальні операції: тепловізори та лідари для виявлення об'єктів у складних умовах, наприклад, уночі або у лісистій місцевості.

Інтеграція сенсорних даних та застосування машинного навчання для оптимізації роботи БПЛА. Управління БПЛА вимагає обробки великого обсягу інформації, яка надходить від численних сенсорів, таких як інерційні вимірювальні блоки, барометри, GPS, GNSS, лідари та камери. Поєднання цих даних за допомогою сучасних алгоритмів, зокрема фільтра Калмана, дозволяє зменшити похибки і забезпечити високу точність навігації навіть у складних умовах, наприклад, у міських середовищах або за обмеженого сигналу GPS.

Фільтр Калмана є потужним інструментом для оптимізації навігаційних систем, що є ключовою частиною систем управління безпілотними літальними апаратами (БПЛА). У контексті статті, його роль зосереджена на забезпеченні точності та надійності навігації, зменшенні похибок у вимірюваннях і підвищенні стабільності польоту.

Фільтр Калмана забезпечує оптимізацію прогнозування траєкторії на основі вимірювань з шумом.

Математична модель:

1. Передбачення:

$$x_{k|k-1} = x_{k-1|k-1}, P_{k|k-1} = P_{k-1|k-1} + Q$$

2. Оновлення:

$$k_k = \frac{P_{k|k-1}}{P_{k|k-1} + R}, x_{k|k} = x_{k|k-1} + K_k(z_k - x_{k|k-1}),$$

$$P_{k|k} = (1 - K_k)P_{k|k-1},$$

де $x_{k|k}$ – оцінка, $P_{k|k}$ – похибка, Q – шум процесу, R – шум вимірювання, z_k – вимірювання.

На графіку (Рис. 2) представлено модель прогнозування траєкторії руху БПЛА за допомогою фільтра Калмана.

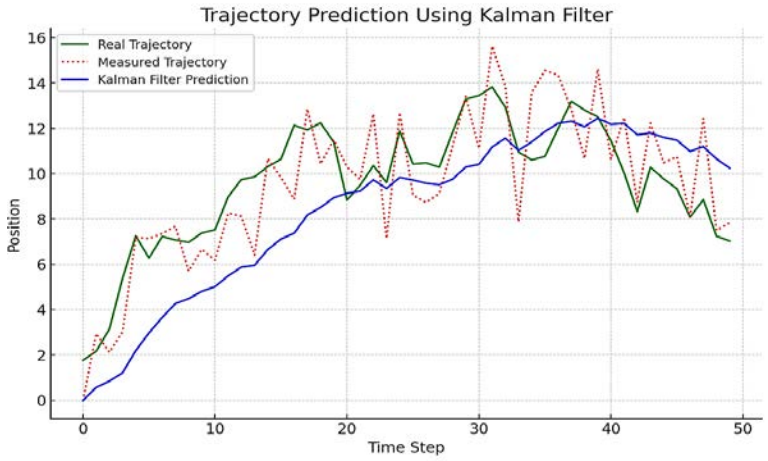


Рис. 2. Модель прогнозування траєкторії руху БПЛА за допомогою фільтра Калмана

На графіку представлено модель прогнозування траєкторії руху БПЛА за допомогою фільтра Калмана.

– Зелена лінія: реальна траєкторія.
– Червона пунктирна лінія: виміряна траєкторія з шумом.
– Синя лінія: траєкторія, спрогнозована фільтром Калмана.

Алгоритми машинного навчання відіграють ключову роль в оптимізації роботи БПЛА. Вони забезпечують розпізнавання об'єктів і місцевості, прогнозування траєкторій руху, адаптивне управління та оптимізацію енергоспоживання. Енергоспоживання залежить від ваги вантажу w, відстані маршруту d та квадратичного приросту через аеродинамічний опір.

Модель:

$$E(d,w) = E_0 + \alpha w d + \beta d^2$$

де E_0 – базове енергоспоживання, α – коефіцієнт залежності від ваги, β – коефіцієнт квадратичного приросту.

На графіку (Рис. 3) показано залежність енергоспоживання БПЛА від довжини маршруту для різних ваг вантажу (0.5 кг, 1 кг, 1.5 кг).

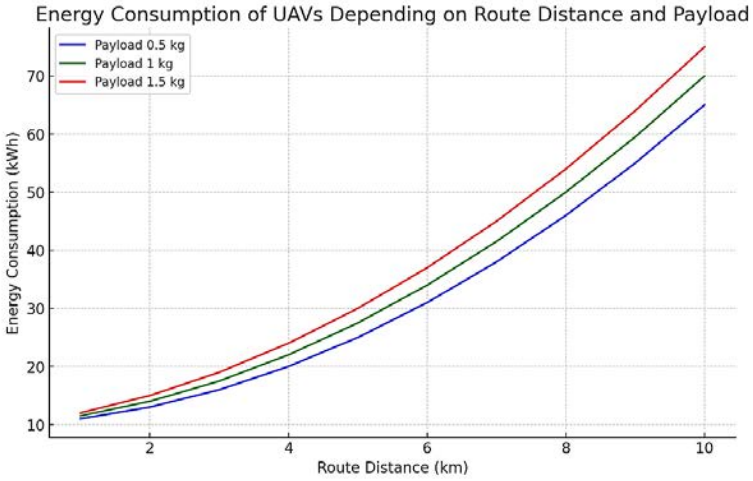


Рис. 3. Моделювання енергоспоживання

Модель враховує базове енергоспоживання, збільшення через вагу вантажу і квадратичний ріст, пов'язаний з довжиною маршруту. Це ілюструє, як підвищення ваги і тривалості польоту впливають на витрати енергії.

Завдяки машинному навчанню апарати можуть аналізувати великі масиви даних, ухвалювати оптимальні рішення в реальному часі та автоматично адаптувати свої дії до змінних умов, таких як погода чи наявність перешкод. Комп'ютерний зір, що базується на глибокому навчанні, дозволяє БПЛА

ідентифікувати об'єкти або цілі під час місій, наприклад, у пошуково-рятувальних операціях або сільському господарстві. В агрономії такі системи застосовуються для аналізу зображень рослинності, що допомагає виявляти ділянки, які потребують додаткового зрошення або обробки.

Інноваційним рішенням є багатоагентні системи, які використовують алгоритми координації для забезпечення ефективної роботи групи БПЛА. Однак впровадження таких технологій супроводжується низкою викликів, зокрема потребою у великій кількості даних для навчання моделей, високих обчислювальних потужностях і забезпеченні обробки інформації в реальному часі. Проте сучасні апаратні платформи, такі як NVIDIA Jetson або Raspberry Pi із підтримкою GPU, вже сьогодні роблять реалізацію цих рішень більш доступною.

Використання алгоритмів машинного навчання та інтеграція даних із сенсорів дають змогу досягти високого рівня автономності БПЛА у виконанні складних завдань. Наприклад, системи комп'ютерного зору на основі глибоких нейронних мереж забезпечують ефективне розпізнавання об'єктів у реальному часі. У пошуково-рятувальних операціях це дозволяє ідентифікувати людей або транспортні засоби у важкодоступних місцях, наприклад, у лісистій місцевості чи під завалами. В агрономії такі системи використовуються для аналізу стану рослинності, що дозволяє визначати ділянки з дефіцитом вологи або ураженням хворобами, оптимізуючи внесення добрив або пестицидів.

Сенсорні системи, які комбінують дані з IMU, GPS і лідарів, забезпечують точне позиціювання навіть у складних умовах. Наприклад, у міських середовищах із перешкодами для GPS-сигналу об'єднання даних із цих джерел дозволяє уникнути втрати координат і забезпечити стабільність польоту. У транспортній логістиці це дає змогу БПЛА ефективно виконувати доставку вантажів у щільно забудованих зонах [3].

Машинне навчання також активно використовується для прогнозування траєкторій руху об'єктів. У контексті управління дорожнім рухом БПЛА можуть використовувати нейронні мережі для аналізу поведінки транспортних засобів та прогнозування їхнього місця розташування в майбутні моменти часу. Це дозволяє уникати зіткнень і ефективно планувати маршрути для безпілотників, які виконують моніторинг або доставку.

Багатоагентні системи, побудовані на основі алгоритмів координації, є іншим прикладом конкретного застосування. Наприклад, у лісовому господарстві група БПЛА може проводити одночасний моніторинг великих територій, виявляючи осередки пожеж чи незаконну вирубку лісу. У таких системах алгоритми дозволяють синхронізувати рух дронів, забезпечуючи максимальне покриття території без перетинів чи прогалин.

На графіку (Рис. 4) представлено траєкторії п'яти дронів у багатоагентній системі управління на 2D площині.

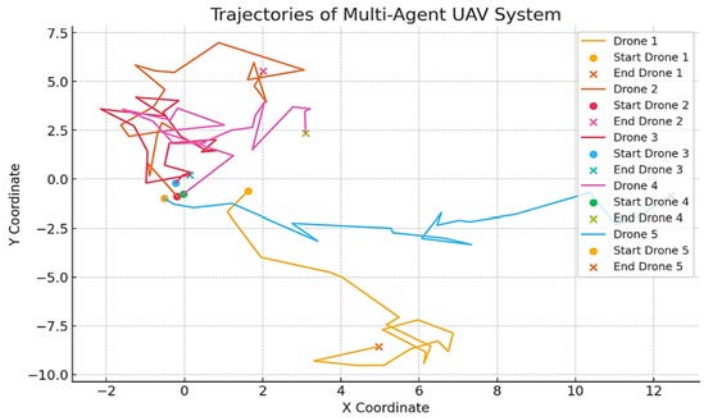


Рис. 4. Моделювання траєкторії польоту дронів

– Лінії: шляхи руху кожного дрона.
– Кружки: стартові точки дронів.
– Хрестики: кінцеві точки дронів.

Для траєкторій дронів використовувалися випадкові прогулянки:

$$T_i(t) = T_i(t-1) = +\Delta x, \Delta x \sim N(0, \sigma^2),$$

де $T_i(t)$ – координати i-го дрона в момент часу t, Δx – зміна координат, яка моделюється нормальним розподілом, σ^2 – дисперсія, яка визначає варіацію або розкид значень.

У контексті оптимізації енергоспоживання алгоритми машинного навчання аналізують поточний стан батареї, характеристики маршруту та умови польоту. Це дозволяє вибирати найбільш енергоефективні траєкторії, що є критично важливим для тривалих місій, наприклад, у пошуково-рятувальних операціях чи моніторингу екологічного стану.

Висновки. Отже, у ході дослідження було розглянуто основні логічні та конструктивні блоки для створення систем керування БПЛА, включаючи компоненти автопілота, апаратні платформи різних архітектур та програмні рішення. Було проведено аналіз 16 апаратних і програмних платформ, які мають потенціал для використання як у практичних завданнях, так і в академічних дослідженнях. Здійснено детальне порівняння функціональних можливостей платформ, їхньої сумісності, гнучкості та відповідності до сучасних вимог галузі. Також виконано огляд дев'яти високорівневих систем управління, що дозволило виявити їхні переваги, недоліки та основні характеристики.

Особливу увагу приділено питанням інтеграції даних із різних сенсорів, використанню алгоритмів машинного навчання для оптимізації роботи БПЛА, а також перспективам впровадження інноваційних рішень, таких як багатоагентні системи та технології комп'ютерного зору. Разом із тим, виявлено низку проблем, зокрема, недостатню кількість доступної документації щодо енергоспоживання платформ та обмеженість інформації про взаємодію програмно-апаратних рішень у реальних умовах.

Подальші дослідження доцільно зосередити на детальному аналізі новітніх програмних і апаратних платформ, оцінці їхнього енергоспоживання, а також дослідженні економічної ефективності комбінованих рішень, що сприятиме розширенню можливостей використання БПЛА у різних сферах та підвищенню їхньої автономності, функціональності й ефективності.

Список використаних джерел:

1. Chengqi X., Cen Q., Yan Z. Design and research of human-computer interaction interface in autopilot system of aircrafts. 2009 IEEE 10th International Conference on Computer-Aided Industrial Design & Conceptual Design. 2009. С. 1498–1501. https://doi.org/10.1109/CAIDCD.2009.5374997.

2. D. Perez et al. A ground control station for a multi-UAV surveillance system: design and validation in field experiments. Journal of Intelligent & Robotic Systems. 2013. Т. 69. С. 119–130. https://doi.org/10.1007/s10846-012-9759-5.

3. Dakhno N., Barabash O., Shevchenko H., Leshchenko O., & Dudnik A. (2021, October). Integro-differential models with a K-symmetric operator for controlling unmanned aerial vehicles using a improved gradient method. In 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD) (pp. 61–65). IEEE.

4. Gabriel D. L., Meyer J., du Plessis F. Brushless DC motor characterisation and selection for a fixed wing UAV. AFRICON 2011, Victoria Falls, Livingstone, Zambia, 13–15 sept. 2011 p. 2011. https://doi.org/10.1109/afrcon.2011. 6072087.

5. Ivanenko Yuliia «Огляд методів керування безпілотними літальними апаратами» / Yuliia Ivanenko, Oleksii Liashenko, Tetiana Filimonchuk. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2023. Т. 1 (71). С. 26–30. doi:https://doi.org/10.26906/SUNZ.2023.1.026.

6. L. Meier et al. PIXHAWK: A micro aerial vehicle design for autonomous flight using onboard computer vision. Autonomous Robots. 2012. Т. 33, № 1-2. Pp. 21–39. https://doi.org/10.1007/s10514-012-9281-4.

7. L. Meier et al. PIXHAWK: A system for autonomous flight using onboard computer vision. 2011 IEEE International Conference on Robotics and Automation (ICRA), Shanghai, China, 9–13 May 2011. 2011. Pp. 2992–2997. https://doi.org/10.1109/icra.2011.5980229.

8. Sabikan S., Nawawi S. W. Open-Source Project (OSPs) Platform for Outdoor Quadcopter. Journal of Advanced Research Design. 2016. Т. 24, № 1. Groves P. D. Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition. Artech House, 2013.

9. Trush O., Kravchenko I., Trush M., Pliushch O., Dudnik A., & Shmat K. (2021, December). Model of the sensor network based on unmanned aerial vehicle. In 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT) (pp. 138–143). IEEE.

10. Микола Микийчук, Наталія Зіганшин «Аналіз методів керування безпілотними літальними апаратами». *Вісник Національного університету «Львівська політехніка». Інформаційні системи та технології*. 2019. Т. 80, № 4. URL: https://science.lpnu.ua/istcmtm/all-volumes-and-issues/volume-80-no4-2019/analysis-unmanned-aerial-vehicles-control-methods

УДК 004.05
DOI https://doi.org/10.32689/maup.it.2024.4.9

Максим ДЬЯЧЕНКО
аспірант, Державний торговельно-економічний університет, m.diachenko@knute.edu.ua
ORCID: *0009-0002-0279-2497*

Андрій РОСКЛАДКА
доктор економічних наук, професор,
завідувач кафедри цифрової економіки та системного аналізу,
Державний торговельно-економічний університет, a.roskladka@knute.edu.ua
ORCID: *0000-0002-1297-377X*

ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕС МЕНЕДЖМЕНТУ ІНЦИДЕНТІВ

Анотація. *Швидкий розвиток технологій вимагає трансформації практик управління IT послугами (ITSM). У цій статті досліджується інтеграція штучного інтелекту для IT Операцій (AIOps) та інтелектуальної автоматизації в рамках ITSM, зокрема, з акцентом на їхній вплив на управління інцидентами, операційну ефективність та загальну якість обслуговування. На основі огляду останніх літературних джерел та кейс-стаді, стаття має на меті надати інсайти щодо переваг, викликів та майбутніх напрямків цих технологій у покращенні IT операцій. Результати дослідження вказують на значний потенціал AIOps та інтелектуальної автоматизації у підвищенні ефективності управління IT послугами, проте реалізація цих технологій вимагає ретельного планування та врахування особливих аспектів. Запропонована методологія впровадження може бути широко використана організаціями для подальшого розвитку напрямку AIOps.*

Метою дослідження *є створення методології інтеграції AI автоматизацій у технічні та бізнес процеси організації. Завдання, які необхідно виконати для цього, включають дослідження існуючих підходів у класифікації і використанні AI автоматизацій у сфері, аналіз існуючих систем і досвід їх впровадження, та опис методології впровадження AI автоматизацій.*

Методологія *включає аналіз літературних джерел та аналіз існуючих варіантів застосування автоматизацій у процесах. Засобами системного аналізу розроблено методологію впровадження таких автоматизацій у бізнес процес.*

Наукова новизна *полягає в адаптації новітніх підходів у менеджменті інцидентів до поточних процесів технологічних організацій.*

Висновки. *В цій роботі запропонована покрокова методологія впровадження в бізнес-процеси автоматизацій на базі штучного інтелекту, розгортаючи інфраструктуру AIOps. Застосовування розробленої методології і проведення подальших кейс-стаді із визначеннях можливих особливостей процесів організацій є перспективним напрямком подальших досліджень.*

Ключові слова: *AIOps, менеджмент інцидентів, штучний інтелект, ITSM, впровадження процесу.*

Maksym DIACHENKO, Andrii ROSKLADKA. IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE INTO THE INCIDENT MANAGEMENT PROCESS

Abstract. *The rapid advancement of technology necessitates the transformation of IT Service Management (ITSM) practices. This article examines the integration of Artificial Intelligence for IT Operations (AIOps) and intelligent automation within ITSM, focusing on their impact on incident management, operational efficiency, and overall service quality. Based on a review of recent literature and case studies, the article aims to provide insights into the benefits, challenges, and future directions of these technologies in improving IT operations. The findings highlight the significant potential of AIOps and intelligent automation to enhance IT service management efficiency; however, their implementation requires careful planning and consideration of specific factors. The proposed implementation methodology can be widely utilized by organizations to further advance AIOps adoption.*

The goal *of the study is to develop a methodology for integrating AI-driven automations into an organization's technical and business processes. The tasks required to achieve this include researching existing approaches to the classification and application of AI automations in the field, analyzing current systems and implementation experiences, and describing the methodology for integrating AI automations.*

The methodology *includes a review of literature and an analysis of existing use cases for automation in processes. Using system analysis tools, a methodology for integrating such automations into business processes has been developed.*

The scientific novelty *lies in the adaptation of cutting-edge approaches in incident management to the current processes of technology-driven organizations.*

Conclusions. *This study proposes a step-by-step methodology for implementing AI-based automation in business processes through the deployment of AIOps infrastructure. Applying the developed methodology and conducting further case studies to identify potential organizational process nuances represent promising directions for future research.*

Key words: *AIOps, incident management, Artificial Intelligence, ITSM, process implementation.*

Вступ. Сучасні IT-інфраструктури стають дедалі більшими та складнішими через постійний розвиток технологій та зміну робочих методів. Підтримка ефективності та надійності в таких середовищах є складним завданням. Багато організацій переходять від традиційних продуктів до надання послуг,

обираючи динамічні комбінації локальних, керованих, приватних та публічних хмарних середовищ. Через такі фактори, як мобільність пристроїв, зміни в середовищах виконання, часті оновлення, ці системи стають вразливішими до збоїв. Наприклад, згідно з даними Lin та інших, система Microsoft Azure щодня зазнає збоїв приблизно у 0,1% серверних вузлів [13]. Такі збої можуть призвести до зниження доступності систем, фінансових втрат і погіршення досвіду користувачів. Дослідження IDC показують, що простій додатків може коштувати бізнесу до $550,000 за годину [17]. Ці значні втрати стимулюють потребу в автономних системах, які здатні самостійно керувати собою та усувати основні причини збоїв для підвищення якості та швидкості IT-послуг. Традиційні рішення для управління IT, що покладаються на експертні системи та механізми на основі правил, часто виявляються недостатньо адаптивними, ефективними та масштабованими. Такі підходи можуть ігнорувати актуальний стан системи в реальному часі, що призводить до неточних прогнозів та аналітики, заснованих на поточному стані системи. Крім того, вони опираються на традиційне інженерне мислення, яке акцентує увагу на ручному виконанні повторюваних завдань та аналізі окремих випадків, зокрема відтворенні помилок або аналізі логів [22]. Ці проблеми спонукали інтерес до заміни традиційних інструментів обслуговування на інтелектуальні платформи, здатні навчатися на великих обсягах даних та проактивно реагувати на інциденти. Організації все частіше звертаються до методів штучного інтелекту для менеджменту інформаційних технологій (Artificial Intelligence for IT Operations, AIOps) для попередження та усунення інцидентів, що мають значний вплив. Термін AIOps вперше був введений у 2017 році компанією Gartner, щоб охопити виклики, пов'язані з впровадженням штучного інтелекту (Artaficial Intelligence, AI) у процеси DevOps [20]. Спочатку цей термін походив від ITOA (аналітики IT-операцій), але з поширенням штучного інтелекту у різних галузях Gartner переосмислив його як AI для операційних систем. AIOps використовує технології великих даних та машинного навчання для інтелектуального вдосконалення, зміцнення та автоматизації різних IT-операцій. AIOps навчається на різноманітних даних, зібраних від сервісів, інфраструктур та процесів, і автономно вживає заходів для виявлення, діагностики та виправлення інцидентів у реальному часі.

Матеріали та методи досліджень. Ми зосередили увагу цього дослідження на досвіді компаній, що займаються розробкою AIOps рішень. Сьогодні організації розділяються на тих, хто займається розробкою системи для внутрішнього використання, і тих, хто впроваджує готові рішення від сторонніх розробників. Для цього ми скористалися наступними методами: створення проблеми, формування гіпотези, аналіз відкритих джерел, узагальнення і систематизація результатів наукової діяльності та практичної діяльності компаній. Додатково було проаналізовано досвід впровадження організацій першопроходьців в цьому напрямку [1, 3].

Як основну проблему дослідження ми визначили *відсутність стандарту, загальноприйнятого методу інтеграції існуючих рішень у процес*. Сьогодні можна спостерігати велику кількість наукових досліджень і програмних продуктів у сфері AIOps для вирішення різноманітних проблем. Сабхарвал та інші опублікували книгу «Практичний AIOps», у якій обговорюються практичні аспекти та впровадження AIOps [16]. Доступні кілька оглядів літератури з AIOps, які допомагають аудиторії краще зрозуміти цю сферу [15, 14]. Однак, більшість оглядів, пов'язаних зі штучним інтелектом, все ще залишаються тематичними, як-от виявлення аномалій за допомогою глибинного навчання, управління відмовами та аналіз першопричин. Наразі існує обмежена кількість досліджень, які надають цілісне уявлення про процес впровадження AIOps, охоплюючи ситуацію як у науковій спільноті, так і в промисловості. Проведені в даній статті дослідження заповнюють цю прогалину та зосереджують більше уваги на самому процесі розгортання інфраструктури AIOps. В результаті необхідно дати відповідь на наступні запитання:

- Що впливає на рішення організації щодо впровадження AIOps ?
- Які планувати очікування ?
- Якими є етапи процесу імплементації ?

Аналіз предметної області. Підходи, які застосовуються AIOps на сьогоднішній день, знаходяться на стадії активного розвитку. Нижче наведено короткий огляд кожного кроку менеджменту інцидентів і можливих рішень [2]:

1. Реєстрація інциденту – початковий етап життєвого циклу будь-якого інциденту. Великі дата-центри та хмарні послуги повинні мати проактивний моніторинг систем для вирішення інцидентів до того, як їх виявлять клієнти. Однак сьогодні більшість сповіщень налаштовуються відповідно до суворих правил, заснованих на раніше виявлених помилках і порогових значеннях. Використання AI для виявлення аномалій може ідентифікувати більшу кількість інцидентів до їх виникнення і до налаштування сповіщення. AI може ідентифікувати критичні компоненти системи та пріоритизувати помилки відповідно до їхнього впливу.

Існують різні підходи в ідентифікації і навіть передбаченні появи інциденту. Підходи до передбачення інцидентів є проактивними методами, спрямованими на запобігання збоям (або відмовам у крайніх

випадках) шляхом обробки як статичних аспектів, таких як вихідний код, так і динамічних аспектів, наприклад, доступності обчислювальних ресурсів. Основна мета полягає в тому, щоб запропонувати превентивні заходи або вжити негайних дій якомога раніше. Ці стратегії значно відрізняються залежно від запропонованої таксономії (тобто даних, що використовуються, сфери застосування тощо).

1.1. Прогнозування дефектів програмного забезпечення забезпечення (Software Defect Prediction, *SDP)* – це підхід, який використовується для оцінки ймовірності виникнення програмної помилки в функціональній одиниці коду, такій як функція, клас, файл або модуль. Основне припущення, що пов'язує SDP з виникненням збоїв, полягає в тому, що код із дефектами призводить до помилок і збоїв під час виконання. Традиційно програмне забезпечення, схильне до дефектів, ідентифікується за допомогою метрик коду, які використовуються для побудови предикторів дефектів. Нагаппан та інші запропонували підхід SDP на основі метрик складності коду [11] ще в 2010 році. В іншому дослідженні 2020 року Сюй та ін. [5] запропонували підхід для характеристики програмних дефектів, використовуючи дефектні піддерева в абстрактних синтаксичних деревах (Abstract Syntax Trees, AST). Цей підхід включає інформацію про зміни, що викликають виправлення коду. Спочатку розробляється тематична модель для узагальнення функціональних концепцій, пов'язаних із дефектами. Кожен вузол у дефектних піддеревах збагачений атрибутами, такими як типи, зміни, що викликають виправлення, та концепції коду. Після цього використовується класифікатор на основі графових нейронних мереж (Graph Neural Networks, GNN), де піддерева представлені як орієнтовані ациклічні графові структури. В 2022 Уддін та ін. [10] використали модель двоспрямованої довгої короткочасної пам'яті (Bidirectional Long Short-Term Memory Network, BiLSTM) разом із підходом до семантичних ознак на основі двоспрямованих кодувальних представлень з трансформерів (Bidirectional Encoder Representations from Transformers, BERT) для прогнозування дефектів у програмному забезпеченні. Ця комбінація захоплює семантичні ознаки коду, витягуючи контекстну інформацію з векторів токенів, які були навчені моделлю BERT за допомогою BiLSTM. Також інтегровано механізм уваги, який захоплює найбільш важливі ознаки для прогнозування. Ця методологія була покращена за рахунок техніки розширення даних, яка генерує додаткові тренувальні дані. Оцінка включає експерименти як із прогнозування дефектів у межах проєкту, так і з прогнозування дефектів між проєктами.

1.2. Прогнозування відмов апаратного забезпечення. У масштабних обчислювальних інфраструктурах проблема забезпечення надійності апаратного забезпечення є ключовою для досягнення цілей доступності послуг. Однак, через велику кількість компонентів і необхідність використання загальнодоступного апаратного забезпечення в дата-центрах, відмови апаратного забезпечення створюють значні виклики. Наприклад, компанія Google повідомляє, що 20-57% дисків мають принаймні одну помилку сектора протягом 4-6 років [8]. Жорсткі диски є найбільш часто замінюваними компонентами в хмарних обчислювальних системах і є однією з основних причин збоїв серверів. Щоб вирішити цю проблему, виробники жорстких дисків впровадили технології самостійного моніторингу, такі як метрики на базі технології самоконтролю, аналізу й звітування (Self Monitoring Analysis and Reporting Technology, SMART) у своїх пристроях зберігання. У підході, запропонованому Чжао та ін., використовуються приховані марковські та напівмарковські моделі для оцінки ймовірних послідовностей подій на основі спостережень метрик SMART із набору даних приблизно 300 дисків, дві третини яких були справними [21]. У дослідженні 2020 року Халіл та ін. [9] представили підхід для прогнозування потенційних апаратних відмов, спричинених старінням або зміною стану в ланцюгах передачі сигналів. Підхід використовує швидке перетворення Фур'є (Fast Fourier Transform, FFT) для виявлення частотних сигнатур відмов, застосовує аналіз головних компонент (Principal Component Analysis, PCA) для зменшення розмірності даних і виділення важливих характеристик, а також використовує згорткову нейронну мережу (Convolutional Neural Network, CNN) для навчання та класифікації відмов. Ця робота є особливо помітною, оскільки вперше вирішує проблему прогнозування відмов на рівні транзисторів для апаратних систем, охоплюючи відмови через старіння, коротке замикання та відкриті ланцюги.

1.3. Прогнозування відмов програмного забезпечення зосереджене на виявленні можливих збоїв на різних рівнях додатків, таких як процеси, задачі, віртуальні машини (Virtual Machine, VM), контейнери або вузли. Відомі підходи переважно ґрунтуються на аналізі системних метрик, станів сервісів, трасувань, логів і топологій. Одним із прикладів є підхід, запропонований Коеном та ін. [4], який використовує Баєсові мережі для виявлення зв'язків між спостережуваними змінними та станами сервісів. Ця стратегія дозволяє передбачати та запобігати порушенням цілей обслуговування (Service Level Objective, SLO) та збоям веб-сервісів. Система відстежує ключові метрики, такі як час процесора, читання з диска, використання простору підкачки, та інші, створюючи модель, яка описує складні залежності між цими метриками. Оптимальна структура графа, яка охоплює найбільш релевантні вхідні метрики, визначається за допомогою евристичного процесу відбору.

2. *Класифікація інциденту.* Після реєстрації важливо визначити постраждалу область і призначити квиток (ticket) компетентному інженеру або команді. Багато порушень договору про рівень обслуговування (Service Level Agreement, SLA) трапляються через те, що інцидент залишається непризначеним протягом тривалого часу. Існують рішення на основі AI, які можуть поєднувати машинне навчання та правила для призначення інцидентів на основі раніше вирішених запитів, поточного завантаження і доступності. Численні підходи на основі даних були запропоновані для оптимізації процесу призначення інцидентів, який також називається маршрутизацією або триажем (triage – розподіл), автоматично призначаючи інциденти відповідній сервісній команді чи особі. Зазвичай ці підходи передбачають навчання класифікатора на основі історичних звітів про інциденти, які містять текстову інформацію, дані про топологію або пріоритетні оцінки. Навчений класифікатор використовується для призначення нових інцидентів. Попередні роботи здебільшого покладалися на методи попередньої обробки текстів та моделі класифікації в рамках традиційного машинного навчання і статистичних підходів. Нещодавно увага зосередилася на сучасних методах обробки природної мови (Natural Language Processing, NLP) у поєднанні з глибоким навчанням. Наприклад, Лі та ін. [18] використали CNN і попередньо навчені вбудовування Word2Vec для призначення інцидентів. У роботі [7] процес триажу за допомогою глибинного навчання клітинного типу (Cell-type Deep Learning, DeepCT) представлено як безперервний процес, що включає інтенсивні обговорення між інженерами, використовуючи модель керованих рекурентних блоків (Gated Recurrent Units, GRU) з масковою стратегією уваги для поетапного оновлення результатів триажу на основі знань з обговорень.

3. *Пріоритизація інциденту*. Процес пріоритезації слід виконувати на основі впливу та угоди SLA з клієнтом. Сучасні технології NLP можуть виділяти факти та виконувати аналіз настроїв для встановлення правильного пріоритету. Людське втручання та перевірка зазвичай все ще потрібні, але завдяки автоматизації цей процес можна значно мінімізувати. Хен та ін. [6] провели масштабний емпіричний аналіз інцидентів в реальних онлайн-сервісних системах. Їхні результати підкреслюють категорію інцидентів під назвою «випадкові інциденти» (Incidental Incidents), які часто вважаються менш значущими та не пріоритизуються для негайного вирішення. Для розв'язання цієї проблеми автори запропонували пріоритезацію інцидентів за допомогою глибинного навчання (DeepIP, Deep learning-based Incident Prioritization) – систему, що використовує CNN на основі механізму уваги для ідентифікації та пріоритезації випадкових інцидентів, ґрунтуючись на їх історичних описах та інформації про топологію системи.

4*. Розслідування інциденту*. Залежно від категорії інциденту та інфраструктури програми, інженер вивчає можливі журнали, конфігурації, дані тощо. Кожне джерело розслідування слід розглядати окремо, залежно від підтримуваного додатка. Об'єднання процесу розслідування в один інтерфейс на основі AI є перспективною сферою для подальших досліджень та розробок. Помічники на основі AI можуть навчатися на попередніх інцидентах і робити висновки на основі отриманих даних, однак у більшості випадків для діагностики інциденту потрібне втручання людини, оскільки критерії можуть надходити з різних джерел. На сьогоднішній день дослідження сфокусовані на аналізі окремих рівнів інфраструктури, таких як база даних, мережеве з'єднання, програний код, хмарне середовище.

5. *Вирішення інциденту* – дії, що виконуються для відновлення нормального функціонування системи, усуваючи вплив інциденту. Подібно до попередніх етапів, участь людини необхідна через складність підтримуваних систем і різноманітні нетехнічні фактори, які потрібно враховувати, такі як можливість людських помилок, поточні відносини з клієнтом, інформація з джерел, над якими відсутній процес моніторингу. У дослідженні [19] запропоновано алгоритми на основі схожості для генерації рішень повторюваних проблем на основі інцидентних запитів. Цей підхід передбачає використання методу найближчих сусідів (k-Nearest Neighbors, k-NN) для отримання варіантів вирішення інциденту. Схожість між квитками оцінюється за допомогою комбінації числових, категоріальних та текстових даних з визначеними індивідуальними та агрегованими показниками схожості. Рішення було розширене для врахування хибнопозитивних квитків як в історичних даних, так і в поточних, за допомогою класифікації квитків за допомогою бінарного класифікатора і зважування їх важливості на основі прогнозів. Фінальна рекомендація щодо вирішення квитків враховує як важливість, так і схожість. Важливим результатом є покращення методів вилучення ознак, зокрема виявлення тем та навчання метрик для підвищення ефективності рекомендацій.

6. *Визначення та виконання запобіжних дій*. Для ефективного функціонування системи для кожного інциденту повинні бути визначені та виконані запобіжні дії. Для цього головна причина повинна бути чіткою і точною. Через складність і різноманітність джерел і факторів це наразі завдання, що вимагає когнітивних навичок людини, тому це перспективна область для подальших досліджень рішень на основі AI. У нещодавньому дослідженні був представлений підхід eWarn [12], який спрямований на онлайн-сервісні системи, що використовує історичні дані та інформацію про реальні тривожні сигнали для прогнозування ймовірності майбутніх інцидентів. Він поєднує такі інноваційні техніки:

– ефективна інженерія ознак для представлення відповідних шаблонів тривог;

– інтеграція багатоприкладного навчання (multi-instance learning), щоб мінімізувати вплив несуттєвих тривог;

– генерація зрозумілих звітів за допомогою техніки пояснень (Local Interpretable Model-Agnostic Explanations, LIME).

Цей підхід дозволяє не тільки передбачати інциденти, але й надавати пояснення для прийняття більш обґрунтованих рішень щодо інцидент-менеджменту. Таким чином, подібні методи дозволяють не лише передбачати можливі відмови систем, але й допомагати з аналізом причин і пропонувати превентивні заходи для їх уникнення.

Розробка методології імплементації методів AIOps.

В цьому дослідженні ми визначили, які інструменти існують вже сьогодні для реалізації автоматизацій етапів процесу вирішення інцидентів. Однак, питання їх впровадження в бізнес процес залишається відкритим. У науковій літературі описані різні підходи у використанні тих чи інших алгоритмів нейронних мереж, проте відсутня загальна схема впровадження технології відповідно до потреб організації.

Враховуючи ромаїття підходів, ми пропонуємо наступну схему впровадження AIOps (рис. 1):

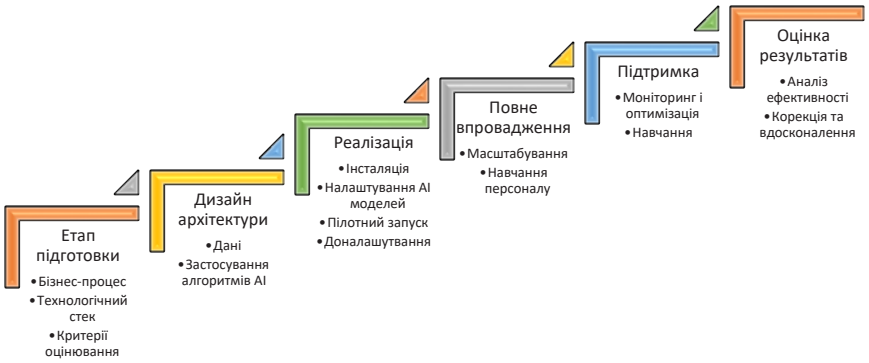


Рис. 1. Етапи впровадження AIOps

Проаналізуємо більш детально етапи імплементації AIOps у бізнес-процеси:

1. Етап підготовки

a) Аналіз бізнес процесу. Тут необхідно визначити стадії процесу, які будуть піддаватися AI автоматизації. Проводиться аналіз існуючих бізнес-процесів та IT-інфраструктури, щоб визначити, які саме операції найбільше потребують автоматизації або підвищення ефективності.

b) Технологічний стек. Це може бути внутрішня розробка, використання готових рішень або гібридне використання обох підходів.

c) Критерії оцінювання – метрики, які мають покращитися в результаті успішного впровадження. Встановлюються ключові показники ефективності (Key Performance Indicators, KPI), наприклад, час на відновлення після інциденту, середній час реакції на інциденти тощо.

2. Дизайн архітектури AIOps

a) Дані. Відповідно до стадії процесу, різні дані будуть піддаватися обробці алгоритмами AI. Проте визначення структури цих даних, способу нормалізації і місця зберігання є першим кроком у побудові AI-інфраструктури. Визначаються всі джерела даних, такі як журнали подій, моніторинг ресурсів, бази даних. Це можуть бути сервери, мережеві пристрої, хмарні сервіси.

b) Застосування алгоритмів AI. Розробляються моделі машинного навчання для моніторингу і прогнозування інцидентів. Це можуть бути моделі для виявлення аномалій або прогнозування інцидентів на основі минулих даних.

3. Реалізація

a) Інсталяція платформ для моніторингу та аналізу. Вибирається і встановлюється відповідне програмне забезпечення для управління та обробки великих обсягів даних. Інструменти на кшталт Prometheus, Splunk, чи ELK використовуються для моніторингу.

b) Налаштування AI-моделей. Інтеграція моделей AI та машинного навчання для обробки зібраних даних і виявлення аномалій в реальному часі.

c) Пілотне впровадження. Проводиться тестування системи на окремих частинах інфраструктури, щоб переконатися у правильності збору та аналізу даних.

d) Доналаштування алгоритмів. Налаштування моделей машинного навчання для більш точного прогнозування, виходячи з результатів тестування.

4. Впровадження на рівні всієї компанії

a) Масштабування. Після успішного тестування і налаштування на обмеженій кількості проектів система впроваджується у всі бізнес-процеси та IT-середовища компанії, що стосуються менеджменту інцидентів.

b) Навчання персоналу. Проводяться тренінги для співробітників з використання нових інструментів і процедур для взаємодії з системою AIOps.

5. Операційна підтримка

a) Моніторинг і оптимізація. Проводиться постійний моніторинг результатів роботи AIOps для вдосконалення моделей і підвищення ефективності.

b) Реалізація навчання на основі інцидентів. Використання зворотного зв'язку від інцидентів для навчання моделей AI, покращення прогнозування і швидкості реакції.

6. Оцінка результатів

a) Аналіз ефективності. Проводиться регулярний аналіз ефективності впровадженої системи на основі заздалегідь визначених метрик.

b) Корекція та вдосконалення. На основі аналізу результатів впровадження за ключовими метриками проводиться корекція процесів для забезпечення постійного вдосконалення.

Ця методологія може варіюватися в залежності від специфіки компанії або індустрії, але загальний підхід залишиться незмінним: від підготовки до масштабного впровадження і постійної оптимізації.

Висновки. Для підвищення ефективності процесу управління інцидентами ключовою є покрокова методологія впровадження в бізнес-процеси автоматизацій на базі штучного інтелекту з розгортанням інфраструктури AIOps. Досвід пілотних імплементацій таких технологій у галузі IT дав можливість систематизувати існуючі підходи відповідно до стадій процесу менеджменту інцидентів. Дана методологія може бути використана в організаціях і адаптована відповідно до конкретних потреб і цілей, адже враховує критерії оцінювання відповідно до вибраних KPI і постійне вдосконалення, що забезпечить максимальну адаптацію. Подальші дослідження є необхідними в цій галузі для визначення найкращих практик і створення стандартів, оскільки впровадження AI це процес із яким уже зіштовхуються більшість технологічних організацій. Застосовування розробленої методології і проведення кейс-стаді із визначенням можливих особливостей процесів організацій, є перспективним напрямком досліджень у галузі.

Список використаних джерел:

1. Databricks. Effective AIOps with Open Source Software in a Week. Youtube, 2021. URL: https://www.youtube.com/watch?v=NuL1u_CIkQw (дата звернення: 20.11.2024).

2. Diachenko Maksym, Roskladka Andrii. 2023. Approaches in managing IT services and implementation of AI automations. X INTERNATIONAL CONFERENCE Information Technology and Implementation (Satellite).C. 233.

3. Google Cloud Tech. Build an AIOps platform at enterprise scale with Google Cloud. Youtube. 2023 URL: https://www.youtube.com/watch?v=UdVaexipP6w (дата звернення: 20.11.2024).

4. Ira Cohen, Jeffrey S Chase, Moises Goldszmidt, Terence Kelly, and Julie Symons. 2004. Correlating Instrumentation Data to System States: A Building Block for Automated Diagnosis and Control. In OSDI, Vol. 4. 16–16. URL: https://dl.acm.org/doi/10.5555/1251254.1251270 (дата звернення: 20.11.2024).

5. Jiaxi Xu, Fei Wang, Jun Ai. Defect prediction with semantics and context features of codes based on graph representation learning. IEEE Transactions on Reliability 70. 2020. 613–625. URL: https://doi.org/10.1109/TR.2020.3040191 (дата звернення: 20.11.2024).

