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 2 (21), 2026
Issue 2 (21), 2026

Видавничий дім
«Гельветика»
2026

УДК 004

Засновник видання: Міжрегіональна Академія управління персоналом
Періодичність: 4 рази на рік

Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 9 від 10 липня 2026 року)

Інформаційні технології та суспільство / [головний редактор І. Остроумов]. – Київ : Міжрегіональна Академія управління персоналом, 2026. – Випуск 2 (21). – 132 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.

Головний редактор: **Остроумов Іван Вікторович** – доктор технічних наук, професор, професор кафедри комп'ютерних інформаційних систем і технологій, Міжрегіональна Академія управління персоналом, Україна

Редакційна колегія:
Дуднік Андрій Сергійович, доктор технічних наук, доцент, доцент кафедри мережевих та інтернет технологій, Київський національний університет імені Тараса Шевченка, Україна
Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна
Заліський Максим Юрійович, доктор технічних наук, професор кафедри телекомунікаційних та радіоелектронних систем, Державний університет «Київський авіаційний інститут», Україна
Кавун Сергій Віталійович, доктор економічних наук, професор, завідувач кафедри комп'ютерних інформаційних систем та технологій, Міжрегіональна Академія управління персоналом, Україна
Кузьменко Наталія Сергіївна, кандидат технічних наук, старший дослідник, керівник науково-дослідної роботи, Державний університет «Київський авіаційний інститут», Україна
Побережна Заріна Миколаївна, доктор економічних наук, професор, професор кафедри національної безпеки та підприємництва, Державний університет «Київський авіаційний інститут», Україна
Попов Олександр Олександрович, доктор технічних наук, професор, директор Центру інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, Україна
Чолишкіна Ольга Геннадіївна, кандидат технічних наук, доцент, доцент кафедри інтелектуальних технологій, Київський національний університет імені Тараса Шевченка, Україна
Aseri Vinay, PhD, Associate Professor, Associate Professor of Cybersecurity and Digital Forensics at the Narnarayan Shastri Institute of Technology, National Forensic Sciences University, India
Duczmal Wojciech, Dr.hab, Professor, Vice-Rector for Finance and Development Academy of Applied Sciences, Higher School of Management and Administration in Opole, Poland
Lengyelfalusy Tomas, Dr.hab, Professor, Rektor of DTI University, Slovakia
Okoro Onyedikachi Chioma, PhD, Researcher at the Department of Geomatics Engineering, Schulich School of Engineering, University of Calgary, Canada
Timilehin Olasoji Olubiyi, DSc, PhD, Dean of the Faculty of Management and Social Sciences, West Midlands Open University, Nigeria
Sharon Nir, Ph.D, Associate Professor, Associate Professor of the Department of Applied Mathematics, Tel Aviv University, Israel

Реєстрація суб'єкта у сфері друкованих медіа:
Рішення Національної ради України з питань телебачення і радіомовлення № 1173 від 11.04.2024 року.
Ідентифікатор медіа: R30-03890

Суб'єкт у сфері друкованих медіа – Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» (вул. Фрометівська, буд. 2, м. Київ, 03039, iapm@iapm.edu.ua, тел. (044) 490-95-00).

Мова видання: українська, англійська, німецька, французька та польська.

Журнал включений до Переліку наукових фахових видань України відповідно до Наказу МОН України № 928 від 11 червня 2026 року (додаток 7) з присвоєнням категорії «Б».
Кластер: Інформаційні технології та електроніка.
Спеціальності: F2 – Інженерія програмного забезпечення; F3 – Комп'ютерні науки; F4 – Системний аналіз та наука про дані; F5 – Кібербезпека та захист інформації; F6 – Інформаційні системи і технології; F7 – Комп'ютерна інженерія.

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.

© Міжрегіональна Академія управління персоналом, 2026
© Автори статей, 2026

UDC 004

Founder: Interregional Academy of Personnel Management
Frequency: 4 issues per year

Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 9 dated 10 July 2026)

Information Technology and Society / [chief editor Ivan Ostroumov]. – Kyiv : Interregional Academy of Personnel Management, 2026. – Issue 2 (21). – 132 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.

Chief editor: **Ivan Ostroumov** – Doctor of Engineering, Professor, Professor of the Department of Computer Information Systems and Technologies, Interregional Academy of Personnel Management, Ukraine