6. Junjie Chen, Shu Zhang, Xiaoting He, Qingwei Lin, Hongyu Zhang, Dan Hao, Yu Kang, Feng Gao, Zhangwei Xu, Yingnong Dang, et al. 2020. How incidental are the incidents? characterizing and prioritizing incidents for largescale online service systems. In Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering. C. 373–384. URL: https://doi.org/10.1145/3324884.3416624 (дата звернення: 20.11.2024).

7. Junjie Chen, Xiaoting He, Qingwei Lin, Hongyu Zhang, Dan Hao, Feng Gao, Zhangwei Xu, Yingnong Dang, Dongmei Zhang. 2019. Continuous incident triage for large-scale online service systems. 34th IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE. C. 364–375. URL: https://doi.org/10.1109/ASE.2019.00042 (дата звернення: 20.11.2024).

8. Justin Meza, Qiang Wu,Sanjev Kumar, and Onur Mutlu. 2015. A large-scale studyof flash memory failures in the field. ACM SIGMETRICS Performance Evaluation Review 43, 1. C.177–190. URL: https://doi.org/10.1145/2796314.2745848 (дата звернення: 20.11.2024).

9. Kasem Khalil, Omar Eldash, Ashok Kumar, Magdy Bayoumi. 2020. Machine learning-based approach for hardware faults prediction. IEEE Transactions on Circuits and Systems I: Regular Papers 67, 11. C. 3880–3892. URL: https://doi.org/10.1109/TCSI.2020.3010743 (дата звернення: 20.11.2024).

10. Md Nasir Uddin, Bixin Li, Zafar Ali, Pavlos Kefalas, Inayat Khan, Islam Zada. 2022. Software defect prediction employing BiLSTM and BERT-based semantic feature. Soft Computing 26, 16. C.7877–7891. URL: https://doi.org/10.1007/s00500-022-06830-5 (дата звернення: 20.11.2024).

11. Nagappan Nachiappan, Ball Thomas, Zeller Andreas. 2006. Mining metrics to predict component failures. In Proceedings of the 28th international conference on Software engineering. C. 452–461. URL: http://dx.doi.org/10.1145/1134349 (дата звернення: 20.11.2024).

12. Nengwen Zhao, Junjie Chen, Zhou Wang, Xiao Peng, Gang Wang, Yong Wu, Fang Zhou, Zhen Feng, Xiaohui Nie, Wenchi Zhang, et al. 2020. Real-time incident prediction for online service systems. In Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering.C. 315–326. URL: https://doi.org/10.1145/3368089.3409672 (дата звернення: 20.11.2024).

13. Qingwei Lin, Ken Hsieh, Yingnong Dang, Hongyu Zhang, Kaixin Sui, Yong Xu, Jian-Guang Lou, Chenggang Li, Youjiang Wu, Randolph Yao, et al. 2018. Predicting node failure in cloud service systems. In Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. C. 480–490. URL: https://doi.org/10.1145/3236024.3236060 (дата звернення: 20.11.2024).

14. Reiter Lena. 2021. AIOps – A Systematic Literature Review. Seminar IT-Management in the Digital Age. FH Wedel, Germany. URL: https://www.fh-wedel.de/fileadmin/Mitarbeiter/Records/Reiter_2021_-_AIOps_-_A_Systematic_Literature_Review.pdf (дата звернення: 20.11.2024).

15. Remil Youcef, et al. 2024. Aiops solutions for incident management: Technical guidelines and a comprehensive literature review. URL: https://arxiv.org/abs/2404.01363 (дата звернення: 20.11.2024).

16. Sabharwal N. 2022. Hands-on AIOps. Springer.

17. Stephen Elliot. 2014. Dev Ops and the cost of downtime: Fortune 1000 best practice metrics quantified. International Data Corporation (IDC).

18. Sun-Ro Lee, Min-Jae Heo, Chan-Gun Lee, Milhan Kim, Gaeul Jeong. 2017. Applying deep learning based automatic bug triager to industrial projects. In ESEC/FSE. ACM. C.926–931. URL: https://doi.org/10.1145/3106237.3117776 (дата звернення: 20.11.2024).

19. Wubai Zhou, Liang Tang, Chunqiu Zeng, Tao Li, Larisa Shwartz, and Genady Ya Grabarnik. 2016. Resolution recommendation for event tickets in service management. IEEE Transactions on Network and Service Management 13, 4 (2016), 954–967. URL: https://doi.org/10.1109/INM.2015.7140303 (дата звернення: 20.11.2024).

20. Xianping Quand Jingjing Ha. 2017. Next generation of devops: Aiops in practice. SREcon17.

21. Ying Zhao, Xiang Liu, Siqing Gan, and Weimin Zheng. 2010. Predicting disk failures with HMM-and HSMM-based approaches. In Advances in Data Mining. Applications and Theoretical Aspects: 10th Industrial Conference, ICDM 2010, Berlin, Germany, July 12-14. Proceedings 10. Springer. C. 390–404. URL: https://doi.org/10.1007/978-3-642-14400-4_30 (дата звернення: 20.11.2024).

22. Yingnong Dang, Qingwei Lin, and Peng Huang. AIOps: real-world challenges and research innovations. In 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion). IEEE, 2019. C. 4–5. URL: https://doi.org/10.1109/ICSE-Companion.2019.00023 (дата звернення: 20.11.2024).

УДК 004.9:555
DOI https://doi.org/10.32689/maup.it.2024.4.10

Денис ЄФІМОВ
старший науковий співробітник науково-дослідного відділу
перспектив розвитку та проблем супроводження моделей
операцій центру імітаційного моделювання,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0002-8101-9699*

Роман ТИМОШЕНКО
кандидат технічних наук,
начальник науково-дослідного відділу перспектив розвитку
та проблем супроводження моделей операцій,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0001-8069-023X*

Катерина ВОЙТЕХ
старший науковий співробітник науково-дослідної лабораторії розробки моделей видів забезпечення операцій та бойових дій науково-дослідного відділу розробки моделей операцій та бойових дій,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0003-4290-1766*

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА СУЧАСНІ БОЙОВІ СТРАТЕГІЇ

Анотація. *У статті досліджено питання щодо впливу інформаційних технологій на сучасні бойові стратегії.*
У статті досліджено вплив інформаційних технологій на сучасні бойові стратегії.

Мета роботи *полягає у вивченні того, як новітні технологічні досягнення змінюють способи ведення бойових дій і формують нові стратегії, зокрема в контексті гібридної війни.*

Методологія *включає аналіз сучасних технологій, таких як комп'ютери, електроніка, інформаційні системи, штучний інтелект, а також їх вплив на тактику і стратегію ведення війни. Автори використовують порівняльний та історичний аналіз для оцінки трансформації військових методів за допомогою новітніх інновацій.*

Наголошено на тому, що війна, як явище, є динамічною за своєю суттю, враховуючи постійно змінювані тенденції. Сучасне геополітичне середовище та технологічний розвиток формують нові стратегії й наслідки ведення бойових дій. Сучасні методи, які активно впроваджуються, в поєднанні з традиційним розумінням війни, складають основу концепції гібридної війни. Елементи цієї концепції можна спостерігати на всіх етапах історії.

Сучасні технологічні досягнення, такі як комп'ютери, електроніка, інформаційні системи, засоби зв'язку, нові види зброї, підвищена швидкість, ефективні датчики, швидке розгортання, приховані технології, економія пального, смертоносність, космічні системи, біохімія та штучний інтелект, суттєво трансформують способи ведення війни. У цій новій системі противники використовують інформацію як засіб маніпуляції, що, в свою чергу, веде до виникнення нестабільних умов

Як висновок, сказано про те, що вплив інформаційних технологій на сучасні бойові стратегії є беззаперечним. Вони не лише трансформують традиційні підходи до ведення війни, але й відкривають нові можливості для збирання, аналізу та використання інформації. Кібербезпека, автоматизація, штучний інтелект – всі ці елементи формують нову реальність військових дій, де інформація стає не менш важливою, ніж зброя. У майбутньому, з огляду на постійний розвиток технологій, важливо буде враховувати ці зміни, аби адаптувати стратегії до нових умов ведення війни.

Наукова новизна *роботи полягає у виокремленні інформаційних технологій як ключового елемента, що визначає сучасні бойові стратегії, а також у визначенні ролі кібербезпеки та автоматизації у новій реальності військових дій.*

Висновки *свідчать, що інформаційні технології значно трансформують традиційні методи ведення війни, відкриваючи нові можливості для збирання, аналізу та використання інформації. Враховуючи швидкий розвиток технологій, майбутні стратегії повинні адаптуватися до нових умов, де інформація стає не менш важливою за зброю.*

Ключові слова: *війна, технології, штучний інтелект, прогрес, розвиток.*

Denis YEFIMOV, Roman TYMOSHENKO, Kateryna VOITEKH. THE INFLUENCE OF INFORMATION TECHNOLOGIES ON MODERN COMBAT STRATEGIES

Abstract. *The article examines the impact of information technologies on modern combat strategies.*
The article examines the influence of information technologies on modern combat strategies.

The purpose *of the work is to study how the latest technological advances change the ways of conducting military operations and form new strategies, in particular in the context of hybrid warfare.*

The methodology *includes the analysis of modern technologies, such as computers, electronics, information systems, artificial intelligence, as well as their impact on the tactics and strategy of warfare. The authors use comparative and historical analysis to assess the transformation of military methods through the latest innovations.*

It is emphasized that war, as a phenomenon, is dynamic in nature, taking into account constantly changing trends. The modern geopolitical environment and technological development shape new strategies and consequences of conducting hostilities. Modern methods, which are actively implemented, in combination with the traditional understanding of war, form the basis of the concept of hybrid war. Elements of this concept can be observed at all stages of history.

Modern technological advances such as computers, electronics, information systems, communications, new weapons, increased speed, effective sensors, rapid deployment, stealth technology, fuel economy, lethality, space systems, biochemistry, and artificial intelligence are essential transform the ways of waging war. In this new system, adversaries use information as a means of manipulation, which in turn leads to unstable conditions

As a conclusion, it is said that the influence of information technologies on modern combat strategies is undeniable. They not only transform traditional approaches to warfare, but also open new opportunities for gathering, analyzing and using information. Cyber security, automation, artificial intelligence – all these elements form a new reality of military operations, where information becomes no less important than weapons. In the future, given the constant development of technology, it will be important to take these changes into account in order to adapt strategies to the new conditions of warfare.

***The scientific novelty** of the work consists in identifying information technologies as a key element that determines modern combat strategies, as well as in determining the role of cyber security and automation in the new reality of military operations.*

***The conclusions** show that information technology significantly transforms traditional methods of warfare, opening up new opportunities for gathering, analyzing and using information. Given the rapid development of technology, future strategies must adapt to new conditions where information becomes as important as weapons.*

***Key words:** war, technology, artificial intelligence, progress, development.*

Вступ. Постановка проблеми. У наш час інформаційні технології (ІТ) стають не лише супутником, але й основою сучасних бойових стратегій. Військові конфлікти все більше переходять у цифрову площину, де інформація та її обробка відіграють ключову роль у прийнятті рішень. Від дронів до систем управління боєм, інформаційні технології змінюють саму суть війни, роблячи її більш комплексною, швидкою та ефективною.

Виклад основного матеріалу. Незважаючи на певні позитивні зміни у військово-політичній ситуації наприкінці ХХ – на початку ХХІ століття, що зменшили загрозу масштабної звичайної та ядерної війни, основний принцип політики щодо забезпечення національної безпеки й захисту національних інтересів залишається незмінним. Він полягає в активному використанні всіх можливостей держави: дипломатичних, інформаційних, військових та економічних.

З огляду на активне впровадження новітніх досягнень у сфері комунікації та інформатизації, військові фахівці надають особливого значення ролі інформаційного простору, визнаючи його важливість у розв'язанні міждержавних суперечностей і досягненні зовнішньополітичних цілей.

Враховуючи характер завдань та дій, заходи інформаційного менеджменту включають:

Залучення стратегічної комунікації – це комплекс заходів, які проводять військові сили для інформування іноземних аудиторій про позиції держави та для просування національних інтересів, впливу на інші сторони та схиляння їх до співпраці в інтересах держави. Ці заходи проводяться в координації з програмами публічної дипломатії.

Участь у засіданнях міжвідомчої групи – дорадчого органу, який створюється для забезпечення командувача всебічною ситуативною обізнаністю в зоні відповідальності. Учасники цієї групи, окрім військових, включають представників державних органів, уряду та регіональних організацій.

Забезпечення зв'язку з громадськістю – це скоординовані дії з підготовки та поширення інформації про діяльність держави, спрямовані на формування позитивного сприйняття громадянами.

Військово-цивільні операції – це заходи зі співпраці з урядовими та неурядовими організаціями й цивільним населенням для досягнення оперативних цілей. Вони можуть відбуватися до, під час або після бойових дій.

Операції в кіберпросторі – це комплекс заходів, спрямованих на вплив на об'єкти противника у кіберпросторі, які проводяться за єдиним планом для досягнення стратегічних цілей.

Війна, як явище, є динамічною за своєю суттю, враховуючи постійно змінювані тенденції. Сучасне геополітичне середовище та технологічний розвиток формують нові стратегії й наслідки ведення бойових дій.

Сучасні методи, які активно впроваджуються, в поєднанні з традиційним розумінням війни, складають основу концепції гібридної війни. Елементи цієї концепції можна спостерігати на всіх етапах історії [1, с. 52].

Термін «гібридна війна» є порівняно новим, тому немає єдиного загальноприйнятого визначення цього поняття. Суб'єктивність терміна призводить до появи різних трактувань у міжнародному контексті. Вперше цей термін ввів Вільям Дж. Немет у 2002 році, висунувши ідею про те, що гібридна війна є поєднанням синхронізованих невійськових і військово-стратегічних елементів [2, с. 73].

Еволюція війни тісно пов'язана з технологічним прогресом, який забезпечує створення вдосконаленої зброї та нових стратегій ведення бойових дій. Історично можна виділити кілька етапів цієї еволюції.

Війна першого покоління виникла після Вестфальського договору 1648 року, коли було сформульовано поняття територіального суверенітету, що заклало основи державної монополії на ведення війни.

Друге покоління війни, яке з'явилося за часів французької армії, завершилося після Першої світової війни. В цей час культурні норми порядку були збережені, а жива сила була замінена масовою вогневою потужністю, що дозволяло домінувати на полі бою. Третє покоління війни, розроблене Німеччиною під час Другої світової, ґрунтувалося на тактиці проникнення, яку Німеччина застосовувала в Першій світовій війні і яка призвела до появи танків у Другій світовій [3, с. 58].

Війна четвертого покоління, що розвивалася протягом останніх шістдесяти років, представила недержавних акторів як учасників конфлікту, чим завершила державну монополію на ведення бойових дій. Війна п'ятого покоління радикально змінила філософію ведення бойових дій, інтегруючи інструменти для сприйняття та обробки інформації. Ця ідея передбачає, що конкуренція між державами відбувається на основі маніпуляцій сприйняттям світу і політики, що призводить до нестабільності.

Інформаційні технології займають ключову роль у всіх аспектах життя сучасного суспільства. Процес інформатизації набуває все більшого поширення, впливаючи як на внутрішню, так і на зовнішню політику держав. Особливо важливу роль інформаційні технології відіграють у забезпеченні інформаційної безпеки.

Створення єдиного інформаційного простору сприяє розвитку та застосуванню інформаційної зброї, яка є важливим елементом національної безпеки. Рівень захисту держави значною мірою залежить від володіння інформаційною зброєю, її ефективності, методів використання та засобів захисту.

Нині існує безліч визначень поняття «інформаційна зброя», і жодне з них не можна вважати остаточно правильним чи неправильним. Більшість визначень базуються на переліку суб'єктів та об'єктів інформаційного впливу. Проте для кращого розуміння інформаційної зброї важливо спочатку визначити, що саме мається на увазі під терміном «зброя».

Зброя – це засоби та пристрої, які використовуються у збройних конфліктах для ураження та знищення противника. У контексті інформаційного протиборства цей термін набуває додаткового значення. За одним з визначень, інформаційна зброя – це спеціальні технології, засоби й інформація, здатні здійснювати вплив на інформаційний простір суспільства, завдаючи шкоди політичним, оборонним, економічним та іншим важливим інтересам держави.

Інформаційну зброю можна поділити на дві основні категорії: інформаційно-технічну та інформаційно-психологічну. Перший вид спрямований на вплив на технічні системи, тоді як другий має за мету вплив на людей. Інформаційна зброя може також включати технології, призначені для втручання в роботу управлінських систем противника, поширення дезінформації, а також психологічний вплив на керівництво та населення з метою отримання переваги в інформаційному протиборстві.

Інформаційна зброя має ряд особливих характеристик, що відрізняють її від інших видів зброї:

1. Керованість – здатність здійснювати вплив на об'єкти у конкретний момент і з заданою інтенсивністю.
2. Прихованість – важко визначити момент початку дії та джерело атаки.
3. Універсальність – здатність уражати різноманітні об'єкти в широкому спектрі.
4. Низька вартість створення в поєднанні з високою ефективністю застосування.
5. Доступність – легке поширення та можливість високого контролю за виконанням операцій.
6. Тривалість – можливість тривалого використання без втрати ефективності.
7. Використання в мирний час – раптове застосування можливе як під час конфліктів, так і в мирний період.

Принципова відмінність інформаційного протистояння від звичайної війни полягає в тому, що інформаційне протиборство певною мірою регулюється законодавством. Єдина мета інформаційної зброї – завдання інформаційних систем супротивника найбільшої шкоди. Досягнення цієї мети противники реалізують практично певні завдання. Інформаційна зброя відрізняється від звичайного озброєння керованістю, прихованістю, універсальністю, економічністю та тривалістю. Крім того, різні види інформаційної зброї впливають на людську психіку, управлінські та радіоелектронні системи, а також на програмно-технічне оснащення, використовуючи при цьому найбільш відповідні методи впливу. Що стосується сфери законодавства з проблеми, то можна зробити висновок, що у зв'язку із встановленням інформаційного простору та розвитком інформаційних технологій, структура українського законодавства включає в себе малу кількість нормативно-правових актів. З розвитком даного сектора база офіційних 37 документів буде поповнюватися, що допоможе покращити контроль за процесом регулювання проведення інформаційного протиборства.

Цілісність сучасного світу забезпечується в основному за рахунок інтенсивного інформаційного обміну. Інформаційна зброя здатна призупинити глобальні інформаційні потоки, що може призвести до

глобальної кризи. Для того, щоб розібратися в питанні застосування інформаційної зброї, необхідно виявити сферу її застосування. Найбільш широкодоступною областю є світові інформаційні мережі. Світові інформаційні мережі – це сукупність електронно-обчислювальних машин, що пов'язані між собою каналами телекомунікації. Такі інформаційні мережі дозволяють користувачам обмінюватися інформацією, спільно використовувати необхідні інформаційні ресурси [4].

Глобальна інформаційна мережа поділяється на загальнодоступну та спеціалізовану. Загальнодоступна мережа (Internet, електронна пошта) знаходиться у вільному та рівному доступі для звичайних користувачів. Спеціалізовані мережі є корпоративними або відомчими, тобто призначені для обмеженого кола осіб. Перша комутована мережа ARPANET розпочала своє існування у США у 1969 р. Тоді до неї було підключено лише 4 комп'ютери. На сьогоднішній день на Заході існує безліч глобальних мереж. Наприклад, BITNET – мережа, що об'єднує понад 800 колективних учасників, переважно серед університетів, коледжів і наукових центрів. Ця мережа охоплює 35 країн Європи, Азії та Америки.

Сучасні технологічні досягнення, такі як комп'ютери, електроніка, інформаційні системи, засоби зв'язку, нові види зброї, підвищена швидкість, ефективні датчики, швидке розгортання, приховані технології, економія пального, смертоносність, космічні системи, біохімія та штучний інтелект, суттєво трансформують способи ведення війни. У цій новій системі противники використовують інформацію як засіб маніпуляції, що, в свою чергу, веде до виникнення нестабільних умов.

Сучасні бойові дії характеризуються комплексною інтеграцією ІТ у різні аспекти військових операцій. У класичних війнах інформація часто була обмежена, і її збір вимагав значних зусиль.

Сьогодні ж завдяки безпілотним літальним апаратам (БПЛА), супутникам і розвідувальним системам дані про противника можна отримати в режимі реального часу. Ці технології дозволяють військовим командувачам здійснювати більш точні аналізи ситуації на полі бою, що впливає на прийняття стратегічних рішень.

Системи супутникового спостереження, наприклад, забезпечують можливість відстеження переміщень ворога, виявлення його позицій та ресурсів. Це дозволяє планувати атаки з максимальною ефективністю, скорочуючи час реакції на дії противника. У сучасній війні, де кожна секунда може стати вирішальною, швидкість обробки даних і їх аналізу є критично важливими.

Окрім фізичного ведення бойових дій, ІТ внесли значні зміни у ведення кібервійни. Кібернетичні атаки можуть призводити до збою в системах управління, знищення важливих даних або навіть до паралічу критично важливих інфраструктур. На відміну від традиційної війни, де противник вражається фізично, кібервійна діє на інформаційному рівні, що робить її менш передбачуваною [5].

Відомими прикладами є атаки на енергетичні системи та інформаційні мережі держав, що призводять до серйозних наслідків для національної безпеки.

Кіберзахист став невід'ємною частиною стратегій держав, адже втрата інформації або збої у системах можуть мати катастрофічні наслідки.

Штучний інтелект (ШІ) стає важливим інструментом у сучасних бойових стратегіях. Алгоритми машинного навчання здатні аналізувати величезні обсяги даних, виявляти патерни та робити прогнози. Це дозволяє військовим планувати операції з врахуванням ймовірних дій противника.

Крім того, ШІ застосовується у системах управління боєм, що дозволяє автоматизувати ряд завдань, зменшуючи навантаження на військовий персонал. Це також допомагає зменшити ймовірність помилок, адже рішення приймаються на основі об'єктивних даних та аналізу.

Конфлікти останніх років, такі як війна в Україні, продемонстрували важливість ІТ у бойових діях. Військові з різних країн активно використовують дрони для розвідки та нанесення ударів, а також для ведення інформаційної війни. Інформаційні технології стали важливим елементом у комунікації між підрозділами, що дозволяє забезпечити координацію дій у реальному часі [6].

Війна в Україні також показала, як соціальні медіа та інформаційні платформи можуть використовуватися для пропаганди та маніпуляції. З одного боку, технології допомагають поширювати правду про конфлікт, з іншого – можуть бути використані для дезінформації та створення паніки.

Висновки. Отже, вплив інформаційних технологій на сучасні бойові стратегії є беззаперечним. Вони не лише трансформують традиційні підходи до ведення війни, але й відкривають нові можливості для збирання, аналізу та використання інформації. Кібербезпека, автоматизація, штучний інтелект – всі ці елементи формують нову реальність військових дій, де інформація стає не менш важливою, ніж зброя. У майбутньому, з огляду на постійний розвиток технологій, важливо буде враховувати ці зміни, аби адаптувати стратегії до нових умов ведення війни.

В умовах російсько-української війни існує нагальна потреба в адекватній системній інформаційній протидії, яка повинна включати ефективні стратегії для виявлення та реагування на дезінформацію, а також сприяти розвитку інформаційної грамотності серед населення. Посилення кібербезпеки,

створення прозорих інформаційних каналів і активна комунікація є основними складовими цієї інформаційної стратегії.

Важливо вивчати міжнародний досвід, аналізувати законодавство та стратегії інших країн, які успішно протистоять інформаційним загрозам, а також впроваджувати відповідні нормативні акти та заходи в Україні. Крім того, корисним буде вивчення ефективних практично-організаційних методів виявлення та розкриття дезінформації, а також розробка механізмів співпраці з міжнародними партнерами для спільної боротьби з інформаційними загрозами.

Список використаних джерел:

1. Довгань Б. В., Мартинюк О. В. Становлення та розвиток поняття інформаційної війни. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2020. № 12. С. 51–56.
2. Дунаєва Л. М. Дезінформаційні виклики під час російсько-української війни: політологічний аналіз. *Політикус* : наук. журнал. 2022. № 5. С. 73–78.
3. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка»*. Серія : Юридичні науки. 2020. Т. 7, № 2. С. 56–61.
4. Hayat,R. A. B. B. I. A. Hybrid Warfare: A Challenge to National Security. *PCL Student Journal of Law*, 5(1). 2021. P. 102.
5. Solmaz, T. Hybrid warfare': one term, many meanings. Small Wars Journal, 25. 2022.
6. Steingartner W., Galinec D. Cyber threats and cyber deception in hybrid warfare. *Acta Polytechnica Hungarica*, 18(3). 2021. P. 25.

УДК 004.72
DOI https://doi.org/10.32689/maup.it.2024.4.11

Олексій КЛИМЕНКО
аспіранті кафедри комп'ютерних систем, мереж та кібербезпеки, факультету інформаційних технологій, Національний університет біоресурсів та природокористування України, o.klymenko@nubip.edu.ua
***ORCID:** 0009-0005-2590-1803*

СТВОРЕННЯ SELF-HEALING МЕРЕЖІ

Анотація. *У статті розглянуто створення системи самовідновлення працездатності мережі під час збоїв, описано логічну та фізичну схему комунікацій для створення Self-Healing мережі, алгоритм роботи та функціональну схему такої мережі, частково автоматизовано процес комунікації з Інтернет-провайдером, виконано розрахунки з метою визначення, на який час дана система дає змогу пришвидшити процес вирішення аварій.*

Метою роботи *є обмін напрацюваннями щодо автоматизації відновлення мереж після аварій, створення самовідновлювальної мережі на певних ділянках та висвітлення принципів реалізації Self-Healing.*

Методологія дослідження. *За допомогою методів вимірювання та порівняння деякого набору даних перевіряється спроможність даної автоматичної системи моніторингу бути ефективною. Вимірювання – це метод дослідження, за допомогою якого визначається числове значення деякої величини з використанням одиниці вимірювання об'єкта. Порівняння – один із найбільш поширених методів пізнання, який дозволяє встановити подібність та розбіжність об'єктів [1]. Основну роль в такій системі має програма, написана на мові Python, система моніторингу Zabbix, яка контролює стан Інтернет-каналів та запускає програму у випадку аварії, а також камера ESP32CAM, яка значно спрощує процес отримання стану індикації мережевого обладнання постачальника послуг на точках включення замовника. Для надійного збереження та використання секретів використовується SOPS та Age.*

Наукова новизна. *У статті представлено нову систему самовідновлення працездатності мережі у разі проблем на стороні постачальника послуг, розглянуто приклад автоматизованої взаємодії з провайдером для вирішення типових проблем.*

Висновки. *Розглянута схема комп'ютерної мережі з автоматичною системою моніторингу реалізує відмовостійку самовідновлювальну мережу та практично не залежить від обладнання замовника, здатна закривати типові інциденти з мінімальною участю інженера. Згідно розрахункам, час тривалості аварій на об'єктах можна знизити на третину.*

Ключові слова: *self-healing, моніторинг, автоматизація, комп'ютерна мережа, програмування, скрипт, відмовостійкість.*

Oleksii KLYMENKO. CREATING A SELF-HEALING NETWORK

Abstract. *The article considers the creation of a system for Self-Healing of network performance during failures, describes the logical and physical communication scheme for creating a Self-Healing network, the algorithm of operation and the functional diagram of such a network, partially automates the process of communication with the Internet provider, and performs calculations to determine how long this system can speed up the process of resolving failures.*

The purpose of the work *is to share best practices in automating network recovery after disasters, creating a self-healing network in certain areas, and highlighting the principles of Self-Healing.*

Research methodology. *The ability of a given automatic monitoring system to be effective is tested by measuring and comparing a certain set of data. Measurement is a research method that determines the numerical value of a certain value using a unit of measurement of an object. Comparison is one of the most common methods of cognition, which allows to establish similarities and differences between objects [1]. The main role in such a system is played by a program written in Python, the Zabbix monitoring system, which monitors the status of Internet channels and launches the program in the event of an accident, as well as the ESP32CAM camera, which greatly simplifies the process of obtaining the status of the indication of the service provider's network equipment at the customer's switch-on points. SOPS and Age are used to securely store and use secrets.*

Scientific novelty. *The article presents a new system for self-healing of the network in case of problems on the side of the service provider, and an example of automated interaction with the provider to solve typical problems is considered.*

Conclusions. *The considered scheme of a computer network with an automatic monitoring system implements a fault-tolerant self-healing network and is practically independent of the customer's equipment, capable of closing typical incidents with minimal involvement of an engineer. According to calculations, the duration of accidents at facilities can be reduced by a third.*

Key words: *self-healing, monitoring, automation, computer network, programming, script, redundancy.*

Вступ. Вирішення інцидентів, пов'язаних з Інтернет-каналом, займає значну частину часу мережевих інженерів. Автоматизація процесу вирішення таких проблем, особливо за умови, коли філіал адмініструється віддалено та не має ІТ-спеціалістів по місцю, може зменшити загальну тривалість аварій на об'єктах та вивільнити інженерів під інші задачі, що в свою чергу дозволить більш оптимально розподіляти людські ресурси. В даній статті розглянуто автоматизацію мережі в частині реактивного моніторингу.

Постановка проблеми. Велика розподілена комп'ютерна мережа потребує детального налаштування систем моніторингу для відслідковування інцидентів на різних рівнях. Збільшення кількості

логів та попереджень про можливі чи вже такі, що трапились, аварій, розсіює увагу інженерів. Чим більше подій може бути опрацьовано автоматично, тим більш відмовостійкою та надійною стає мережа, інженери вивільняються від рутинних задач.

Self-Healing (самовідновлювальна) мережа необхідна для мінімізації людських зусиль і витрат, пов'язаних із визначенням причин збою в складних системах.

Аналіз досліджень і публікацій. У досліджені [7] чітко визначено значення терміну Self-Healing. Це – властивість, яка дозволяє системі зрозуміти, що вона працює неправильно, і без (або з) втручання людини вносити необхідні корективи, щоб відновити нормальну роботу. Кожна система з властивостями самовідновлення має здатність виявляти, діагностувати та реагувати на збої.

У попередній статті [2] було розкрито декілька прикладів Self-Healing мереж. Проте, варто зазначити, що досліджень в цьому напрямку небагато, хоча вони тривають. Як правило, в таких дослідженнях розглянуто конкретну ділянку мережі, якій за допомогою програмованої складової надано властивість самовідновлювання [5, 7, 10]. Також зазначається, що основною метою інтеграції функцій самовідновлення в будь-яку мережу є підвищення її надійності та зручності обслуговування. Ці атрибути якості традиційно підвищуються в системах самовідновлення.

Виклад основного матеріалу. В даній статті основна увага приділена деяким прикладам автоматизації реактивного моніторингу.

Реактивний моніторинг – спостереження за IT-інфраструктурою та іншими сервісами в режимі реального часу, можливість визначення невідповідності параметрів та вузьких місць роботи кожного компоненту відносно поточних показників [3].

Фізичне підключення комунікацій. Побудова відмовостійкої мережі з точки зору uplinks (висхідні лінії) часто складається з двох маршрутизаторів, які мають окреме підключення до ISP (Internet Service Provider) [8]. Додатково треба зарезервувати комунікації на рівні розподілення. Наприклад, кореневі комутатори зібрані в Stack, від кожного комутатора є підключення до кожного маршрутизатора. Ці декілька підключень між комутатором та маршрутизаторам мають працювати в режимі LAG (Link Aggregation Group), тобто фізичні кабелі об'єднані в одне логічне з'єднання. У разі неполадок з одним з кабелів мережа продовжить працювати через інші. Критично важливо мати резервне живлення, щонайменше ДБЖ (джерело безперебійного живлення), аби обладнання не було чутливим до проблем в електромережі та не перезавантажувалось. Якщо обладнання має декілька блоків живлення, то їх треба підключати до різних ДБЖ (рис.1).

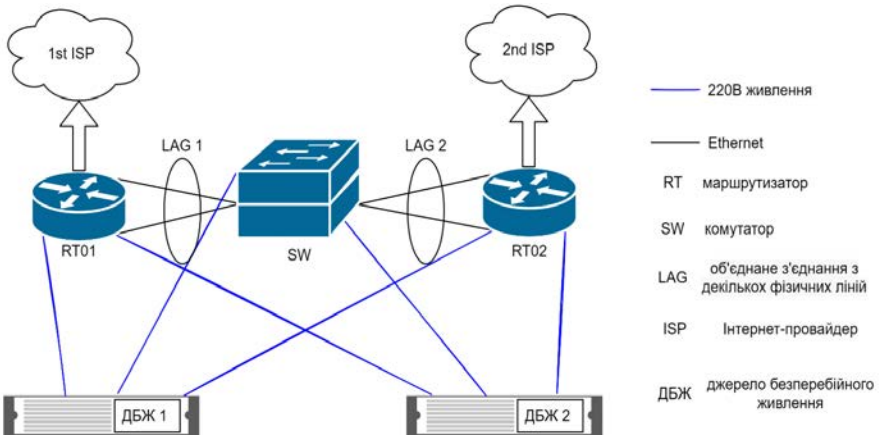


Рис. 1. Базова схема побудови відмовостійкого ядра мережі

Логічна схема комунікацій. Базова логічна конфігурація складається зі стеку технологій IP SLA+TRACK, HSRP (Hot Standby Router Protocol) та EEM (Embedded Event Manager). Перша пара інструментів реалізує перевірку доступності певних ресурсів в мережі Інтернет через підключений Інтернет-канал. Якщо за визначений час на запит не прийшла відповідь, тест IP SLA вважається не пройденим. Запускається лічильник TRACK і, якщо за цей час повторні IP SLA не повернуть позитивний результат, у дію запускається протокол HSRP. На інтерфейсі змінюється пріоритет, і роль головного маршрутизатора перехоплює резервний маршрутизатор. EEM в свою чергу потрібен для очищення NAT-трансляцій аби запобігти переповненню пам'яті, оскільки при перенаправлені трафіку через інший маршрутизатор дані записи втрачають свою актуальність [2].

Моніторинг комунікацій. В цілях моніторингу можна використовувати різні протоколи та системи моніторингу. В даному прикладі розглядається безкоштовна багатофункціональна система моніторингу Zabbix та протокол SNMP, по якому можуть працювати в тому числі пристрої, що були виготовлені раніше. На сервері Zabbix треба додати маршрутизатори. За допомогою шаблона, наприклад, Template SNMP Cisco IP SLA, сервер моніторингу може отримувати дані з маршрутизатора про доступність Інтернет-каналів. На Zabbix треба налаштувати Trigger actions, який буде запускати команду, якщо Інтернет-канал стане недоступним. Ця команда в свою чергу запускає на виконання програму, написану на мові Python, або локально на Zabbix-сервері, або на віддаленому сервері за допомогою Zabbix-agent.

Програмне забезпечення. Програма підключається до потрібного маршрутизатора по SSH (Secure Shell) та виконує команди для діагностики. Якщо з отриманих даних зрозуміло, що проблема на стороні провайдера, програма самостійно підставляє потрібні дані з БД (база даних), такі як ідентифікатор каналу, адреса об'єкту, фото індикації обладнання провайдера, контактні дані адміністратора по місцю тощо та формує лист-заявку в технічну підтримку провайдера. В іншому випадку лист з результатами діагностики надсилається інженерам компанії для подальшого розгляду проблеми. На рисунку 2 зображено частину коду даної програми.

```
59  def get_isp_crd(isp_id, isp_id_range, branch_ip):
60      keys = ["name", "id", "ip", "ip_gw", "location"]
61      params = ["name",
62                f"id_{isp_id_range[isp_id]}",
63                f"ip_{isp_id_range[isp_id]}",
64                f"ip_{isp_id_range[isp_id]}_gw",
65                "location"]
66      values = []
67      for param in params:
68          sops_command = ["sops-v3.8.1.exe", "-d", "-extract",
69                          f"['{branch_ip}']['{param}']",
70                          "c:\\git\\pyneng\\pyneng\\exercises\\isp.yaml"]
71          value = sops(sops_command, branch_ip)
72          if value == "null":
73              err_generate(f"Parameter '{param}' got a value 'null'", branch_ip)
74          else:
75              values.append(value)
76      return dict(zip(keys, values))
77
78
79  def sops(sops_command, branch_ip):
80      value = subprocess.run(sops_command, stdout=subprocess.PIPE,
81                             stderr=subprocess.PIPE, encoding='utf-8')
82      if value.returncode == 0:
83          return value.stdout.strip()
84      else:
85          err_generate(value.stderr.strip(), branch_ip)
```

Рис. 2. Частина коду програми

Захист чутливої інформації. Для підключення до обладнання програмне забезпечення використовує логін та пароль. Крім того, програма взаємодіє з чутливою інформацією про ідентифікатори послуг провайдера, точною адресою точок включення послуг, персональними даними контактів по місцю тощо. Тому вкрай важливо зберігати чутливі дані у зашифрованому вигляді.

З цією метою у даній системі задіяно SOPS+Age. Це система, яка часто використовується у проектах на Git – розподіленої системи керування версіями файлів та спільної роботи. Оскільки файли git проектів розташовуються на публічному або приватному сервері виникає потреба шифрування секретів. Навіть у випадку використання приватного git сервера доступ до нього можуть мати інженери з різними правами [6]. Проте, як в рамках одного файлу надати доступ одному інженеру до однієї ділянки коду, а іншому інженеру – для іншої? Програма Age, використовуючи сучасні алгоритми шифрування (AES 256 GCM), створює криптостійку пару ключів – приватний та публічний. Програма SOPS за допомогою публічного ключа може зашифрувати цілий файл або окремі поля, наприклад, yaml файлу. Публічний ключ зберігається на системі, де буде виконуватись дешифрування, а права доступу до нього надаються тільки відповідному користувачу [9].

Аналогічним чином чутлива інформація для програмного забезпечення може зберігатися на сервері, до якого мають доступ різні адміністратори, у вигляді yaml файлу. Цей файл (або окремі його поля) знаходиться у зашифрованому стані. Право доступу до приватного ключа має лише той адміністратор, який має право запускати на виконання дану програму. Програмне забезпечення в ході своєї роботи запускає програму SOPS для дешифрування чутливої інформації, наприклад, логіну та паролю мережевого обладнання. Далі за допомогою захищеного протоколу SSH відбувається підключення до

мережевого обладнання та взаємодія з ним. Таким чином чутлива інформація не зберігається та не використовується у відкритому вигляді ані в межах системи, ані поза її межами.

Система перевірки індикації обладнання. Досить часто Інтернет-провайдер просить додати фото індикації МК (медіаконвертер). Цей процес також можна автоматизувати. На створення цього рішення надихнув проект «AI-on-the-edge-device» ресурсу GitHub, у якому автор за допомогою камери в автоматичному режимі збирає дані з лічильників води [4]. Для реалізації цього етапу можна використовувати камеру ESP32CAM (рис.3). Для стабільного створення якісних знімків камеру та МК можна з'єднати за допомогою корпусу, розробленого на 3D-принтері. Щоб отримати знімок програма звертається за посиланням до камери. Далі програма аналізує знімок на предмет наявності потрібної індикації на МК та додає цю інформацію до заявки в технічну підтримку провайдера.

Рис. 3. Камера ESP32CAM

Побудова комунікації з Інтернет-провайдером. Оскільки вирішення заявок мають однакові етапи, цей процес також можна автоматизувати. Для цього потрібно домовитись про коди повідомлень з провайдером послуг (таблиця 1). Програма додає потрібний код у лист з міткою, наприклад, «Code:», а відповіді парсить у пошуку аналогічного поля. Коли код-відповідь ідентифіковано, програма на основі цієї інформації приймає рішення про подальші дії. У випадку, якщо надати відповідь без участі людини неможливо, програма переводить запит на інженера. В іншому випадку програма автоматично збирає потрібну інформацію та надсилає відповідь (наприклад, повторна перевірка працездатності Інтернет-каналу).

Приклад послідовності вирішення типової заявки, коли проблема на стороні постачальника послуг:

1. Замовник послуги створює заявку з результатами діагностики.
2. Постачальник послуги підтверджує, що заявку прийнято, та перевіряє інформацію.
3. Постачальник послуги просить повторно перевірити працездатність каналу.
4. Замовник перевіряє роботу Інтернет-каналу та підтверджує, що проблема вирішена.
5. Постачальник закриває заявку.

Таблиця 1

Таблиця кодів

Код	Ініціатор повідомлення	Значення
100	Замовник	Первинний запит (створення заявки)
200	Постачальник	Заявка прийнята
210	Постачальник	Надайте додаткову інформацію
211		Надайте повторно інформацію про індикацію МК
212		Перезавантажте МК
213		Перезавантажте маршрутизатор
214		Уточніть робочі години об'єкту з метою доступу
110	Замовник	Передача додаткової інформації
220	Постачальник	Проблему вирішено. Перевірте працездатність Інтернет-каналу
120	Замовник	Відмова, проблему не вирішено
130	Замовник	Підтвердження, що проблема відсутня. Запит на закриття заявки
230	Постачальник	Заявку закрито

Таким чином більшість заявок може бути вирішено взагалі без участі людини зі сторони замовника, оскільки вони пов'язані з вирішенням типових проблем на стороні провайдера, наприклад, обрив оптичної лінії, відмова кінцевого чи транзитного вузлу тощо. Така автоматизація процесу вигідна в тому числі й постачальнику послуг, тому що дозволяє опрацьовувати заявки швидше та вивільняє додатковий час для їх інженерів.

Алгоритм роботи автоматичної системи моніторингу. На рисунку 4 зображено алгоритм роботи даної системи. Окремо виділено контури IP SLA та Zabbix, які працюють постійно та збирають інформацію про стан мережі. Програма в свою чергу виконується лише за певних підстав.

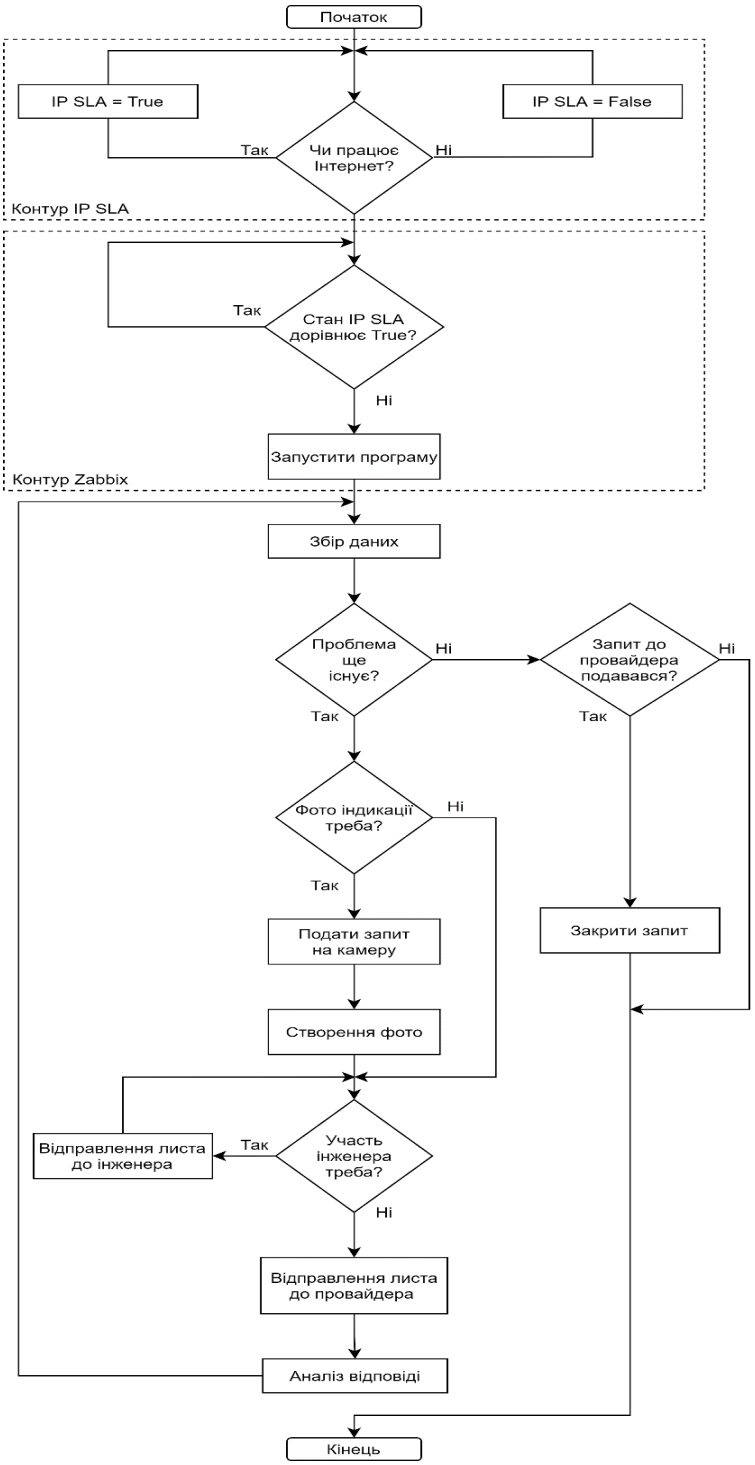


Рис. 4. Алгоритм роботи автоматичної системи моніторингу

Функціональна схема автоматичної системи моніторингу. На рисунку 5 зображено функціональну схему даної системи. Основну роль в ній відіграє програма, написана на мові Python.

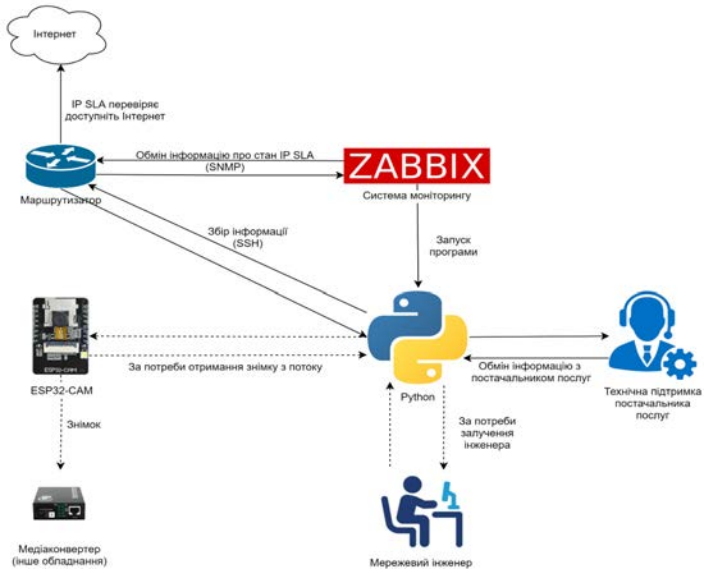


Рис. 5. Функціональна схема автоматичної системи моніторингу

Розрахунки. З метою аналізу, як зазначені вище програмні та апаратні засоби і система взаємодії з Інтернет-провайдером вплинули на час вирішення проблеми, було зібрано ряд даних за останні 6 місяців. В таблиці 2 вказано скільки часу зайняло вирішення проблеми від її початку. У вибірку потрапили лише ті аварії, вирішення яких можна покращити за рахунок перерахованих засобів та систем. Як правило, це обрив ВОЛЗ (волоконно-оптична лінія зв'язку), зависання чи вихід з ладу МК або антени, проблеми на стороні провайдера, що не потребують додаткових дій зі сторони замовника послуг.

Варто зазначити, що на вирішення проблеми мають істотний вплив час реакції на аварію [2], час на уточнення індикації (та\або іншої інформації) та час витрачений на повторну перевірку працездатності сервісу, якщо в результаті виявилось, що сервіс досі не працює.

Таблиця 2

Тривалість аварії

Номер об'єкту	Тривалість аварій на об'єктах за останні 6 місяців						Середній час вирішення заявки (год)	Середній час вирішення заявки (хв)
1	46 год 10 хв	84 год 33 хв	7 год 3 хв				45 год 55 хв	2755
2	24 год 59 хв	3 год 2 хв					14 год 1 хв	841
3	6 год 20 хв	8 год 47 хв					7 год 34 хв	454
4	129 год 6хв	21 год 20 хв	179 год 20 хв				109 год 55 хв	6595
5	239 год 5 хв	19 год 34 хв	21 год 44 хв	6 год 11 хв	191 год 5 хв	165 год 20 хв	107 год 9 хв	6429
6	15 год 31 хв	18 год 51 хв	23 год 51 хв	4 год 40 хв	31 год 20 хв		18 год 51 хв	1131
7	176 год 15 хв	7 год 9 хв	29 год 19 хв	8 год 16 хв	25 год 38 хв		49 год 19 хв	2959
8	24 год 8 хв	4 год 39 хв	36 год	15 год 17 хв			20 год 1 хв	1201
9	19 год 22 хв	28 год 1 хв					23 год 42 хв	1422
10	25 год 32 хв	43 хв	9 год 46 хв	28 год 55 хв			16 год 14 хв	974
11	25 год 6 хв	49 год 48 хв					37 год 27 хв	2247
12	45 год 52 хв	33 хв					23 год 13 хв	1393
13	67 год 15 хв	25 год 17 хв					46 год 16 хв	2776
14	35 хв	6 год 54 хв	3 год 33 хв	13 год 52 хв	3 год		5 год 35 хв	335
15	1 год 29 хв	1 год 17 хв	2 год 1 хв				1 год 36 хв	96
16	81 год 34 хв	15 год 11 хв	20 год 26 хв				39 год 4 хв	2344
17	2 год 10 хв	4 год 43 хв	25 год 24 хв				10 год 46 хв	646
18	2 год 10 хв	1 год 9 хв	8 год 33 хв				3 год 57 хв	237

Таблиця 3

Час реакції

Номер об'єкту	Час реакції на аварії на об'єктах за останні 6 місяців						Загальний час реакції (хв)	Середній час реакції (хв)
1	1 год 44 хв	3 год 21 хв	17 хв				322	107
2	58 хв	17 хв					75	36
3	22 хв	26 хв					48	24
4	8 год 32 хв	24 хв	12 год 37 хв				1293	431
5	10 год 15 хв	19 хв	20 хв	22 хв	9 год 44 хв	2 год 39 хв	1419	237
6	46 хв	25 хв	37 хв	21 хв	52 хв		184	37
7	15 хв	27 хв	2 год 33 хв	44 хв	3 год 13 хв		419	84
8	4 год 9 хв	17 хв	3 год 5 хв	41 хв			492	123
9	57 хв	1 год 14 хв					131	66
10	1 год 17 хв	10 хв	28 хв	53 хв			168	42
11	46 хв	7 год 3хв					469	235
12	2 год 4 хв	15 хв					139	70
13	8 год 3 хв	47 хв					530	265
14	15 хв	24 хв	17 хв	59 хв	35 хв		150	30
15	19 хв	20 хв	18 хв				57	19
16	15 год 10 хв	3 год 17 хв	2 год 13 хв				1240	413
17	25 хв	18 хв	1 год 28 хв				131	44
18	23 хв	16 хв	47 хв				86	29

Таблиця 4

Час на уточнення індикації

Номер об'єкту	Час на уточнення індикації під час аварій на об'єктах за останні 6 місяців						Загальний час уточнення (хв)	Середній час уточнення (хв)
1	1 год 19 хв	2 год 41 хв	0 хв				240	80
2	33 хв	0 хв					33	17
3	0 хв	41 хв					41	21
4	0 хв	1 год 5 хв	2 год 59 хв				244	81
5	5 год 43 хв	0 хв	33 хв	0 хв	4 год 1 хв	6год 14 хв	991	165
6	0 хв	14 хв	29 хв	0 хв	1 год 15 хв		118	24
7	41 хв	0 хв	49 хв	37 хв	0 хв		127	25
8	54 хв	0 хв	1 год 21 хв	0 хв			135	34
9	0 хв	1 год 35 хв					95	48
10	27 хв	0 хв	13 хв	51 хв			91	23
11	44 хв	1 год 33 хв					137	69
12	1 год 19 хв	0 хв					69	35
13	3 год 27 хв	1 год 14 хв					281	141
14	0 хв	31 хв	0 хв	26 хв	0 год		57	11
15	14 хв	10 хв	0 хв				24	12
16	5 год 3 хв	1 год 3 хв	2 год				486	162
17	0 хв	0 хв	49 хв				49	16
18	0 хв	0 хв	34 хв				34	11

У даному випадку час реакції на аварію залежить не тільки від уважності інженера, але й від того, в який час трапилася аварія. Наприклад, якщо це неробочі або вихідні години. Як правило, Інтернет-провайдери мають чергових інженерів NOC (Network Operations Center, центр керування мережею), які працюють цілодобово. Проте, більшість підприємств наймають мережевих інженерів на денну ставку. Крім того, згадані у вибірці об'єкти мають один-два резервних канали, що лишає статусу критичності проблеми з одним з постачальників послуг.

Таблиця 3 показує час реакції на проблему – час між тим, як трапилася аварія на мережі, та тим, коли було направлено листа постачальнику послуг.

В таблиці 4 відображено час, витрачений на уточнення індикації обладнання (наприклад, МК або антени). Тобто ті випадки, коли провайдер запросив інформацію про поточний стан обладнання. Окремо варто зазначити, що дві третини об'єктів підприємства, дані якого взято для вибірки, не мають ІТ-спеціаліста на місці. Це означає, що процес уточнення індикації обладнання часом може займати декілька годин.

Крім того, у семи випадках було витрачено час на повторну перевірку працездатності сервісу, в результаті якої виявилось, що сервіс досі не працює. Сумарно цей час дорівнює 2 години та 7 хвилин.

Керівництвом департаменту ІТ було вирішено, що заявка в Інтернет-провайдер має бути надіслана не раніше 15 хвилин з моменту аварії. У випадку реалізації системи автоматичного моніторингу час реакції на аварію буде фактично сталим. Для цього в Zabbix потрібно вказати необхідний час для виконання команди, яка в свою чергу запускає програму.

У таблиці 3 загальний час реакції для 59 інцидентів дорівнює 7353 хвилин. Якщо б ці інциденти опрацьовувались автоматично, то це би зайняло:

$$T_{автоматичної\ реакції} = 59 * 15 = 885\ (хвилин)$$

У таблиці 4 загальний час на уточнення індикації дорівнює 3252 хвилин. Якби індикація надсилалась у листі-запиті автоматично, то це би не зайняло додаткових хвилин.

Таким чином автоматизована система моніторингу дозволила би заощадити наступну кількість хвилин:

$$T_{заощаджено} = T_{звичайної\ реакції} - T_{автоматичної\ реакції} + T_{уточнення} + T_{повторної\ перевірки} =$$
$$= 7353 - 885 + 3252 + 127 = 9847\ (хвилин)$$

Що складає майже третину часу від сумарної тривалості усіх аварій:

$$9847 / 34835 = X / 100\%$$
$$X = (9847 / 34835) * 100 = 28.27\%$$

Крім того, швидкість вирішення інцидентів має підвищити зменшення часу очікування на відповідь постачальником послуг зі сторони замовника, оскільки такі відповіді частково можуть бути автоматизовані, про що зазначено у пункті «Побудова комунікації з Інтернет провайдером».

Висновки. Розглянута схема комп'ютерної мережі з автоматичною системою моніторингу реалізує відмовостійку самовідновлювальну мережу.

Об'єкт з такою мережею продовжить працювати, якщо:

1. Наявні проблеми з електроживленням.
2. Обривається один з кабелів комунікацій.
3. Виникає аварія з роботою Інтернет-каналу.
4. Виходить з ладу один маршрутизатор або комутатор рівня ядра чи розподілення мережі.

Автоматизований реактивний моніторинг здатен без участі інженера закривати типові інциденти.

Згідно розрахункам, час тривалості аварій на об'єктах можна знизити на третину.

Ключову роль у такій системі має програмне забезпечення, що виконує збір даних, опрацьовує їх та приймає необхідні рішення. Така програма може бути написана на Python або інших мовах програмування, що додає гнучкості системі – інженер може виконувати автоматизацію мережі за аналогічною схемою в тому числі, коли він володіє іншою мовою програмування. Крім того, сервер моніторингу має вміти виконувати або запускати віддалено програми, а мережеве обладнання – відслідковувати стан Інтернет-каналів, що реалізовано у більшості розробників. Таким чином, розглянута автоматична система є масштабованою, гнучкою та фактично незалежною від розробка мережевого обладнання.

Подальші дослідження будуть пов'язані з доопрацюванням розглянутої системи, а також розробкою інших універсальних інструментів для створення Self-Healing мереж.

Список використаних джерел:

1. Білецький В. С. Методологія наукових досліджень технічних об'єктів та їх оптимізація (Навчальний посібник). НТУ «ХПІ». 2023. С. 18 с.

2. Клименко О. Є. Тенденції розвитку самовідновлювальних мереж. Інформаційні технології та суспільство. 2023. № 5 (11). С. 21–27. URL: https://doi.org/10.32689/maup.it.2023.5.3

3. Системи моніторингу та керування – IT-Solutions, Україна. IT-Solutions, Україна. URL: https://it-solutions.ua/servisi/sistemi-monitoringu-ta-keruvannya/

4. AI-on-the-edge-device. URL: https://it-solutions.ua/servisi/sistemi-monitoringu-ta-keruvannya/

5. Al-Oqily I., Bani-Mohammad S., Subaih B., Alshaer J.J. A survey for self-healing architectures and algorithms. *Proc. of the International Multi-Conference on Systems, Signals Devices*. 2012. P. 1–5.

6. Chacon S., Straub B. Pro Git (Second Edition). *Apress open.* 2014. P. 101–122.

7. D. Ghosh Self-healing systems – survey and synthesis. *Decision Support Systems*. 2007. Vol. 42, no. 4. P. 2164–2185.

8. Empson S., Roth H. CCNP ROUTE Command Guide: Implementing Path Control. Cisco Press. 2010. P. 199–208.

9. Manage Kubernetes secrets with SOPS. URL: https://fluxcd.io/flux/guides/mozilla-sops/

10. Ochoa-Aday L., Cervelló-Pastor C., Fernández-Fernández A. Self-healing and SDN: bridging the gap. *Digital Communications and Networks*. 2020. Vol. 6, no. 3. P. 354–368.

УДК 004.8:005.8
DOI https://doi.org/10.32689/maup.it.2024.4.12

Владислав КОЗУБ
доктор філософії з комп'ютерних наук,
асистент кафедри математики та інформатики,
ДЗ «Луганський національний університет імені Тараса Шевченка»
***ORCID:** 0000-0003-2710-7206*

ІНФОРМАЦІЙНА ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЙ РОЗПОДІЛЕННОГО ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. *Стаття присвячена інформаційній підтримці прийняття рішень з використанням технологій розподіленого штучного інтелекту. При цьому стає зрозуміло, що розподілений ШІ є силою на сучасному ринку, яка робить компанії більш ефективними, надійними та адаптивними.*

Метою роботи *є розробка власної концепції інформаційної підтримки прийняття рішень за допомогою технологій штучного інтелекту на основі розподілених обчислень.*

Методологія. *Методологія цього дослідження побудована на оцінці теоретичних розробок і практичного використання технологій розподіленого штучного інтелекту (ШІ) в діяльності з прийняття рішень. Акцент зроблено на впровадженні методів машинного навчання для аналізу великих масивів даних у розподілених системах, що дає змогу ефективно та оперативно підтримувати прийняття рішень. Використані інструменти та підходи: Python та мультипроцесинг для побудови паралельної обробки даних, логістична регресія для опису процесів прийняття рішень та оцінки класифікації і точності отриманих моделей, PCA – аналіз головних компонент з метою зменшення розмірності даних для цілей кластеризації та класифікації, методи контролю конфіденційності для забезпечення безпеки передачі даних між вузлами та обмеження доступу до даних.*

Наукова новизна. *Основний матеріал підкреслює переваги розподіленого ШІ як функціональні (швидкість обробки даних, паралелізм і висока масштабованість, технічна реалізованість), так і з точки зору розробки (менші витрати, можливість повторного використання та гнучкість реалізації). Він також бере на себе кілька проблем, таких як відповідальність ШІ, питання конфіденційності та безпеки даних, а також питання впровадження.*

З'ясовано, що розподілений штучний інтелект – це дуже потужна технологія, і слід бути обережним, застосовуючи її для прийняття рішень, оскільки, хоча вона має переваги, вона також має і деякі недоліки. У цій роботі продемонстровано, як системи штучного інтелекту, що працюють у розподілених архітектурах, можуть бути використані для прийняття рішень, на прикладі нашої власної розробки на мові Python. Описано таку систему, яка використовує логічну регресію, аналіз головних компонент та візуалізацію результатів.

Акцентовано увагу на пошуці розв'язку шляхом виконання коду на мові Python, розробленого в інтегрованому середовищі розробки PyCharm 2024.2, який демонструє розподілену систему прийняття рішень на основі ШІ з використанням методів багатопроцесорної обробки та машинного навчання. Код включає функції для навчання моделей на окремих вузлах, управління розподіленим процесом навчання та візуалізації границі рішення найкращої моделі. Використано логістичну регресію для бінарної класифікації та PCA для зменшення розмірності для полегшення візуалізації.

Код створює пул процесів, які відповідають заданій кількості вузлів. Потім ці процеси асинхронно навчають моделі на підмножинах даних. Після завершення процесу навчання обирається найкраща модель, а границя рішення в найпростішому випадку зображується у вигляді двовимірного графа. Розподілений ШІ, описаний у цьому прикладі, втілює потенційне застосування технології у прийнятті рішень: можливість приймати рішення над розподіленими даними та розподіленими акторами шляхом обробки даних на декількох вузлах.

Висновки. *Можна стверджувати, що технології розподіленого ШІ можуть бути інтегровані в процеси прийняття рішень у будь-якому випадку. Не виключено, що організації хотіли б спиратися на культуру критичної оцінки та безперервного навчання, щоб приймати більш обґрунтовані, справедливі та ефективні рішення. Цей розроблений код є прикладом того, як така система може бути реалізована на практиці.*

Ключові слова: *розподілений штучний інтелект, системи підтримки прийняття рішень, машинне навчання, глибинне навчання, обробка даних, прогнозна аналітика, паралельне обчислення, кібербезпека.*

Vladyslav KOZUB. INFORMATION SUPPORT FOR DECISION-MAKING USING DISTRIBUTED ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Abstract. *The methodology of this study is based on the assessment of theoretical developments and practical use of distributed artificial intelligence (AI) technologies in decision-making activities. The emphasis is on the implementation of machine learning methods for analysing large amounts of data in distributed systems, which allows for efficient and prompt decision-making support. Tools and approaches used*

Python and multiprocessing to build parallel data processing.

Logistic regression is used to describe decision-making processes and to assess the classification and accuracy of the resulting models.

PCA – principal component analysis to reduce the dimensionality of data for clustering and classification purposes.

Privacy control methods to ensure the security of data transmission between nodes and restrict access to data.

Methodology. *The methodology of this study is based on the assessment of theoretical developments and practical use of distributed artificial intelligence (AI) technologies in decision-making activities. The emphasis is on the implementation of machine learning methods for analysing large amounts of data in distributed systems, which allows for efficient and effective*

decision-making support. Tools and approaches used: Python and multiprocessing to build parallel data processing, logistic regression to describe decision-making processes and evaluate the classification and accuracy of the resulting models, PCA – principal component analysis to reduce the dimensionality of data for clustering and classification purposes, privacy control methods to ensure the security of data transmission between nodes and restrict access to data.

Scientific novelty. *The main material emphasises the advantages of distributed AI, both functional (data processing speed, parallelism, and high scalability, technical feasibility) and development (lower costs, reusability, and implementation flexibility). It also takes on several challenges, such as AI liability, data privacy and security issues, and implementation issues.*

It has been found that distributed AI is an immensely powerful technology and care should be taken when applying it to decision-making, as while it has advantages, it also has some disadvantages. In this paper, we demonstrate how AI systems running in distributed architectures can be used for decision making, using our own Python development as an example. We describe such a system that uses logical regression, principal component analysis, and visualisation of results.

The article focuses on finding a solution by executing Python code developed in the PyCharm 2024.2 integrated development environment, which demonstrates a distributed AI-based decision-making system using multiprocessing and machine learning methods. The code includes functions for training models on individual nodes, managing the distributed learning process, and visualising the decision boundary of the best model. It uses logistic regression for binary classification and PCA for dimensionality reduction to facilitate visualisation.

The code creates a pool of processes that correspond to a given number of nodes. These processes then train the models asynchronously on subsets of the data. After the training process is complete, the best model is selected, and the decision boundary is represented as a two-dimensional graph in the simplest case. The distributed AI described in this example embodies a potential application of the technology in decision-making: the ability to make decisions over distributed data and distributed actors by processing data on multiple nodes.

Conclusions. *It can be argued that distributed AI technologies can be integrated into decision-making processes in any case. It is possible that organisations would like to rely on a culture of critical evaluation and continuous learning to make more informed, fair, and effective decisions. The code developed here is an example of how such a system could be implemented in practice.*

Key words: *distributed artificial intelligence, decision support systems, machine learning, deep learning, data processing, predictive analytics, parallel computing, cybersecurity.*

Постановка проблеми. У сучасному ландшафті технологій і бізнесу впровадження технологій розподіленого штучного інтелекту (ШІ) стало революційною силою в процесах прийняття рішень. Розподілений штучний інтелект – це підхід, який використовує кілька комп'ютерних систем, які працюють у мережі, щоб розподілити інтелектуальну діяльність та виконання завдань. Це дозволяє системам ділитися інформацією, ресурсами та діями, що підвищує їхню ефективність, надійність та здатності до розширення.

Ці системи розширюють можливості обробки даних, сприяють створенню середовища для спільної роботи та покращують масштабованість і гнучкість, що робить їх основними інструментами для організацій, які прагнуть до ефективності та гнучкості. Однак є помітні контраргументи щодо надмірної залежності від штучного інтелекту, занепокоєння щодо конфіденційності та безпеки даних і проблем, пов’язаних із впровадженням.

Аналіз останніх досліджень і публікацій. Mohsen Soori, Fooad Karimi Ghaleh Jough, Roza Dastres [11] досліджують різні підходи, застосування AI, переваги, виклики та перспективи використання цих систем у різних галузях промисловості, зосереджуючись на їхній ролі у підвищенні ефективності, автоматизації процесів, оптимізації рішень, а також на їхньому внеску в інноваційний розвиток. В. Рос [12] зосереджується на інструментах, які допомагають керівникам приймати рішення більш свідомо, швидко та точно, включаючи використання інформації, аналізу даних, інноваційних підходів, навчання на основі досвіду, інтуїції та інших чинників, які формують прийняття рішень на різних рівнях організації. Хассан Ель Хаджа [7] досліджує, як технології, зокрема штучний інтелект, змінюють спосіб прийняття рішень людиною, підкреслює важливість розуміння цифрових інструментів, їхньої здатності надавати інформацію, інформованість, а також їхнього впливу на прийняття рішень як на індивідуальному, так і на корпоративному рівні. А. Осьмак, Ю. Карпенко, І. Семененко [4] зосереджується на використанні AI-інструментів у мережевому управлінні. Автори дискутують про переваги, ризики та перспективи розвитку цієї галузі, а також розглядають їхній вплив на різні аспекти управлінської діяльності. А.І. Шевченко [5] розглядає різні аспекти використання AI-технологій у країні, зокрема їхній розвиток, інституційну підтримку, інноваційний потенціал та інші. Ю. Когуть [6] розглядає використання AI-технологій у галузі національної безпеки, досліджує як ці інструменти можуть підтримувати процеси прийняття рішень, підвищуючи рівень захисту інформаційних систем, передбачення загроз та оперативність реагування на них. С. Гордієнко та І. Доронін [2] аналізують можливості AI у вирішенні завдань оборони, безпеки, правоохоронної діяльності та іншого, а також підіймають питання, пов'язані з їхнім використанням, такі як етичні, правові, а також конституційні вимоги, які їхнє використання імпліцитно передбачає. Тож у наукових працях [8, 9, 10] приділяється незначна увага застосуванню штучного інтелекту без виділення ролі розподілених моделей штучного інтелекту. Цей аспект своєю чергою має бути з’ясований виходячи із наукових здобутків та практичних навичок програмування.

Мета статті – розробка власного рішення для задачі інформаційної підтримки прийняття рішень із застосуванням технологій розподіленого штучного інтелекту.

Виклад основного матеріалу. Технології штучного інтелекту, що розгортаються, значно покращують функції управління даними, які є вкрай необхідними для організацій, що стикаються з потоком даних. Прийняття несприятливих рішень з високим рівнем складності даних і часу їх обробки є проблемою для традиційних методів прийняття рішень. Однак розподілені системи можуть обробляти такі великі обсяги даних з величезною швидкістю. Ці технології, що використовують аспекти паралельної обробки в засобах хмарних обчислень, можуть обробляти терабайти даних за лічені секунди, що дозволяє особам, які приймають рішення, отримувати необхідну інформацію майже в режимі реального часу. Ці можливості добре підходять для таких галузей, як фінанси, охорона здоров'я та логістика, де час має першорядне значення, а рішення, прийняті на основі великих даних, можуть сприяти або зашкодити бізнесу. Крім того, обробка даних у реальному часі також підвищує якість інформації, необхідної для прийняття рішень, що полегшує організаціям прийняття правильних рішень. Наприклад, розподілений штучний інтелект, який тісно пов'язаний з концепцією великих даних, може передбачати певні тенденції та можливі проблеми, що може бути корисним для завчасної підготовки. Неминуче вища потужність обробки даних розподіленого штучного інтелекту призводить до кращих можливостей для прогнозного аналізу, що дозволяє особам, які приймають рішення, підготуватися до майбутнього і адаптувати свої підприємства до викликів, що відіграє важливу роль у створенні менш вразливої і більш адаптивної системи.

Проте, використання розподіленого дизайну ШІ тягне за собою покращення обробки даних та широку співпрацю у прийнятті рішень, що є критично важливим у сучасному суспільстві. Така відкритість систем розподіленого ШІ сприяє більш повному залученню різних зацікавлених сторін і одночасному використанню найкращих з їхніх напрацювань. Наприклад, за допомогою телекомунікацій організації можуть створювати крос-функціональні команди з різних відділів, кожна з яких має різний досвід. Існування декількох точок зору збагачує процес прийняття рішень, оскільки групова гетерогенність практично зводить нанівець небезпеку групового мислення – явища, яке призводить до негативних наслідків через гомогенізацію ідей. Крім того, механізми співпраці, розроблені інструментами штучного інтелекту, посилюють взаємодію між зацікавленими сторонами, дозволяючи їм досягати консенсусу, незважаючи на складні структури прийняття рішень. Наприклад, у процесі прийняття рішень деякі учасники можуть домінувати, а інші соромитися, тоді як за допомогою штучного інтелекту всі точки зору будуть просунуті та враховані, що призведе до прийняття більш ефективних рішень. Я також побачив, що інтегральний підхід, який пропагується в цій організаційній структурі, також дає можливість людям і заохочує команди всередині компанії, що так важливо сьогодні при веденні бізнесу в умовах зростаючої невизначеності, підвищення ролі нематеріальних активів як основних факторів організаційної та економічної діяльності.

Ще однією перевагою технологій розподіленого штучного інтелекту є здатність підвищувати масштабованість і гнучкість організацій, які беруть участь у процесах прийняття рішень. Це також свідчить про те, що в міру того, як бізнес просувається по етапах свого подальшого розвитку і набуває більшої складності, виникає потреба в масштабуванні рішень, що приймаються, а розподілений ШІ може сприяти цьому посиленню без законодавчих втрат. Організації можуть використовувати розподілені системи, які можна масштабувати для більш високих рівнів даних і зростаючої кількості користувачів, а це означає, що прийняття рішень постійно відбувається на високій швидкості незалежно від рівня складності. Крім того, технології штучного інтелекту є самоналагоджуваними, тобто вони можуть змінювати свої дії залежно від заздалегідь визначених умов і потреб бізнесу, що є дуже вигідним у сучасному нестабільному бізнес-середовищі. Наприклад, в умовах нестабільності організації можуть коригувати стратегії для вирішення нових проблем без значних змін. Крім того, розподілений ШІ дозволяє отримувати дані з різних джерел, а також поєднувати результати аналізу з однієї системи з іншою завдяки гнучкості джерела даних. Сьогодні цей погляд дозволяє краще приймати рішення, оскільки врахування широкого спектру факторів і проблем сприяє кращому прийняттю стратегічних рішень відповідно до цілей і планів організації та ринку. (Рис. 1):

Рис. 1. Переваги розподілених нейронних мереж

Незважаючи на переваги розподілених технологій штучного інтелекту, існує значне занепокоєння щодо надмірної залежності від цих систем, що може призвести до упередженого прийняття рішень. Системи штучного інтелекту не застраховані від упереджень, присутніх у їхніх навчальних даних, часто успадковуючи ці упередження та зберігаючи їх у своїх результатах. Наприклад, якщо наявні дані відображають системну нерівність, то якщо ШІ дає рекомендації без урахування цієї системної нерівності, то проблема лише поглиблюється. Крім того, особи, які приймають рішення, можуть бути схильні сліпо довіряти тому, що рекомендує штучний інтелект, занадто швидко і навіть не контролювати рекомендовані результати. Наслідком такої надмірної довіри є те, що зацікавлені сторони, які використовують штучний інтелект, можуть випустити з уваги важливий контекст або нюанс, який штучний інтелект не вловив. Крім того, упередженість, притаманна штучному інтелекту, може призвести до прийняття рішень, які не відповідають дійсності, і навіть посилити існуючі диспропорції в організаціях чи громадах. Як наслідок, результати розподіленого штучного інтелекту можуть дати цінну інформацію, але особам, які приймають рішення, необхідно зберігати критичну перспективу і збалансувати результати штучного інтелекту з людським судженням, щоб нівелювати ці ризики.

Питання конфіденційності та безпеки даних, які можуть стати на заваді ефективному прийняттю рішень, є ще однією серйозною проблемою розподілених технологій штучного інтелекту [1, 3, 9]. Поширеною схемою використання розподілених систем є робота з інтелектуальною інформацією, якою необхідно обмінюватися та обробляти між різними платформами та зацікавленими сторонами, а отже, ризик витоку даних та неналежного доступу до них є вищим. Ці вразливості можуть підірвати довіру організацій та приватних осіб, які створюють системи штучного інтелекту, тому вони не поспішають їх впроваджувати. Крім того, витік даних не лише загрожує довірі до компанії, але й може призвести до юридичних і фінансових наслідків, зокрема до дорогих судових розглядів і заплямувати репутацію компанії. Крім того, технології розподіленого штучного інтелекту можуть ускладнюватися вимогою дотримання багатьох нормативних актів щодо захисту даних, таких як Загальний регламент про захист даних (General Data Protection Regulation, GDPR). Однак розгортання таких систем в організації підпорядковується складному ландшафту законодавчих вимог, які часто уповільнюють їх розгортання, а отже, іноді обмежують їхню ефективність у прийнятті рішень. Розподілений ШІ пропонує унікальні можливості для прийняття кращих рішень, але ми не можемо ігнорувати ризики, пов'язані з конфіденційністю та безпекою даних.

Ще однією серйозною перешкодою для ефективного використання технологій розподіленого штучного інтелекту в процесі прийняття рішень є труднощі з впровадженням. Однак впровадження цих передових технологій вимагає великих витрат і може бути непомірно дорогим, що особливо складно для невеликих організацій з обмеженими ресурсами. Виділення коштів на інвестиції в інфраструктуру, програмне забезпечення та поточне обслуговування забирає гроші з інших важливих сфер. Крім того, розподілені системи штучного інтелекту, як правило, є високотехнологічними, в результаті чого організаціям часто бракує спеціальних знань, необхідних для впровадження та експлуатації цих систем. Більше того,

через брак навичок організаціям важко отримати максимальну віддачу від технологій ШІ, що додає проблем до поточних проблем, з якими стикаються компанії. Крім того, це уповільнює процес впровадження систем і робочих процесів, оскільки працівники можуть неохоче сприймати нові й сучасні системи та робочі процеси в організації. Одним із пояснень такого опору може бути страх втратити роботу, відчуття дискомфорту при роботі з технологіями або просто нерозуміння цінності розподіленого ШІ. Як наслідок, потенційні технічні переваги розподіленого штучного інтелекту в процесі прийняття рішень є дуже багатообіцяючими, але його впровадження викликає значні технічні труднощі.

Враховуючи вищезазначені недоліки, пов'язані з технологіями розподіленого штучного інтелекту, ми запропонували власний підхід, а саме розробку коду на мові програмування Python. Код не оптимізований для справжніх розподілених систем, але його можна використовувати як багатопоточну симуляцію при прототипуванні, при аналізі великих датасетів. Це реалізовано у файлі-скрипті main.py в інтегрованому середовищі розробки PyCharm 2024.2.

```
import multiprocessing as mp
import numpy as np
import matplotlib.pyplot as plt
from sklearn.linear_model import LogisticRegression
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
from sklearn.decomposition import PCA

# Function to train a model on a single node
def train_model_on_node(data, target, node_id):
print(f"Node {node_id}: Training started.")
X_train, X_test, y_train, y_test = train_test_split(data, target, test_size=0.3, random_state=node_id)

# Logistic Regression model
model = LogisticRegression(max_iter=1000)
model.fit(X_train, y_train)

# Accuracy evaluation
y_pred = model.predict(X_test)
accuracy = accuracy_score(y_test, y_pred)

print(f"Node {node_id}: Training complete with accuracy {accuracy}")

return model, accuracy

# Main function to manage distributed training
def distributed_ai_decision_system(data, target, num_nodes):
pool = mp.Pool(processes=num_nodes)
results = []

for node_id in range(num_nodes):
result = pool.apply_async(train_model_on_node, (data, target, node_id))
results.append(result)

pool.close()
pool.join()

# Collect results from nodes
models = []
accuracies = []
for result in results:
model, accuracy = result.get()
models.append(model)
accuracies.append(accuracy)
```

```
best_model_idx = np.argmax(accuracies)
print(f"Best model trained on node {best_model_idx} with accuracy {accuracies[best_model_idx]}")

return models[best_model_idx]

# Visualizing the decision boundary of the best model
def plot_decision_boundary(model, data, target):
# Using PCA to reduce data to 2D for visualization
pca = PCA(n_components=2)
reduced_data = pca.fit_transform(data)

# Create a mesh grid
x_min, x_max = reduced_data[:, 0].min() – 1, reduced_data[:, 0].max() + 1
y_min, y_max = reduced_data[:, 1].min() – 1, reduced_data[:, 1].max() + 1
xx, yy = np.meshgrid(np.arange(x_min, x_max, 0.1),
np.arange(y_min, y_max, 0.1))

# Predict on the mesh grid
Z = model.predict(pca.inverse_transform(np.c_[xx.ravel(), yy.ravel()]))
Z = Z.reshape(xx.shape)

# Plot decision boundary
plt.contourf(xx, yy, Z, alpha=0.8)
plt.scatter(reduced_data[:, 0], reduced_data[:, 1], c=target, edgecolor='k', s=20)
plt.title('Decision Boundary of the Best Model')
plt.show()

# Example dataset for training
if __name__ == '__main__':
# Generating a random dataset for demonstration
data, target = np.random.rand(1000, 10), np.random.randint(0, 2, 1000)

# Launching the distributed decision system
num_nodes = 4 # Number of nodes in the system
best_model = distributed_ai_decision_system(data, target, num_nodes)

# Plotting the decision boundary of the best model
plot_decision_boundary(best_model, data, target)

print("Best model selected from the distributed AI system.")
```

Джерело: власна розробка

Це реалізація розподіленої системи прийняття рішень ШІ на мові Python та багатопроцесорної бібліотеки.

Імпорт:

1. Розподілене навчання ШІ можна моделювати за допомогою паралельної обробки до мультипроцесорної обробки, яка підтримує паралельну обробку декількох вузлів у розподіленому навчанні.

2. numpy (np) підтримує деякі числові операції та генерування випадкових даних.

3. Використовуємо matplotlib.pyplot (plt) для відображення границі розв'язку навченої моделі ШІ.

4. LogisticRegression – модель машинного навчання з `sklearn`, яка виконує бінарну класифікацію.

5. train_test_split розділяє набір даних на навчальний та тестовий набори.

6. accuracy_score обчислює точність моделі.

7. PCA виконує аналіз головних компонент для зменшення набору даних до 2 вимірів для візуалізації.

Основні компоненти

1. train_model_on_node: Функція, яка навчає модель логістичної регресії на одному вузлі, використовуючи підмножину даних.

2. distributed_ai_decision_system: Основна функція, яка керує розподіленим процесом навчання.

3. plot_decision_boundary: Функція, яка візуалізує границю рішення найкращої моделі.

Розподілений процес навчання

1. Функція distributed_ai_decision_system створює пул процесів за допомогою класу multiprocessing. Pool, з кількістю процесів, встановленою в num_nodes.

2. Потім вона застосовує функцію train_model_on_node до кожного вузла у пулі, передаючи дані, ціль та ідентифікатор вузла як аргументи. Метод apply_async використовується для асинхронного виконання функції на кожному вузлі.

3. Результати з кожного вузла збираються у списку results.

4. Методи pool.close() та pool.join() використовуються для очікування завершення всіх процесів та закриття пулу.

5. Списки models та accuracies заповнюються результатами з кожного вузла.

6. Вибирається найкраща модель на основі найвищої точності, і повертається відповідна модель.

Вибір моделі та візуалізація

1. Функція plot_decision_boundary використовується для візуалізації границі рішення найкращої моделі.

2. Дані зводяться до 2D за допомогою функції PCA (аналіз головних компонент).

3. Потім створюється сітка для прогнозування міток класів для кожної точки сітки.

4. Функція contourf використовується для побудови границі розв'язку, а функція scatter – для візуалізації міток класів.

Приклад набору даних та виконання програми

1. Для ілюстрації програма створює випадковий набір даних.

2. Викликається функція distributed_ai_decision_system з набором даних, метою та кількістю вузлів, на яких ми її запускаємо.

3. Повертає найкращу модель.

4. Межа рішення нашої найкращої моделі візуалізується за допомогою функції plot_decision_boundary.

По суті, цей код показує, як створити розподілену систему прийняття рішень зі штучним інтелектом, де кілька моделей логістичної регресії навчаються паралельно і вибирається остання, яка має найкращу точність. Потім границя рішення найкращої моделі візуалізується за допомогою PCA та контурних графіків.