Editorial Board:
Dudnik Andriy S., Doctor of Engineering, Associate Professor, Associate Professor of Department of Networking and Internet Technologies, Taras Shevchenko National University of Kyiv, Ukraine
Yevseiev Serhii P., Doctor of Engineering, Professor, Head of the Department of Cybersecurity, National Technical University "Kharkiv Polytechnic Institute", Ukraine
Zaliskyi Maksym Yu., Doctor of Engineering, Professor of the Department of Telecommunications and Radio Electronic Systems, State University "Kyiv Aviation Institute", Ukraine
Kavun Sergii V., Doctor of Economics, Professor, Head of the Department of Computer Information Systems and Technologies, Interregional Academy of Personnel Management, Ukraine
Kuzmenko Nataliia S., PhD of Engineering, Senior Researcher, Head of Research Work, State University "Kyiv Aviation Institute", Ukraine
Poberezhna Zarina M., Doctor of Economics, Professor, Professor of the Department of National Security and Entrepreneurship, State University "Kyiv Aviation Institute", Ukraine
Popov Oleksandr O., Doctor of Engineering, Professor, Director the Center for Information-analytical and Technical Support of Nuclear Power Facilities Monitoring of the National Academy of Sciences of Ukraine, Ukraine
Cholyshkina Olha H., PhD of Engineering, Associate Professor, Associate Professor of the Department of Intelligent Technologies, Taras Shevchenko National University of Kyiv, Ukraine
Aseri Vinay, PhD, Associate Professor, Associate Professor of Cybersecurity and Digital Forensics at the Narnarayan Shastri Institute of Technology, National Forensic Sciences University, India
Duczmal Wojciech, Dr.hab, Professor, Vice-Rector for Finance and Development Academy of Applied Sciences, Higher School of Management and Administration in Opole, Poland
Lengyelfalusy Tomas, Dr.hab, Professor, Rektor of DTI University, Slovakia
Okoro Onyedikachi Chioma, PhD, Researcher at the Department of Geomatics Engineering, Schulich School of Engineering, University of Calgary, Canada
Timilehin Olasoji Olubiyi, DSc, PhD, Dean of the Faculty of Management and Social Sciences, West Midlands Open University, Nigeria
Sharon Nir, Ph.D, Associate Professor, Associate Professor of the Department of Applied Mathematics, Tel Aviv University, Israel

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.
Media ID: R30-03890

Media entity – Private Joint-Stock Company «Higher education institution «Interregional Academy of Personnel Management»
(03039, Kyiv, Frometivska str., 2, iapm@iapm.edu.ua, tel. (044) 490-95-00).

Language of publication: Ukrainian, English, German, French, and Polish.

The journal is included in the List of Scientific Professional Publications of Ukraine in accordance with Order No. 928 of the Ministry of Education and Science of Ukraine dated June 11, 2026 (Appendix 7). The journal has been assigned Category "B".
Cluster: Information Technology and Electronics.
Specialties: F2 – Software Engineering; F3 – Computer Sciences; F4 – Systems Analysis and Data Science; F5 – Cybersecurity and Data Protection; F6 – Information Systems and Technologies; F7 – Computer Engineering.

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.

© Interregional Academy of Personnel Management, 2026
© Copyright by the contributors, 2026

ЗМІСТ

А. С. Возниця, А. С. Савченко
ФОРМАЛІЗАЦІЯ ОПЕРАЦІЙНОЇ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ
ЗА ДОПОМОГОЮ МЕТОДІВ НЕЧІТКОЇ ЛОГІКИ 6

Г. А. Довгаленко, Ю. М. Селін, Ю. В. Куєвда
МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ВИРОБНИЦТВА ВІДНОВЛЮВАНОЇ ЕЛЕКТРОЕНЕРГІЇ 14

А. О. Коваль, Ю. В. Каменецька, А. К. Кобринець
АВТОМАТИЗАЦІЯ ГЕНЕРАЦІЇ ЦИФРОВИХ ТЕКСТУР ІЗ ВИКОРИСТАННЯМ
ГЕНЕРАТИВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ 25

О. І. Марків, Ю. В. Ришковець
МОДЕЛЬ ПРОСТОРОВО-ЧАСОВОГО ПОПИТУ НА ЗАРЯДНІ СТАНЦІЇ ЕЛЕКТРОМОБІЛІВ
ІЗ ВРАХУВАННЯМ СЕЗОННИХ І ТРАНЗИТНИХ ФАКТОРІВ 32

О. А. Нємкова, А. М. Ахекян
АРХІТЕКТУРА ЗАХИЩЕНОЇ КОНСОРЦІУМНОЇ ВИДАЧІ БЛОКЧЕЙН-СЕРТИФІКАТІВ З ДОТРИМАННЯМ
ЄВРОПЕЙСЬКИХ ВИМОГ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ СИСТЕМ
ЕЛЕКТРОННОГО НАВЧАННЯ 43

D. I. Prokopovych-Tkachenko
A COMPROMISE-TOLERANT CROSS-LAYER RESILIENCE CONTROLLER ARCHITECTURE
AND AN EQUAL-BUDGET BENCHMARK FOR PROGRAMMABLE NETWORKS 53

H. O. Rozhkov, I. A. Klymenko
OPTIMIZATION OF LORAWAN GATEWAY PLACEMENT IN WASTE CONTAINER MONITORING SYSTEMS
WITH ADR CONSIDERATION 61

Т. В. Савченко, І. С. Майстер
ТЕХНІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ СТВОРЕННЯ ЦИФРОВИХ ДВІЙНИКІВ
ПРОМИСЛОВИХ ПІДПРИЄМСТВ 71

В. Б. Сахневич
МОДЕЛЮВАННЯ ВЗАЄМОДІЇ ПІШОХОДІВ І ТРАНСПОРТНИХ ЗАСОБІВ
В УМОВАХ НЕКОНТРОЛЬОВАНОГО РУХУ НА ОСНОВІ ГРИ СТАКЕЛБЕРГА 81

Л. О. Соляник, В. І. Коваль
КВАНТОВО-ХІМІЧНІ ОСНОВИ ФУНКЦІОНАЛЬНОСТІ $LINBO_3$ У ФОТОННИХ КРИПТОСИСТЕМАХ
ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ 92

Yu. Ye. Khokhlachova
MULTILEVEL EXPERIMENTAL VALIDATION OF A SMART-REGION CYBER-RESILIENCE METHODOLOGY:
FROM FORMAL VERIFICATION TO HARDWARE-IN-THE-LOOP TESTING, PILOT DEPLOYMENT,
AND EXTERNAL REPLICATION 100

О. С. Чикалов, О. Б. Берест
ОБРОБКА ТЕЛЕМЕТРИЧНИХ ДАНИХ ТА ВИЗНАЧЕННЯ РЕЛЕВАНТНИХ ОЗНАК
ДЛЯ РОБОТИ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У КОНТЕКСТІ
ОЦІНКИ ФУНКЦІОНАЛЬНОГО СТАНУ РЕЛЯЦІЙНИХ БАЗ ДАНИХ 111

К. Є. Шамонін, Д. В. Прилепа
АДАПТАЦІЯ ІНФОРМАЦІЙНО-ЕКСТРЕМАЛЬНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТЕХНОЛОГІЇ
ДО АНАЛІЗУ ВЕЛИКИХ ДАНИХ НА ПРИКЛАДІ ЖУРНАЛІВ ПОДІЙ OFFICE 365 123

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

CONTENTS

Anastasiia Voznytsia, Alina Savchenko
FORMALIZATION OF IT PROJECT OPERATIONAL EFFICIENCY USING FUZZY LOGIC METHODS 6

Hlib Dovgalenko, Yurii Selin, Yuliia Kuevda
MODELING AND FORECASTING OF RENEWABLE ELECTRICITY PRODUCTION 14

Alina Koval, Yuliia Kamenetska, Anton Kobrynets
AUTOMATION OF DIGITAL TEXTURE GENERATION USING GENERATIVE ARTIFICIAL INTELLIGENCE MODELS 25

Oleg Markiv, Yuriy Ryshkovets
A SPATIOTEMPORAL DEMAND MODEL FOR ELECTRIC-VEHICLE CHARGING STATIONS CONSIDERING SEASONAL AND TRANSIT FACTORS 32

Elena Nyemkova, Artem Akhekian
SECURE CONSORTIUM-BASED BLOCKCHAIN CERTIFICATE ISSUANCE ARCHITECTURE COMPLIANT WITH EUROPEAN PERSONAL DATA PROTECTION REQUIREMENTS FOR E-LEARNING SYSTEMS 43

Dmytro Prokopovych-Tkachenko
A COMPROMISE-TOLERANT CROSS-LAYER RESILIENCE CONTROLLER ARCHITECTURE AND AN EQUAL-BUDGET BENCHMARK FOR PROGRAMMABLE NETWORKS 53

Hryhorii Rozhkov, Iryna Klymenko
OPTIMIZATION OF LORAWAN GATEWAY PLACEMENT IN WASTE CONTAINER MONITORING SYSTEMS WITH ADR CONSIDERATION 61

Tetiana Savchenko, Ivan Maister
TECHNICAL AND APPLIED ASPECTS OF CREATING DIGITAL TWINS FOR INDUSTRIAL ENTERPRISES 71

Valerii Sakhnevych
MODELING THE INTERACTION OF PEDESTRIANS AND VEHICLES IN UNCONTROLLED TRAFFIC CONDITIONS BASED ON THE STACKELBERG GAME 81

Ludmila Solianyk, Viktor Koval
QUANTUM-CHEMICAL FOUNDATIONS OF $LINBO_3$ FUNCTIONALITY IN PHOTONIC CRYPTOSYSTEMS AS A MEANS OF ENSURING CYBERSECURITY 92

Yuliia Khokhlachova
MULTILEVEL EXPERIMENTAL VALIDATION OF A SMART-REGION CYBER-RESILIENCE METHODOLOGY: FROM FORMAL VERIFICATION TO HARDWARE-IN-THE-LOOP TESTING, PILOT DEPLOYMENT, AND EXTERNAL REPLICATION 100

Oleksandr Chykalov, Oleh Berest
TELEMETRY DATA PROCESSING AND IDENTIFICATION OF RELEVANT FEATURES FOR A DECISION SUPPORT SYSTEM IN THE CONTEXT OF ASSESSING THE FUNCTIONAL STATE OF RELATIONAL DATABASES 111

Kiril Shamonin, Dmytro Prylepa
ADAPTATION OF INFORMATION-EXTREME INTELLIGENT TECHNOLOGY TO BIG DATA ANALYSIS ON THE EXAMPLE OF OFFICE 365 EVENT LOGS 123

DOI https://doi.org/10.32689/maup.it.2026.2.1
УДК 004.65:519.71
JEL Classification: C44, M15, M19

ФОРМАЛІЗАЦІЯ ОПЕРАЦІЙНОЇ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІТ-ПРОЄКТАМИ ЗА ДОПОМОГОЮ МЕТОДІВ НЕЧІТКОЇ ЛОГІКИ