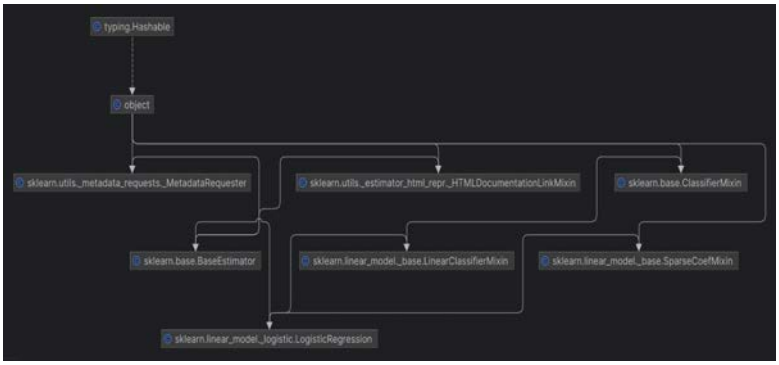


Рис. 2. Візуалізація логічної структури власного проєкту

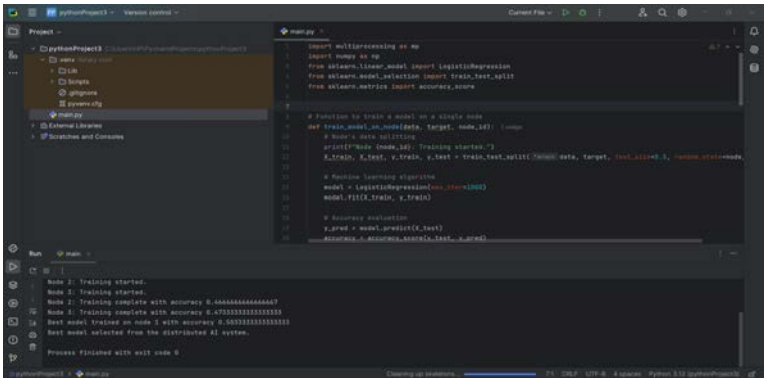


Рис. 3. Процес навчання моделі

Джерело: скріншот роботи коду авторського скрипту

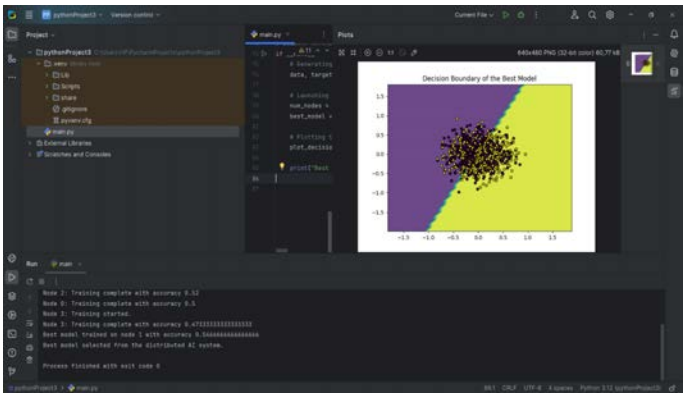


Рис. 4. Візуалізація процесу навчання

Джерело: Скріншот роботи авторського коду

Система, як видно з прикладу, може бути розширена шляхом створення вузлів, але для кращої реалізації в реальних розподілених системах, управління ресурсами, розподіл навантаження та мінімізація витрат на зв'язок між вузлами заслуговують на більш детальний розгляд.

У поточному коді, передбаченому для побудови розподіленого навчання, не розглядаються питання реагування на катастрофи або дублювання даних. Це є вирішальним фактором, особливо коли мова йде про великі виробничі системи для розподілених систем, щоб гарантувати, що деякі дані не будуть втрачені або будуть доступні кожному [1].

Реалізація може бути не оптимальною з точки зору продуктивності для великого обсягу даних, оскільки кожен процес навчання виконується окремо і не враховує залежності або колізії між процесами. У виробничих системах необхідно враховувати такі аспекти продуктивності, як час відгуку і використання ресурсі [3].

При роботі з розподіленими системами і великими даними важливим аспектом є безпека передачі даних між вузлами, а також шифрування даних і обмеження доступу для неавторизованих користувачів [9].

Реалізація не враховує аспекти узгодженості, особливо в умовах збою або зміни даних на одному з вузлів. Реальні розподілені системи повинні забезпечувати управління помилками і гарантувати цілісність даних навіть у випадку відмови деяких вузлів.

Висновки. Розподілений штучний інтелект є потужною технологією, яка має широке коло застосувань. Він підтримує швидке, надійне та ефективне прийняття рішень, особливо у сферах, де необхідне оброблення великих обсягів інформації.

Власний код підходить для задачі інформаційної підтримки прийняття рішень із застосуванням технологій розподіленого штучного інтелекту. Він використовує бібліотеку multiprocessing для паралельного тренування моделей на кількох «вузлах» (процесах) одночасно, що є прикладом розподіленого навчання. Потім обирається модель з найкращою точністю, що відповідає концепції підтримки прийняття рішень. Основними компонентами, які відповідають цій задачі є: паралельне тренування моделей на декількох вузлах для підвищення ефективності, оцінка точності моделей для вибору найкращого варіанту, візуалізація рішення, що може допомогти в аналізі та прийнятті рішень.

У підсумку було виявлено, що технології розподіленого штучного інтелекту, коли вони впроваджуються в процес прийняття рішень, несуть як переваги, так і труднощі. Покращення функціональності обробки даних, уможливлення прийняття рішень на різних рівнях, підвищення масштабованості та гнучкості є вагомими причинами для їхнього впровадження. Однак такі ризики, як надмірна залежність від штучного інтелекту, питання конфіденційності та безпеки даних, а також проблеми, пов'язані з впровадженням, залишаються стримуючими факторами для більшості організацій. Щоб максимізувати переваги розподіленого штучного інтелекту, особи, які приймають рішення, повинні застосовувати найкращі практики, які розширюють можливості цих технологій, уникаючи при цьому викриття їхніх слабких сторін. Розподілений ШІ не тільки підкреслює необхідність ставити під сумнів рішення, але й показує, як організації можуть розвивати культуру, яка вчить вчитися в процесі ставити під сумнів системи прийняття рішень, тим самим покращуючи їхні результати.

Список використаних джерел:

1. Бондарчук О., Козуб В., Козуб Ю. Аналіз ефективності алгоритмів машинного навчання в обробці великих даних. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2024. № 56. С. 107–116. DOI: https://doi.org/10.36910/6775-2524-0560-2024-56-13

2. Гордієнко С. Г., Доронін І. М. Правові проблеми використання технологій штучного інтелекту у контексті забезпечення національної безпеки України. *Інформація і право*. 2024. № 2(49). С. 128–137. DOI: https://doi.org/10.37750/2616-6798.2024.2(49).306155.

3. Когут Ю. І. Штучний інтелект і безпека: практ. посіб.; за ред. док-ра тех. наук, проф. А.С. Довгопологo. Київ: СІДКОН; В Д Дакор, 2024. 294 с. URL: https://jurkniga.ua/contents/shtuchniy-intelekt-i-bezpeka.pdf (дата звернення: 11.10.2024).

4. Козуб В. Ю., Бобень І. Ю., Боярінова Ю. Є. Етичні аспекти використання штучного інтелекту в аналізі даних. *Наукові перспективи*. 2024. № 6(34). С. 880–894. DOI: https://doi.org/10.52058/2786-6025-2024-6(34)-880-893.

5. Осьмак А., Карпенко Ю., Семененко І. Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. *Аспекти публічного управління*. 2023. № 11(3). С. 38–42. DOI: https://doi.org/10.15421/152333.

6. Стратегія розвитку штучного інтелекту в Україні: монографія / А.І. Шевченко та ін.; за заг. ред. А.І. Шевченка. Київ: Інститут проблем штучного інтелекту МОН та НАН України, 2023. 305 с. URL: https://jai.in.ua/archive/2023/ai_mono.pdf (дата звернення: 11.10.2024).

7. El Hajj H. Decision-Making in the Digital Age: How Technology Is Transforming Our Choices. 2023. URL: https://www.linkedin.com/pulse/decision-making-digitalage-how-technology-our-choices-hassan-el-hajj (data of access: 11.10.2024).

8. Janbi N., Katib I., Albeshri A., Mehmood R. Distributed artificial intelligence-as-a-service (DAIaaS) for smarter IoE and 6G environments. *Sensors (Switzerland)*. 2020. 20. DOI: https://doi.org/10.3390/s20205796.

9. Janbi N., Katib I., Mehmood R. Distributed artificial intelligence: Taxonomy, review, framework, and reference architecture. *Intelligent Systems with Applications*. 2023. Volume 18. DOI: https://doi.org/10.1016/j.iswa.2023.200231. URL: https://www.sciencedirect.com/science/article/pii/S266730532300056X (data of access: 11.10.2024).

10. Makarenko O., Borysenko O., Horokhivska T., Kozub V., Yaremenko D. Embracing Artificial Intelligence in Education: Shaping the Learning Path for Future Professionals. *Multidisciplinary Science Journal*. 2024. Vol. 6. Article ID 2024ss0720. DOI: https://doi.org/10.31893/multiscience.2024ss0720

11. Mohsen Soori, Fooad Karimi Ghaleh Jough, Roza Dastres, Behrooz Arezoo AI-Based Decision Support Systems in Industry 4.0. A Review. *Journal of Economy and Technology*. 2024. DOI: https://doi.org/10.1016/j.ject.2024.08.005.

12. Ross W. Approaches for Decision-making. New Era Organizations. Medium. 2024. URL: https://medium.com/painless-management/approaches-for-decision-making-3870bcc5161e (data of access: 11.10.2024).

13. Shen Li and al. PyTorch distributed: Experiences on accelerating data parallel training. *Proceedings of the VLDB Endowment*. 2020. vol. 13. no. 12, pp. 3005–3018. DOI: https://doi.org/10.14778/3415478.3415530

УДК 004.056.5
DOI https://doi.org/10.32689/maup.it.2024.4.13

Богдан КОРНІЄНКО
доктор технічних наук, професор, професор кафедри інформаційних систем та технологій, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського, bogdanko@gmx.net
***ORCID:** 0000-0002-2521-0878*

Леся ЛАДІЄВА
кандидат технічних наук, доцент, доцент кафедри технічних та програмних засобів автоматизації, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», lrynus@yahoo.com
***ORCID:** 0000-0002-1706-0072*

Ксенія УЛЬЯНИЦЬКА
кандидат технічних наук, доцент кафедри інформаційних систем та технологій, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», ulianitskaya.k@gmail.com
***ORCID:** 0000-0003-0240-6250*

Лілія ГАЛАТА
доктор філософії, доцент кафедри кібербезпеки,
Національний авіаційний університет, galataliliya@gmail.com
***ORCID:** 0000-0002-7978-3954*

Андрій НЕСТЕРУК
аспірант кафедри інформаційних систем та технологій, асистент кафедри інформаційних систем та технологій, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», aonesterukr@gmail.com
***ORCID:** 0000-0002-1563-7245*

ЗАХИСТ КРИТИЧНИХ РЕСУРСІВ ВЕБ-ЗАСТОСУНКУ З ОРЕНДИ НЕРУХОМОСТІ

***Анотація. Мета** цієї роботи полягає в розробці системи захисту веб-застосунку з використанням сучасних технологій програмування та розроблення бази даних, яка буде стійкою до змін та сторонніх втручань, буде здатна запобігати неавторизованому доступу до веб-застосунку з оренди нерухомості.*

***Методологія**, використана в роботі, полягає у розробці системи захисту веб-додатків з використанням сучасних технологій NET Framework, ASP. NET Core, EF, SSMS, Swagger. Система стійка до змін і стороннього втручання, здатна запобігти несанкціонованому доступу. Описано найпопулярніші готові сервіси для реалізації відповідного захисту.*

***Наукова новизна** роботи полягає у визначенні моделі білого списку розробки захищених веб-додатків та основні кроки реалізації моделі. Реалізовано модель білого списку для веб-додатку за допомогою системи ролей і доступу. Розроблено серверну частину веб-додатку, яка включає вбудований функціонал основних методів запобігання злому. Розроблено метод доступу до приватної інформації користувача за допомогою алгоритму шифрування Rijndael.*

***Висновки**, зроблені на основі проведених досліджень, підкреслюють важливість захисту веб-додатків від зловмисників, що залежить від технологій і компонентів, які використовуються при створенні веб-додатків, а також відможливих вразливостей цих компонентів. Існують різні класифікації вразливостей, кожна атака через вразливість має свої особливості, а причиноювразливостей є помилки в розробці, реалізації та застосуванні компонентів веб– додатків, звідси необхідність пошуку і протидії вразливостям.*

В результаті створено програмний продукт, веб-застосунок для оренди та продажу нерухомості із вбудованою системою захисту інформації. Архітектура проекту запобігає загрозі SQL-ін'єкцій. Таким чином, представлена робота робить значний внесок у сферу захисту критичних ресурсів веб-застосунку, пропонуючи інноваційні підходи до протидії загрозам та покращуючи ефективність цього процесу. Ця програма стане незамінним інструментом для інженерів та аналітиків, сприяючи підвищенню якості захисту критичних ресурсів веб-застосунку.

***Ключові слова:** веб-додаток; безпека; система захисту; загрози; білий список; модель.*

Bogdan KORNIYENKO, Lesya LADIEVA, Kseniia ULIANYTSKA, Liliia GALATA, Andrii NESTERUK. PROTECTION OF CRITICAL RESOURCES OF THE REAL ESTATE RENTAL WEB APPLICATION

***Abstract. The purpose** of this work is to develop a web application protection system using modern programming technologies and database development, which will be resistant to changes and third-party interventions, will be able to prevent unauthorized access to the real estate rental web application.*

The methodology *used in the work consists in the development of a web application protection system using modern technologies NET Framework, ASP. NET Core, EF, SSMS, Swagger. The system is resistant to changes and third-party intervention, capable of preventing unauthorized access. The most popular ready-made services for the implementation of appropriate protection are described.*

The scientific novelty *of the work consists in defining the white list model for the development of secure web applications and the main steps of implementing the model. Implemented a whitelist model for a web application using a role and access system. The server part of the web application has been developed, which includes the built-in functionality of the main hacking prevention methods. A method of accessing private user information using the Rijndael encryption algorithm has been developed.*

The conclusions *drawn from the conducted studies emphasize the importance of protecting web applications from attackers, which depends on the technologies and components used in the creation of web applications, as well as on the possible vulnerabilities of these components. There are different classifications of vulnerabilities, each vulnerability attack has its own characteristics, and the cause of vulnerabilities is errors in the development, implementation and application of components of web applications, hence the need to find and counter vulnerabilities.*

As a result, a software product was created, a web application for renting and selling real estate with a built-in information protection system. The architecture of the project prevents the threat of SQL injections. Thus, the presented work makes a significant contribution to the protection of critical web application resources, offering innovative approaches to countering threats and improving the effectiveness of this process. This program will become an indispensable tool for engineers and analysts, helping to improve the quality of protection of critical web application resources.

Key words: *web application; security; protection system; threats; white list; model.*

Вступ. Постановка проблеми. Захист веб-ресурсів залишається одним із важливих напрямків інформаційної безпеки. Щороку кількість веб-ресурсів збільшується, зростає також кількість конфіденційної інформації, яка локалізується на серверах віддаленого доступу (особливо із використанням хмарних технологій).

У результаті цього зростають не тільки кількість атак на веб-ресурси, але й економічні наслідки таких атак. Останнім часом вразливість веб-ресурсів до атак отримала політичний вимір унаслідок як поширення гібридних війн у світі, так і зростання терористичних загроз.

Зі збільшенням залежності компаній будь-якого напрямку діяльності від ІТтехнологій, гостро постає питання забезпечення інформаційної безпеки. Одним з ключових заходів в забезпеченні інформаційної безпеки компанії є тестування на проникнення. Це дозволяє упевнитися в надійності захисту від несанкціонованого доступу та інших загроз інформаційної безпеки [1–7].

Сьогодні веб-вразливості перевершують за кількістю і можливій шкоді будь-які інші проблеми інформаційної безпеки. Більшість зовнішніх атак на корпоративні інформаційні системи націлені саме на вразливості веб-додатків.

Аналіз попередніх досліджень. Для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів, в якому вбудовані механізми перевірки, шифрування та валідації вхідних даних [8–16].

На даний час найбільш розповсюдженими методологіями проведення тестування на проникнення є:

- The Open Source Security Testing Methodology Manual (OSSTMM);
- The National Institute of Standards and Technology (NIST) SpecialPublication 800-115;
- OWASP Testing Guide;
- Penetration Testing Execution Standard (PTES);
- Information Systems Security Assessment Framework (ISSAF);
- BSI – Study A Penetration Testing Model.

Методологія The Open Source Security Testing Methodology Manual (OSSTMM) є досить формалізованим і добре структурованим документом для тестування мережі. Документ має так звану «Карту безпеки» – візуальний показник безпеки. На карті вказуються основні галузі безпеки, які включають в себе набори елементів, які повинні бути протестовані на відповідність методиці [17-19].

Методологія NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment. Створена і підтримується підрозділом NIST та виділяє як мінімум 3 фази проведення оцінювання інформаційної безпеки: планування, виконання, пост-експлуатація (аналізотриманих даних, виявлення причин що призвели до появи вразливостей, розробка рекомендацій до знешкодженню вразливостей і розробка звіту). У розділі «Техніки оцінки вразливостей мети», в як одна з технік описуються Тестина проникнення, а саме Фази і Логістика тестів [20].

Методологія OWASP (Open Web ApplicationSecurity Project) Testing Guide.OWASP (Open Web Application Security Project) -міжнародне відкрите співтовариство, яке орієнтоване на поліпшення безпеки програмного забезпечення. OWASP Testing Guide є більш широкою методологію в порівнянні з іншими, тому що дає вказівки не тільки по тестах на проникнення, але і з аналізу веб-додатків в цілому

(наприклад – вихідного коду), оскільки ця методика фокусує свою увагу саме на виявленнях вразливостей веб-додатків [21].

Методологія PTES – Penetration Testing Execution Standard – Technical Guidelines. Стандарт, розроблений для об'єднання як бізнес вимог, так і можливостей служб безпеки, і масштабування тестів на проникнення. На першому підготовчому етапі детально розглядаються встановлюються канали комунікацій, правила взаємодії і контролю, конкретні способи реагування і моніторингу інцидентів. Далі виділені наступні етапи: збір інформації; моделювання загроз; методи аналізу вразливостей; забезпечення обходу контрзаходів і виявленнянайкращого шляху атаки; пост-експлоітація – аналіз інфраструктури, подальше проникнення вінфраструктуру, зачистка і живучість [22].

Методологія ISSAF – Information System Security Assessment Framework. Розроблено для внутрішніх контрольних перевірок. Документ охоплює величезну кількість питань, пов'язаних з інформаційною безпекою. Описана оцінка безпеки міжмережевих екранів, маршрутизаторів, антивірусних систем і багато іншого. Методологія ISSAF дозволяє змоделювати вимоги до внутрішніх заходів з безпеки, і направлена на оцінку безпеки комп'ютерних мереж, систем та додатків [23].

Методологія BSI – Study A Penetration Testing Model.Розроблено німецьким підрозділом «Federal Office for Information Security ». У документі описується проведення коректних випробувань системи на міцність. Детально описуються тільки сама методологія тестів, але і необхідні вимоги, правові аспекти застосування методології та процедури, які необхідно виконати для успішного проведення тестів. Наводиться класифікація тестів на міцність івизначені її критерії [24].

Метою статті є розробка системи захисту веб-застосунку з використанням сучасних технологій програмування та розроблення бази даних, яка буде стійкою до змін та сторонніх втручань, буде здатна запобігати неавторизованому доступу до веб-застосунку.

Виклад основного матеріалу. Проаналізувавши проблему створення веб-застосунків встановили, що ця проблема актуальна і має спільні риси з загальною концепцією створення безпечного прикладного забезпечення. Дана проблема частково залежить від механізмів захисту використовуваних веб-каркасів на яких будується веб-застосунок, використовуваній базі даних, безпеки в цілому від сервера на якому виконується веб-застосунок. Розроблено серверну частину веб-застосунку, що містить в собі функціонал запобігання методам злому.

Метод білий список для забезпечення безпеки у веб-застосунках

Концепція білого списку загально відома і використовується досить давно у багатьох сферах ще до появи інформаційних і цифрових технологій. В теорії використання моделі білого списку під час безпечної розробки веб– застосунків дозволяє запобігати деяким вразливостям які ігноруються усіма відомими веб-каркасами [25–28].

Веб-фреймворки запобігають більшості відомих вразливостям веб-додатків таких як SQL-ін'єкції, XXS, але вони не можуть запобігти деяким специфічним вразливостям які притаманні саме конкретній програмі яка розробляється деяким фреймворком, відповідальність за запобігання таких вразливостей залишається за розробниками.

Невідповідність між очікуваною і реальною поведінкою веб-застосунку може являтися індикатором атаки на веб-застосунок. Дана робота зосереджена на OWASP 4 і 7 вразливостях: небезпечні прямі посилання на об'єкти. відсутність контролю доступу функцій. Реалізовано механізм безпеки для веб-застосунку шляхом передбачення дозволених операцій. У роботі визначено, створено і впроваджено список дозволених взаємодій веб-застосунку. Ці правила керують HTTP-запитами і відповідями які обробляє веб-застосунок. Визначення елементів які входять до білого списку повинно розроблятися під час етапу проектування.

Формальне визначення моделі білого списку розробки безпечних веб-застосунків

Визначимо білий список як набір чотирьох множин {C, D, W, S}, де:

C – множина елементів {u, c_1, c_2,...,c_n}, де c_1, c_2,...,c_n – складові компонент які входять в межі системи, а u компоненти які за межею системи;

D – множина елементів {d_1, d_2,...,c_n}, де d_1, d_2,...,c_n стани компонентів;

W – множина впорядкованих пар {($c_{o,}$ c_d) : $c_{o,}$ c_d є C} кожна пара представляє собою перехід з початкового компоненту c_0 до кінцевого c_d;

S – матриця розмірності |C| X |C| $S_{co,\ cd}$ = $c_{безпечний(safe)}$ визначає безпечні компоненти {c_s : c_s є C} де c_d не може слідувати з c_o.

Кожна комірка матриці розмірності |C| X |C| містить унікальну підмножину x, {x: x ⊆ D}. Якщо оцінка станів x повертає 1, то упорядкована пара переходу стану з $c_{початковий(origin)}$ до $c_{кінцевий}$-(destination) додається до множини W.

Перехід з однієї складової до іншої керується функцією переходу де перехід з $c_{початковий}$ до $c_{кінцевий}$ відбувається тоді і тільки тоді якщо ($c_{o,}$ c_d) є W, інакше функція переходу визивається через (c_o, $S_{co,\ cd}$).

$$T(c_0, c_d) = \begin{cases} c_d, якщо (c_0, c_d) \in W \text{ інакше} \\ T(c_0, S_{c_0 c_d}) \end{cases}$$

Визначено кілька операцій які виконуються за допомогою білого списку. Операції поділені на дві категорії відповідно до того коли вони можуть бути застосовані. Наступні операції будуть використовуватися під час розробки:

– створення ($c_{o,}$ c_d) у множині W: додавання впорядкованої пари до множини;
– видалення ($c_{o,}$ c_d) з множини W: видалення впорядкованої пари з множини;
– введення {d_x} до множини D: додавання станів d_x до множини D;
– видалення {d_x} з множини D: видалення станів d_x з множини D;
– додавання {d_x} до підмножини x множини $W_{co,cd}$;
– видалення {d_x} з підмножини x множини $W_{co,cd}$;
– введення {c_s} у комірку матриці $S_{co,cd}$;
– оновлення {c_s} у комірці матриці.

Операції білого списку які дозволені при виконані:

– обчислення T($c_{o,}$ c_d);
– верифікація c_o à c_d:

c_d може слідувати до c_o якщо дане твердження хибне, то усі стани які належать підмножині x у $W_{co,cd}$ будуть повертати істину. Інакше перехід до безпечного стану c_s.

Множина усіх компонентів C і відношень W можуть бути представлені у вигляді двійкової матриці, де 1 означає дозволений перехід стану а 0 означає не дозволений. Кожна комірка матриці прийматиме значення або 0 або 1 відповідно до значень підмножини станів. Матриця S міститиме безпечні переходи станів у випадку коли перехід стану з c_o до c_d не буде дозволений.

Кроки впровадження моделі

В першу чергу потрібно ідентифікувати дозволену поведінку веб– застосунку шляхом створення діаграми яка буде відображати яким чином поводить себе програма. Діаграма повинна відображати усі дозволені взаємодії міжкомпонентами застосунку. Потрібно дослідити кожну операцію і ідентифікувати підмножину переходів станів (c_o,c_d) і помістити їх у відповідні комірки матриці W. Також потрібно ідентифікувати безпечні компоненти і переходи у разі повертанні хибного значення перевірки дозволу переходу стану. Безпечні компоненти c_s слід помістити у комірки які відповідають (c_o,c_d) у матриці W до матриці S. Отже на даному етапі розробки ми маємо підмножини переходу станів які записані у матрицю W і приймають значення 1 або 0 в залежності від дозволу переходів станів. Для простоти назвемо таке представлення як M, де

|C| X |C| = M де $M_{co,cd}$ = 1 якщо (c_o,c_d) є W і $M_{co,cd}$ = 0 якщо (c_o,c_d) не належить W. Модель білого списку може змінюватися або доповнюватися в залежності від ходу розробки. Варто також зазначти що, стани в множині D повинні бути простими а не комплексними.

Основні кроки побудови моделі білого списку:

– створити діаграму яка відображає назначену допустиму поведінку веб –застосунку;
– задати підмножини станів за для змоги аналізу і визначення дозволених переходів і взаємозв'язків застосунку;
– розмістити кожну підмножину переходу станів c_o,c_d відповідну коміркуматриці |C|x|C|;
– ідентифікувати безпечні компоненти c_s і розмістити їх у комірки які відповідають (c_o,c_d) у матриці W до матриці S;
– присвоїти значення 1 або 0 для кожної підмножини переходу станів взалежності відповідності білого списку;
– $M_{co,cd}$ = 1 якщо (c_o,c_d) є W і $M_{co,cd}$ = 0 якщо (c_o,c_d) не належить;
– належним чином налаштувати процес розробки для впровадження методики білого списку в уже існуючий процес розробки на будь-якому етапі.

Реалізація методу білий список для веб-застосунків

Розглядається веб-застосунок, який вимагає обов'язкову аутентифікацію користувача для можливості його використання. Застосунок дозволяє 3 спроби аутентифікації. Якщо користувач успішно пройде аутентифікацію застосунок пере направить користувача на його персональну сторінку. Користувач матиме змогу редагувати свій профіль або зв'язатися з іншими користувачами. Користувач також має змогу вийти зі свого профілю в будь-який час.

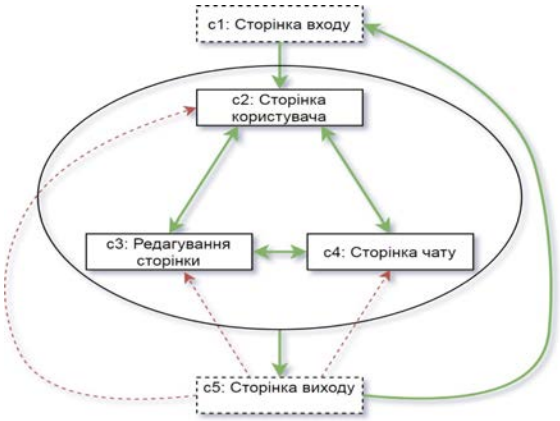


Рис. 1. Приклад діаграми, яка відображає поведінку програми

Модель за стосунку даного прикладу складається з 5 компонент. C = {u, c_1,c_2, c_3, c_4, c_5}. U представляє собою компоненти за границею системи і включаєтьсядо C за для повноти. Щодо глобальної множини станів D, припустимо що вони означають наступні стани:

- d1: користувач анонімний.
- d2: коистувач авторизований.
- d3: час існування сесії валіний.
- d4: попереднє представлення.
- d5: представлення підпослідовності
- d6: спроби аутентифікації < 3.

Білий список містить підмножину D у кожній комірці матриці. Для прикладу, білий список нижче відображає підмножину дозволених переходів станів з c_1, c_2 і іншу підмножину яка приводить до недозволеного переходу з c_5 до c_4. Для дозволеного переходу з c_1 до c_2, підмножина станів: x = {d_2, d_3, d_4 = login view, d_5 = user portal view, d_6}. Усі стани у x мають повертати істину. Для недозволених переходів з c_5 до c_4, підмножина станів x = {d_2, d_3, d_4 = edit profile view або user portal view, d_6}.

Очевидно, перехід з стану c_5 до c_4 не дозволений, бо перший стан у підмножині d_2 не може бути досягненим якщо користувач вийшов з аканту. Заповнимо наші переходи у матрицю переходів станів.

Нехай множина впорядкованих пар переходу станів наступна

W = {(u; u) ; (u; c1) ; (c1; c1) ; (c1; c2) ; (c2; c2) ; (c2; c3) ; (c2; c4) ; (c2; c5) ;(c3; c2) ; (c3; c3) ; (c3; c4) ; (c3; c5) ; (c4; c2) ; (c4; c3) ; (c4; c4) ; (c4; c5) ; (c5; c1)}

Наступник крок це заповнити матрицю S безпечними компонентами для перенаправлення переходу на безпечний стан якщо він не дозволений.

Таким чином, проаналізована концепція типового використання білого списку у IT а також розроблена модель білого списку і методика використання даної моделі для розробки безпечних веб-застосунків. А також приклад використання. Можна зробити висновок, що будь-яку концепцію захисту чи розмежування доступу можна адаптувати під будь-який процес, а саме під процес розробки захищених веб-застосунків. Згідно аналізу створеного прикладу модель являється працюючою і успішно забезпечує безпеку спроектованого застосунку.

Захист критичних ресурсів веб-застосунку

Для реалізації проекту використовували ASP.NET – технологію створення веб-застосунків і веб-сервісів, яка була створена компанією Microsoft. Ця технологія є основною частиною платформи Microsoft.NET і розвитком старішої технології Microsoft ASP. На цей час останньою версією цієї технології є ASP.NET Core 2.0 [29-30].

Засіб Web API засноване на додаванні в додаток ASP.NET MVC Framework контролера спеціального виду. Цей різновид контролерів, яка називається контролером API, володіє двома характеристиками:

- методи дій повертають об'єкти моделей, а не об'єкти типу ActionResult;
- методи дій вибираються на основі HTTP-методу, використовуваного в запиті.

На рис. 2 зображено Структура додатку, написаного за допомогою технології ASP.NET Web API.

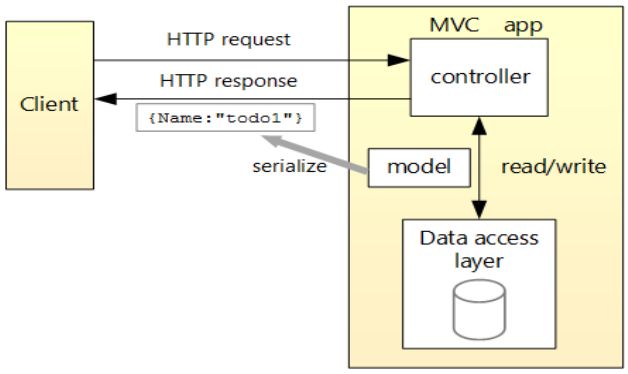


Рис. 2. Структура додатку, написаного за допомогою технології ASP.NET Web API

Кожен великий проект використовує паттерни для кращої структуризації коду та його підтримки в майбутньому.

Основні можливості програми показано на діаграмі прецедентів (рис. 3):

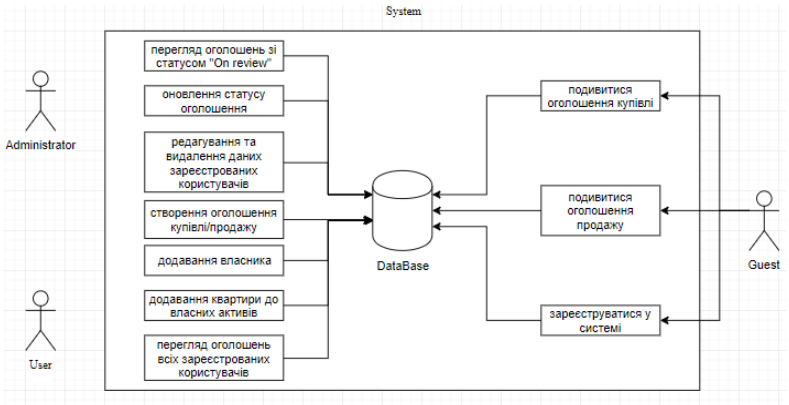


Рис. 3. Діаграма прецедентів

Для розробки системи використовувалась об’єктно-орієнтована мова програмування C# та наступні технології: .NET Framework, ASP.NET Core, EF, SSMS, Swagger. Для побудови запитів до БД обрано мову SQL. На рис. 4 наведено вигляд сайту для користувача.

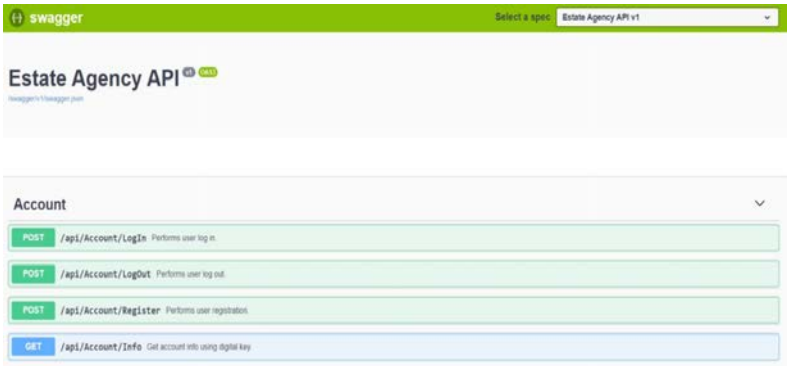


Рис. 4. Вигляд сайту

Сервер автентифікації Microsoft Identity Web – це набір бібліотеки ASP.NET Core, розширення підтримки авторизації веб-додатків та веб-API, інтегрованих з платформою Microsoft Identity. Він надає зручний високопродуктивний API рівня, зв'язуючий ASP.NET Core, за допомогою проміжного слова для перевірки справжності та бібліотеки перевірки підлинності Майкрософт (MSAL) для .NET.

Реалізоване запобігання SQL-ін’єкціям. SQL-ін’єкція є виконанням довільного запиту до бази даних додатка за допомогою поля форми або параметра URL. У разі використання стандартної мови Transact

SQL можливо вставити шкідливий код. Внаслідок чого будуть отримані, змінені або видалені дані таблиць. Щоб запобігти цьому, використайте запити, які параметризуються, які підтримуються більшістю мов веб-програмування.

Висновки. В результаті створено програмний продукт, веб-застосунок для оренди та продажу нерухомості із вбудованою системою захисту інформації. Архітектура проекту запобігає загрозі SQL-ін'єкцій. За допомогою системи ролей та доступів реалізовано модель білого списку. За допомого алгоритму шифрування Rijndael розроблено метод доступу до приватної інформації користувача.

Захист веб-додатків від зловмисників залежить від технологій і компонентів, що використовуються при створенні веб-додатків, а також відможливих вразливостей цих компонентів. Існують різні класифікації вразливостей, кожна атака через вразливість має свої особливості, а причиноювразливостей є помилки в розробці, реалізації та застосуванні компонентів веб– додатків, звідси необхідність пошуку і протидії вразливостям.

Список використаних джерел:

1. Галата Л. П., Корнієнко Б. Я., Заболотний В. В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. *Наукоємні технології*. 2019. Том 43. № 3. С. 300–306.
2. Корнієнко Б. Я., Галата Л. П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. *Моделювання та інформаційні технології*. 2018. Вип. 83. С. 34–42.
3. Корнієнко Б. Я. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології*. 2017. № 4 (36). С. 316–322.
4. Корнієнко Б. Я., Юдін О. К., Снігур О. С. Безпека аутентифікації у web-ресурсах. *Захист інформації*. 2012. № 1 (54). С. 20–25. DOI: 10.18372/2410– 7840.14.2056 (ukr).
5. Корнієнко Б. Я., Максімов Ю. О., Марутовська Н. М. Прикладні програми управління інформаційними ризиками. *Захист інформації*. 2012. № 4 (57). С. 60–64. DOI: 10.18372/2410-7840.14.3493 (ukr).
6. Корнієнко Б. Я. Безпека інформаційно-комунікаційних систем та мереж. Навчальний посібник для студентів спеціальності 125 «Кібербезпека». К.: НАУ, 2018. 226 с.
7. Корнієнко Б. Я., Галата Л. П. Оптимізація системи захисту інформації корпоративної мережі. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2019. Випуск 19. С. 56–62.
8. Корнієнко Б. Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. Наукоємні технології. 2012. № 3 (15). С. 83–89, doi.org/10.18372/2310– 5461.15.5120 (ukr).
9. Корнієнко Б. Я., Галата Л. П. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології*. 2017. № 4 (36). С. 316–322. doi.org/10.18372/2310-5461.36.12229.
10. Корнієнко Б. Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив :монографія. К.: Вид-во Аграр Медіа Груп. 2014. 288 с.
11. Корниенко Б. Я. Кибернетическая безопасность – операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2017. 122 P.
12. Корниенко Б. Я. Информационная безопасность и технологии компьютерных сетей: монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2016. 102 с.
13. Galata L., Korniyenko B., Yudin A. Research of the simulation polygon for the protection of critical information resources. CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017), 30 Nov 2017, Kyiv, Ukraine. vol. 2067. P. 23–31. urn:nbn:de:0074-2067-8.
14. Kornienko Y. M., Liubeka A. M., Sachok R. V., Korniyenko B. Y. Modeling of heat exchangement in fluidized bed with mechanical liquid distribution. *ARPN Journal of Engineering and Applied Sciences*. 2019. No14 (12). P. 2203–2210.
15. Korniyenko B. Modeling of information security system in computer network. *Безпека інформаційних систем і технологій*. 2019. Том №1 (1). С.36–41.
16. Korniyenko B., Galata L. Implementation of the information resources protection based on the CentOS operating system. Conference Proceedings of 2019 IEEE 98 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON -2019) July 2-6, 2019, Lviv, Ukraine. P. 1007–1011.
17. Korniyenko B., Yudin A., Galata L. Risk estimation of information system. // *Wschodnioeuropejskie Czasopismo Naukowe*. 2016. № 5. P. 35–40.
18. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. Conference Proceedings of 2019 IEEE Inernational Conference on Advanced Trends in Information Theory (IEEE ATIT-2019) Dezember 18-20, 2019, Kyiv, Ukraine. P. 244–248.
19. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2019) Kyiv, Ukraine, November 28, 2019. Vol-2577. P. 281–291.
20. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. *Наукоємні технології*. 2017. № 2 (34). С. 114–118.
21. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system // *Sciences of Europe*. 2016. V. 2. No 2 (2). P. 61–63.
22. Korniyenko B. The classification of information technologies and control systems // *International scientific journal*. 2016. № 2. P. 78–81.

23. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources. CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) Kyiv, Ukraine, November 27, 2018. Vol-2318. P. 176–187. urn:nbn:de:0074-2318-4

24. Korniyenko B., Yudin O., Novizkij E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*. 2013. Issue 8. P. 53–56.

25. Korniyenko B., Ladieva L., Galata L. Control system for the production of mineral fertilizers in a granulator with a fluidized bed. 2020 2nd IEEE International Conference on Advanced Trends in Information Theory. 2020. No 9349344. P. 307–310.

26. Kornienko Y. M., Haidai S. S., Sachok R. V., Liubeka A. M., Korniyenko B. Y. Increasing of the heat and mass transfer processes efficiency with the application of non-uniform fluidization. *ARPN Journal of Engineering and Applied Sciences*. 2020. No 15(7). P. 890–900.

27. Korniyenko B., Kornienko Y., Haidai S., Liubeka A., Huliienko S. Conditions of Non-uniform Fluidization in an Autooscillating Mode. Advances in Computer Science for Engineering and Manufacturing. ISEM 2021 Lecture Notes in Networks and Systems. 2022. No 463. P. 14–27.

28. Korniyenko B., Kornienko Y., Haidai S., Liubeka A. The Heat Exchange in the Process of Granulation with Non-uniform Fluidization. Advances in Computer Science for Engineering and Manufacturing. ISEM 2021 Lecture Notes in Networks and Systems. 2022. No 463. P. 28–37.

29. Korniyenko B. Y. The two phase model of formation of mineral fertilizers in the fluidized–bed granulator. *The Advanced Science Journal*. 2013. № 4. P. 41–44.

30. Zhulynskyi A. A., Ladieva L. R., Korniyenko B. Y. Parametric identification of the process of contact membrane distillation. *ARPN Journal of Engineering and Applied Sciences*. Volume 14. Issue 17. September 2019. P. 3108–3112.