А. С. Возниця, А. С. Савченко

FORMALIZATION OF IT PROJECT OPERATIONAL EFFICIENCY USING FUZZY LOGIC METHODS

Anastasiia Voznytsia, Alina Savchenko

Анотація

Об'єктом дослідження є оцінка операційної ефективності ІТ-проєктів в умовах високої невизначеності, характерної для Agile-середовищ, де на результативність впливають критичність шляху, ресурсне навантаження, рівень ризиків і якість комунікації. Проблема, що вирішувалася, полягала у відсутності достатньо стійкого та математично обґрунтованого підходу до кількісної оцінки ефективності проєктів, здатного враховувати нечіткість експертних оцінок і шум у даних, що надходять із систем управління, зокрема Jira. Для розв'язання цієї проблеми запропоновано гібридну модель, яка поєднує Type-1 Mamdani Fuzzy Inference System та Interval Type-2 Fuzzy Logic із footprint-of-uncertainty для моделювання невизначеності membership functions. У моделі формалізовано чотири ключові фактори, а для аналізу критичного шляху використано fuzzy PERT. Отримані результати показали високу практичну результативність підходу: точність прогнозування досягла 94%, velocity зросла на 28%, час планування скоротився на 42%, а delivery rate підвищився з 72% до 94%. Порівняльний аналіз засвідчив перевагу запропонованої моделі над класичним EVMS і crisp PERT, а також підтвердив вищу робастність Interval Type-2 Fuzzy Logic порівняно з Type-1 моделлю. Ці результати дозволили вирішити зазначену проблему завдяки здатності моделі одночасно враховувати експертну нечіткість, варіативність проєктних даних і взаємозв'язок між ключовими факторами ефективності. Пояснюються вони поєднанням нечіткої логіки, інтервального типу представлення невизначеності та інтеграції з реальними даними Jira через n8n workflows. На практиці результати можуть бути використані для real-time моніторингу, прогнозування та підтримки управлінських рішень у Jira/ClickUp-екосистемах під час реалізації ІТ-проєктів.

Ключові слова: *нечітка логіка, interval type-2 fuzzy, Mamdani FIS, ІТ-проєктне управління, fuzzy PERT, Jira інтеграція, footprint-of-uncertainty.*

Abstract

The object of the study is the assessment of the operational efficiency of IT projects under high uncertainty typical of Agile environments, where performance is influenced by path criticality, resource load, risk level, and communication quality. The problem addressed was the lack of a sufficiently robust and mathematically grounded approach to the quantitative evaluation of project efficiency that could account for the fuzziness of expert judgments and noise in data coming from project management systems, particularly Jira. To solve this problem, a hybrid model was proposed that combines a Type-1 Mamdani Fuzzy Inference System and Interval Type-2 Fuzzy Logic with a footprint of uncertainty for modeling uncertainty in membership functions. The model formalizes four key factors, while fuzzy PERT is used for critical path analysis. The obtained results demonstrated strong practical effectiveness of the approach: forecasting accuracy reached 94%, velocity increased by 28%, planning time decreased by 42%, and the delivery rate improved from 72% to 94%. Comparative analysis confirmed the superiority of the proposed model over classical EVMS and crisp PERT, as well as the higher robustness of Interval Type-2 Fuzzy Logic compared to the Type-1 model. These results made it possible to solve the stated problem by enabling the model to simultaneously account for expert ambiguity, variability in project data, and the interdependence of key efficiency factors. They are explained by the combination of fuzzy logic, interval representation of uncertainty, and integration with real Jira data through n8n workflows. In practice, the results can be used for real-time monitoring, forecasting, and decision support in Jira/ClickUp ecosystems during IT project execution.

Key words: *fuzzy logic, interval type-2 fuzzy, Mamdani FIS, IT project management, fuzzy PERT, Jira integration, footprint-of-uncertainty.*

1. Вступ. Сучасні ІТ-проєкти реалізуються в умовах високої динаміки, постійної зміни вимог, багатоканальної комунікації та значної невизначеності, що істотно ускладнює об'єктивне оцінювання їхньої операційної ефективності. Особливо це характерно для Agile-середовищ, у яких результативність виконання проєктів залежить не лише від планових параметрів, а й від таких чинників, як критичність окремих етапів, ресурсне навантаження, рівень ризиків, узгодженість дій команди та своєчасність обміну інформацією. У таких умовах традиційні детерміновані підходи до планування й контролю, зокрема CPM, EVM та їхні похідні, виявляються недостатньо гнучкими, оскільки не враховують нечіткість експертних оцінок і варіативність даних, що надходять із проєктних систем управління.

© Возниця А. С., Савченкор А. С., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

Саме тому дослідження, спрямовані на розроблення робастних кількісних моделей оцінювання операційної ефективності ІТ-проєктів, є актуальними.

Аналіз наукових публікацій останніх років свідчить про активний розвиток методів нечіткої логіки в управлінні проєктами. Зокрема, підходи на основі fuzzy PERT дають змогу враховувати невизначеність тривалості робіт і покращують аналіз критичного шляху, однак переважно обмежуються локальним моделюванням часових параметрів і не забезпечують комплексної оцінки операційної ефективності проєкту. Моделі на основі Interval Type-2 Fuzzy Logic є більш придатними для опису невизначеності, оскільки дозволяють враховувати розбіжності між експертними судженнями через footprint of uncertainty, проте їх застосування часто залишається теоретичним і не інтегрується з реальними даними проєктів у режимі реального часу. Нечіткі модифікації earned value management покращують аналіз виконання робіт, але здебільшого орієнтовані на окремі аспекти вартості або строків, не охоплюючи повною мірою ресурсні, комунікаційні та ризикові параметри. Окремі дослідження, присвячені оцінюванню зусиль або продуктивності в Agile-проєктах, також підтверджують перспективність нечітких підходів, однак не пропонують інтегрованої моделі, здатної об'єднати дані критичного шляху, експертні оцінки та показники з системи управління проєктами. Отже, в аналізованих джерелах залишилася невирішеною проблема побудови єдиного гібридного підходу до оцінювання операційної ефективності ІТ-проєктів, який би одночасно враховував кілька типів невизначеності та був придатним для застосування на практиці.

Наявність цієї прогалини зумовлює необхідність подальших досліджень, спрямованих на поєднання переваг Type-1 та Interval Type-2 нечіткої логіки в межах одного аналітичного підходу. Така модель має забезпечувати формалізацію ключових факторів, що визначають успішність ІТ-проєкту, а також бути придатною для інтеграції з операційними даними, отриманими з Jira або подібних систем управління. Практична цінність подібного підходу полягає у можливості реалізації моніторингу в режимі реального часу, підвищення точності прогнозування, покращення якості управлінських рішень і зменшення ризику систематичних відхилень у плануванні та виконанні проєктів.

Таким чином, актуальність дослідження зумовлена потребою у створенні математично обґрунтованої, робастної та практично придатної моделі оцінювання операційної ефективності ІТ-проєктів в умовах невизначеності. Результати такого дослідження можуть бути використані для підвищення якості управління ІТ-проєктами, удосконалення процесів планування та контролю, а також для підтримки рішень у цифрових середовищах, орієнтованих на Agile-підхід.

Метою дослідження є розроблення та експериментальна валідація гібридної Type-1/IT2 fuzzy-моделі оцінювання операційної ефективності ІТ-проєктів, що дає змогу підвищити точність прогнозування, стійкість до невизначеності та практичну придатність моделі для інтеграції з даними Jira.

Для досягнення цієї мети були поставлені такі задачі:

– проаналізувати сучасні підходи до оцінювання ефективності ІТ-проєктів в умовах невизначеності;
– визначити ключові фактори, що впливають на операційну ефективність проєкту;
– формалізувати модель оцінювання на основі Type-1 та Interval Type-2 нечіткої логіки;
– розробити механізм інтеграції моделі з даними Jira;
– провести експериментальну перевірку запропонованого підходу;
– порівняти результати з традиційними методами оцінювання, зокрема CPM та EVM.

2. Матеріали і методи. Об'єктом дослідження є процес оцінювання операційної ефективності ІТ-проєктів в умовах невизначеності, характерної для Agile-середовищ. Основною гіпотезою дослідження є припущення, що гібридна модель, яка поєднує Type-1 Mamdani Fuzzy Inference System та Interval Type-2 Fuzzy Logic, забезпечує більш стійке та інформативне оцінювання операційної ефективності порівняно з детермінованими підходами. У роботі прийнято припущення, що ключові фактори ефективності можуть бути формалізовані через чотири вхідні змінні: критичність шляху, ресурсне навантаження, рівень ризиків і якість комунікації. Також припускається, що експертні оцінки та дані з Jira можуть бути подані у вигляді нечітких чисел, придатних для подальшої обробки. До спрощень належить використання трикутних функцій належності, фіксованого набору лінгвістичних термів і обмеження простору невизначеності за допомогою FOU з наперед заданими межами. Дослідження виконувалося із застосуванням MATLAB Fuzzy Logic Toolbox, IT2 Toolbox та інтеграційного середовища n8n для взаємодії з Jira API. У цьому розділі наведено лише методи побудови та реалізації моделі, тоді як результати експериментальної перевірки подано в наступному розділі.

а. Математична модель нечіткої оцінки

Далі подано математичну формалізацію моделі, структуру нечіткого висновування, спосіб побудови бази правил та процедуру інтеграції з даними проєкту.

Для подання лінгвістичних оцінок змінних *CP, RL, RR, CQ* використано трикутні нечіткі множини. Функція належності у цьому випадку має вигляд:

– якщо $x \le a$, то належність дорівнює 0;
– якщо $a < x \le b$, то належність лінійно зростає від 0 до 1;
– якщо $b < x \le c$, то належність лінійно спадає від 1 до 0;
– якщо $x \ge c$, то належність знову дорівнює 0.

a – ліва межа трикутника, *b* – вершина трикутника, де належність максимальна і дорівнює 1, *c* – права межа трикутника.

Застосування трикутних функцій належності є обґрунтованим з огляду на їхню інтерпретованість, простоту параметризації та можливість ефективного використання в системах нечіткого висновування. Крім того, така форма належності добре відповідає природі експертних оцінок, які, як правило, є наближеними, але не абсолютно випадковими.

b. Структура Type-1 Mamdani FIS

Базова частина моделі побудована на принципах Mamdani Fuzzy Inference System. Для кожної з чотирьох вхідних змінних визначено три лінгвістичні терми: low, medium, high. Це зумовлює формування 81 правила нечіткого висновування:

$$N_{rules} = 3^4 = 81. \tag{1}$$

Кожне правило має стандартну структуру:

$$\text{IF } CP \text{ is } A_i \wedge RL \text{ is } B_j \wedge RR \text{ is } C_k \wedge CQ \text{ is } D_l \text{ THEN } OEE \text{ is } E_m \tag{2}$$