УДК 004.738.5:004.42
DOI https://doi.org/10.32689/maup.it.2024.4.14

Максим КУНДОС
кандидат технічних наук, старший викладач кафедри інформаційних систем та обчислювальних методів, ПВНЗ «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука», Kundosm@gmail.com
***ORCID:** 0009-0001-0310-357*

Людмила СОЛОВЕЙ
старший викладач кафедри інформаційних систем та обчислювальних методів
ПВНЗ «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука», lyuda_solovej@ukr.net
***ORCID:** 0009-0001-2832-1741*

WEB ДОДАТКИ У ЕКОСИСТЕМІ IOT

Анотація. *Інтернет речей (IoT) є динамічною технологічною галуззю, яка охоплює численні сфери, включаючи промисловість, транспорт, охорону здоров'я, енергетику та сільське господарство. IoT дозволяє автоматизувати процеси та забезпечити ефективний обмін даними між різноманітними пристроями через мережу, створюючи інтегровані екосистеми.*

Мета. *Аналіз архітектури та функціональних можливостей Web-додатків в екосистемі IoT, визначення їх переваг та недоліків, а також розробка рекомендацій щодо подолання існуючих проблем.*

Методологія. *У статті розглядається концепція IoT, його архітектура, функціональні можливості та основні області застосування. Особливу увагу приділено IoT Web-додаткам, які виступають основним інтерфейсом взаємодії користувачів з IoT-системами, надаючи можливість дистанційного контролю, автоматизації процесів і аналітики даних у реальному часі. Представлено аналіз переваг та недоліків IoT Web-додатків, таких як зручність використання, інтеграція з різними системами, але також і проблеми, що виникають у вигляді ризиків безпеки, проблем із сумісністю та залежності від стабільного інтернет-з'єднання. Окремо розглядаються сучасні підходи для подолання існуючих проблем у використанні IoT Web -додатків, включаючи новітні технології, що підвищують безпеку, ефективність та знижують витрати, такі як блокчейн, Edge Computing та штучний інтелект.*

Наукова новизна. *У статті також підкреслюється важливість розробки єдиних стандартів для сумісності між пристроями різних виробників, що дозволить створювати ефективні та адаптивні IoT-системи. Запропоновані рішення мають на меті розширити використання IoT у повсякденному житті та бізнесі, сприяючи подальшій цифровій трансформації та підвищенню рівня автоматизації та продуктивності в різних галузях.*

Висновки*. Подальший розвиток технологій, таких як 5G і квантові обчислення, та різних систем захисту, відкриває нові перспективи для масштабування IoT-рішень, забезпечуючи більш швидкий і надійний зв'язок, який стане основою для створення ще складніших і потужніших IoT-екосистем.*

Ключові слова: *Інтернет речей, IoT, Web-додаток, архітектура IoT, автоматизація, безпека даних, екосистема.*

Maksym KUNDOS, Liudmyla SOLOVEI. IOT WEB APPLICATIONS IN THE ECOSYSTEM

Abstract. *The Internet of Things (IoT) is a dynamic technology industry that spans numerous fields, including industry, transportation, healthcare, energy, and agriculture. IoT enables the automation of processes and the efficient exchange of data between various devices over the network, creating integrated ecosystems.*

The purpose of the work. *Analysis of the architecture and functionality of Web applications in the IoT ecosystem, determination of their advantages and disadvantages, as well as development of recommendations for overcoming existing problems.*

Methodology. *The article discusses the concept of IoT, its architecture, functionality and main areas of application. Special attention is paid to IoT Web-applications, which act as the main interface of user interaction with IoT-systems, providing the possibility of remote control, automation of processes and real-time data analytics. An analysis of the advantages and disadvantages of IoT Web applications is presented, such as ease of use, integration with different systems, but also the problems that arise in the form of security risks, compatibility problems and dependence on a stable Internet connection. Modern approaches to overcome existing problems in the use of IoT Web applications are separately considered, including the latest technologies that increase security, efficiency and reduce costs, such as blockchain, edge computing and artificial intelligence.*

Scientific novelty. *The article also emphasizes the importance of developing common standards for interoperability between devices from different manufacturers, which will allow creating efficient and adaptive IoT systems. The proposed solutions aim to expand the use of IoT in everyday life and business, contributing to further digital transformation and increasing the level of automation and productivity in various industries.*

Conclusions. *The further development of technologies such as 5G and quantum computing and various protection systems opens up new perspectives for scaling IoT solutions, providing faster and more reliable communication, which will become the basis for creating even more complex and powerful IoT ecosystems.*

Key words: *Internet of Things, IoT, Web application, IoT architecture, automation, data security, ecosystem.*

Постановка проблеми. З розвитком IoT постає проблема інтеграції численних пристроїв у єдину ефективну систему, яка забезпечуватиме безперервний обмін даними, безпеку та ефективність роботи. Одним з ключових елементів цієї екосистеми є Web-додатки, що забезпечують користувачам можливість взаємодії з пристроями та аналізу отриманих даних.

Аналіз останніх досліджень і публікацій. Інтернет речей (IoT) є технологією, що швидко розвивається і все більше впливає на різні аспекти життя і бізнесу. Сучасні дослідження охоплюють питання інтеграції нових технологій, таких як 5G, блокчейн, а також розглядають їх використання в різних сферах, включаючи промисловість, енергетику та міську інфраструктуру.

Дослідники [1, 2] підкреслюють важливість інтеграції технології 5G з IoT-системами для підвищення їх продуктивності. Вони зазначають, що 5G значно підвищує швидкість передачі даних, зменшує затримки та покращує стабільність мережі, що особливо важливо для застосувань у реальному часі, таких як автономний транспорт, промислова автоматизація та інтелектуальне відеоспостереження.

Автори [5] розглядають, як IoT допомагає в управлінні міською інфраструктурою. Вони аналізують різні системи, які дозволяють контролювати освітлення, управління трафіком, водопостачання та збір відходів.

Дослідники [9] аналізують можливості використання блокчейн-платформ для децентралізованого управління доступом до IoT-пристроїв. Вони зазначають, що використання блокчейну дозволяє забезпечити надійний захист від несанкціонованого доступу та підробки даних завдяки незмінності записів і прозорості транзакцій.

Автори [6] висвітлюють використання IoT для управління електричними мережами. Вони підкреслюють важливість сенсорів та розумних лічильників для моніторингу споживання енергії та забезпечення безперебійної роботи електромереж.

Дослідники [7] охоплюють огляд застосування IoT у розумних містах, включаючи енергетику, транспорт та охорону здоров'я. Вони аналізують, як різні стандарти допомагають інтеграції IoT-систем, підвищують ефективність управління міськими ресурсами та сприяють розвитку.

Попри зусилля дослідників, деякі ключові аспекти залишаються відкритими для подальших досліджень. Актуальним залишаються питання забезпечення безпеки даних, що генеруються та передаються IoT-пристроями. Крім того, проблема високих витрат на впровадження та інтеграцію систем, складність налаштування різних протоколів зв'язку, а також необхідність забезпечення безперебійного підключення до мережі вимагають подальшого дослідження та розробки інноваційних підходів.

Постановка завдання. Здійснити аналіз архітектури та функціональних можливостей Web-додатків в екосистемі IoT. Розглянути сучасні технології для покращення безпеки, ефективності інтеграції та зниження витрат на розробку і впровадження IoT-систем.

Виклад основного матеріалу. Інтернет речей (IoT) – це мережа розумних пристроїв, які можуть спілкуватися один з одним через інтернет. Вони працюють автономно, без участі людини, збираючи і передаючи дані, що допомагає автоматизувати різні процеси в повсякденному житті та бізнесі.

Найбільш поширені терміни в цьому середовищі: Internet of Things device та Internet of Things ecosystem.

Internet of Things device або IoT-пристрої – це будь-які предмети, що можуть підключатися до інтернету для обміну даними. Такими можуть бути звичні побутові речі, як розумні лампи чи холодильники, промислове обладнання, медичні прилади (кардіостимулятори), або навіть сенсори, вживлені у сільськогосподарських тварин. Вони мають свої унікальні ідентифікатори, що дозволяє їм спілкуватися через мережу та виконувати свої функції автоматично або за командою.

Internet of Things ecosystem або Екосистема IoT – це комплекс всіх елементів, які роблять можливим функціонування таких пристроїв. Вона включає самі пристрої, мережі, які забезпечують передачу даних, програмне забезпечення для обробки інформації та інтерфейси, через які користувачі взаємодіють з системами. Все це працює разом, забезпечуючи безперервний обмін даними і можливість керувати пристроями незалежно від того, де вони знаходяться [4].

Архітектура систем IoT є складною та багаторівневою, оскільки IoT-системи об'єднують величезну кількість пристроїв. Для розуміння цього питання важливо розглянути архітектуру IoT-системи, що зазвичай складається з декількох основних рівнів [13]:

1. Фізичний рівень (рівень пристроїв або сенсорів) – цей рівень включає датчики, пристрої та будь-які інші об'єкти, підключені до мережі, які збирають дані. Пристрої можуть бути оснащені мікроконтролерами, сенсорами, які здатні збирати дані з навколишнього середовища та взаємодіяти з ним. Дані, зібрані на цьому рівні, надсилаються для подальшої обробки до вищих рівнів.
2. Мережевий рівень (рівень передачі даних) – цей рівень відповідає за передачу даних від пристроїв до центральної системи або до інших пристроїв через мережі зв'язку. Зазвичай включає різні типи

комунікаційних протоколів, такі як Wi-Fi, Bluetooth, LTE, 4G тощо. Основним завданням цього рівня є безпечне та надійне транспортування даних від сенсорів до систем зберігання або обробки.

3. Рівень «хмари» – зібрані дані зберігаються, обробляються та аналізуються. Зазвичай використовується хмарна інфраструктура, яка забезпечує доступність даних для аналізу з будь-якої точки світу. Тут працюють аналітичні інструменти, машинне навчання, штучний інтелект для отримання цінної інформації з необроблених даних.

4. Рівень бізнес-логіки – цей рівень займається представленням результатів обробки даних користувачам через веб-інтерфейси або мобільні додатки. Web-додатки на цьому рівні дозволяють користувачам отримувати доступ до даних та управляти IoT-системами в реальному часі. Даний рівень також включає інтеграцію з іншими системами, інтерфейси для користувачів (графічні інтерфейси, API).

Web-додатки відіграють важливу роль в екосистемі IoT, забезпечуючи зручний і ефективний інтерфейс для взаємодії користувачів з IoT-пристроями. Вони створюють міст між фізичними об'єктами, які збирають і передають дані, і користувачами, які можуть керувати цими пристроями, отримувати інформацію та аналізувати її [11, с. 53].

IoT надає можливість автоматизувати і покращувати процеси в різних галузях, використовуючи зібрані дані від підключених пристроїв.

Основні типи Web-додатків в екосистемі IoT надані в табл. 1.

Так ми бачимо, що Web-додатки в екосистемі IoT охоплюють різні сфери застосування – від розумних будинків до промисловості та фінансів [3].

Web-додатки дозволяють користувачам взаємодіяти з IoT-системами через стандартний веб-браузер, що забезпечує зручний доступ до інформації, віддалене управління пристроями. Користувач може переглядати інформаційні панелі (dashboard), що в реальному часі відображають дані, зібрані IoT-пристроями (температура, тиск, стан обладнання тощо).

Web-додатки дозволяють користувачам контролювати стан підключених пристроїв, наприклад, у розумних будинках (smart homes), промислових системах (IIoT), або транспортних системах. Вони надають можливість віддаленого управління – користувачі можуть змінювати налаштування пристроїв, керувати режимами роботи або запускати команди для виконання певних завдань.

Важливою частиною екосистеми IoT є аналіз даних, що генеруються пристроями. Web-додатки можуть надавати засоби для аналітики даних, візуалізації результатів та побудови прогнозів на основі машинного навчання або алгоритмів обробки великих даних. Інтеграція з хмарними платформами

Таблиця 1

Типи Web-додатків в екосистемі IoT

Тип Web-додатків	Світові типи	Типи в Україні	Функції
Керування розумними будинками та пристроями	Google Home, Amazon Alexa, Philips Hue, Samsung SmartThings	Ajax Systems, додатки для розумних розеток та ламп	Керування пристроями в розумних будинках, налаштування правил і взаємодії між пристроями
Промислові IoT додатки	Siemens MindSphere, GE Predix, IBM Watson IoT, Cisco Kinetic	Delfast (розробка електробайків з IoT-системами)	Моніторинг стану обладнання, аналіз продуктивності, прогнозне обслуговування
Розумні міста (Smart Cities)	Barcelona's Smart City Platform, Smart Dubai, Streetline, Cleverciti	Kyiv Smart City	Управління міською інфраструктурою, моніторинг трафіку, контроль якості повітря
Здоров'я та медицина (e-Health)	Teladoc, HealthTap, AliveCor, iHealth MyVitals	Helsi.me, Medics	Відстеження стану здоров'я пацієнтів, автоматичні сповіщення про необхідність медичного втручання
Логістика та транспорт	Fleet Complete, Samsara, Verizon Connect, Shipwell	Nova Poshta (трекінг посилок), Meest Express	Відстеження транспортних засобів, планування маршрутів, управління автопарком
Енергетика та управління ресурсами	Schneider Electric EcoStruxure, Enel X, GridPoint, SolarEdge	ДТЕК (моніторинг енергоспоживання)	Моніторинг енергоспоживання, управління електромережами, інтеграція з відновлюваними джерелами
Сільське господарство	John Deere Precision Ag, CropX, FarmLogs, Climate FieldView	AgroOnline, SmartFarming	Контроль вологості ґрунту, прогнозування погоди, управління системами поливу
Фінанси та банківська справа	PayPal, Stripe Radar, Square, FICO Falcon Fraud Manager	Portmone, iPay.ua	Забезпечення безпеки транзакцій, моніторинг і аналіз для виявлення підозрілих дій

(наприклад, Amazon Web Services, Microsoft Azure або Google Cloud) дозволяє Web -додаткам отримувати доступ до потужних обчислювальних ресурсів і аналізувати величезні масиви даних [10].

Web-додатки в IoT можуть інтегруватися з різними сторонніми сервісами через API, забезпечуючи ефективність у використанні та обмін даними між різними системами. Наприклад, Web-додаток може інтегруватися з CRM-системою, автоматизованими системами управління підприємствами (ERP) або логістичними платформами для оптимізації бізнес-процесів [8].

Важливою роллю Web-додатків є забезпечення безпеки доступу до IoT-систем, що включає шифрування даних, аутентифікацію користувачів, захист від несанкціонованого доступу до пристроїв [12].

Попри всі переваги, використання IoT Web-додатків також стикається з певними недоліками. Переваги і недоліки використання IoT Web-додатків надано в табл. 2.

Аналізуючи вище надану інформацію, ми бачимо, що IoT Web-додатки мають значні переваги, такі як ефективне управління ресурсами, автоматизація процесів, покращення якості послуг та зручність використання. Проте існують і недоліки, пов'язані з безпекою, високими витратами на розробку та впровадження, а також залежністю від стабільного інтернет-з'єднання. Розвиток IoT технологій повинен зосереджуватись на вирішенні цих проблем, щоб забезпечити надійність та безпеку роботи систем.

Таблиця 2

Переваги та недоліки IoT Web-додатків

Тип веб-додатків	Переваги	Недоліки
Керування розумними будинками та пристроями	Дистанційне керування побутовими пристроями, зручність налаштування автоматизації	Залежність від стабільного інтернет-з'єднання, ризики безпеки
	Можливість інтеграції різних пристроїв у єдину систему для зручності користувача	Можливість зломів і несанкціонованого доступу до пристроїв, проблеми з конфіденційністю
Промислові IoT додатки	Моніторинг виробничих процесів, прогнозне обслуговування для зниження простоїв	Високі початкові витрати на встановлення, складність інтеграції з існуючими системами
	Аналіз даних для підвищення ефективності виробництва, автоматизація процесів	Необхідність захисту даних, особливо у випадку чутливих виробничих процесів
Розумні міста (Smart Cities)	Оптимізація міської інфраструктури, покращення якості послуг для громадян	Проблеми з конфіденційністю даних, зокрема відеоспостереження в публічних місцях
	Моніторинг трафіку, управління освітленням і комунальними послугами в реальному часі	Високі витрати на встановлення та обслуговування інфраструктури, складність підтримки
Здоров'я та медицина (e-Health)	Віддалене моніторування стану здоров'я пацієнтів, швидке реагування на зміни	Питання захисту медичних даних, що потребують високого рівня безпеки
	Персоналізація лікування завдяки аналізу даних, автоматичне нагадування про ліки	Можливість витоку конфіденційної інформації, висока вартість технічного обслуговування
Логістика та транспорт	Оптимізація маршрутів і часу доставки, зниження витрат на паливо	Залежність від GPS і мобільного зв'язку, можливість втрати зв'язку
	Відстеження транспортних засобів у реальному часі, поліпшення логістичних процесів	Ризики безпеки, потреба в постійному оновленні програмного забезпечення
Енергетика та управління ресурсами	Ефективне управління енергоспоживанням, інтеграція відновлюваних джерел енергії	Високі витрати на впровадження, можливість помилок при інтеграції з іншими системами
	Зниження витрат на електроенергію, аналіз енергоспоживання для планування	Ризики безпеки даних, необхідність постійного моніторингу для забезпечення стабільної роботи
Сільське господарство	Контроль стану врожаю, автоматизація систем поливу, зменшення витрат	Залежність від погодних умов, вартість обладнання для автоматизації
	Оптимізація використання добрив і ресурсів, прогнозування врожайності	Необхідність підтримки інфраструктури, ризики збоїв у роботі систем автоматизації
Фінанси та банківська справа	Підвищення безпеки транзакцій, швидкий аналіз для запобігання шахрайству	Висока вартість інтеграції із системами запобігання шахрайству, складність налаштувань
	Зручний контроль фінансів, автоматизація обробки транзакцій для зниження витрат	Проблеми з безпекою фінансових даних, складність управління масштабними фінансовими операціями

На основі виявлених недоліків у використанні IoT Web -додатків в різних галузях, можна запропонувати наступні сучасні підходи та технології для їх подолання:

1. Підвищення рівня безпеки для розумних будинків та пристроїв:

– впровадження технологій блокчейн для управління доступом та автентифікації, що забезпечить прозорість і незмінність даних та допоможе запобігти несанкціонованому доступу до розумних пристроїв;

– кожен пристрій може мати унікальний ідентифікатор у блокчейн-мережі, що ускладнить злом або підробку пристроїв.

2. Зменшення витрат на встановлення та інтеграцію для промислових IoT-додатків:

– використання «Digital Twin» для моделювання та планування – це створення цифрових двійників (моделей) виробничого обладнання, що дозволить перевіряти процеси інтеграції, прогнозувати можливі збої і оптимізувати ресурси перед фізичним встановленням;

– автоматизація процесів інтеграції з використанням штучного інтелекту допоможе автоматично налаштовувати підключення між різними системами та протоколами, що значно спрощує інтеграцію IoT-пристроїв у виробничі процеси.

3. Подолання проблем конфіденційності та витрат для розумних міст:

– застосування системи «Zero Trust» для забезпечення конфіденційності, що передбачає перевірку кожного пристрою чи користувача, що підключається до системи, навіть якщо вони перебувають всередині мережі;

– використання модульного підходу до інфраструктури розумних міст дозволить поступово розгортати нові сервіси без необхідності повного переоснащення системи, що знижує витрати на обслуговування і підтримку.

4. Підвищення рівня захисту та зниження витрат для e-Health:

– розширене шифрування медичних даних з використанням алгоритмів ШІ, що допоможе детальніше аналізувати потоки даних для виявлення аномалій і автоматично шифрувати чутливі медичні записи перед їх зберіганням або передачею;

– розробка «Federated Learning» для медичних додатків, що дозволить навчати моделі машинного навчання на розподілених пристроях, не переміщуючи дані до централізованих серверів.

5. Підвищення надійності і зниження залежності для логістики та транспорту:

– інтеграція з мережею 5G і підготовка до 6G для більш стабільного зв'язку;

– використання обчислень на периферії (Edge Computing) зменшить залежність від постійного підключення до централізованого сервера, що дозволить виконувати критично важливі функції на місцевих пристроях, навіть якщо з'єднання з мережею тимчасово втрачається.

6. Підтримка та інтеграція відновлюваних джерел енергії для енергетики та управління ресурсами: розробка самовідновлюваних мереж з «туманними обчисленнями», які можуть самостійно переналаштовуватись і відновлювати роботу у випадку відмови окремих елементів, що знижує ризики збоїв та підвищує стабільність енергетичних систем.

7. Підвищення ефективності управління та зниження ризиків для сільського господарства:

– інтеграція технологій «Digital Twin» для моніторингу стану ґрунту та врожаю – це дозволить відстежувати стан полів, проводити аналіз впливу різних умов на врожайність і оптимізувати використання добрив та води;

– використання автономних дронів і роботів для автоматичного збирання інформації, обприскування або збору врожаю зменшить залежність від погодних умов та підвищить ефективність роботи в полі.

8. Підвищення безпеки транзакцій та зниження витрат для фінансів і банківської справи:

– впровадження біометричних методів автентифікації, таких як розпізнавання відбитків пальців, обличчя або голосу, дозволяє забезпечити додатковий рівень захисту фінансових операцій;

– штучний інтелект може аналізувати транзакції та виявляти аномалії, що можуть свідчити про спроби шахрайства, що дозволить швидко реагувати на загрози та зменшити кількість неправомірних транзакцій.

Реалізація цих пропозицій дозволить значно покращити роботу Web-додатків в архітектурі IoT, підвищити їхню безпеку та ефективність, а також забезпечить легшу інтеграцію різних систем у єдину екосистему.

Висновки. Існуючі IoT-системи мають значний потенціал для автоматизації та покращення ефективності в різних галузях, проте стикаються з низкою проблем. Запропоновані технологічні рішення, такі як використання блокчейн для автентифікації та Edge Computing для локальної обробки даних, дозволяють значно знизити ризики втрати даних та забезпечити безперебійну роботу IoT-систем.

Застосування сучасних підходів до інтеграції IoT-пристроїв дозволяє знизити залежність від централізованих мереж та підвищити надійність передачі даних, що сприяє безпечній експлуатації систем та створює умови для подальшої цифрової трансформації суспільства, відкриваючи нові можливості для бізнесу та повсякденного життя.

Список використаних джерел:

1. A. K. M. Bahalul Haque et al. 5G and Internet of Things–Integration Trends, Opportunities, and Future Research Avenues. 5G and Beyond, Springer Tracts in Electrical and Electronics Engineering. С. 217–245. URL: https://doi.org/10.1007/978-981-99-3668-7_11

2. Alhassan Jamilu Ibrahim, Abba Hassan, Abdulkadir Hassan Disina, Zahraddeen Abubakar Pindar The Technologies of 5G: Opportunities, Applications and Challenges. *International Journal of Systems Engineering*. 2021. 5(2), С. 59–68.

3. Atiko. Що таке IoT простими словами? URL: https://www.atiko.com.ua/articles-ua/chto-takoe-iot-prostymi-slovami/

4. Evergreens. Internet of Things: вступ і огляд можливостей. URL: https://evergreens.com.ua/ua/articles/the-internet-of-things.html

5. Hari Mohan Rai, Atik-Ur-Rehman, Aditya Pal, Sandeep Mishra, Kaustubh Kumar Shukla Use of Internet of Things in the context of execution of smart city applications: a review. Discover Internet of Things (2023) 3:8. URL: https://link.springer.com/article/10.1007/s43926-023-00037-2

6. Jorge Cárdenas, David Menéndez Internet of Things: How the Electrical Grid can be controlled and managed in other dimensions. *The Journal of Engineering*. URL: https://www.researchgate.net/publication/326510909_Internet_of_Things_How_the_Electrical_Grid_can_be_controlled_and_managed_in_other_dimensions

7. Mostafa Zaman, Nathan Puryear, Sherif Abdelwahed, Nasibeh Zohrabi A Review of IoT-Based Smart City Development andManagement. Smart Cities 2024, 7, С. 1462–1500. URL: https://doi.org/10.3390/smartcities7030061

8. Stfalcon. Як мобільні додатки впливають на інтернет речей. URL: https://stfalcon.com/uk/blog/post/internet-of-things-apps

9. Yunus Kareem, Djamel Djenouri, Essam Ghadafi A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things.

10. Zdnet. What is the IoT? Everything you need to know about the Internet of Things right now. URL: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

11. Джерелейко А. О., Яковенко Н. Д., Марченко Г. В., Аташкаде Р. В. IoT у сучасному веб-розробленні. *Наука, експлуатація, виробництво*. ЗВ'ЯЗОК, № 2, 2021. С. 53–55.

12. Пановик У. П. Стандартизація інтернету речей: сучасний стан та перспективи розвитку. *Технічні науки. Поліграфія і видавнича справа*. 2023. 1 (85). С. 51–64

13. Школа Автоматики. Лекція 1. Основи Інтернету Речей. URL: http://edu.asu.in.ua/mod/book/view.php?id=112&chapterid=230

УДК 004.9:555
DOI https://doi.org/10.32689/maup.it.2024.4.15

Сергій ЛУК'ЯНЕНКО
начальник науково-дослідної лабораторії проблем супроводження моделей операцій та бойових дій науково-дослідного відділу перспектив розвитку та проблем супроводження моделей операцій центру імітаційного моделювання,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0002-9286-4636*

Павло ВДОВІН
науковий співробітник науково-дослідного відділу перспектив розвитку та проблем супроводження моделей операцій центру імітаційного моделювання,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0009-0000-7819-5125*

Валентин ГРОМИКО
науковий співробітник науково-дослідної лабораторії розробки моделей видів забезпечення операцій та бойових дій науково-дослідного відділу розробки моделей операцій та бойових дій центру імітаційного моделювання,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0009-0008-2195-2568*

Роман ТИМОШЕНКО
кандидат технічних наук,
начальник науково-дослідного відділу перспектив розвитку
та проблем супроводження моделей операцій,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0001-8069-023X*

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СУЧАСНІЙ УКРАЇНСЬКІЙ ВІЙСЬКОВІЙ СПРАВІ

Анотація. *У статті досліджено питання щодо ролі інформаційних технологій в сучасній українській військовій справі.*

Мета роботи *полягає в аналізі того, як інформаційні технології впливають на ефективність протистояння України агресору та сприяють відновленню країни після війни, зокрема через інституційні реформи та інтеграцію до європейських стандартів.*

Методологія *дослідження включає аналіз використання цифрових систем управління, розвідки, кібербезпеки та їх вплив на ведення бойових дій, а також на процеси відновлення країни після конфлікту.*

Наголошено на тому, що наразі основний фокус України спрямований на протистояння агресору, звільнення своїх територій та пошук шляхів відновлення економіки як під час війни, так і після перемоги, з акцентом на швидку реконструкцію країни. Завдання полягає не тільки в мінімізації збитків і подоланні наслідків руйнувань, але й у закладенні основ для майбутнього економічного зростання. Фундамент цього розвитку включає інституційні реформи відповідно до європейських стандартів, інтеграцію транспортної, енергетичної та соціальної інфраструктури до європейського ринку, створення сприятливого інвестиційного середовища для інвесторів та постачальників технологій, а також відновлення міст з використанням сучасних технологій дизайну та міського планування. Також важливим є розвиток транспортних систем і відновлення соціального капіталу, що сприятиме здатності громадян до спільних дій задля досягнення спільних цілей.

Наукова новизна *роботи полягає в оцінці важливості ІТ у військовій справі як елементу стратегічної оборони та розвитку інфраструктури України в умовах війни.*

Як висновок, сказано про те, що інформаційні технології стали ключовим фактором у сучасній військовій справі, зокрема у протистоянні України російській агресії. Впровадження цифрових систем управління, засобів розвідки та кібербезпеки дозволяє значно підвищити ефективність ведення бойових дій. Хоча Україна зіткнулася з великими викликами на цьому шляху, активний розвиток інформаційних технологій дає змогу досягти значних успіхів як на полі бою, так і в захисті національних інтересів у кіберпросторі.

Роль ІТ у сучасній українській військовій справі буде тільки зростати, і для подальшого підвищення обороноздатності країни необхідно розвивати технологічні спроможності та залучати інноваційні підходи. Успішне використання інформаційних технологій може стати тим вирішальним фактором, який забезпечить перемогу України в цьому конфлікті.

Висновки *свідчать, що впровадження інформаційних технологій значно підвищує ефективність ведення бойових дій і сприяє розвитку інфраструктури та соціального капіталу, що є важливими для майбутнього економічного зростання країни. Для подальшого зміцнення обороноздатності України необхідно активно розвивати технологічні спроможності та залучати інноваційні підходи. Впровадження ІТ в військову справу є вирішальним фактором для здобуття перемоги в конфлікті.*

Ключові слова: *інформаційні технології, війна, військо.*

Serhii LUKIANENKO, Pavlo VDOVIN, Valentyn HROMYKO, Roman TYMOSHENKO. THE ROLE OF INFORMATION TECHNOLOGIES IN MODERN UKRAINIAN MILITARY AFFAIRS

Abstract. *The article examines the issue of the role of information technologies in modern Ukrainian military affairs.*

The purpose *of the work is to analyze how information technologies affect the effectiveness of Ukraine's resistance to the aggressor and contribute to the recovery of the country after the war, in particular through institutional reforms and integration to European standards.*

The research methodology *includes the analysis of the use of digital systems of management, intelligence, cyber security and their impact on the conduct of hostilities, as well as on the processes of post-conflict recovery of the country.*

It was emphasized that currently Ukraine's main focus is on confronting the aggressor, liberating its territories and finding ways to restore the economy both during the war and after victory, with an emphasis on the rapid reconstruction of the country. The task is not only to minimize damage and overcome the consequences of destruction, but also to lay the foundations for future economic growth. The foundation of this development includes institutional reforms in accordance with European standards, the integration of transport, energy and social infrastructure into the European market, the creation of a favorable investment environment for investors and technology providers, as well as the regeneration of cities using modern design and urban planning technologies. Also important is the development of transport systems and the restoration of social capital, which will contribute to the ability of citizens to take joint action to achieve common goals.

The scientific novelty *of the work consists in assessing the importance of IT in military affairs as an element of strategic defense and infrastructure development of Ukraine in wartime conditions.*

As a conclusion, it was said that information technologies have become a key factor in modern military affairs, in particular in Ukraine's resistance to Russian aggression. The implementation of digital control systems, intelligence and cyber security allows to significantly increase the effectiveness of combat operations. Although Ukraine has faced great challenges on this path, the active development of information technologies makes it possible to achieve significant success both on the battlefield and in the protection of national interests in cyberspace.

The role of IT in modern Ukrainian military affairs will only grow, and in order to further increase the country's defense capabilities, it is necessary to develop technological capabilities and involve innovative approaches. The successful use of information technologies can become the decisive factor that will ensure Ukraine's victory in this conflict.

The conclusions *show that the introduction of information technologies significantly increases the effectiveness of warfare and contributes to the development of infrastructure and social capital, which are important for the future economic growth of the country. In order to further strengthen Ukraine's defense capabilities, it is necessary to actively develop technological capabilities and involve innovative approaches. The implementation of IT in military affairs is a decisive factor for winning the conflict.*

Key words: *information technology, war, army.*

Вступ. Постановка проблеми. В сучасних умовах військових конфліктів технології відіграють вирішальну роль. Інформаційні технології (ІТ) стали невід'ємною частиною не тільки цивільного життя, але й оборонної стратегії держав. Українська армія, протистоячи російській агресії, зіткнулася з потребою впровадження сучасних ІТ для підвищення ефективності управління, зв'язку, розвідки та аналізу ситуацій. Постає питання, яким чином інформаційні технології допомагають Україні протистояти ворогу і як їх застосування впливає на перебіг війни.

З огляду на ці обставини, основними аспектами проблеми є:

1. Недостатній рівень впровадження новітніх технологій у військову сферу в порівнянні з провідними арміями світу.
2. Потреба в інтеграції ІТ-рішень у процес управління бойовими діями та розвідки.
3. Зростаюча роль кібервійни та кіберзахисту в умовах сучасних збройних конфліктів.
4. Необхідність підготовки персоналу до роботи з новими технологіями.

Ці питання є нагальними для оборони України та вимагають аналізу ролі інформаційних технологій у сучасній військовій справі.

Виклад основного матеріалу. Інформаційні технології радикально змінили підходи до планування, координації та управління військовими операціями.

Сучасні війни вимагають високої швидкості ухвалення рішень і точності передачі інформації. Українська армія активно використовує цифрові системи управління військами, що забезпечують миттєву передачу інформації між підрозділами та штабами [1, с. 5].

Цифрові платформи, такі як системи автоматизованого управління військовими операціями, дають змогу в режимі реального часу координувати дії різних підрозділів, аналізувати хід бою та швидко реагувати на зміни в тактичній обстановці.

Наразі основний фокус України спрямований на протистояння агресору, звільнення своїх територій та пошук шляхів відновлення економіки як під час війни, так і після перемоги, з акцентом на швидку реконструкцію країни. Завдання полягає не тільки в мінімізації збитків і подоланні наслідків руйнувань, але й у закладенні основ для майбутнього економічного зростання [2].

Фундамент цього розвитку включає інституційні реформи відповідно до європейських стандартів, інтеграцію транспортної, енергетичної та соціальної інфраструктури до європейського ринку, створення сприятливого інвестиційного середовища для інвесторів та постачальників технологій, а також відновлення міст з використанням сучасних технологій дизайну та міського планування.

Також важливим є розвиток транспортних систем і відновлення соціального капіталу, що сприятиме здатності громадян до спільних дій задля досягнення спільних цілей. Якісний людський капітал має бути орієнтований на розширення економічних відносин у межах європейської моделі економіки.

Для цього необхідна консолідація зусиль у сфері вищої освіти, що спрямована на розвиток інтелектуального потенціалу, а також співпраця з провідними зарубіжними освітніми та науковими інституціями.

ХХ століття відзначилося численними війнами та збройними конфліктами, які продовжуються й досі в різних куточках світу. На жаль, Україна не стала винятком.

З 2014 року відбувся значний прогрес у розвитку військової справи – запроваджуються нові методи розвідки, управління військами стає більш мобільним та ефективним, особливо завдяки впровадженню ГІС-технологій.

Геоінформаційні системи (ГІС) є інформаційною основою автоматизованої системи управління збройних сил і невід'ємним елементом прийняття рішень командирами та штабами на всіх рівнях. Сучасний розвиток Збройних Сил України (ЗСУ) вимагає ефективного та безперервного контролю за пересуванням, концентрацією та маневруванням військ і техніки, що потребує точної інформації про їхнє місцеположення.

Автоматизація процесу управління значно скорочує час на координацію та узгодженість дій військ в умовах швидкої зміни ситуації та високої динаміки бойових дій, зокрема при застосуванні високоточної зброї. Основою сучасного підходу до автоматизації управління військами, де паперові карти замінюються цифровими, є інтеграція ГІС-технологій у цей процес.

ГІС-технології у військовій сфері виконують низку важливих завдань, серед яких:

– планування руху техніки з урахуванням конкретної бойової ситуації, характеристик місцевості, прихованості, часу доби та особливостей бойової техніки;

– планування польотів авіації та безпілотних літальних апаратів (БПЛА) для нанесення ударів, транспортування вантажів і особового складу;

– оптимізація графіків і маршрутів переміщення;

– визначення можливих шляхів пересування противника та планування розміщення засобів для протидії;

– тривимірне моделювання місцевості для навчання особового складу на тренажерах (авіаційних, танкових, автомобільних тощо);

– відтворення переміщення об'єктів за зафіксованими траєкторіями та параметрами руху;

– навігація та диспетчерський супровід об'єктів;

– використання у бортових та портативних навігаційних системах з відображенням поточного місцезнаходження на карті й координат руху;

– контроль переміщення цінних або небезпечних вантажів;

– моделювання військових конфліктів та бойових ситуацій;

– геопросторова розвідка (ГПР).

Таким чином, для програмного забезпечення ГІС, що використовується у збройних силах, важливими є такі вимоги:

– глобальність і єдиність бази даних обстановки (з можливістю її розподіленості);

– синхронізація інформації з різних джерел, можливість спільної роботи та автономної роботи з подальшою синхронізацією локальних даних із централізованими сховищами;

– ведення карт відповідно до стандартів, прийнятих у військових структурах;

– забезпечення надійного збереження даних;

– оперативність і функціонування в реальному часі;

– обробка великих обсягів даних у реальному масштабі часу;

– розмежування доступу до інформації;

– можливість адаптації та вдосконалення ГІС під нові вимоги військових підрозділів.

Серед країн, чиї силові структури мають штатні підрозділи для здійснення геопросторової розвідки, особливе місце посідають Сполучені Штати Америки. Головним координатором забезпечення військ необхідними геопросторовими продуктами в США виступає Національне агентство геопросторової розвідки (NGA), що підпорядковується Міністерству оборони США та входить до складу National Intelligence Community. NGA надає геопросторові й аналітичні матеріали для підтримки національної оборони й безпеки, а також надає консультації та технічну допомогу військовим розвідувальним центрам (Combatant Command's Joint Intelligence Operations Center).

У збройних силах США – сухопутних військах, ВМС і повітряних силах – функціонують власні підрозділи ГПР, які здатні розробляти як стандартні, так і спеціальні ГІС-продукти. Однак, розвідувальні

космічні апарати з високоточними бортовими системами зйомки, що дозволяють отримувати зображення з роздільною здатністю в десятки сантиметрів, є надзвичайно дорогими.

Наприклад, створення, запуск і технічна підтримка одного супутника серії KeyHole обійшлися США в майже $1,5 млрд. Щоб зменшити витрати, багато країн звернулися до комерційних рішень. У США приватна компанія, використовуючи технології одного з супутників серії KeyHole, успішно вивела на орбіту супутник Ikonos-2 у 1998 році, який здатен знімати земну поверхню з роздільною здатністю до одного метра. Як державні силові структури, так і приватні установи, включаючи іноземні, мають можливість замовляти космічну зйомку та отримувати високоякісні матеріали попередніх космічних спостережень.

Унікальною перевагою ГПР є можливість проведення всебічного геопросторового аналізу операційного середовища, точність і достовірність аналітичних оцінок, простота та наочність подання інформації. Завдяки цьому ГПР стає основою у забезпеченні всебічною і надійною інформацією про об'єкти інтересу.

Для України потреби економічного розвитку, ЗСУ, інших силових відомств у ГПР є вкрай значущими. З огляду на це, удосконалюючи систему розвідувально-інформаційного забезпечення сил оборони України і силових відомств, слід врахувати аналіз розвитку ГПР провідних держав і приділити належну увагу розробленню національної системи геопросторової розвідки та її невідкладної реалізації.

Зважаючи на вищезазначене, підтримка розвитку високих технологій, зокрема ІТ-галузі, є важливою як під час війни, так і в поствоєнний період. Це може стати каталізатором економічної трансформації України та її регіонів у напрямку переходу до високих технологій, що зміцнить позиції країни на світовій арені. ІТ-сектор, навіть під час війни, продемонстрував свою стійкість.

Згідно з результатами опитування найбільших українських ІТ-компаній, галузі вдалося зберегти кадровий потенціал, залучаючи приблизно 285 тисяч спеціалістів.

ІТ-бізнес швидко адаптувався до умов воєнного стану, здійснивши масову релокацію персоналу та забезпечивши безперервність робочих процесів завдяки створенню безпечних умов праці, використанню Starlink і генераторів для підтримки зв’язку та електропостачання [3, с. 45].

Однак загальна тенденція до скорочення персоналу, яку спостерігають світові гіганти ІТ-індустрії через зниження активності в інтернет-сервісах, також вплинула на українські компанії. У 2022 році наймання українських ІТ-спеціалістів знизилося на 13%, що стало першим випадком за останні 10 років, коли кількість нових працівників була меншою, ніж у попередньому році.

Продуктивність фахівців зменшилася лише на 10%, проте деякі компанії втратили проєкти та клієнтів через геополітичні ризики, проблеми з безпекою, релокацію команд або мобілізацію працівників (до лав ЗСУ вступило 3% ІТ-спеціалістів). Незважаючи на це, українські сервісні та продуктові компанії успішно адаптувалися до нових викликів. Особливо активно розвиваються галузі штучного інтелекту, кібербезпеки та military tech.

Україна використовує прогресивні системи управління вогнем, які дозволяють точно наводити артилерію або безпілотні літальні апарати на цілі [4].

Прикладом є система «GIS Arta», яка дозволяє ефективно управляти вогневими засобами, оптимізуючи час та ресурси для нанесення ударів по ворогу. Це значно підвищує боєздатність української армії, дозволяючи завдавати точкових ударів з мінімальними втратами серед цивільного населення.

Інформаційні технології також відіграють важливу роль у зборі розвідувальних даних та спостереженні за ворогом. Використання супутникових технологій, безпілотних літальних апаратів (БПЛА) та сенсорних мереж дає змогу зібрати інформацію про пересування, кількість і розташування військ противника. Українські військові активно використовують як комерційні, так і спеціалізовані безпілотники для спостереження за ворожими позиціями та коригування вогню артилерії.

Супутникові знімки та дані з дронів дозволяють точно визначати місця концентрації військової техніки та особового складу ворога, планувати удари та оцінювати їх ефективність. Завдяки таким технологіям українська армія змогла значно підвищити ефективність своїх розвідувальних операцій, що особливо важливо в умовах гібридної війни, де важко визначити чіткі фронти чи виявити сили противника.

Кіберпростір став новим полем бою у сучасних військових конфліктах. Україна, зазнавши численних кібератак з боку Росії ще з 2014 року, була змушена інвестувати значні ресурси у посилення своєї кібербезпеки. Атаки на критичну інфраструктуру, військові об'єкти та системи управління показали, що слабкі місця в кіберзахисті можуть мати катастрофічні наслідки.

Для захисту від таких атак Україна розвиває системи кібербезпеки та кібероборони. Створені спеціалізовані підрозділи, що займаються моніторингом та запобіганням кібератак, а також вживають заходів для відновлення пошкоджених систем. Такі заходи включають використання сучасних технологій шифрування даних, виявлення та нейтралізацію загроз, що виходять із кіберпростору.

Одночасно з обороною, українські фахівці розвивають кібернаступальні можливості. Це дозволяє не тільки захищатися від атак, але й завдавати удари у відповідь по критичних інфраструктурах ворога. Такі дії можуть включати виведення з ладу систем управління, порушення роботи військових об'єктів чи дезінформацію, що робить інформаційні технології потужною зброєю в руках української армії.

Один з ключових напрямків сучасної військової справи – це використання великих даних (Big Data) та штучного інтелекту (ШІ) для аналізу та прогнозування ситуацій на полі бою. Збір величезної кількості даних від різних джерел, таких як супутники, дрони, сенсори та інші системи, дозволяє аналізувати ці дані та робити обґрунтовані прогнози щодо дій ворога. Штучний інтелект допомагає оптимізувати процес прийняття рішень та передбачити можливі сценарії розвитку бойових дій [5, с. 5].

Україна також працює над впровадженням подібних технологій. Штучний інтелект може аналізувати дані з численних джерел та надавати військовому керівництву готові аналітичні звіти, що допомагає ефективніше планувати операції та ухвалювати стратегічні рішення.