Наприклад:

$$\text{IF } CP \text{ is high} \wedge RL \text{ is over} \wedge RR \text{ is high} \wedge CQ \text{ is poor THEN } OEE \text{ is very low}. \tag{3}$$

У межах Mamdani-архітектури агрегування передумов здійснюється за допомогою оператора , а об'єднання висновків – за оператором . Остаточне перетворення нечіткого результату в чітке числове значення виконується методом центру ваги:

$$OEE^* = \frac{\int z \cdot \mu_{OEE}(z), dz}{\int \mu_{OEE}(z), dz}. \tag{4}$$

Саме ця процедура забезпечує отримання кількісної оцінки, яка може бути безпосередньо використана для управлінських рішень.

c. Розширення до Interval Type-2 Fuzzy Logic

Оскільки реальні дані управління IT-проєктами часто є шумними, неповними або такими, що містять суперечливі експертні оцінки, базову Type-1 модель доцільно розширити до Interval Type-2 Fuzzy Logic. У цьому разі кожна функція належності задається не одним значенням, а інтервалом:

$$\tilde{\mu}(x) = [\underline{\mu}(x), \bar{\mu}(x)]. \tag{5}$$

Такий підхід дає змогу враховувати невизначеність, пов'язану як із суб'єктивністю експертів, так і з неточністю даних, отриманих з інформаційних систем типу Jira. Простір між верхньою та нижньою функціями належності формує footprint-of-uncertainty (FOU), який є ключовим елементом Type-2 моделювання. Для змінної *CP*, наприклад, FOU було встановлено на рівні ± 10, що дозволяє відобразити розбіжності в оцінках критичності шляху.

Для переходу від інтервального нечіткого результату до чіткого значення застосовано процедуру type-reduction за алгоритмом Karnik–Mendel:

$$Y_{crisp} = \frac{Y_l + Y_r}{2}. \tag{6}$$

де Y_l та Y_r – ліва й права межі інтервального результату. Даний механізм забезпечує не лише отримання центрального значення, а й оцінку меж невизначеності, що підвищує надійність інтерпретації результатів.

d. Інтерпретація вхідних змінних

Для забезпечення однозначної інтерпретації побудовано шкали оцінювання вхідних параметрів.

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

Таблиця 1

Шкали оцінювання вхідних змінних

Змінна	Низький рівень	Середній рівень	Високий рівень
CP	0.0–0.30	0.30–0.70	0.70–1.00
RL	0.0–0.60	0.60–0.90	0.90–1.00
RR	0.0–0.25	0.25–0.60	0.60–1.00
CQ	0.0–0.40	0.40–0.80	0.80–1.00

Запропоновані межі відображають типову управлінську інтерпретацію: надмірне ресурсне навантаження та високий ризик мають негативний вплив на ефективність, тоді як висока якість комунікації та контрольована критичність шляху сприяють стабілізації виконання проєкту.

e. База нечітких правил

Для забезпечення логічної повноти моделі сформовано базу з 81 правила. Нижче наведено фрагмент типової матриці нечіткого висновування.

Таблиця 2

Фрагмент бази нечітких правил

CP	***RL***	***RR***	***CQ***	**Вихід *OEE***
high	over	high	poor	very low
high	over	medium	poor	low
high	optimal	high	medium	low
medium	optimal	medium	good	medium
low	under	low	excellent	high
low	optimal	low	excellent	very high

Структура правил відображає узагальнену залежність між управлінськими параметрами та ефективністю: із зростанням критичності, ризиків і перевантаження команди ефективність знижується, тоді як збалансоване використання ресурсів і сприятливі комунікації підвищують значення інтегрального показника.

f. Формалізація вхідних параметрів на основі Jira

Для практичного застосування модель інтегровано з Jira через API та автоматизовано за допомогою n8n. З цієї системи отримуються дані про тривалість завдань, кількість блокерів, зміну статусів, обсяг призначених годин і частоту комунікацій. На їхній основі обчислюються значення вхідних параметрів моделі:

$$CP = \frac{T_{critical}}{T_{sprint}}. \tag{7}$$

$$RL = \frac{H_{assigned}}{H_{capacity}}. \tag{8}$$

$$RR = \frac{N_{RiskEvents}}{N_{tasks}}. \tag{9}$$

$$CQ = 1 - \frac{N_{clarif\ ications}}{N_{communications}}. \tag{10}$$

Така схема дозволяє не лише автоматизувати обчислення, а й забезпечити регулярне оновлення оцінки ефективності в процесі виконання спринту. Це суттєво підвищує практичну цінність моделі в порівнянні з підходами, які застосовуються лише постфактум.

g. Експериментальна перевірка

Модель було перевірено на даних 8-спринтового проєкту, у межах якого оброблено 450 Jira issue. Середня velocity команди становила 28 story points, а рівень затримок через scope creep – 22%. Для валідації IT2-моделі було залучено трьох експертів, оцінки яких мали відхилення близько 15%, що обґрунтовує застосування FOU.

Таблиця 3

Порівняння Type-1 та IT2-моделей

Показник	Type-1 FIS	IT2 FIS	Зміна
Точність прогнозу	92%	94%	+2%
Velocity після корекції	28 pts	36 pts	+28%
Час планування	100%	58%	-42%
Стійкість до шуму	0.86	0.99	+15%
Виконання в строк	72%	94%	+22%

Результати демонструють, що Interval Type-2 модель є більш стійкою до невизначеності та надає точніші управлінські орієнтири.