Висновки. Отже, інформаційні технології стали ключовим фактором у сучасній військовій справі, зокрема у протистоянні України російській агресії. Впровадження цифрових систем управління, засобів розвідки та кібербезпеки дозволяє значно підвищити ефективність ведення бойових дій. Хоча Україна зіткнулася з великими викликами на цьому шляху, активний розвиток інформаційних технологій дає змогу досягти значних успіхів як на полі бою, так і в захисті національних інтересів у кіберпросторі.

Роль ІТ у сучасній українській військовій справі буде тільки зростати, і для подальшого підвищення обороноздатності країни необхідно розвивати технологічні спроможності та залучати інноваційні підходи. Успішне використання інформаційних технологій може стати тим вирішальним фактором, який забезпечить перемогу України в цьому конфлікті.

Список використаних джерел:

1. Дзямулич М. І., Шматковська Т. О. Вплив сучасних інформаційних систем і технологій на формування цифрової економіки. *Економічний форум.* 2022. № 2. С. 3–8.
2. Довгань О., Ткачук Т. (2019). Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право,* № 1, С. 86–99. URL: http://nbuv.gov.ua/UJRN/Infpr_2019_1_12
3. Курбан О. В. Сучасні інформаційні війни в мережевому онлайн просторі: навч. посіб. Київ: ВІКНУ. 2016. 286 с. URL: http://www.mil.univ.kiev.ua/ files/222_1044284240.pdf.
4. Макаренко Л. П. Еволюція форм та методів ведення інформаційної війни. URL: http://oaji.net/articles/2014/797-1402908125.pdf
5. Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукр. наук.практ. конф. (м. Маріуполь, 9 черв. 2017 р.). Маріуполь: ДонДУУ, 2017, 311 с.

УДК 004.77:004.031
DOI https://doi.org/10.32689/maup.it.2024.4.16

Геннадій МОГИЛЬНИЙ
кандидат технічних наук, доцент, директор Навчально-наукового інституту математики та інформаційних технологій,
ДЗ «Луганський національний університет імені Тараса Шевченка», g.mogilniy@gmail.com
***ORCID:** 0000-0001-5317-2795*

Володимир ДОНЧЕНКО
старший викладач кафедри інформаційних технологій та систем,
ДЗ «Луганський національний університет імені Тараса Шевченка», ifmit.s.2014@gmail.com
***ORCID:** 0000-0003-0359-3051*

Світлана ДОНЧЕНКО
асистент викладач кафедри інформаційних технологій та систем,
ДЗ «Луганський національний університет імені Тараса Шевченка», donchenko.lana77@gmail.com
***ORCID:** 0000-0002-2374-2109*

ОГЛЯД ТА АНАЛІЗ ІНСТРУМЕНТІВ СТВОРЕННЯ КОРПОРАТИВНОГО СЕРЕДОВИЩА

Анотація. *Стаття присвячена аналізу сучасних підходів до створення об'єднаних інформаційних середовищ для організацій із розгалуженою структурою підрозділів. Особливу увагу приділено використанню сучасних засобів для організації віддаленого доступу для зовнішніх користувачів та інтеграції з локальною мережею підприємства. В умовах необхідності інтеграції локальних мереж підрозділів, що розташовані в різних регіонах, розглянуто рішення, які базуються на технологіях віртуальних приватних мереж (VPN), переадресації портів (PAT) і функції DMZ.*

Мета роботи *– аналіз засобів створення корпоративного середовища в умовах мінімального обсягу фінансування.*

Методологія*. Аналіз наукової літератури з питань створення корпоративного середовища. Аналіз нормативних документів з налаштування різноманітних роутерів. На засадах системного аналізу запропоновано варіанти створення корпоративного середовища в умовах швидкого впровадження нових технологій.*

Наукова новизна *дослідження полягає в обґрунтуванні варіантів створення корпоративного середовища в умовах обмеженого фінансування. Доведено, що технології DMZ та PAT можуть бути застосовано на всіх сучасних роутерах, як засоби створення корпоративного середовища. Встановлено, що використання мережевої технології VPN на клієнтських обчислювальних машинам має суттєві недоліки і може бути застосовано за умови додаткового налаштування.*

Висновки*. У роботі детально проаналізовано особливості впровадження віддаленого доступу до корпоративних ресурсів шляхом налаштування DMZ, PAT та VPN (PPTP, L2TP) на різних моделях роутерів: Tp_link TL-WR840N, Mercusys AC12g, Tp-link AX1500 та Mikrotik. На основі практичних експериментів оцінюються переваги та недоліки кожного методу. Проведений аналіз дозволяє прискорити створення корпоративних мереж у межах обмежених бюджетів, зокрема для малих підприємств і навчальних закладів. Представлено рекомендації щодо модернізації мережевої інфраструктури, вибору роутерів і впровадження засобів контролю доступу, які можуть бути застосовані для побудови інтегрованих інформаційних систем у бізнесі, освіті та інших галузях.*

Ключові слова: *корпоративна мережа, віддалений доступ, роутер, VPN, DMZ, переадресація портів.*

Hennadii MOHYLNYI, Volodymyr DONCHENKO, Svitlana DONCHENKO. REVIEW AND ANALYSIS OF TOOLS FOR CREATING A CORPORATE ENVIRONMENT

Abstract. *The article is devoted to the analysis of modern approaches to creating unified information environments for organizations with a branched structure of departments. Particular attention is paid to the use of modern tools for organizing remote access for external users and integration with the enterprise's local network. In the conditions of the need to integrate local networks of departments located in different regions, solutions based on virtual private network (VPN) technologies, port forwarding (PAT) and DMZ functions are considered.*

The purpose *of the work is to analyze the means of creating a corporate environment with minimal funding.*

Methodology. *Analysis of scientific literature on the creation of a corporate environment. Analysis of regulatory documents on the configuration of various routers. On the basis of system analysis, options for creating a corporate environment in conditions of rapid implementation of new technologies are proposed.*

The scientific novelty *of the study lies in the substantiation of options for creating a corporate environment in conditions of limited funding. It is proven that DMZ and PAT technologies can be used on all modern routers as a means of creating a corporate environment. It is established that the use of VPN network technology on client computers has significant disadvantages and can be applied subject to additional configuration.*

Conclusions*. The paper analyzes in detail the features of implementing remote access to corporate resources by configuring DMZ, PAT and VPN (PPTP, L2TP) on different router models: Tp_link TL-WR840N, Mercusys AC12g, Tp-link AX1500 and Mikrotik. Based on practical experiments, the advantages and disadvantages of each method are assessed. The analysis allows you to accelerate the creation of corporate networks within limited budgets, in particular for small businesses and educational institutions. Recommendations are presented for the modernization of network infrastructure, the selection of routers and the implementation of access control tools that can be used to build integrated information systems in business, education and other industries.*

Key words: *corporate network, remote access, router, VPN, DMZ, port forwarding.*

Вступ. Постановка проблеми. Сьогодні багато організацій мають розгалужену мережу підрозділів, що фізично розташовані в різних регіонах. У таких умовах одним із ключових завдань стає об'єднання всіх підрозділів у єдину, надійну та безпечну локальну мережу. Таким чином, перед багатьма закладами та установами виникає питання створення загальнодоступних інформаційних баз даних та сервісів шляхом впровадження корпоративних мереж між відокремленими підрозділами та надання можливості віддаленим користувачам використовувати внутрішні локальні ресурси.

Враховуючи сучасні обставини, які виникають в умовах військового стану можна стверджувати, що різноманітні питання програмного та апаратного забезпечення, спрямовані на створення об'єднаних корпоративних мереж, є своєчасною та актуальною задачею.

Аналіз останніх досліджень і публікацій. Загальновідомі методи з'єднання віддалених підрозділів з локальною мережею полягали в тому, що підключення працювало по загальній мережі, що комутується, PSTN (public switched telephone network), або використовували спеціалізовану орендовану WAN (wide area network,), користуючись фрейм-ретранслятором або синхронною схемою протоколу PPP (Point-to-Point Protocol) [13]. Ці методи вимагають значних витрат часу на адміністрування й доволі не дешеві в обслуговуванні. Використання Internet-рішень дозволяє задовольнити потреби віддаленої роботи в організаційній мережі через кілька інтернет-підключень, наданих інтернет-провайдерами (Internet Service Providers або ISP), і VPN-сервери. У цьому контексті перспективними рішеннями є надійні та недорогі пристрої з великим вибором протоколів маршрутизації та віртуальних приватних мереж (VPN). Це дозволяє гнучко підлаштовувати пристрої під різні вимоги провайдерів інтернет-мереж, а також забезпечувати високу безпеку та надійність тунелів між підрозділами.

У роботі [3] представлено найпростіші та швидкі способи створення інформаційної системи з віддаленим доступом, описано їх реалізацію, яка не потребує значної модернізації. Проведено аналіз варіантів організації доступу до навчальної комп'ютерної лабораторії, побудованої за принципом перенаправлення окремих портів. Також розроблено рекомендації щодо модернізації обладнання лабораторії та визначено етапи налаштування системи з використанням віддаленого робочого столу. Автори [4] проаналізували різні підходи до організації віддаленого доступу до комп'ютерної лабораторії, яка може бути побудована або на базі одного вузла з різними ресурсами (інформаційними, апаратними, програмними), або декількох вузлів, серед яких є сервери віддаленого робочого столу, вебсервери та інші ресурси з окремими IP-адресами. Особливу увагу приділено структурним компонентам системи віддаленого доступу на основі VPN, надано рекомендації з їх налаштування та використання. Наведено специфіку застосування VPN за допомогою роутерів MikroTik.

У дослідженні [2] розглядаються актуальні питання захисту інформації у віртуальних приватних мережах (VPN), зокрема аспекти масштабованості, гнучкості управління, вимог до підключень та витрат на впровадження. У статті [15] досліджено сучасні методи та інструменти створення сервісу віртуальних приватних мереж, а також проведено аналіз їх реалізації за допомогою апаратно-програмних рішень на прикладі приватної мережі, побудованої з використанням CISCO FlexVPN.

У статті [5] описано принципи побудови мереж передачі даних для забезпечення послуг VPN та Інтернету на основі концепції Metro Ethernet. Запропоновано підходи до пошуку рішень, сформульовано ідеологію таких мереж, наведено їх архітектуру, параметри й характеристики. Також синтезовано структуру мережі та визначено ієрархію вузлів і обладнання. У статті [6] проаналізовано методи та способи реалізації захищених каналів VPN, їх переваги та недоліки. Розглянуто принципи функціонування та цільове призначення VPN у рамках розподілених корпоративних мереж, що використовують інфраструктуру відкритого доступу.

Метою статті є аналіз засобів створення корпоративного середовища в умовах мінімального обсягу фінансування.

Виклад основного матеріалу дослідження. В цілому задача створення корпоративного середовища це складний та багатоетапний процес. В межах цієї роботи будемо вважати, що підприємство вже має реальну IP-адресу та виконало аналіз інформаційних ресурсів, які будуть використані в об'єднаному середовищі корпоративної мережі. Таким чином, можна виділити основні складові корпоративної мережі: створення доступу окремих користувачів до внутрішніх локальних ресурсів певного підрозділу (рис. 1); об'єднання окремимих підрозділів за рахунок впровадження певного тунелю (рис. 2).

Рис. 1. Загальна схема приєднання віддалених користувачів

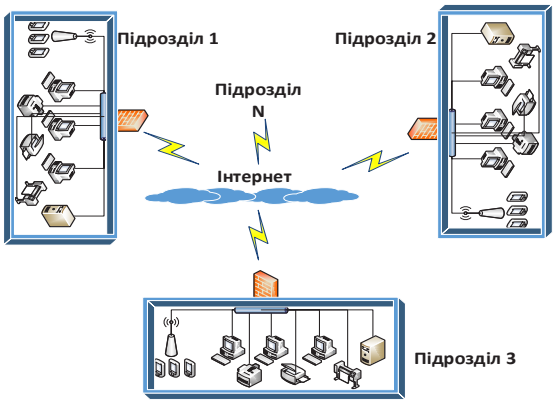


Рис. 2. Загальна схема з'єднання віддалених підрозділів

Крім того слід врахувати, що вирішення кожної задачі можливо вирішити різноманітними шляхами, однак самим поширеним є використання спеціалізованого порогового окремого роутера.

Досвід показує, що значна кількість організацій в умовах військового стану не вкладають багато коштів у мережну інфраструктуру та, в більшості випадків, використовують недорогі роутери, наприклад:

- WI-FI роутер Tp_link TL-WR840N [14] – 700 грн;
- WI-FI роутер Mercusys AC12g [7] – 1100 грн;
- WI-FI роутер Tp_link AX1500 Wi-Fi 6 [8] – 2200 грн;
- WI-FI роутер Mikrotik RBD53iG-5HacD2Hn [16] – 4000 грн.

В межах цієї роботи особливу увагу приділено вирішенню першої задачі — забезпеченню доступу віддалених користувачів до локальної мережі певного підрозділу, що є більш поширеним випадком і вимагає детального аналізу. Розглянемо декілька загальних підходів.

Наприклад, всі основні інформаційні ресурси розташовані на одному вузлі локальної мережі підрозділу (рис. 3, 4) – це найпростіший спосіб організації віддаленого доступу до інформаційних ресурсів локальної мережі, який не вимагає значних змін в інформаційній структурі підрозділу.

Встановлено, що на багатьох сучасних не дорогих роутерах можна скористатися функцією DMZ [1]. Безумовно, в такому випадку, адреса локального вузлу повинна бути статичною, тобто без використання протоколу DHCP.

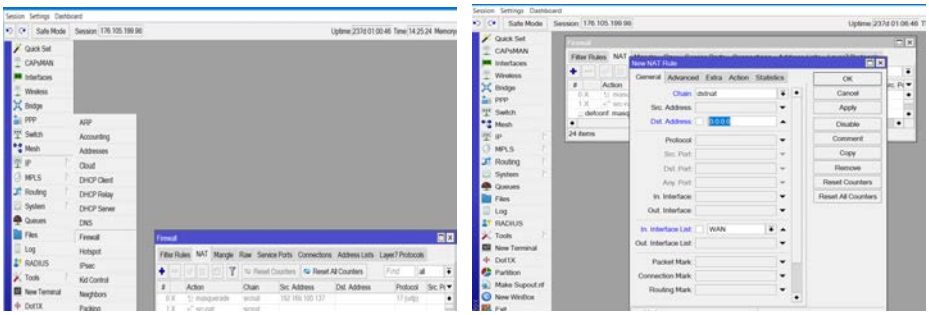
На рисунках 3–4 показано як це зробити на роутерах Mercusys AC12g та Tp_link AX1500, однак, аналогічні налаштування є на більшості роутерах та можуть бути швидко впроваджені.

Основним недоліком такого рішення є обмежена можливість використання різноманітного програмного забезпечення, яке зазвичай встановлюється на різних операційних системах, вимагає застосування декількох IP-адрес і не може бути розміщене на одній адресі. Безумовно створити один обчислювальний інформаційний ресурс на якому працювало б багато служб (сервісів) практично не можливо. Таким чином, використання DMZ можливе тільки для малих підприємств, які використовують обмежену кількість сервісів, що розташовані на одному вузлі.

Рис. 3. Налаштування DMZ для Mercusys AC12g

Рис. 4. Налаштування DMZ для Tp_link AX1500

Роутер Mikrotik не використовує поняття DMZ. Для такого налаштування необхідно скористатися програмою Winbox [10] та перейти до меню IP–Firewall–NAT (рис. 5,а), створити правило DST-NAT (рис. 5,б) та призначити Action dst-nat на необхідну IP-адресу.



а) б)

Рис. 5. Налаштування DMZ для Mikrotik: а) меню NAT; б) створення dst-nat

Слід відзначити [1], що використання DMZ має значну кількість недоліків з точки зору інформаційної безпеки тому, що IP вузол, у багатьох випадках, не відділяється від внутрішньої мережі та може вільно підключитися до внутрішніх ресурсів. Налаштування DMZ на всіх досліджених роутерах не дозволяє застосувати будь яких заходів безпеки. Отже для ліквідації такого суттєвого недоліку треба: встановлювати та налаштовувати додатковий міжмережевий екран у локальній мережі підрозділу або ретельно налаштувати фаєрвол вузла з контролем вхідного та вихідного трафіку.

У випадку коли, різноманітні ресурси розташовані на разних вузлах локальної мережі підрозділу, для організації віддаленого доступу необхідно ретельно проаналізувати особливості протоколів, які використовує кожен ресурс. Наприклад: веб-сервер –порти 80 і 443, e-mail сервер – 1 порти 25 і 110, FTP-сервер –порти 21, 20 і 1024–1240.

Практично для віх роутерів ця задача вирішується шляхом використання переадресації портів PAT [11], Налаштування робиться у меню «віртуальний сервер» або «port forwarding» (рис. 6).

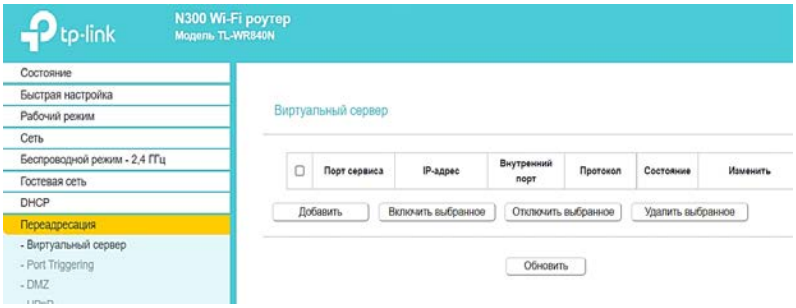


Рис. 6. Переадресація (PAT) у роутері Tp_link TL-WR840N

На рисунках 7–8 представлено відповідні меню роутерів Tp-Link TL-WR840N, Mercusys AC12G та AX1500 Wi-Fi 6. Детальне налаштування наведено лише для роутера AX1500 Wi-Fi 6 (рис. 9–10), тоді як для інших роутерів процедура є аналогічною.

Таким чином, можна створювати правила для всіх локальних інформаційних ресурсів підрозділу та контролювати використані порти. Такий підхід є доцільним для простих інформаційних систем підрозділу, де заздалегідь визначено список IP-портів, які не конфліктують між собою та можуть бути перенаправлені. Крім того, важливо враховувати, що віддалені користувачі матимуть доступ лише до зовнішньої IP-адреси пристрою, який виконує роль шлюзу. Водночас цей пристрій може стикатися з обмеженнями, пов'язаними з недостатньою кількістю місця у таблиці перенаправлення портів.

Рис. 7. Переадресація (PAT) у роутері Mercusys AC12g

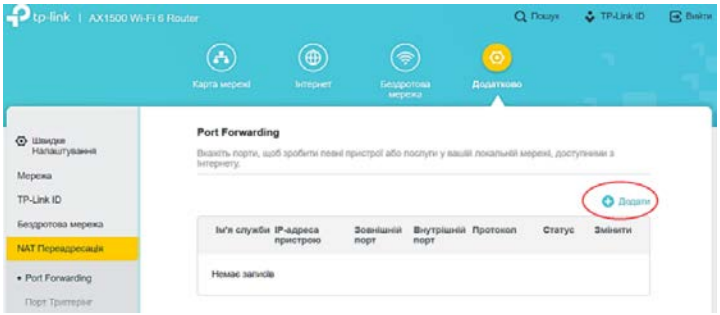


Рис. 8. Переадресація (PAT) у роутері AX1500 Wi-Fi 6

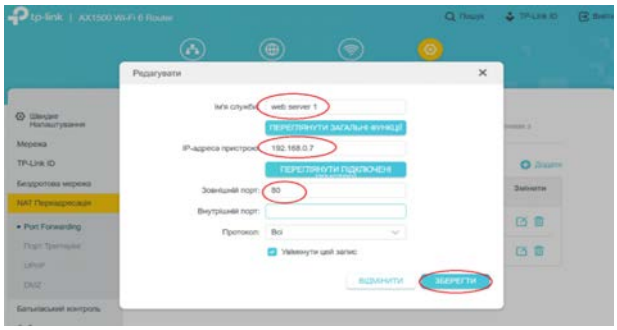


Рис. 9. Додавання вебсерверу – порт TCP/IP 80

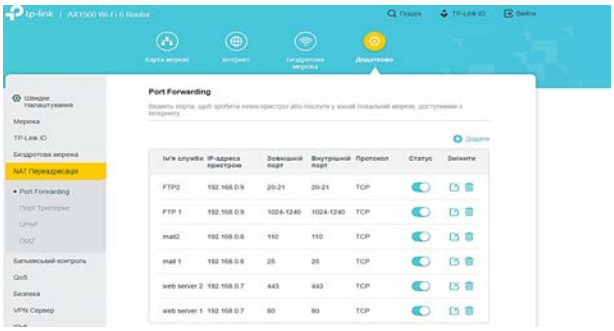


Рис. 10. Загальна таблиця налаштувань переадресування

Роутер Mikrotik не використовує поняття PAT. Таке налаштування робиться аналогічно створенню DMZ у програмі Winbox. Для цього переходимо до меню IP–Firewall–NAT (рис. 5,а), створюємо правило DST-NAT, вказуємо певні порти (рис. 5,б). Після чого треба призначити Action dst-nat на необхідну локальну IP-адресу та порт.

До недоліків цього методу відноситься складність налаштування фаєрволу на пороговому приладі, необхідність налаштування брандмауерів кожного вузла і, таким чином, необхідність індивідуальної конфігурації кожного вузла локальної мережі.

Для забезпечення повного доступу віддалених користувачів до всіх інформаційних ресурсів локальної мережі підрозділу доцільно використовувати VPN-сервіс [12]. Існує кілька типів VPN, зокрема PPTP, L2TP, SSTP, OpenVPN та різні види тунелів. Хоча це широке питання, у рамках даної роботи розглянуто організацію найпростішого типу VPN – PPTP. Цей тип має багато недоліків у сфері безпеки, однак відрізняється легкістю та швидкістю налаштування.

Використання такого сервісу дозволяє забезпечити доступ віддалених користувачів до всіх ресурсів локальної мережі та майже повністю імітувати їхню присутність у цій мережі. Водночас слід зазначити, що функція VPN інтегрована лише в обмежену кількість роутерів, вартість яких зазвичай вища. Серед роутерів, розглянутих у межах дослідження, таку можливість мають лише Wi-Fi роутер Tp-Link AX1500 Wi-Fi 6 і роутер Mikrotik.

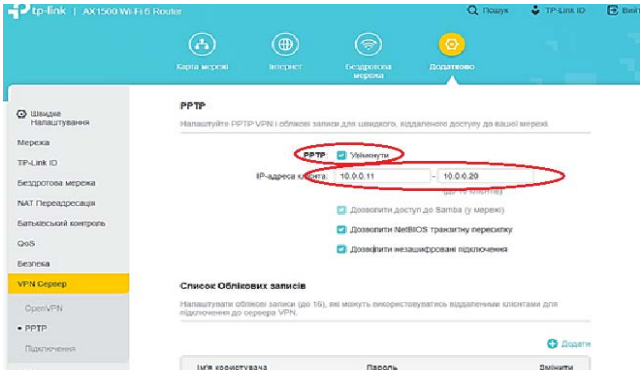


Рис. 11. Налаштування VPN PPTP на роутері Tp_link AX1500

Для створення VPN PPTP на роутері Tp_link AX1500 необхідно перейти на вебсторінку керування приладом та обрати меню «Додатково» – «VPN Сервер» – «PPTP» (рис. 11–12). Включити «PPTP», призначити діапазон IP-адрес користувачів, додати користувачів, вказавши їх паролі та імена.

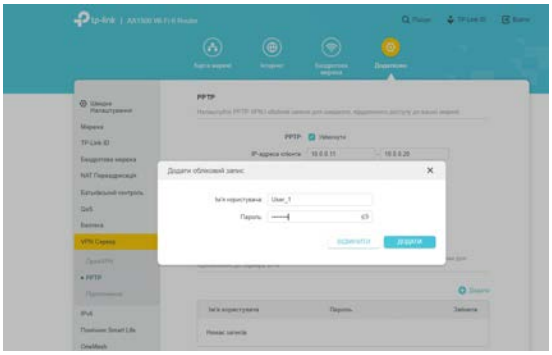
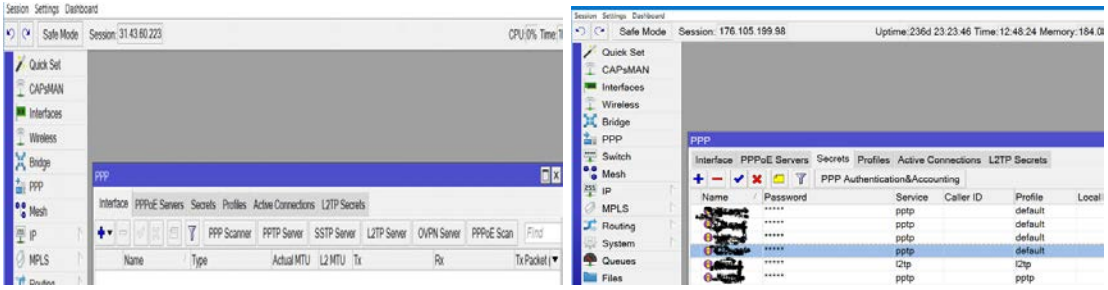


Рис. 12. Створення користувача на роутері Tp_link AX1500 у VPN PPTP

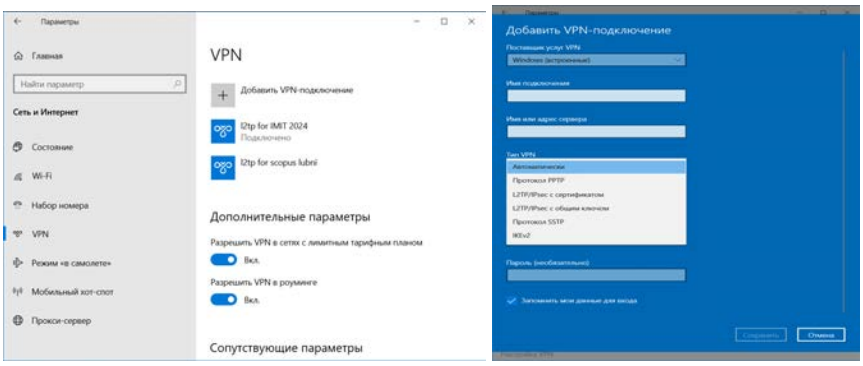
Слід відзначити, що для цього роутера є можливість створити до 16 користувачів, але одночасно можуть працювати тільки 10. Однак, роутер Miktotik такого обмеження не має [9]. У роутері Mikrotik для налаштування PPTP/L2tp/SSTP/OVPN у програмі Winbox [10] треба перейти до меню PPP/interface (рис. 13) та виконати налаштування та активізацію PPTP Server, L2TP Server, а потім налаштувати користувачів та профілі їх приєднання.



а) б)

Рис. 13. Меню Winbox для налаштування VPN у роутері Mikrotik:
а) створення VPN; б) створення користувачів

Усі створені користувачі зможуть підключатися до VPN на своїх персональних комп'ютерах після відповідного налаштування. Наприклад, у ОС Windows 10 це виконується через додаток «Параметри»: потрібно перейти до розділу «Мережа та Інтернет» – VPN – і вибрати «+ Додати VPN-підключення» (рис. 14).



а) б)

Рис. 14. Налаштування VPN у Windows 10:
а) перелік існуючих VPN; б) процес додавання та налаштування VPN

Така система VPN потенційно може бути використана для створення корпоративного середовища для підключення віддалених користувачів. Для цього необхідно більш ретельно провести вибір та перенаалагодження порогових пристроїв, але попередньо, провести ґрунтовний аналіз безпеки ресурсів спрямованих на загальне використання.

Висновки. Серед популярних моделей роутерів лише деякі здатні забезпечувати створення інтегрованої інформаційної системи та об'єднувати користувачів із можливістю віддаленого доступу. Проведений аналіз дозволяє прискорити створення корпоративних мереж у рамках обмежених бюджетів, зокрема для малих підприємств і навчальних закладів.

1. Якщо всі ресурси зосереджені на одному сервері підрозділу, організація віддаленого доступу до нього вирішується на всіх досліджених роутерах за допомогою функції DMZ. Необхідно відзначити, що є можливість використання двох і більше вузлів. Для цього слід мати необхідну кількість реальних IP-адрес: одна адреса на кожен вузол DMZ. Однак, така можливість є тільки у роутера Mikrotik за рахунок створення окремих правил для аналізу IP-адреси призначення. З іншого боку, цей підхід можливо використати при об’єднанні декількох підрозділів. Слід відзначити [1], що, IP вузол, який призначено DMZ не відділяється від внутрішньої мережі та може вільно підключитися до внутрішніх ресурсів. Налаштування DMZ на всіх досліджених роутерах не дозволяє застосувати будь яких заходів безпеки. Для ліквідації такого суттєвого недоліку треба встановлювати та налаштовувати додатковий міжмережевий екран у локальній мережі підрозділу.

2. Коли ресурси різного типу працюють з різними протоколами та розташовані на окремих вузлах підрозділу, організація єдиного інформаційного середовища здійснюється шляхом перенаправлення цих протоколів з урахуванням відповідних портів. Більшість сучасних роутерів підтримують такий підхід, однак необхідно ретельно враховувати специфіку протоколів і портів, які використовуються кожним ресурсом, адже деякі програмні додатки можуть задіювати велику кількість портів одночасно. До недоліків цього методу відноситься складність налаштування фаєрволу й відсутність централізованого контролю доступу, що вимагає індивідуальної конфігурації на кожному вузлі локальної мережі. Водночас цей спосіб може бути застосований для інтеграції кількох підрозділів в єдину систему.

3. Найефективнішим способом організації об'єднаного інформаційного середовища є використання системи серверів VPN. Серед досліджених моделей роутерів лише Tp-Link AX1500 і Mikrotik підтримують використання VPN-серверів з протоколами PPTP/L2TP. Проте залишається актуальною проблема забезпечення безпеки інформаційних ресурсів, яка вимагає окремого налаштування фаєрволу. Практичне впровадження цього підходу також виявило ряд інших недоліків:

– У випадку (рис. 15), коли декілька користувачів знаходяться за одним приладом з NAT виникає конфлікт навіть у разі використання різних імен користувачів. Таким чином одночасно може працювати тільки один.

– З’єднання VPN у операційній системі Windows 10 призначає шлюз за замовчанням на пороговий пристрій. Це приводить до того, що увесь трафік віддаленого користувача проходить через пороговий прилад в незалежності від того використовує користувач локальні ресурси чи ні.

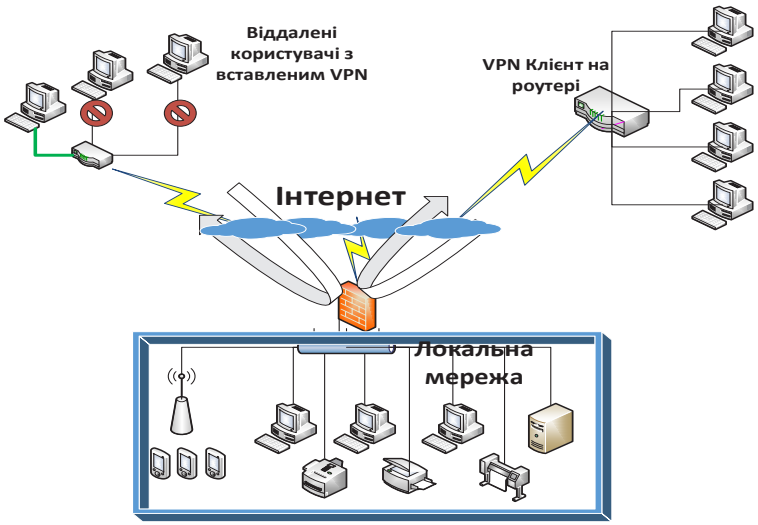


Рис. 15. Особливості VPN

Таким чином, встановлення системи VPN на користувацьких приладах це перший крок створення корпоративного інформаційного середовища, однак його не слід використовувати для об'єднання віддалених підрозділів. Для цього необхідно провести окремий аналіз можливості встановлення VPN клієнтів безпосередньо на порогових приладах віддалених підрозділів.

Отримані результати можуть бути застосовані для побудови інтегрованих інформаційних систем у бізнесі, освіті та інших галузях, які вимагають надійного й безпечного віддаленого доступу користувачів до локальних ресурсів.

Список використаних джерел:

1. Демілітаризована зона (комп'ютерні мережі) URL: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D0%BC%D1%96%D0%BB%D1%96%D1%82%D0%B0%D1%80%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D0%B7%D0%BE%D0%BD%D0%B0_(%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%96_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96)#cite_ref-FOOTNOTE%D0%A1%D0%BC%D1%96%D1%822006_2-0

2. Кардашук В., Бортник К., Багнюк Н. Проблеми захисту інформації у віртуальних приватних мережах та відбиття атак на Web-додатки. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2023. № 53. С. 117–124. URL: https://doi.org/10.36910/6775-2524-0560-2023-53-18 .

3. Могильний Г. А. Аналіз програмно-апаратних засобів створення системи з віддаленим доступом до навчальних комп'ютерних лабораторій закладів середньої освіти. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2023. № 1 (277). С. 5–19. URL: https://doi.org/10.33216/1998-7927-2019-256-8-5-19.

4. Могильний Г. А., Семенов М. А., Кірєєв І. Ю. Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2022. № 2 (272). С. 7–14. URL: https://doi.org/10.33216/1998-7927-2022-272-2-7-14

5. Недашківський О. Принципи побудови мереж передачі даних для надання vpn і інтернет послуг. *Сучасний захист інформації*. 2017. No2(30). С. 35–41. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/1487/1419.

6. Пархоменко І., Галкін В. Способи захисту каналів корпоративних мереж на базі vpn-рішень. *Сучасний захист інформації*. 2016. № 4. С. 35–40.

7. AC12g Dvukhdyapazonnыi hyhabytnыi Wi-Fi router. URL: https://www.mercusys.com/ru/product/details/ac12g (дата звернення: 21.10.2024).

8. AX1500 Wi-Fi 6 marshrutyzator URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/archer-ax10/ (дата звернення: 21.10.2024)

9. Main Page. Welcome to the MikroTik documentation wiki. URL: https://wiki.mikrotik.com/Main_Page (дата звернення: 21.10.2024)

10. MikroTik Software. Downloads. URL: https://mikrotik.com/download (дата звернення: 21.10.2024)

11. PAT URL: https://uk.wikipedia.org/wiki/PAT (дата звернення: 21.10.2024)

12. Point-to-Point Tunneling Protocol (PPTP) URL: https://www.ietf.org/rfc/rfc2637.txt (дата звернення: 21.10.2024).

13. PPP Protocol. URL: https://www.javatpoint.com/ppp-protocol (дата звернення 21.11.2023).

14. TL-WR840N V6.20. URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr840n/ (дата звернення: 21.10.2024).

15. Tyshyk I. CHOICE OF REMOTE ACCESS TECHNOLOGY FOR EFFECTIVE ORGANIZATION OF PROTECTION OF NETWORK CONNECTIONS. Cybersecurity: Education, Science, Technique. 2023. T. 3, № 19. С. 34–45. URL: https://doi.org/10.28925/2663-4023.2023.19.3445.

16. Wi-Fi роутер MikroTik hAP ac3 (RBD53iG-5HacD2HnD). URL: https://www.mikrotik.ua/ru/product/mikrotik-hap-ac3-rbd53ig-5hacd2hnd (дата звернення: 21.10.2024).

УДК 004.415-047.2:005.8
DOI https://doi.org/10.32689/maup.it.2024.4.17

Олександр ПСАРЬОВ
аспірант кафедри інформаційних технологій,
Сумський державний університет, aleksua18@gmail.com
***ORCID:** 0000-0003-2107-2751*

Євген ДРУЖИНІН
доктор технічних наук, професор кафедри інформаційних технологій проектування, Національний аерокосмічний університет імені М.Є. Жуковського,
druzhinin105@gmail.com
***ORCID:** 0000-0003-3121-4178*

AGILE-ФРЕЙМВОРК ЯК КАТАЛІЗАТОР ЕФЕКТИВНОГО ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЄЮ

Анотація. Предметом *даної статті є дослідження застосування гнучких методологій управління проектами, зокрема Agile, у контексті ефективного виконання та впровадження інформаційних систем управління. У статті розглядаються ключові аспекти впровадження Agile-підходів, їх вплив на продуктивність команди, якість результатів та задоволеність клієнтів, а також аналізуються проблеми та перспективи підвищення ефективності управлінських процесів в умовах сучасного бізнес-середовища. Ця стаття досліджує суть Agile-фреймворків та аналізує їхні управлінські характеристики. Вона підкреслює роль нагляду та контролю за проектом як ключових для досягнення успішних результатів у проектах і послугах, сприяючи послідовності та підвищенню продуктивності в різних ініціативах.*

Метою *цього дослідження є створення структурованого набору практик на основі Agile, які допомагають проектним командам досягати своїх цілей і сприяють цифровій трансформації. Зосереджуючись на компетенціях у сфері управління проектами, гнучких методологіях і масштабованих Agile-фреймворках, цей підхід акцентує увагу на техніках, необхідних для орієнтованої на послуги та проектної доставки. Запропонований фреймворк визначає конкретні завдання та оптимальні методи їх виконання, охоплюючи всі ключові області, такі як стратегія, планування, мобілізація ресурсів, управління, розробка та операційна діяльність – кожна з яких є важливою для впровадження рішень. Спеціально адаптоване для систем управління знаннями, це дослідження має на меті створити систему, яка забезпечує єдину мову та стандартизований підхід, що сприяє узгодженості у глобальній взаємодії. Завдяки дисциплінованим, індустріалізованим процесам цей фреймворк також підтримує надійну, високоякісну доставку рішень у різних локаціях, командах та культурних контекстах, забезпечуючи стабільну якість і своєчасне виконання.*

Висновки. *На основі наданих результатів дослідження можна стверджувати, що гнучкі способи виконання є ключем до наділення людей повноваженнями у формуванні майбутнього компанії.*

Ключові слова: *управління доставкою, підвищення ефективності, agile-фреймворк, системи управління інформацією, безперервне вдосконалення.*

Oleksandr PSAROV, Evgeniy DRUZHININ. AGILE FRAMEWORK AS A CATALYST FOR EFFECTIVE INFORMATION MANAGEMENT SYSTEM DELIVERY

Abstract. *The* ***subject*** *of this article is the study of applying agile project management methodologies, particularly Agile, in the context of the effective execution and implementation of information management systems. The article examines key aspects of Agile approach implementation, its impact on team productivity, result quality, and customer satisfaction, as well as analyzes challenges and prospects for improving management efficiency in the modern business environment. This paper delves into the core of agile frameworks and investigates their managerial attributes. It highlights the role of project oversight and control as essential for delivering successful outcomes in both projects and services, fostering consistency, and enhancing performance across initiatives.*

The purpose *of this research is to establish a structured set of Agile-based practices that support project teams in achieving their objectives and promote digital transformation. By focusing on competencies in project management, agile methodologies, and scalable Agile Frameworks, this approach emphasizes the techniques essential for service-oriented, project-based delivery. The proposed framework outlines specific tasks and optimal methods for execution, encompassing all critical domains such as strategy, planning, resource mobilization, management, development, and operations–each vital to solution implementation. Tailored specifically for knowledge management systems, this study aims to create a system that ensures a unified language and standardized approach, fostering consistency in global engagement. Through disciplined, industrialized processes, the framework also supports reliable, high-quality solution delivery across diverse locations, teams, and cultural contexts, ensuring dependable quality and timely results.*

Conclusions. *Based on the provided research outcomes, it can be stated that agile ways of working are key to empowering people in shaping the company's future.*

Key words: *delivery management, increasing efficiency, agile framework, information management systems, continuous improvement.*

Вступ. Сучасний бізнес стикається з численними викликами, пов'язаними з швидкими змінами ринку, технологічними інноваціями та зростаючими вимогами клієнтів. У цьому контексті гнучкі

методології управління проектами, такі як Agile, набувають особливої актуальності. Вони дозволяють організаціям швидко адаптуватися до змін і забезпечувати високу якість продуктів та послуг.

Проте впровадження Agile-фреймворків не завжди проходить успішно. Часто організації стикаються з проблемами, пов'язаними з недостатнім розумінням принципів Agile, опором змінам з боку команди, а також відсутністю належної підтримки з боку керівництва. Це може призводити до затримок у виконанні проектів, зниження продуктивності та незадоволеності клієнтів.

Таким чином, постає питання: як ефективно інтегрувати Agile-практики в управління проектами для досягнення високих результатів та задоволення потреб усіх учасників процесу? Це питання вимагає ретельного аналізу та дослідження, щоб виявити можливі шляхи підвищення ефективності та успішності впровадження гнучких методів у сучасних організаціях.

Завдання дослідження. Для досягнення поставленої мети дослідження необхідно вирішити низку завдань, які спрямовані на розкриття ключових аспектів проблематики.

Завдання дослідження:

1. Дослідити основні характеристики та принципи Agile-фреймворків у контексті управління інформаційними системами.

2. Визначити вплив Agile-підходів на продуктивність команди, якість результатів та задоволеність клієнтів.

3. Проаналізувати проблеми, що виникають при впровадженні Agile-методологій в інформаційних системах управління.

4. Розробити структурований набір практик на основі Agile для підтримки проектних команд у досягненні їхніх цілей.

5. Запропонувати рекомендації щодо підвищення ефективності управлінських процесів у проектно-орієнтованих та сервісно-орієнтованих середовищах.

Методологія та наукова новизна. Це дослідження використовує змішаний методичний підхід, поєднуючи якісний аналіз застосування Agile-фреймворків та кількісну оцінку результатів проектів на основі декількох кейс-стадій. Дані збиралися через інтерв'ю з керівниками проектів та членами команд, які впроваджують Agile-практики в різних середовищах. Додатково було проведено порівняльний аналіз для оцінки впливу методик на основі Agile на терміни виконання проектів, послідовність і якість у системах управління знаннями. **Новизна** цього дослідження полягає в адаптованому підході до застосування гнучких методологій, спеціально орієнтованому на сферу систем управління знаннями. Воно пропонує масштабований, стандартизований фреймворк, розроблений для подолання розриву між теорією Agile та практичною реалізацією в проектах на основі знань, акцентуючи увагу на культурній та географічній адаптивності. Це дослідження вносить внесок у існуючу літературу, пропонуючи структуровану, засновану на доказах модель, яка підвищує глобальну участь у проектах та забезпечує послідовні, високоякісні результати в складних, багатолокаційних середовищах.

Цільові права клієнтів. Управління портфелем клієнтів (Client Portfolio Management) – це процес використання відповідної інформації для прийняття рішень щодо портфеля клієнтів, категоризації клієнтів на основі їхнього потенціалу зростання та врахування інформації про пріоритетність клієнтів у поточних рішеннях щодо продажів. Регулярне управління портфелем клієнтів є важливим для того, щоб вони могли зосередити свої інвестиції на відносинах з найбільшим потенціалом віддачі [3, 13].

У результатах дослідження клієнти класифіковані на кілька категорій. Ці класифікації використовуються для впливу та/або управління діями у таких сферах, як планування та визначення цільових клієнтів для продажів, планування рахунків, інвестиції в розвиток бізнесу, схвалення нових бізнес-ініціатив та протоколи доступу. На рис. 1. зоброжено робочий процес для залучення нових клієнтів.

Рис. 1. Робочий процес залучення нових клієнтів

Бугалтерське планування. Бугалтерське планування є ключовим засобом для стимулювання органічного зростання, а також засобом розуміння проблем та невдач у досягненні довгострокової стратегічної програми зростання. Дослідження базуються на щоденному спілкуванні з як мінімум 1500 клієнтами щодо реалізації проектів та те, що ще можна зробити для розвитку клієнтських рахунків. Таким чином, у рамках гнучких методів роботи було запроваджено роль Ліда з Доставки (Delivery Lead) [4, 7], щоб можна було застосувати одну з методик доставки для підтримки клієнта та загальної команди управління проектами та портфелем.

Галузеве середовище. Індустрія консалтингу в галузі інформаційних технологій переживає безпрецедентні виклики у вигляді слабких ринків, глобального економічного сповільнення, консолідацій та злиттів, суворих регуляцій, природних катастроф та необхідності працювати на глобальному рівні. Ці перешкоди ускладнюються появою різних операційних викликів [8]:

– виведення нових продуктів і каналів на ринок;

– необхідність альтернативних каналів дистрибуції;

– заміна основних застарілих систем на системи наступного покоління;

– необхідність агрегування ризиків та формування єдиного уявлення про клієнта;

– тиск на ціни, послуги та час від нових учасників на ринку;

– труднощі з виходом на нові глобальні ринки – відсутність розуміння унікальних ринкових умов кожної країни.

Управління дотриманням нормативних вимог. Управління дотриманням нормативних вимог – це процес оцінки та моніторингу відповідності міжнародним стандартам і політикам взаємодії, таких як захист даних клієнтів, управління записами, виявлення та відстеження коригувальних дій для уникнення або зменшення ризиків взаємодії [9].

Програма захисту даних клієнтів є основним компонентом захисту інформаційної безпеки. Програма захисту даних клієнтів забезпечує команди, залучені до проекту, стандартизованим підходом до управління ризиками через набір процесів управління, контролю та метрик.

– Впровадження контролю захисту даних клієнтів – для кожного необхідного контролю необхідно визначити відповідальну особу за контроль, провести аналіз прогалин для кожного призначеного контролю, розробити план дій для усунення виявлених прогалин у контролі, здійснити моніторинг загальної відповідності контролю протягом усього терміну контракту(-ів).

– Контроль дотримання політик взаємодії, пов'язаних із поїздками, часом і витратами, закупівлями, обов'язковим навчанням, використанням методології.

– Виявлення питань відповідності та впровадження коригувальних або запобіжних заходів.

Якість бізнесу. План безперервності бізнесу – це план дій, спрямований на забезпечення продовження основних бізнес-процесів та послуг проекту у разі переривання, спричиненого будь-яким внутрішнім або зовнішнім фактором [6, 12]. Це набір документів, що визначають стратегію відновлення у випадку кризи. Як важлива частина фреймворку Agile Delivery, він враховує такі аспекти:

– люди – безпека та захист людей;

– комунікація – контроль комунікацій для уникнення чуток та хаосу;

– інфраструктура – здатність офісу підтримувати надання послуг у разі перебоїв з електроживленням та забезпечення безпеки;

– технології – вплив технологічних ресурсів на надання послуг;

Існує встановлена система управління безперервністю бізнесу, яка включає:

– політику управління безперервністю бізнесу;

– старше керівництво, відповідальне за управління безперервністю бізнесу;

– задокументовані плани безперервності бізнесу для проектів;

– можливості управління інцидентами;

– програму тестування та підтримки планів безперервності бізнесу та заходів з відновлення.

Призначені особи зі спеціалізації Agile відповідають за співробітників, які працюють у невеликих проектах із забезпечення ресурсами, а також за людей на «лавці запасних», щоб інформувати їх про заходи з безперервності бізнесу та необхідне навчання.

Огляд якості. Якість – це важливий спосіб захисту репутації як всередині компанії, так і зовнішнього бренду. Це передбачає як неформальне наставництво, так і структуровані огляди. Очікується, що забезпечення якості буде застосоване до всіх сфер роботи/послуг, які ми надаються, та на всіх етапах життєвого циклу проекту – починаючи з належної оцінки ризиків на етапі виникнення можливостей і закінчуючи контролем якості та постійним моніторингом і зниженням ризиків шляхом впровадження найкращих практик [10, 14].

Оцінка зрілості процесів проекту здійснюється для забезпечення відповідності проекту [11, 15]:

– політикам;

– методам доставки та найкращим практикам використання процесів і автоматизації у спеціалізованих напрямках;

– найкращим галузевим практикам, заснованим на моделі інтеграції зрілості можливостей (Capability Maturity Model Integration – CMMI) (рис. 2);

– визначеним процесам проекту.

Рис. 2. Модель інтеграції зрілості можливостей

Рівень зрілості (mature level) – це ступінь вдосконалення процесу в межах попередньо визначеного набору областей процесів, у яких досягнуті всі цілі:

– Базується на практиках нижчих рівнів.

– Представляє збільшення функціональності та можливостей.

– Може додавати нові функції.

Забезпечення якості доставки. Огляд забезпечення якості доставки (Delivery Quality Assurance) – це незалежні оцінки, що проводяться директорами з контролю якості (Quality Assurance Directors – QAD). Ці спеціалсти створені для огляду та оцінки загального ризику на основі фреймворку оцінки ризиків (Risk Assessment framework). Це здійснюється шляхом визначення рівня ризику, пов'язаного з та відповідністю по чотирьох блоках [1, 2]:

– Блок 1: Очікування клієнта та контекст.

– Блок 2: Структура контракту та угоди.

– Блок 3: План рішення та вартість.

– Блок 4: Базові можливості.

Для областей, що вважаються високоризиковими або з ризиком вище норми, оцінка вимагає документованих заходів щодо зменшення ризику та чіткого визначення відповідальних осіб за ці заходи [5].

Щомісяця команда QA проекту отримує дані, що витягуються з інструменту забезпечення якості та ризиків. Дані QA проекту включають:

– Статус плану QA проекту (Активний, Відхилений).

– Статус QA доставки від QAD (Зелений, Червоний, Жовтий).

– Дата останнього проведення.

– Дата наступного порушення терміну.

– Ім'я директора QA.

Дані проекту з глобального звіту ідентифікуються за номером контракту проекту. У разі відсутності проекту у глобальному витягу команда звертається до команди підтримки QA та уточнює причину.

Постійне вдосконалення. Підвищення продуктивності є частиною ціннісної пропозиції для клієнтів. Щоб надавати більше цінності клієнтам і компаніям, повинно прагнути до більш ефективної доставки з часом. Процес постійного вдосконалення – це безперервні зусилля, спрямовані на поліпшення продуктів, послуг або процесів.

Lean – це підхід, заснований на принципах, який спрямований на скорочення часу виконання, прискорення швидкості роботи та зниження операційних витрат шляхом постійної ідентифікації втрат (non-value-adding activities) у процесі (value stream) та їх усунення.

Опитування задоволеності команди клієнта (Client Team Satisfaction Survey – CTSS) дає змогу зрозуміти оцінку командою клієнта наданих послуг і цінності, яку було надано, наскільки добре було виправдано загальні очікування клієнта та загальну силу відносин. Опитування проводяться двічі на рік або при закритті проекту командою Delivery Excellence у співпраці з лідерами портфелів та проектів для уточнення обсягу опитування та аудиторії.

Якщо результати CTSS для проекту хоча б за одним із питань є нижчими за очікувані у фінансовому році, проекти повинні визначити заходи з покращення та реалізувати їх. Керівники доставки та проектів залучені до цього процесу шляхом організації обговорень щодо покращень, допомагаючи визначити завдання та відстежуючи прогрес їх реалізації. Усі створені дії щодо покращення CTSS відображаються як метрики.

Кожен проект повинен пройти наступний цикл:

1. Аналіз отриманого зворотного зв'язку.
2. Обговорення результатів із джерелом зворотного зв'язку.
3. Узгодження заходів з покращення та їх реалізація у встановлений термін.

Ефективна оцінка покращень у Lean-доставці та задоволеності клієнтів (CTSS) вимагає використання набору ключових показників (KPI). Ці метрики допоможуть виявити слабкі місця в процесах, підвищити ефективність і покращити клієнтський досвід. Основні метрики, які можна використовувати, включають:

1. Ефективність Lean-доставки (Efficiency)

Метрика, що показує, наскільки успішно були усунені неефективні процеси, виражається як співвідношення часу виконання (Lead Time) до та після Lean-доставки.

$$\text{Efficiency Improvement} = \frac{\text{Lead Time}_{\text{initial}} - \text{Lead Time}_{\text{new}}}{\text{Lead Time}_{\text{initial}}} \times 100\%, \quad (1)$$

де $\text{Lead Time}_{\text{initial}}$ – початковий час виконання;

$\text{Lead Time}_{\text{new}}$ – час виконання після оптимізації.

2. Показник виконання дій щодо покращення CTSS (CTSS Implementation Rate)

Цей показник відображає, який відсоток від запропонованих покращень був виконаний, і допомагає відстежити прогрес у виконанні поставлених завдань:

$$\text{CTSS Implementation Rate} = \frac{\text{Number of Implemented Actions}}{\text{Total Number of Actions Proposed}} \times 100\%, \quad (2)$$

де Number of Implemented Actions – кількість виконаниз дій;

Total Number of Actions Proposed – загальна кількість запропонованих дій з покращення.

3. Індекс задоволеності CTSS (Satisfaction Index)

Для оцінки рівня задоволеності клієнтів можна ввести індекс задоволеності, який розраховується на основі даних з опитувань CTSS. Середня оцінка по всіх питаннях ділиться на максимально можливий бал:

$$\text{CTSS Satisfaction Index} = \frac{\text{Total Score Obtained}}{\text{Maximum Possible Score}} \times 100\%, \quad (3)$$

де Total Score Obtained – сума балів, отриманих в опитуванні;

Maximum Possible Score – максимально можливий бал для всіх питань.

4. Рентабельність покращень (Return on Improvements, ROI)

Ця формула може бути корисною для розрахунку ефективності покращень, де підвищення продуктивності виражається через економію часу та ресурсів:

$$\text{ROI of Improvements} = \frac{\text{Cost Savings from Lean}}{\text{Cost of Implementing Improvements}} \times 100\%, \quad (4)$$

де Cost Savings from Lean – економія витрат від застосування Lean-доставки;

Cost of Implementing Improvements – витрати на реалізацію покращень.

5. Час циклу виконання завдань (Cycle Time)

Час циклу допомагає оцінити, скільки часу потрібно для завершення конкретного завдання, що є ключовим показником для виявлення можливостей скорочення часу в рамках Lean-доставки.

$$\text{Cycle Time} = \frac{\text{Total Time Spent on Tasks}}{\text{Number of Completed Tasks}}, \quad (5)$$

де Total Time Spent on Tasks – загальний час, витрачений на виконання завдань;

Number of Completed Tasks – кількість завершених завдань.

6. Швидкість виконання проекту (Velocity)

Швидкість дозволяє оцінити, як швидко команда може завершувати роботу за певний проміжок часу (спринт), що також може використовуватися для прогнозування тривалості проекту.

$$\text{Velocity} = \frac{\text{Total Story Points Completed}}{\text{Number of Itarations}}, \quad (6)$$

де Total Story Points Completed – загальна кількість завершених "Story Points" (задач, оцінених у балах);

Number of Itarations – кількість ітерацій або спринтів.

7. Індекс усунення помилок (Defect Removal Efficiency, DRE)

Ця метрика показує, наскільки ефективно команда виявляє та виправляє помилки до того, як продукт досягне кінцевого користувача.

$$\text{DRE} = \frac{\text{Defects Found During Development}}{\text{Total Defects (Found During Dev.} + \text{Found After Release)}} \times 100\%, \quad (7)$$

де Defects Found During Development – кількість дефектів, знайдених під час розробки;

Total Defects – загальна кількість дефектів, знайдених під час розробки та після випуску.

8. Індекс зменшення відходів (Waste Reduction Rate)

Ця метрика показує рівень зменшення «відходів» (нецінових активностей) у процесі за певний період.

$$\text{Waste Reduction Rate} = \frac{\text{Initial Waste} - \text{Current Waste}}{\text{Initial Waste}} \times 100\%, \quad (8)$$

де Initial Waste – кількість нецінових активностей до застосування Lean-доставки;

Current Waste – кількість нецінових активностей після оптимізації процесу.

9. Рівень задоволеності клієнтів (Customer Satisfaction Score, CSAT)

Рівень задоволеності клієнтів можна виміряти, використовуючи результати опитувань або відгуків, з метою оцінки того, наскільки Lean-доставка відповідає потребам клієнта.

$$\text{CSAT} = \frac{\text{Number of Satisfied Responses}}{\text{Total Number of Responses}} \times 100\%, \quad (9)$$

де Number of Satisfied Responses – кількість позитивних відповідей;

Total Number of Responses – загальна кількість відповідей.

10. Час до внесення змін (Change Implementation Time)

Ця метрика вимірює, наскільки швидко команда здатна вносити зміни після їхнього виявлення або запиту.

$$\text{Change Impl. Time} = \text{Time of Change Compl.} - \text{Time of Change Request} \quad (10)$$

де Time of Change Completion – час завершення внесення змін

Time of Change Request – час запиту на внесення змін.

Застосування цих метрик забезпечує комплексний підхід до оцінки ефективності Lean-доставки, а також дозволяє фокусувати зусилля на подальшому вдосконаленні процесів і підвищенні рівня задоволеності клієнтів.

Комплексний контроль ефективності: Використання зазначених метрик забезпечує цілісний огляд процесу Lean-доставки та ефективності виконання завдань. Це дозволяє командам оперативно виявляти слабкі місця та спрямовувати зусилля на їх усунення.

Покращення взаємин з клієнтами: Регулярний моніторинг індексу задоволеності CTSS допомагає не лише підтримувати високий рівень обслуговування, а й зміцнювати довіру клієнтів до процесу постійного покращення, що є важливим для збереження конкурентоспроможності.

Економічна вигода від оптимізації: Показник рентабельності покращень (ROI) демонструє, що витрати на впровадження Lean-доставки виправдовуються завдяки економії часу та ресурсів. Це підкреслює цінність інвестицій у постійні вдосконалення.

Прогнозування майбутніх результатів: Вимірювання показника швидкості та часу циклу дозволяє прогнозувати майбутні терміни виконання завдань, що дає змогу більш точно планувати ресурси та управління проектами.

Підвищення адаптивності команди: Систематичне застосування Lean-метрик допомагає команді швидше реагувати на зміни в вимогах клієнтів і адаптуватися до нових умов, підвищуючи її гнучкість

і стійкість до ринкових викликів.

Висновки. Закриття проекту або програми потрібно планувати ще на етапі виконання проекту. Це включає обмірковування того, як кінцеві результати будуть переглянуті та затверджені клієнтом, а також операційні дії, необхідні для закриття контракту/проекту в системах проектного управління. Дані та процеси, отримані під час закриття, допомагають створювати тематичні дослідження та трендові дані для постійного розвитку та вдосконалення процесів.

На основі наданих результатів досліджень, видно, що підходи Agile Delivery є ключовими для надання людям можливості брати відповідальність за майбутнє компанії. Це означає, що кожен має право голосу та роль у створенні більшої цінності для клієнтів, особливо в доставці систем управління інформацією як проектів, повсякденних операцій і стратегічних змін.

Список використаних джерел:

1. Berntzen M., Moe N. B., Stray V. The product owner in large-scale agile: an empirical study through the lens of relational coordination theory. *Agile Processes in Software Engineering and Extreme Programming*: 20th International Conference, XP 2019, Montréal, QC, Canada, May 21–25, 2019: Proceedings / Eds.: P. Kruchten, S. Fraser, F. Coallier. Canada: Springer, 2019. P. 121–136. DOI: 10.1007/978-3-030-19034-7_8
2. Girma M., Garcia N., Kifle M. Agile Scrum Scaling Practices for Large Scale Software Development. *2019 4th International Conference on Information Systems Engineering (ICISE 2019)*, 4-6 May, Shanghai, China, 2019. P. 34–38. DOI: 10.1109/ICISE.2019.00014
3. Hoelbeche L. Designing sustainably agile and resilient organizations. *Systems Research and Behavioral Science*. 2019. Vol. 36, Issue 5. P. 668–677. DOI: https://doi.org/10.1002/sres.2624
4. Hofman M., Grela G. Project portfolio risk identification – application of Delphi method. *Journal of Business and Economics*. 2015. Vol. 6, No. 11. P. 1857–1867. DOI: 10.15341/jbe(2155-7950)/11.06.2015/004
5. Horlach B., Schirmer I., Böhmann T., Drews P. Agile Portfolio Management Patterns: A Research Design. *Proceedings of the 19th International Conference on Agile Software Development: Companion*. May 21-25, 2018, Porto Portugal / ed. A. Aguiar. New York : Association for Computing Machinery, 2018. Article 9. P. 1–6. DOI: https://doi.org/10.1145/3234152.3234179
6. Ivanov V. Process-Oriented Approach to Fixture Design. *Advances in Design, Simulation and Manufacturing:* Proceedings of the International Conference on Design, Simulation, Manufacturing: The Innovation Exchange, DSMIE-2018, June 12–15, 2018, Sumy, Ukraine / Eds.: V. Ivanov et al. Springer, Cham, 2019. P. 42–50. DOI: https://doi.org/10.1007/978-3-319-93587-4_5
7. Ivanov V., Liaposhchenko O., Denysenko Y., Pavlenko I. Ensuring economic efficiency of flexible fixtures in multiproduct manufacturing. *Engineering Management in Production and Services*. 2021. Vol. 13, Issue 1. P. 53–62. DOI: 10.2478/emj-2021-0004
8. Kischelewski B., Richter J. Implementing large-scale agile – an analysis of challenges and success factors. *Proceedings of the 28th European Conference on Information Systems (ECIS*), Marrakech, Morocco, June 2020. URL: https://aisel.aisnet.org/ecis2020_rp/176 (Last accessed: 05.11.2024).
9. Kotliar A., Basova Y., Ivanov V., Murzabulatova O., Vasyltsova S., Litvynenko M., Zinchenko O. Ensuring the economic efficiency of enterprises by multi-criteria selection of the optimal manufacturing process. *Management and Production Engineering Review*. 2020. Vol. 11, No. 1. P. 52–61. DOI: 10.24425/mper.2020.132943
10. Medvediev Ie., Muzylyov D., Shramenko N., Nosko P., Eliseyev P., Ivanov V. Design Logical Linguistic Models to Calculate Necessity in Trucks during Agricultural Cargoes Logistics Using Fuzzy Logic. *Acta Logistica -International Scientific Journal about Logistics.* 2020. Vol. 7, Issue 3. P. 155–166. DOI: https://doi.org/10.22306/al.v7i3.165
11. Muzylyov D., Shramenko N. Blockchain Technology in Transportation as a Part of the Efficiency in Industry 4.0 Strategy. *Advanced Manufacturing Processes* : Selected Papers from the Grabchenko's International Conference on Advanced Manufacturing Processes (InterPartner-2019), September 10-13, 2019, Odessa, Ukraine / Eds.: V. Tonkonogyi et al. Springer, Cham, 2020. P. 216–225. DOI: https://doi.org/10.1007/978-3-030-40724-7_22
12. Muzylyov D., Shramenko N., Ivanov V. Management Decision-Making for Logistics Systems Using a Fuzzy-Neural Simulation. *Advances in Industrial Internet of Things, Engineering and Management* / Eds.: D. Cagáňová, N. Horňáková, A. Pusca, P. F. Cunha. Springer, Cham, 2021. P. 175–192. DOI: https://doi.org/10.1007/978-3-030-69705-1_11
13. Nguyen D. S. Success factors that influence agile software development project success. *American Scientific Research Journal for Engineering, Technology and Sciences*. 2016. Vol. 17, No. 1. P. 172–222. URL: https://www.asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/1425 (Last accessed: 18.08.2022).
14. Pavlenko O., Velykodnyi D., Lavrentieva O., Filatov S. The procedures of logistic transport systems simulation in the petri nets environment. *CEUR Workshop Proceedings*. 2020. Vol. 2732. P. 854–868. URL: https://ceur-ws.org/Vol-2732/20200854.pdf (Last accessed: 05.11.2024).
15. Psarov O., Druzhinin E. Enhancing Agile team productivity with metrics. *Scientific Journal of the Ternopil National Technical University*. 2024. № 1 (113). P. 93–99. DOI: https://doi.org/10.33108/visnyk_tntu2024.01.093

УДК 004.275:658.8
DOI https://doi.org/10.32689/maup.it.2024.4.18

Денис РЕДЬКО
аспірант кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, d.redko@knute.edu.ua
ORCID: *0009-0003-5827-264X*

Альона ДЕСЯТКО
доктор філософії «Комп'ютерні науки», доцент кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет, desyatko@knute.edu.ua
ORCID: *0000-0002-2284-3418*

Байтума БІСАРІНОВ
доктор філософії «Комп'ютерні науки», кафедра інформаційних систем, Казахський національний університет імені Аль-Фарабі, Алматинський університет енергетики та телекомунікацій, baituma_bai@gmail.com
ORCID: *0000-0002-2218-0749*

Айгуль БІСАРІАНОВА
доктор філософії «Комп'ютерні науки», доцент кафедри інформаційних систем, Міжнародний університет інформаційних технологій (IITU), King's College London, aigulbis@gmail.com
ORCID: *0000-0001-6629-3051*

ОГЛЯД МЕТОДІВ АНАЛІЗУ ТРАФІКУ КОМПАНІЇ НА ОСНОВІ АНСАМБЛЕВОЇ КЛАСТЕРИЗАЦІЇ

Анотація*. У статті наведено огляд існуючих досліджень, присвячених аналізу трафіку компаній з використанням методів кластеризації даних. Виходячи з аналізу наукових публікацій, розглянутих у цій роботі, підкреслюється важливість розробки нових кібернетичних систем для аналізу трафіку у великих організаціях. Подібні системи, насамперед, мають бути спрямовані на оптимізацію маршрутизації, зниження витрат та підвищення швидкості доставки. Розглядається можливість створення подібної кластерної платформи, що забезпечує розподілену обробку даних та інтеграцію різних типів сховищ даних. Для ефективного збору та зберігання інформації пропонується використовувати такі джерела, як серверні логи, дані з датчиків трафіку, геолокаційні відомості та маршрути пересування користувачів, також залежно від специфіки бізнес-процесів компанії можуть використовуватися й інші дані.*

Метою дослідження *є систематизація існуючих методів та підходів до аналізу трафіку компаній з використанням різних методів кластеризації даних, і в тому числі колективних (ансамблевих) рішень. У статті застосовується* ***методологія*** *аналітичного методу дослідження, який включає огляд існуючої літератури, аналіз попередніх робіт і систематизацію знань в області кластерного аналізу трафіку. Наше дослідження фокусується на оцінці різних підходів та технологій, які використовуються для обробки великих даних.*

Наукова новизна *полягає у розгляді ансамблевих методів кластеризації для аналізу мережевого трафіку, що забезпечують масштабованість, швидкість обробки та гнучкість систем. Запропоновано інтеграцію різних джерел даних для оптимізації бізнес-процесів і прийняття рішень, враховуючи сучасні виклики Big Data.*

Висновки. *Було продемонстровано, що кластерні рішення, у тому числі, на основі колективних (ансамблевих) алгоритмів забезпечують масштабованість, високу швидкість обробки, доступність даних та сервісів, а також гнучкість у застосуванні різноманітних інструментів та технологій. Тим не менш, реалізація таких систем пов'язана з технічними викликами, що вимагають глибоких знань у галузі Big Data, машинного навчання та кластерних технологій, а також значних витрат на обладнання, програмне забезпечення та кваліфікованих фахівців. Незважаючи на ці складності, застосування колективних кластерних рішень для аналізу великих даних може забезпечити компаніям значні конкурентні переваги через оптимізацію бізнес-процесів, покращення якості прийняття рішень та підвищення загальної ефективності діяльності.*

Ключові слова: *мережевий трафік, великі дані, методи аналізу даних, кластеризація, колективні рішення, ансамблеві моделі.*

Denys REDKO, Alona DESIATKO, Baituma BISSARINOV, Aigul BISSARINOVA. OVERVIEW OF COMPANY TRAFFIC ANALYSIS METHODS BASED ON ENSEMBLE CLUSTERING

Annotation*. The article provides an overview of existing research devoted to the analysis of company traffic using data clustering methods. Based on the analysis of scientific publications reviewed in this work, the importance of developing new cybernetic systems for traffic analysis in large organizations is emphasized. Such systems, first of all, should be aimed at optimizing routing, reducing costs and increasing delivery speed. The possibility of creating a similar cluster platform that provides distributed data processing and integration of various types of data storage is under consideration. For effective collection and storage of information, it is suggested to use such sources as server logs, data from traffic sensors, geolocation information and user movement routes, and depending on the specifics of the company's business processes, other data may be used.*

The purpose of the study *is to systematize existing methods and approaches to the analysis of company traffic using various methods of data clustering, including collective (ensemble) solutions. The article uses* ***the methodology*** *of the analytical method of research, which includes a review of existing literature, analysis of previous works and systematization of knowledge in the field of traffic cluster analysis. Our research focuses on evaluating different approaches and technologies used to process big data.*

The scientific novelty *consists in the consideration of ensemble clustering methods for network traffic analysis, which provide scalability, processing speed and flexibility of systems. The integration of various data sources is proposed to optimize business processes and decision-making, taking into account the modern challenges of Big Data.*

Conclusions*. It was demonstrated that cluster solutions, including those based on collective (ensemble) algorithms, provide scalability, high processing speed, availability of data and services, as well as flexibility in the application of various tools and technologies. However, the implementation of such systems is associated with technical challenges that require deep knowledge in the field of Big Data, machine learning and cluster technologies, as well as significant costs for hardware, software and skilled professionals. Despite these difficulties, the application of collective cluster solutions for big data analysis can provide companies with significant competitive advantages by optimizing business processes, improving the quality of decision-making and increasing the overall efficiency of operations.*

Key words: *network traffic, big data, data analysis methods, clustering, collective solutions, ensemble models.*

Вступ. Використання технологій Big Data при вирішенні завдань, пов'язаних з аналізом мережевого трафіку для великих компаній, відіграє ключову роль, зокрема, при його оптимізації та масштабуванні структури мережі компанії, оскільки подібні технології дозволяють отримувати цінну інформацію з величезних масивів корпоративного трафіку, виявляти приховані закономірності та тенденції, що є критично важливим для покращення продуктивності та безпеки, у тому числі для мереж компаній. Ці дані необхідно структурувати, класифікувати та піддавати глибокому аналізу для того, щоб вирішити вищезазначені завдання [1].

Кластерний аналіз (або далі будемо використовувати абревіатуру КА) є основою для багатьох підходів до дослідження трафіку [3, 4]. Кластеризація, є процесом сегментації даних шляхом об'єднання схожих елементів у групи або «кластери», допомагає виявляти однорідні сегменти трафіку, які можуть бути проаналізовані як окремі одиниці з певними характеристиками [2]. В результаті КА формуються групи об'єктів з високим ступенем подібності. Так, наприклад, для завдань аналізу трафіку та структури мережі великої компанії незалежно від галузевої спрямованості (банки, торгівля, логістика, промисловість, сільське господарство та ін.), групи об'єктів з високим ступенем подібності, що формуються в результаті кластеризації, можуть включати такі категорії [5–8, 11–20, 23, 24]:

– типи трафіку, наприклад, веб-трафік (HTTP/HTTPS запити та відповіді, відвідування веб-сайтів, використання веб-додатків); поштовий трафік (SMTP, IMAP, POP3 та інші протоколи електронної пошти); файловий трафік (передача даних через FTP, SFTP, SMB та інші протоколи обміну файлами); потоковий трафік (відео та аудіо потоки, що використовують протоколи, такі як RTP, RTSP, HLS);

– активність користувача, наприклад, групи користувачів (співробітники певних відділів, віддалені користувачі, адміністративний персонал);

– поведінкові патерни, наприклад, типові часові рамки активності, звички використання додатків і сервісів.

– мережеві пристрої, наприклад, типи пристроїв (робочі станції, сервери, мобільні пристрої, IoT-пристрої); функціональні групи (пристрої з однаковими функціями, такі як сервери баз даних, веб-сервери, мережеві шлюзи);

– застосунки та сервіси, наприклад, до цієї категорії можна віднести – кластери додатків (угруповання за використовуваними протоколами та типами даних, що передаються додатками); сервіси (веб-сервіси, бази даних, хмарні сервіси, служби зберігання даних);

– аномалії та загрози, наприклад, аномальна поведінка (трафік, який відхиляється від типових патернів, що може сигналізувати про можливі атаки чи зловживання) тощо.

Подібні та інші групи, які не увійшли до вищенаведеного переліку, допомагають у подальшому аналізі для оптимізації трафіку, виявлення аномалій, покращення безпеки та підвищення ефективності мережі. Таким чином, кластеризація дозволяє ідентифікувати та ізолювати різні типи трафіку та їх джерела, що полегшує управління мережею та забезпечення її надійної роботи.

Постановка проблеми. Проблема полягає в необхідності ефективної обробки та інтерпретації великих обсягів інформації, що отримується з різних джерел, таких як серверні логи, датчики трафіку та геолокаційні дані. Без впровадження сучасних рішень для обробки та аналізу даних, компанії ризикують втратити конкурентні переваги через низьку швидкість аналізу, високі витрати на обробку та нестачу інформації для прийняття обґрунтованих рішень. Необхідність розробки адаптивних та масштабованих систем для обробки та аналізу трафіку стає актуальною, враховуючи динамічні зміни в бізнес-середовищі та зростаючі вимоги до оперативності та точності даних.

Аналіз останніх досліджень та публікацій. Критерієм якості кластеризації є функціонал, який залежить від об'єктів усередині груп та відстаней між ними [2–05, 8, 13, 14, 17, 18, 20, 24]. На відміну від класифікації, при кластеризації спочатку не визначено число та властивості класів (кластерів), що дає можливість, наприклад, для нашого завдання адаптивно аналізувати трафік та виявляти нові аномалії та тенденції.

Відповідно до [14, 17, 18], особливості кластеризації включають:

– можливість виявлення раніше невідомих класів об'єктів з урахуванням початкових характеристик;

– здатність ефективно обробляти великі обсяги даних за короткий термін.

Для підвищення стійкості рішень у задачах кластеризації можна використовувати ансамблі алгоритмів, які формують колективне рішення з урахуванням думок всіх учасників ансамблю. Цей підхід є особливо актуальним при аналізі трафіку, де обсяг даних великий, а структура трафіку може бути складною та різноманітною.

Таким чином, основні переваги та особливості кластерного аналізу роблять його незамінним інструментом для оптимізації та масштабування мережевого трафіку у великих компаніях. Тому в роботі основна увага приділяється розробці ансамблю алгоритмів кластеризації на основі динамічних метрик відстаней для аналізу великих обсягів трафіку, що дозволяє значно покращити якість та швидкість аналізу.

Результати дослідження. У сучасному світі обсяги даних, що генеруються корпоративними мережами, зростають з неймовірною швидкістю, що створює нові виклики та можливості для аналізу мережевого трафіку з метою його оптимізації та підвищення безпеки, пропускної спроможності та ін. Одним з ефективних методів обробки великих обсягів мережевого трафіку є кластеризація даних [1–8, 11– 8, 20, 24]. Кластеризація дозволяє сегментувати трафік на однорідні групи, що сприяє більш точному виявленню закономірностей, аномалій та потенційних загроз.

Дослідження останніх років, що розглядаються далі, демонструють значний прогрес у використанні методів кластерного аналізу (КА) для вирішення завдань, пов'язаних із аналізом мережевого трафіку. Зокрема, вчені у своїх роботах [8, 13, 14, 17, 18] розглядають різні алгоритми кластеризації та їх модифікації для підвищення точності та швидкості обробки даних. Літературний аналіз [6–10, 15–19, 23] показав, що поєднання кластеризації з методами машинного навчання (МН) та штучного інтелекту (ШІ) також є перспективним напрямом.

У даному дослідженні короткий аналіз подано ключові роботи, в основному за останні 5–10 років, присвячені застосуванню КА для дослідження трафіку компаній, їх основні висновки отримані в ході цих досліджень і застосовані авторами розглянутих робіт і методології. Такий аналіз дозволить краще зрозуміти поточний стан досліджень у цій галузі та визначити напрями для подальшого розвитку нових досліджень у даній сфері.

У [20] розглядаються дванадцять існуючих методів кластеризації. Огляд, виконаний авторами роботи, дозволив розглянути існуючі проблеми та рекомендації для подальших досліджень у галузі кластеризації потоків трафіку.

У [13] запропоновано алгоритм класифікації трафіку на основі поліпшеної кластеризації K-means. Авторами дослідження наочно продемонстровано принцип роботи алгоритму для цієї задачі, а також проведено порівняння отриманих результатів та верифікацію на тестовому наборі даних.

У [17] автори порівнюють алгоритми EM, DBScan та RAIN для аналізу трафіку корпоративних мереж.

Зауважимо, що ідея використання кластеризації даних для аналізу мережевого трафіку не є новою. Її коріння сягає кінця 60-х, початок 70-х років минулого століття, коли почалися перші спроби систематизувати і структурувати великі обсяги даних, для виявлення закономірностей і аномалій у мережевих взаємодіях. З того часу дослідники постійно вдосконалюють методи кластеризації, адаптуючи їх до нових викликів, пов'язаних із зростанням обсягу та складності мережевого трафіку.

Вже наприкінці 60-х і на початку 70-х років минулого століття, з'явилися перші публікації, що розглядаються нижче, присвячені кластерному аналізу мережевих даних. Ці ранні роботи, наприклад, [14] заклали основу для подальших досліджень та розробок. З того часу методи кластеризації розвивалися в різних напрямках, від простих алгоритмів, таких як K-means, до складних ансамблевих методів, що поєднують переваги декількох алгоритмів для досягнення більш точних і надійних результатів.

Ранні дослідження [14] показали, що кластеризація може бути ефективно використана для сегментації мережевого трафіку, дозволяючи виділити однорідні групи даних та проводити їх детальніший аналіз.

В останні десятиліття, з розвитком технологій Big Data та збільшенням обчислювальних потужностей, інтерес до КА даних у контексті вивчення та оптимізації мережевого трафіку значно зріс. Сучасні

дослідження фокусуються на розробці більш складних та точних методів, включаючи використання МН та ШІ для покращення якості кластеризації.

У [14] запропоновано неієрархічний метод розбиття. У [18] метод K-means був застосований для розбиття наборів даних на кластери на основі заздалегідь визначеної кількості спочатку вибраних центроїдів (k). Згідно з висновками автора [18] удосконалений алгоритм, запропонований у даній роботі, дозволяє використовувати евклідову відстань для зменшення помилок, що виникають при обчисленні середніх квадратів з цільової функції.

У роботі [8] запропоновано підхід до двоетапної класифікації мережевого трафіку з використанням кластеризації K-means для покращення управління якістю обслуговування (QoS). Метою даного дослідження було розробити ефективний класифікатор, здатний розпізнавати цільові програми та виявляти невідомі потоки (шум) у мережі. Запропонований метод класифікації ґрунтувався на аналізі поведінки потоків трафіку та складався з двох основних фаз: 1) фаза присвоєння; 2) фаза маркування. У фазі присвоєння потоки призначаються певному кластеру, а фазі маркування використовується алгоритм присвоєння потокам відповідних міток. Ці етапи дозволяють оновлювати класифікатор для його подальшого використання у системі управління трафіком.

У роботі [24] автори розглядають метод BIRCH, який включає масштабованість у модель кластеризації. У своєму дослідженні вони використовують дерево ознак кластеризації (CF-дерево), та багаторівневу кластеризацію для обробки великих наборів даних через два основні етапи, кожен з яких має додаткову фазу. На першому етапі великі набори даних або об'єкти даних стискаються в компактне CF-дерево, що зберігає базову структуру кластерів. На другому етапі застосовується агломераційний алгоритм у поєднанні з іншими гнучкими методами кластеризації для створення вихідних кластерів, які потім уточнюються на основі їх центроїдів.

У роботі [12] автори запропонували ієрархічний кластеризаційний алгоритм під назвою Clustering Using Representatives (CURE). Даний алгоритм був розроблений для кластеризації великих наборів даних і здатний ефективно справлятися зі спотвореннями, спричиненими викидами. Він особливо добре підходить для кластерів довільної та несферичної форми з високою дисперсією. На відміну від алгоритму BIRCH, CURE спочатку випадково вибирає підвибірку даних і поділяє її на секції перед початком кластеризації. Потім ці секції частково групуються для видалення викидів. Після видалення викидів часткові кластери повторно кластеризуються для отримання дрібніших кластерів, які потім поєднуються в остаточні кластери. Такий підхід дозволяє покращити стійкість алгоритму до викидів та точніше виявляти структуру даних.

У роботі [11] автори запропонували алгоритм кластеризації, заснований на щільності, названий DBSCAN. Метою цього алгоритму було виявлення кластерів довільної форми та визначення шуму в даних. Грунтуючись на щільності, DBSCAN враховує якість кластерів та їхню здатність ідентифікувати шумові точки. Для визначення кластерів у DBSCAN використовуються два основні параметри: Eps та MinPts. Параметр Eps визначає радіус окружності точки (P), який визначає досяжність щільності, а MinPts – мінімальна кількість точок на окружності Eps, необхідне для формування кластера. Процес кластеризації починається з довільної точки (a), і якщо відстань від точки (a) до (P) менше або дорівнює Eps, точка додається в кластер. Цей процес триває ітеративно для включення нових точок у кластер. DBSCAN має чутливість до вибору параметрів Eps та MinPts, що може ускладнювати їх налаштування. Однак, при правильному налаштуванні, DBSCAN ефективно виявляє кластери довільної форми та стійкий до шуму даних.

У роботі [6] автори запропонували алгоритм OPTICS для подолання недоліків, властивих DBSCAN. На відміну від DBSCAN, OPTICS менш чутливий до налаштування параметрів. Як і інші методи, що ґрунтуються на щільності, OPTICS генерує порядок кластеризації, який містить інформацію про структуру кластерів для широкого діапазону значень параметрів. OPTICS добре масштабується при зміні значень Eps (ε) в діапазоні від 10 000 до 100 000. Це дозволяє алгоритму працювати швидко та ефективно навіть з великими обсягами даних, притаманних трафіку компаній, коли обсяг даних, для короткого проміжку часу, може досягати кількох десятків терабайт. Таким чином, OPTICS забезпечує, на думку авторів, більш гнучку та детальну ідентифікацію кластерних структур порівняно з DBSCAN.

У роботі [19] автори застосували гібридне рішення на основі алгоритмів OPTICS та DBSCAN для вирішення проблеми вибору відповідного порога щільності при виявленні спільнот у соціальних мережах. Вибір правильного порога щільності сприяє отриманню змістовних кластерів. Оскільки щільність визначається функцією відстані, використання OPTICS дозволило авторам вибрати оптимальне значення параметра Eps для DBSCAN, а також реалізувати результати використання змінних порогових значень щільності. Питання про те, чи можливе справжнє визначення спільноти в соціальних мережах, залишається відкритим, як показав аналіз авторів, які проводили це дослідження.

Дослідження в галузі класифікації IP та трафіку з використанням унікальних характеристик потоку також виявилися дуже ефективними. У роботі [23] автори запропонували автоматизований метод класифікації, що ґрунтується на статистичних характеристиках потоку, з використанням NetMate [16]. Цей неконтрольований метод використовує алгоритм максимізації очікувань [15] та алгоритм AutoClass [8]. Пакети спочатку розбиваються на двоспрямовані потоки обчислення характеристик потоку. Разом з атрибутами моделі потоків класи можуть бути вивчені для подальшої класифікації нових потоків. Результати можуть бути використані для оцінки та інших цілей QoS.