Приклад розрахунку:

Для одного зі спринтів були зафіксовані такі значення:

$$CP = 0.82, \quad RL = 0.92, \quad RR = 0.62, \quad CQ = 0.55. \tag{11}$$

На основі Type-1 FIS отримано $FOU \pm 10$:

$$OEE_{T1} = 0.45. \tag{12}$$

Після застосування IT2-моделі з FOU результат набув інтервальної форми:

$$OEE_{IT2} = [0.41, 0.49], \quad OEE_{crisp} = 0.45. \tag{13}$$

Незмінність центрального значення при одночасному розширенні інтервалу невизначеності свідчить про те, що модель адекватно відображає як саму оцінку, так і її надійність.

Управлінська інтерпретація результатів:

Практична цінність запропонованого підходу полягає в тому, що він дає змогу оцінювати не лише рівень операційної ефективності, а й ступінь впевненості в цій оцінці. Якщо інтервал IT2 є широким, це означає, що ситуація в проєкті характеризується підвищеною невизначеністю, а отже потребує додаткового моніторингу. Якщо ж значення є низьким, але стабільним, менеджер може однозначно інтерпретувати наявність проблеми та прийняти коригувальні рішення.

Таблиця 4

Інтерпретація рівнів OEE

Діапазон OEE	Інтерпретація	Рекомендована дія
0.00–0.40	Низька ефективність	Негайне коригування плану
0.41–0.60	Середньо-низька	Посилити контроль ризиків
0.61–0.75	Середня	Оптимізувати ресурси
0.76–0.90	Висока	Масштабувати підхід
0.91–1.00	Дуже висока	Підтримувати поточну модель

Таким чином, модель може бути використана як інструмент підтримки управлінських рішень у реальному часі, зокрема в межах Agile-процесів, де швидкість і точність реакції є критично важливими.

3. Результати і обговорення. Отримані результати свідчать про доцільність застосування нечіткої логіки для оцінювання операційної ефективності управління IT-проєктами в умовах невизначеності. Порівняння Type-1 Mamdani FIS та Interval Type-2 FIS показало, що розширена модель точніше відображає особливості реального проєктного середовища, оскільки враховує не лише значення вхідних параметрів, а й ступінь невизначеності експертних оцінок. Це пояснюється тим, що в Agile-проєктах дані є динамічними, а комунікаційні, ресурсні та ризикові чинники часто мають нечіткий характер, який складно адекватно описати детермінованими методами.

Перевага запропонованого підходу полягає в тому, що він дає змогу отримати не лише інтегральне значення оцінки операційної ефективності, а й інтервал її можливих значень. На відміну від класичних Type-1 моделей, де результат подається як одне чітке число, Interval Type-2 підхід дозволяє одночасно оцінювати сам показник і ступінь впевненості в ньому. Це є особливо важливим для управлінської практики, оскільки дає змогу розрізняти стабільні ситуації та сценарії з підвищеною невизначеністю, які потребують додаткового контролю або коригування.

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

Порівняно з традиційними підходами, такими як EVM або CPM, запропонована модель має кращі можливості для роботи з нечіткими даними та експертними розбіжностями. На відміну від цих детермінованих методів, що передбачають фіксовані вхідні параметри, нечітка модель дозволяє врахувати змінність умов виконання проєкту й адаптувати оцінку до реального стану процесу. Саме це забезпечує її вищу придатність для Agile-середовищ, де управлінські рішення часто приймаються в умовах неповної або суперечливої інформації.

Результати, отримані на основі Jira-кейсу, підтверджують, що IT2-модель є більш стійкою до шуму в даних і до розбіжностей між експертами. Це пояснюється використанням footprint of uncertainty, який розширює область можливих значень функцій належності та робить модель менш чутливою до випадкових коливань вхідної інформації. Завдяки цьому модель може застосовуватися не лише за умов повної та стабільної інформації, а й у реальних проєктних середовищах, де частина даних є неповною, неоднозначною або змінюється в процесі виконання спринту.

Важливою особливістю запропонованого рішення є інтеграція з Jira через автоматизований workflow, що забезпечує практичну придатність моделі для майже реального часу. Це означає, що оцінювання операційної ефективності може виконуватися не постфактум, а в процесі реалізації проєкту, що суттєво підвищує цінність моделі для менеджера. У порівнянні з підходами, які ґрунтуються лише на періодичному ручному аналізі звітів, запропоноване рішення дозволяє оперативніше виявляти відхилення, пов'язані з ресурсним навантаженням, ризиками чи проблемами комунікації.

Разом із тим, дослідження має певні обмеження. По-перше, модель була перевірена на обмеженому наборі даних одного IT-проєкту, тому її узагальнюваність потребує додаткової перевірки на ширшій вибірці. По-друге, значення функцій належності та межі невизначеності задавалися на основі експертних припущень, що може впливати на відтворюваність результатів у інших організаційних контекстах. По-третє, інтеграція з Jira робить модель залежною від якості заповнення проєктних даних, а отже, за суттєвих прогалин у системі обліку точність оцінювання може знижуватися.