Напівконтрольовані методи (semi-supervised clustering) також призвели до нового виміру досліджень у галузі КА. Наприклад, у роботі [10] авторами представлені результати досліджень, присвячених кластеризації з використанням контрольованих та неконтрольованих методів. У проектуванні використовувалися контрольні точки пакетів. Автори досліджували класифікацію трафіку з використанням характеристик потоку в додатках та запропонували напівконтрольований метод класифікації трафіку з відомих та невідомих додатків. Класифікатор навчається шляхом порівняння потоків трафіку переважно з потоками без міток, при цьому мінімально включаються потоки з мітками.

Щоб підвищити точність методів класифікації, у роботі [21] автори запропонували напівконтрольовану стратегію, яка називається обмеженими K-means на основі множин. Статистичні характеристики потоку вилучаються разом із деякою довідковою інформацією про потоки TCP/IP. Для моделювання даних, що спостерігаються використовується гауссова суміш щільностей. У роботі було встановлено, що введення дискретних ознак в кластеризацію потоків може підвищити точність кластеризації. На основі ступеня подібності або відмінності функцій потоку, вони групуються відповідно до п'яти міток кортежів, що включають вихідні та цільові IP-адреси, вихідні та цільові порти, а також протокол, що використовується портом. Потоки, що мають схожість у різних застосунках, швидше за все, будуть згруповані у певний кластер.

У рамках програмно-конфігурованих мереж (SDN) [22] автори розробили метод класифікації трафіку, поєднуючи вимоги щодо якості обслуговування з реалізацією Deep Packet Inspection (DPI). Вони виявляли вхідні потоки з тривалим терміном служби за допомогою комутатора SDN. Використовуючи значення пакета Херста, порту та середнього часу між прибуттям пакетів як вхідні дані у функцію співставлення, трафік класифікувався за відповідними класами QoS. Статистичні ознаки було зібрано, і черги класів формувалися з потоків. Потім потоки класифікувалися за відповідними класами QoS.

Для дослідження якості обслуговування, застосовуючи генеративну модель (прихована марковська модель, ПММ) для напівконтрольованого навчання послідовностей [14] автори запропонували новий метод класифікації трафіку на рівні пакетів. Використання послідовності ПММ кваліфікує цей підхід як напівсупервізійний. Грунтуючись на характеристиках розміру та часу між пакетами, автори розробили класифікацію, що спирається на агреговані характеристики реального мережевого трафіку. Даний метод виявився придатним для використання в зашифрованому трафіку.

В [7] досліджено можливість аналізу мережевого трафіку з використанням методів машинного навчання (ММН). Для зменшення розмірності даних було застосовано вибірка найбільш значущих ознак (15 з 87 ознак) на реальному наборі даних із понад 3 мільйонів екземплярів. Потім була застосована кластеризація K-means для кращого розуміння та розрізнення поведінки трафіку. Результати показали хорошу кореляцію між екземплярами в одному кластері, отриманому за допомогою навчання без учителя.

На підставі виконаного огляду попередніх досліджень, була сформована таблиця 1, в якій узагальнено отримані результати аналізу.

Таким чином, як показав, виконаний аналіз публікацій, для розробки ефективних методів аналізу та обробки великих даних (Big Data), на основі кластерних колективних рішень для аналізу трафіку у великих компаніях, дослідники виявляють великий інтерес до створення більш точних методів класифікації та визначенню моделей трафіку в реальному часі у мережевій безпеці та інших мережевих рішеннях. Багато моделей було сформульовано на основі існуючих неконтрольованих і напівконтрольованих методів кластеризації. Ці моделі включають методи, що демонструють здатність алгоритмів справлятися з шумом, а також їхню продуктивність і здатність класифікувати великі набори даних мережевого трафіку в реальному часі. Хоча класичний підхід K-means є основою розробки кількох методів напівконтрольованої кластеризації, пов’язана з ним обчислювальна складність, обмежує його застосування за умов обмежених обчислювальних ресурсів. Однак, наскільки нам відомо, існує обмежена кількість досліджень, присвячених аналізу роботи алгоритмів за певних параметрів QoS, що є метою для подальшого вивчення.

Таблиця 1

Порівняльний аналіз методів кластеризації для аналізу трафіку у великих компаніях (складено авторами на підставі аналізу літературних джерел [1–24])

Автори та джерело	Цілі	Використовуваний метод кластеризації	Параметри кластеризації	Обмеження	Результат
Lloyd, S. [18]	Зменшити вплив шумів при обчисленні середніх квадратів центроїдів у процесі формування кластерів	Класичний K-means	Функція відстані	Чутливість до шумів даних, не якісна кластеризація при поганій ініціалізації	Формує щільно пов'язані кластери в порівнянні з традиційними ієрархічними методами
Zhang, T. та ін. [24]	Підвищити ефективність використання ресурсів для обробки великих наборів даних	Алгоритм BIRCH (ієрархічний)	Дерево ознак (CF-дерево)	Чутливість до вставки даних (шум), більш високе робоче навантаження на процесор	Обробляє великі набори даних за менший час порівняно з K-Means
Guba, S. та ін. [12]	Дозволяє ідентифікувати несферичні кластери довільної форми та протистояти викидам у великих наборах даних	Алгоритм CURE (ієрархічний)	Репрезентативні точки для кластерів, коефіцієнт стиснення	Висока обчислювальна складність, а отже, і висока вартість	Формує кластери високої якості, час виконання на 50% менший у порівнянні з BIRCH [24] зі збільшенням кількості точок
Ester, M. та ін. [11]	Підвищити якість кластерів за допомогою можливостей алгоритму ідентифікації шумів	Алгоритм DBSCAN	Досяжність (Eps), максимальний радіус сусідства (MinPts)	Чутливість до параметрів (Eps і MinPts), складність обчислення параметрів, час виконання збільшується зі зростанням бази даних	Метод здатний ідентифікувати та виявляти прояви шуму. Також час виконання кращий, ніж алгоритм CLARANS
Ankerst, M. та ін. [6]	Подолати обмеження DBSCAN [14], пов'язані з чутливістю до параметрів	Алгоритм OPTICS (на основі розподілу густини)	Досяжність (Epx), максимальний радіус сусідства (MinPts)	Складність керування параметрами при кластеризації зі зростаючим порядком, час виконання можна порівняти з DBSCAN [14], але з нижчими налаштуваннями параметрів	Діаграма досяжності нечутлива до вхідних даних кластеризації в порівнянні з DBSCAN та іншими алгоритмами, час виконання можна порівняти з DBSCAN, але з нижчими налаштуваннями початкових параметрів
Subramani, K. та ін. [19]	Вибрати відповідний поріг щільності для виявлення спільнот у соціальних мережах	Гібридний підхід (OPTICS в DBSCAN)	поріг щільності	Обчислювальна складність гібридного підходу не обговорюється, визначення порогу щільності може призвести до раптової зміни та залежить від припущень програми	Гібридний підхід забезпечує чітке розуміння кластеризації, простоту вибору порога щільності за допомогою запропонованого методу
Zander, S. та ін. [23]	Підвищити загальну внутрішньокласову однорідність	Алгоритм ймовірнісного підходу (Expectation Maximization and Mixture Models (AutoClass))	Статистичні характеристики (внутрішньо-класова однорідність як метрика)	Продуктивність на великих наборах даних із зростаючою кількістю класів	Досягає середньої точності 85% при кластеризації

Wang, Y. та ін. [21]	Розробка методу класифікації інтернет-трафіку з використанням обмеженої кластеризації.	Обмежені K-meansна основі множин	Статистичні характеристики потоку, інформація про потоки TCP/IP, гаусова щільність суміші, дискретні ознаки	Можливість обробки великого обсягу даних та високі обчислювальні витрати	Поліпшення точності кластеризації, особливо для потоків зі схожими характеристиками у різних додатках
Wang, P. та ін. [22]	Класифікація мережевого трафіку з урахуванням вимог щодо якості обслуговування (QoS) у SDN.	Напівсупервізійне навчання з використанням Deep Packet Inspection (DPI)	Параметри DPI, значення пакета Херста, порти, середній час між прибуттям пакетів	Залежать від точності та доступності даних для навчання; висока обчислювальна складність	Ефективна класифікація трафіку за відповідними класами QoS, покращення управління мережею
Casas, P. та ін. [7]	Розробка платформи для аналізу мережевого трафіку з використанням технологій Big Data	Не зазначено конкретно, використовуються методи в області Big Data Analytics	Параметри аналізу включають часові ряди, статистичні характеристики трафіку.	Складність інтеграції та обробки великих обсягів даних, необхідність значних обчислювальних ресурсів	Ефективна платформа для моніторингу та аналізу мережевого трафіку з можливістю обробки великих обсягів даних у реальному часі

Резюмуючи виконаний огляд попередніх досліджень, можна зробити висновок – завдання розробки системи аналізу трафіку для великої компанії з метою оптимізації маршрутизації, зниження витрат та підвищення швидкості доставки може бути вирішена за допомогою створення кластерної платформи для розподіленої обробки даних з використанням сховищ даних певного типу. Для збирання та зберігання даних можна, наприклад, використовувати логи серверів, див. рис. 1. дані від датчиків трафіку, див. рис. 2., інформацію про розташування користувачів, див. рис. 3. та дані про маршрути, див. рис. 4., 5. і іншу інформацію, специфічну для кожного з бізнес-процесів, які будуть розглянуті в наступних публікаціях.

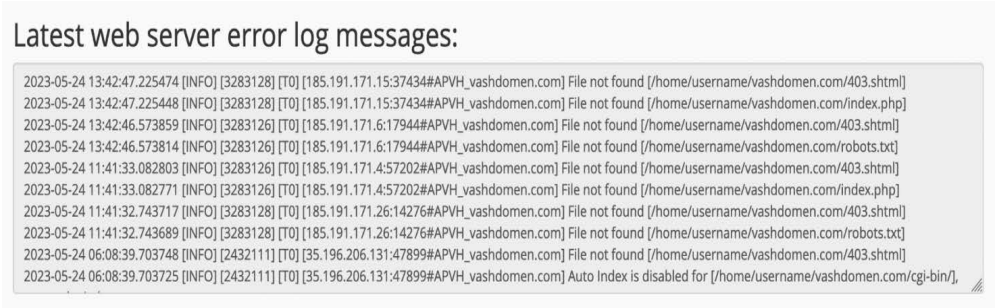


Рис. 1. Приклад логів сервера

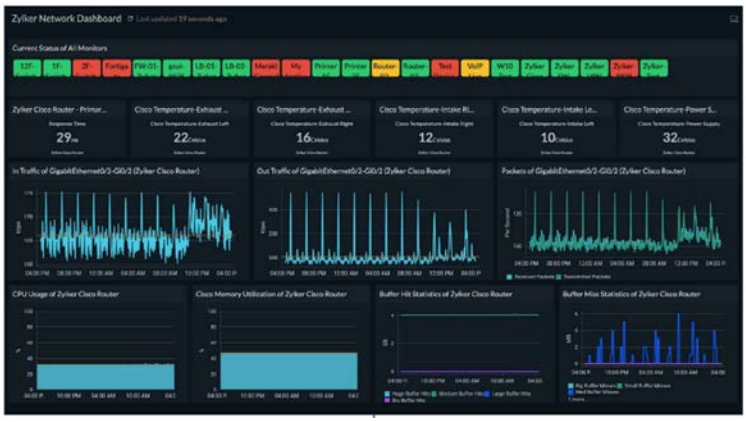


Рис. 2. Приклад даних від датчиків трафіку

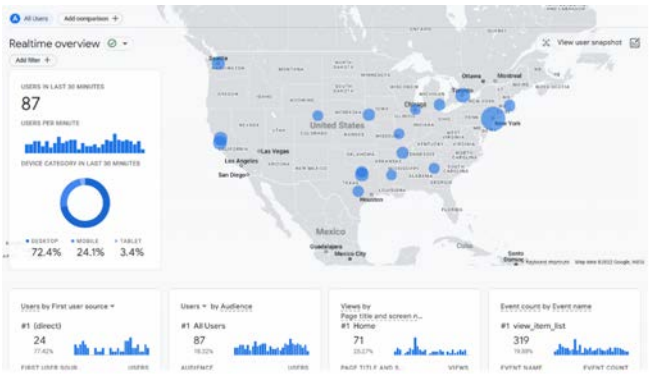


Рис. 3. Приклад інформації про розташування користувачів

Передобробка даних, згідно з класичним підходом, включатиме їх очищення, нормалізацію та перетворення в єдиний формат для структурованого зберігання в кластерній системі, що забезпечує швидкий доступ до потрібних даних.

Аналіз даних можна здійснювати, знов-таки виходячи зі специфіки бізнес-процесів, за допомогою алгоритмів машинного навчання (МН) для класифікації, регресії та кластеризації, аналізу часових рядів для прогнозування трафіку, просторового аналізу для оптимізації маршрутів доставки та аналізу мережевої топології для виявлення вузьких місць та оптимізації маршрутизації. Візуалізацію результатів можна виконати через інтерактивні панелі управління, графіки та діаграми, що дозволить представляти ключові показники та аналітичні дані у наочній формі. Інструменти прийняття рішень нададуть інформацію, необхідну для оптимізації трафіку.

```
Gateway of last resort is not set

R    17.0.0.0/8 [120/2] via 19.1.1.2, 00:00:12, Serial0/1
                [120/2] via 12.1.1.2, 00:00:10, Serial0/2
R    16.0.0.0/8 [120/1] via 19.1.1.2, 00:00:12, Serial0/1
                [120/1] via 12.1.1.2, 00:00:10, Serial0/2
C    19.0.0.0/8 is directly connected, Serial0/1
R    18.0.0.0/8 [120/1] via 19.1.1.2, 00:00:12, Serial0/1
R    192.168.8.0/24 [120/4] via 19.1.1.2, 00:00:12, Serial0/1
                    [120/4] via 12.1.1.2, 00:00:10, Serial0/2
R    21.0.0.0/8 [120/3] via 19.1.1.2, 00:00:15, Serial0/1
                [120/3] via 12.1.1.2, 00:00:13, Serial0/2
R    192.168.9.0/24 [120/4] via 19.1.1.2, 00:00:15, Serial0/1
                    [120/4] via 12.1.1.2, 00:00:13, Serial0/2
R    20.0.0.0/8 [120/4] via 19.1.1.2, 00:00:15, Serial0/1
                [120/4] via 12.1.1.2, 00:00:13, Serial0/2
R    192.168.4.0/24 [120/2] via 12.1.1.2, 00:00:17, Serial0/2
                    [120/2] via 10.1.1.2, 00:00:12, Serial0/0
R    192.168.5.0/24 [120/2] via 19.1.1.2, 00:00:19, Serial0/1
                    [120/2] via 12.1.1.2, 00:00:17, Serial0/2
C    10.0.0.0/8 is directly connected, Serial0/0
R    192.168.6.0/24 [120/1] via 19.1.1.2, 00:00:20, Serial0/1
R    11.0.0.0/8 [120/1] via 12.1.1.2, 00:00:18, Serial0/2
                [120/1] via 10.1.1.2, 00:00:13, Serial0/0
R    192.168.7.0/24 [120/3] via 19.1.1.2, 00:00:20, Serial0/1
                    [120/3] via 12.1.1.2, 00:00:18, Serial0/2
C    12.0.0.0/8 is directly connected, Serial0/2
C    192.168.1.0/24 is directly connected, FastEthernet0/1
R    13.0.0.0/8 [120/1] via 10.1.1.2, 00:00:14, Serial0/0
R    192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:15, Serial0/0
R    14.0.0.0/8 [120/1] via 12.1.1.2, 00:00:20, Serial0/2
R    192.168.3.0/24 [120/1] via 12.1.1.2, 00:00:20, Serial0/2
R    15.0.0.0/8 [120/1] via 12.1.1.2, 00:00:20, Serial0/2
```

Рис. 4. Таблиця маршрутизації маршрутизатора R1

Рис. 5. Топологія мережі

Для ілюстрації такого підходу наведемо невеликий приклад для популярних інтернет-магазинів. Даний приклад реалізації буде включати аналіз трафіку інтернет-магазину, де дані збираються з логів серверів, інформації про замовлення та місцезнаходження користувачів. Обробка даних дозволить агрегувати їх за часом, місцем розташування та типом замовлень. Алгоритми кластеризації виявить групи користувачів зі схожою поведінкою, а застосування регресії дозволить спрогнозувати попит на певні товари. На заключному етапі, можна візуалізувати результати у вигляді теплових карток завантаженості серверів та графіків попиту по регіонах, що допоможе оптимізувати розподіл ресурсів та доставку товарів споживачам. Це типовий приклад, а конкретні рішення з різних галузей економіки ми розглянемо у наступному параграфі даного розділу роботи.

Таким чином, виходячи з результатів виконаного огляду та аналізу попередніх досліджень можна констатувати, що кластерні рішення пропонують масштабованість, високу швидкість виконання завдань завдяки розподіленій обробці, доступність даних та сервісів, а також гнучкість у використанні різних інструментів та технологій. Однак реалізація таких систем все ще пов'язана з технічними складнощами, що вимагають знань у галузі Big Data, ММН та кластерних систем, а також із витратами на обладнання, програмне забезпечення та кваліфікованих фахівців. Однак, незважаючи на вищезазначені складності, використання кластерних рішень для аналізу Big Data потенційно може надати компаніям конкурентні переваги за рахунок оптимізації процесів, прийняття більш обґрунтованих рішень та підвищення ефективності роботи.

Висновки. У процесі досліджень було отримано такі основні результати.

Виконано огляд попередніх досліджень у завданнях, пов'язаних із дослідженням трафіку компаній на основі кластеризації даних. Встановлено, що завдання розробки системи аналізу трафіку для великої компанії з метою оптимізації маршрутизації, зниження витрат та підвищення швидкості доставки може бути вирішено за допомогою створення кластерної платформи для розподіленої обробки даних з використанням сховищ даних різного типу.

Продемонстровано, що для збирання та зберігання даних можна, наприклад, використовувати логи серверів, дані від датчиків трафіку, інформацію про місцезнаходження користувачів та дані про маршрути тощо.

Встановлено, що кластерні рішення пропонують масштабованість, високу швидкість виконання завдань, завдяки розподіленій обробці, доступність даних та сервісів, а також гнучкість у використанні різних інструментів та технологій. Однак реалізація таких систем все ще пов'язана з технічними складнощами, що вимагають знань у галузі Big Data, методах машинного навчання та кластерних систем, а також витратами на обладнання, програмне забезпечення (ПЗ) та кваліфікованих фахівців. Однак, незважаючи на вищезазначені складнощі, використання кластерних рішень для аналізу Big Data потенційно може надати компаніям конкурентні переваги за рахунок оптимізації процесів, прийняття більш обґрунтованих рішень та підвищення ефективності роботи.

Список використаних джерел:

1. Джулій В. М., Солодєєва Л. В., Мірошніченко О. В. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності. *Наукові праці*. 2022. С. 73–82. DOI: https://doi.org/10.17721/2519-481X/2022/74-07.

2. Лунгол О. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2024. Т. 1(25). С. 379–389.

3. Мамарєв В. М. Аналіз сучасних методів виявлення атак на ресурси інформаційно-телекомунікаційних систем. *Ukrainian Information Security Research Journal*. 2011. Т. 13(2 (51)).

4. Морозов Б. Дослідження методів аналізу мережевого трафіку. Матеріали IX Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання". 2016. Т. 1. С. 91–92.

5. Рубан І. В., Мартовицький В. О., Партика С. О. Класифікація методів виявлення аномалій в інформаційних системах. *Системи озброєння і військова техніка*. 2016. Т. 3. С. 100–105.

6. Ankerst M., Breunig M. M., Kriegel H. P., Sander J. OPTICS: Ordering points to identify the clustering structure. *ACM Sigmod record*. 1999. 28(2), pp. 49–60.

7. Aouedi O., Piamrat K., Hamma S., Perera J.M. Network traffic analysis using machine learning: an unsupervised approach to understand and slice your network. *Annals of Telecommunications*. 2022. T. 77(5). pp. 297–309.

8. Cheeseman P. C., Stutz J. C. Bayesian classification (AutoClass): theory and results. Advances in knowledge discovery and data mining. 1996. N. 180. pp. 153–180.

9. Dainotti A., De Donato W., Pescape A., Rossi P.S. Classification of network traffic via packet-level hidden markov models. IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference. 2008. pp. 1–5.

10. Erman J., Mahanti A., Arlitt M., Cohen I., Williamson C. Offline/realtime traffic classification using semi-supervised learning. Performance Evaluation. 2007. N 64, pp. 1194–1213.

11. Ester M., Kriegel H.P., Sander J., Xu X. A density-based algorithm for discovering clusters in large spatial databases with noise. *KDD*. Vol. 96, No. 34. 1996. pp. 226–231.

12. Guha S., Rastogi R., Shim K. CURE: An efficient clustering algorithm for large databases. *ACM Sigmod record*. 1998. T. 27(2). pp. 73–84.

13. Li J., Zhang H., Tang D., Lin C. Traffic classification using cluster analysis. 2021 International Conference on Computer Information Science and Artificial Intelligence (CISAI). 2021. pp. 463–467.

14. MacQueen J. Some methods for classification and analysis of multivariate observations. Proceedings of the fifth Berkeley symposium on mathematical statistics and probability. 1967. T. 1, No. 14. pp. 281–297.

15. McGregor A., Hall M., Lorier P., Brunskill J. Flow clustering using machine learning techniques. Passive and Active Network Measurement: 5th International Workshop, PAM 2004. 2004. pp. 205–214.

16. NetMate Meter. URL: http://sourceforge.net/projects/netmate-meter.

17. Rodriguez Rodriguez J. E., Garcia V.H.M., Usaquén M.A.O. Corporate networks traffic analysis for knowledge management based on random interactions clustering algorithm. Knowledge Management in Organizations: 13th International Conference, KMO 2018. 2018. pp. 523–536.

18. S. Lloyd, "Least squares quantization in PCM", IEEE transactions on information theory. 1982. vol. 28, no. 2, pp. 129–137.

19. Subramani K., Velkov A., Ntoutsi I., Kroger P., Kriegel H. P. Density-based community detection in social networks. In 2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application. 2011. pp. 1–8.

20. Takyi K., Bagga A., Goopta P. Clustering techniques for traffic classification: A comprehensive review. 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). 2018. pp. 224–230.

21. Wang Y., Xiang Y., Zhang J., Zhou W., Wei G., Yang L.T. Internet traffic classification using constrained clustering. IEEE transactions on parallel and distributed systems. 2013. T. 25(11). pp. 2932–2943.

22. Wang P., Lin S.C., Luo M. A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs. 2016 IEEE international conference on services computing (SCC). 2016. pp. 760–765.

23. Zander S., Nguyen T., Armitage G. Automated traffic classification and application identification using machine learning. The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05). 2005. pp. 250–257.

24. Zhang Tian, Raghu Ramakrishnan, Miron Livny. BIRCH: A new data clustering algorithm and its applications. Data mining and knowledge discovery. 1997. N. 1. pp. 141–182.

УДК 004.932
DOI https://doi.org/10.32689/maup.it.2024.4.19

Олександр СТОРОЖУК
кандидат технічних наук, доцент,
завідувач кафедри інформаційних систем та комп'ютерного моделювання,
Національний лісотехнічний університет України, stotozhuk@nltu.edu.ua
***ORCID:** 0000-0001-6566-5271*

Квітослава-Ольга ЯЦИНА
магістр за спеціальністю 122 «Комп'ютерні науки»,
Національний лісотехнічний університет України, acinakvitka@gmail.com
***ORCID:** 0009-0008-9009-7796*

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ AR У ВІЗУАЛІЗАЦІЇ ТА АНАЛІЗІ АНАТОМІЧНИХ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ ЕВКЛІДОВОЇ МЕТРИКИ В НАВЧАЛЬНОМУ ПРОЦЕСІ ПІДГОТОВКИ МЕДИЧНИХ ФАХІВЦІВ

Анотація. *У статті проведено аналіз використання технологій доповненої реальності (AR) у навчанні студентів-медиків, зокрема для покращення засвоєння анатомії, розвитку хірургічних навичок та вивчення функціонування органів у інтерактивному середовищі. AR надає можливість інтерактивної роботи з тривимірними моделями, що дозволяє студентам не лише спостерігати, але й безпосередньо взаємодіяти з навчальним матеріалом, сприяючи його кращому розумінню та засвоєнню.*

Метою роботи *є дослідження можливостей інтеграції технологій доповненої реальності (AR) у навчальний процес для покращення засвоєння студентами-медиками знань з анатомії, розвитку практичних навичок та вивчення функціонування анатомічних структур в інтерактивному середовищі.*

Методологія. *У статті застосовано методи аналізу сучасних AR-технологій, включаючи математичні підходи до візуалізації тривимірних об'єктів та їх інтеграції в освітній процес. Проведено тестування функціональних можливостей AR-додатка, орієнтованого на взаємодію з 3D-об'єктами та адаптивне оцінювання знань студентів.*

Наукова новизна. *Запропоновано систему інтеграції AR-технологій у медичну освіту, що базується на використанні математичних методів для точного позиціонування, орієнтації та масштабування віртуальних об'єктів. Розроблено адаптивну систему тестування, яка дозволяє фокусувати навчальний процес на найскладніших аспектах за допомогою індивідуалізованого підходу.*

Висновки. *Інтеграція доповненої реальності у навчання сприяє підвищенню зацікавленості студентів, поліпшенню засвоєння знань та розвитку практичних навичок. Використання AR-додатків дозволяє створити інтерактивне навчальне середовище, яке долає обмеження традиційних методів навчання та забезпечує доступ до детальної інформації про анатомічні структури. Такий підхід підвищує ефективність освітнього процесу, сприяє формуванню критичного мислення та забезпечує якісну підготовку студентів-медиків.*

Ключові слова: *AR, доповнена реальність, AR-додаток, 3D-об'єкти.*

Oleksandr STOROZHUK, Kvitoslava-Olha YATSYNA. FEATURES OF THE APPLICATION OF AR IN VISUALIZATION AND ANALYSIS OF ANATOMICAL OBJECTS USING EUCLIDIAN METRICS IN THE EDUCATIONAL PROCESS OF TRAINING MEDICAL SPECIALISTS

Abstract. *The article analyzes the use of augmented reality (AR) technologies in the education of medical students, in particular to improve the acquisition of anatomy, the development of surgical skills and the study of the functioning of organs in an interactive environment. AR provides the opportunity to work interactively with three-dimensional models, which allows students not only to observe, but also to directly interact with the educational material, contributing to its better understanding and assimilation.*

The purpose of the article *is to study the possibilities of integrating augmented reality (AR) technologies into the educational process to improve the acquisition of knowledge of anatomy by medical students, the development of practical skills and the study of the functioning of anatomical structures in an interactive environment.*

Methodology. *The article applies methods of analysis of modern AR technologies, including mathematical approaches to the visualization of three-dimensional objects and their integration into the educational process. The functional capabilities of the AR application focused on interaction with 3D objects and adaptive assessment of students' knowledge were tested.*

Scientific novelty. *A system for integrating AR technologies into medical education is proposed, based on the use of mathematical methods for accurate positioning, orientation and scaling of virtual objects. An adaptive testing system has been developed, which allows focusing the educational process on the most complex aspects using an individualized approach.*

Conclusions. *The integration of augmented reality into learning helps to increase student interest, improve knowledge acquisition and develop practical skills. The use of AR applications allows you to create an interactive learning environment that overcomes the limitations of traditional teaching methods and provides access to detailed information about anatomical structures. This approach increases the efficiency of the educational process, promotes the formation of critical thinking and ensures high-quality training of medical students.*

Key words: *AR, augmented reality, AR application, 3D objects.*

Вступ. Постановка проблеми. Впровадження технології доповненої реальності (AR) відкриває нові перспективи для інтеграції віртуальних елементів у реальний світ, створюючи інтерактивні та візуально насичені середовища для навчання. Завдяки цій технології навчання стає більш наочним і залученим, що робить AR корисним інструментом у різних галузях, зокрема в медицині та освіті. Наприклад у медичній освіті ця технологія перетворює складні теоретичні концепції на наочні візуалізації та забезпечує проведення реалістичних симуляцій, що спрощує процес засвоєння матеріалу та тренування навичок.

Аналіз останніх досліджень та публікацій. Проблематика використання доповненої реальності (AR) у навчальному процесі знаходить широке відображення в сучасних дослідженнях. Наприклад, у роботі [4] розглядаються переваги інтерактивних технологій у загальній освіті, зокрема підвищення залученості учнів до навчального процесу завдяки візуалізації складних понять. Організація економічного співробітництва та розвитку (OECD) у своєму звіті [3] аналізує можливості та ризики використання віртуальної реальності в освітньому середовищі, акцентуючи на потенціалі інтерактивних технологій для стимулювання критичного мислення.

У статті Vondrek, Baggili, Casey, Mekni [5] розглядаються технічні аспекти безпеки у віртуальній реальності, що також мають значення для AR, особливо у контексті забезпечення надійної роботи додатків для навчання. Дослідження [6] акцентує увагу на інтеграції AR у вищій освіті, зокрема у підготовці IT-фахівців, що має значну схожість із медичною освітою через необхідність практичної взаємодії з тривимірними об'єктами.

Національні дослідження, такі як робота [1], акцентують увагу на педагогічних аспектах впровадження AR, демонструючи, як ці технології сприяють глибшому розумінню навчального матеріалу. Окремо варто зазначити дослідження [2], яке аналізує використання AR у викладанні математики та підкреслює значення бібліометричного аналізу для вивчення ефективності таких технологій.

Метою статті є визначити вплив AR на медичну практику та освітній процес, а також застосування математичних методів для взаємодії з тривимірними об'єктами.

Дослідження ґрунтується на теоретичних засадах, що обґрунтовують використання доповненої реальності в медичній освіті.

Виклад основного матеріалу. У галузі медицини доповнена реальність (AR) набуває важливого значення, створюючи нові можливості для підвищення ефективності терапевтичних методів та вдосконалення професійних навичок медичних спеціалістів. Технологія дозволяє лікарям інтегрувати віртуальні елементи в реальний світ, що покращує отримання важливої інформації про пацієнтів. Наприклад, під час хірургічних операцій AR може проєктувати тривимірні моделі органів безпосередньо на тілі пацієнта, що сприяє більш точному виконанню маніпуляцій.

Дослідження проблеми починається з декомпозиції, яка дозволяє виявити основну проблему та її підпроблеми (рис. 1.):

1) Брак інтерактивності та залучення студентів до процесу навчання може бути пояснений кількома причинами, які деталізовано розглянуті нижче:

1.1) відсутність доступу до тривимірних моделей анатомічних структур обмежує можливість студентів краще розуміти складні анатомічні концепції та сприяє менш ефективному навчанню;

1.2) необхідність використання новітніх технологій, таких як доповнена реальність, для поліпшення процесу навчання вимагає відповідного технічного забезпечення та навчання викладачів для ефективного їх впровадження [4];

1.3) потреба у віртуальних симуляціях та практичних завданнях створює можливості для активного залучення студентів до процесу навчання, забезпечуючи їм можливість застосовувати теоретичні знання на практиці та поглиблювати їх розуміння [3].

2) Недостатня доступність деталізованої інформації про анатомічні структури зумовлена відсутністю достатньо обсяжних джерел інформації або обмеженим доступом до них, що ускладнює процес вивчення анатомії студентами. А також, складність анатомічних структур ускладнює їх розуміння для студентів.

3) Відсутність можливості практичної взаємодії з анатомічними моделями ускладнює засвоєння матеріалу студентами, оскільки вони не мають можливості візуально та тактильно досліджувати анатомічні структури.

4) Складнощі зі засвоєнням матеріалу через традиційний метод навчання можуть виникати через недостатню інтерактивність та практичність лекцій і підручників, які не враховують індивідуальні потреби студентів.

5) Низький рівень зацікавленості студентів в вивченні анатомії може бути викликаний кількома факторами:

Рис. 1. Графічне представлення структури проблем у вигляді дерева

Розроблено авторами

5.1) нецікавий або нестимулюючий метод презентації матеріалу про анатомію призводить до втрати інтересу студентів та погіршення їхнього сприйняття і засвоєння інформації;

5.2) потреба у стимулюючих та цікавих методах навчання, таких як використання інтерактивних симуляцій або доповненої реальності, для підвищення інтересу студентів та залучення їх до вивчення анатомії [5].

Зважаючи на виявлені проблеми у навчанні анатомії, впровадження AR трансформує освіту медичних фахівців, що робить освітній процес більш інноваційним та ефективним. Завдяки підтримці створення динамічного та інтерактивного середовища AR технологіями в медичній практиці, краще засвоюється анатомія людини в тривимірному форматі. Це, у свою чергу, полегшує розуміння складних концепцій і покращує комунікацію між медичними спеціалістами, а також сприяє індивідуалізації підходів у медичній сфері. Студенти мають можливість навчатися у власному темпі, використовуючи віртуальні об'єкти для відпрацювання конкретних навичок відповідно до своїх потреб і рівня знань, що значно знижує ризики помилок під час реальних процедур [6]. Це дозволяє не лише розвивати професійні якості, а й підвищувати впевненість у своїх діях під час роботи з пацієнтами та дає змогу краще адаптуватися до складних клінічних ситуацій, що зменшує тривалість операцій та поліпшує результати лікування.

На основі аналізу існуючих AR-застосунків для медичної освіти виділяють декілька ключових напрямків їх використання:

1) Практика хірургічних маніпуляцій. Застосунки, такі як Touch Surgery та Proximie, завдяки покроковим симуляціям, дають змогу студентам без ризику для пацієнта відпрацьовувати хірургічні навички. Такі віртуальні операції значно покращують готовність студентів до реальних клінічних маніпуляцій.

2) Вивчення анатомії. Complete Anatomy, 3D Organon Anatomy та HoloHuman, показує, що завдяки можливості масштабування і обертання, полегшує розуміння студентам просторових взаємозв'язків між органами та системами тіла. А отже це суттєво підвищує якість засвоєння знань, порівняно з використанням традиційних друкованих атласів.

3) Фізіологічні процеси. Visible Body відображає віртуальні симуляції роботи органів і систем. Наприклад, дозволяє бачити динамічні процеси, як-от кровообіг чи дихання, у реальному часі. Таким чином, допоможе сформувати у студентів краще уявлення про функціонування систем органів, що складно досягти безпосередньо в навчальній аудиторії.

Проте AR має свої недоліки. Одним із головних викликів є висока вартість обладнання та програмного забезпечення, що може обмежити доступ до цієї технології для багатьох навчальних закладів. Крім того, ефективне використання AR вимагає високого рівня технічної підготовки викладачів і медичних працівників [1]. Існують також технічні обмеження, такі як можливі похибки в позиціонуванні об'єктів або затримки у візуалізації, що можуть знижувати якість взаємодії.

Для роботи з тривимірними об'єктами в AR широко використовуються різноманітні математичні підходи, які дозволяють коректно позиціонувати, переміщувати та змінювати орієнтацію віртуальних елементів у реальному світі. Один із фундаментальних математичних інструментів це «Евклідова метрика», що використовується для визначення відстані між об'єктами у тривимірному просторі. Нехай координати точки захоплення позначимо (x_1, y_1, z_1), а координати центру об'єкта (x_2, y_2, z_2). Тоді формула для визначення відстані *d* між ними запишеться, як:

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}$$

Евклідова метрика допомагає розраховувати просторові відстані між точками, що є ключовим фактором для правильної інтеграції віртуальних об'єктів у реальне середовище. Для коректної взаємодії з AR об'єктами важливо точно знати, де знаходяться ці об'єкти відносно користувача або інших елементів у просторі.

Іншим ключовим математичним методом, що застосовується в AR, є лінійна алгебра. Вона використовується для розрахунку рухів та орієнтації об'єкта під час захоплення і допомагає виконувати такі математичні операції, як:

1) Зміщення – використовується для зміщення об'єкта відносно точки захоплення. Нехай позначимо (x_c, y_c, z_c) – це координати центру об'єкта, а (x_g, y_g, z_g) – координати точки хватання, тоді нові координати об'єкта після хватання (x', y', z') будуть обчислені як:

$$x' = x + (x_g - x_c) \quad (1)$$

$$y' = y + (y_g - y_c) \quad (2)$$

$$z' = z + (z_g - z_c) \quad (3)$$

2) Обертання – використовується для зміни орієнтації об'єкта. x, y та z – початкові координати об'єкта. (x', y', z')– нові координати об'єкта після обертання. Кут обертання θ задається в радіанах.

Для обертання навколо вісі x формула набуде вигляду:

$$x' = x \quad (4)$$

$$y' = y \times \cos(\theta) - z \times \sin(\theta) \quad (5)$$

$$z' = y \times \sin(\theta) + z \times \cos(\theta) \quad (6)$$

Формула для обертання навколо вісі y матиме наступний вигляд:

$$x' = x \times \cos(\theta) + z \times \sin(\theta) \quad (7)$$

$$y' = y \quad (8)$$

$$z' = -x \times \sin(\theta) + z \times \cos(\theta) \quad (9)$$

Для обертання навколо вісі z формула буде мати такий вигляд:

$$x' = x \times \cos(\theta) - y \times \sin(\theta) \quad (10)$$

$$y' = x \times \sin(\theta) + y \times \cos(\theta) \quad (11)$$

$$z' = z \quad (12)$$

3) Масштабування-використовується для зміни розміру об'єкта. Нехай s_x, s_y та s_z представляють коефіцієнти масштабування по відповідним осям x, y та z, тоді для масштабування об'єкта можна використовувати наступну формулу:

$$x' = x + s_x \quad (13)$$

$$y' = y + s_y \quad (14)$$

$$z' = z + s_z \quad (15)$$

Якщо s_x, s_y та s_z менші за 1, то це зменшить розміри об'єкта відповідно до кожної відповідної осі. Якщо вони більші за 1, то це збільшить розміри. Якщо вони рівні 1, то об'єкт залишиться без змін.

Наприклад, коли студент взаємодіє з 3D моделлю у віртуальному середовищі, методи лінійної алгебри дозволяють точно змінювати її орієнтацію та масштаб відповідно до рухів користувача.

Включаючи особливості AR, розроблено систему, у якій студенти медики проходять тести (рис. 2) та взаємодіють з 3D-об'єктом (рис. 3) в інтерактивному середовищі. Алгоритм тестування побудовано таким чином, що під час проходження тесту всі неправильні відповіді зберігаються в окремому списку. Під час наступної спроби цей список використовується, і студенти знову отримують питання, на які раніше відповіли неправильно. А для взаємодії з 3д моделю було використано Евклідову метрику та лінійну алгебру для того, щоб користувач мав змогу зміщувати, обертати та масштабувати об'єкт.

Рис. 2. Проходження тесту

Рис. 3. Розміщення 3д моделі в просторі

Попри значні досягнення в цих галузях, є можливості для подальшого вдосконалення. Наприклад, покращення алгоритмів комп'ютерної графіки може ще більше наблизити візуальні елементи до реальності. Також дослідження нових математичних підходів до розрахунку тривимірних перетворень та орієнтації об'єктів може підвищити швидкість і точність обробки даних, що особливо важливо для складних операцій у реальному часі [2]. Вдосконалення методів машинного навчання також може сприяти автоматизації та оптимізації роботи з AR-середовищами, роблячи їх ще більш ефективними в різних сферах застосування.

Висновки. В освітньому процесі AR має значний вплив, надаючи нові можливості для навчання та професійного розвитку. Математичні методи, що лежать в основі доповненої реальності, забезпечують її точність та ефективність, що робить AR потужним інструментом у різних галузях, зокрема в медицині. Евклідова метрика, лінійна алгебра та алгоритми комп'ютерної графіки допомагають точно позиціонувати й маніпулювати віртуальними об'єктами в реальному просторі, створюючи інтерактивні навчальні та практичні середовища.

З такими можливостями AR має потенціал для трансформації медичної практики, підвищуючи якість надання медичних послуг та забезпечуючи більш безпечний і ефективний процес лікування.

Список використаних джерел:

1. Єфімов Д. В. Використання доповненої реальності (AR) в освіті. *Педагогічні науки: теорія та практика*. 2021. Т. 2, № 1. С. 219–225. URL: https://doi.org/10.26661/2522-4360-2021-1-2-34

2. Hakim L. L., Hidayat H., Salmun A., Sulastri Y. L. Application of Augmented Reality in mathematics learning: A bibliometric and content analysis. 2024. P. 10–13. URL: https://doi.org/10.2991/978-2-38476-206-4_29

3. OECD. Virtual reality and its opportunities and risks. In OECD Digital Economy Outlook 2024. 2024. Vol. 1. P. 122–124.

4. Soroko Nataliia V., Lytvynova Svitlana H. The benefits of using immersive technologies at general school. 2023. Vol. 2. P. 480. URL: https://icteri.org/icteri-2023/proceedings/olume-2/202110480.pdf

5. M. Vondrek, Ibrahim Baggili, Peter Casey, Mehdi Mekni. Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses. Computer & Security. 2022. P. 1–5.

6. Vladyslav V. Babkin, Viktor V. Sharavara, Volodymyr V. Sharavara, Vladyslav V. Bilous, Andrei V. Voznyak, Serhiy Ya. Kharchenko. Using augmented reality in university education for future IT specialists: educational process and student research work. 2021. Vol. 2898. P. 11–13. URL: https://ceur-ws.org/Vol-2898/paper14.pdf

НАУКОВЕ ВИДАННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

ВИПУСК 4 (15)
ISSUE 4 (15)

2024

Коректура
Ірина Чудеснова

Комп'ютерна верстка
Марина Михальченко

Формат 60x84/8. Гарнітура Cambria.
Папір офсет. Цифровий друк.
Підписано до друку 27.12.2024.
Ум. друк. арк. 15,11. Замов. № 0125/026. Наклад 300 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефон +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК No 7623 від 22.06.2022 р.