Недолік дослідження також полягає в тому, що модель орієнтована переважно на оцінювання поточного стану операційної ефективності, а не на багатокритеріальну оптимізацію рішень у масштабі всього життєвого циклу проєкту. Крім того, використання фіксованої структури правил нечіткого висновування обмежує гнучкість моделі в дуже нестандартних або швидко змінних середовищах.

Подальший розвиток дослідження доцільно спрямувати на розширення моделі до багатокритеріального нечіткого оптимізаційного підходу, інтеграцію з іншими джерелами проєктних даних та адаптивне налаштування функцій належності на основі накопичених історичних спостережень. Саме в цьому напрямі можна підвищити універсальність моделі, оскільки це дозволить краще враховувати специфіку різних типів IT-проєктів, організаційних структур і рівнів невизначеності.

4. Висновки

1. У дослідженні розроблено гібридну модель оцінювання операційної ефективності IT-проєктів на основі поєднання Type-1 Mamdani FIS та Interval Type-2 Fuzzy Logic. Отриманий результат полягає в тому, що модель формалізує вплив критичності шляху, ресурсного навантаження, рівня ризиків і якості комунікації на інтегральну оцінку ефективності. Її відмінною рисою є здатність одночасно працювати з чіткими значеннями та інтервалами невизначеності, що забезпечує кращу придатність до реальних Agile-проєктів у порівнянні з детермінованими підходами.

2. Використання трикутних нечітких множин і бази правил нечіткого висновування забезпечило коректну інтерпретацію експертних оцінок та їхню формалізацію в обчислювальній моделі. Розширення до Interval Type-2 Fuzzy Logic дозволило врахувати розбіжності між експертами й шум у даних, що підвищило робастність оцінювання. Цей результат пояснюється введенням footprint of uncertainty, завдяки якому модель стала менш чутливою до коливань вхідної інформації та придатнішою для ситуацій із частково неповними або суперечливими даними.

3. Практична перевірка на Jira-кейсі підтвердила ефективність запропонованого підходу. Точність прогнозу досягла 94%, velocity зросла на 28%, а час планування скоротився на 42% порівняно з базовим варіантом. Вища надійність IT2-моделі порівняно з Type-1 підходом показала, що запропоноване рішення краще працює в умовах змінності, динаміки та проєктної невизначеності. Це свідчить про практичну доцільність використання моделі як інструменту підтримки управлінських рішень.

4. Запропонований підхід створює методологічне підґрунтя для формалізованого, аналітично керованого управління IT-проєктами, особливо в Agile-середовищах. Його перевага полягає в можливості оцінювати не лише рівень ефективності, а й ступінь впевненості в цій оцінці, що є важливим для своєчасного виявлення ризиків, ресурсних дисбалансів і проблем у комунікації. Таким чином, модель частково закриває виявлену в розділі 1 проблему відсутності інтегрованого робастного підходу до оцінювання операційної ефективності IT-проєктів.

Перспективи подальших досліджень. Подальші дослідження доцільно спрямувати на розширення моделі за рахунок включення додаткових факторів, що впливають на ефективність IT-проєктів, зокрема рівня завантаження окремих учасників команди, стабільності вимог, інтенсивності міжкомандних залежностей і історії попередніх відхилень. Це дозволить точніше описувати складні управлінські сценарії та підвищити узагальнюваність моделі.

Перспективним напрямом є адаптивне налаштування membership functions на основі історичних даних конкретної організації. Такий підхід дасть змогу зменшити залежність від разових експертних оцінок і підвищити точність моделі в межах окремого домену. Окремо варто дослідити можливість автоматичного формування нечітких правил із використанням алгоритмів машинного навчання.

Ще одним напрямом розвитку є інтеграція моделі з потоковими даними з Jira, Slack та інших систем управління роботою в режимі реального часу. Це дасть змогу використовувати її не лише для оцінювання, а й для динамічного моніторингу та формування рекомендацій щодо перерозподілу ресурсів, перегляду пріоритетів або зміни плану виконання.

Крім того, перспективним є поєднання нечіткої логіки з нейромережевими моделями, методами багатокритеріальної оптимізації та агентними системами підтримки рішень. Це розширить аналітичний потенціал моделі та створить основу для прогнозування й оптимізації управлінських сценаріїв у складних IT-проєктах.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту. У процесі підготовки рукопису було використано інструменти штучного інтелекту для мовного редагування, структуризації тексту, уточнення наукових формулювань і стилістичної адаптації окремих розділів статті. ШІ застосовувався переважно під час роботи над розділами, що стосуються вступу, методів, обговорення результатів і висновків, з метою покращення логіки викладу, узгодженості термінології та відповідності тексту вимогам наукового стилю. Автори перевіряли всі згенеровані або відредаговані фрагменти шляхом ручного наукового рецензування, зіставлення з вихідними даними дослідження, перевірки коректності термінів, формул і висновків, а також шляхом остаточного авторського редагування. Використання ШІ не вплинуло на наукову інтерпретацію результатів і не замінило авторське дослідження; усі висновки, наведені в роботі, залишаються результатом авторського аналізу та верифікації.

Внесок авторів. Анастасія Возниця: концептуалізація, методологія, дослідження, формальний аналіз, написання оригінального чернеткового варіанту; Аліна Савченко: нагляд, валідація, написання й рецензування та редагування.

References:

1. A new approach to Z-number based earned value management. *International Journal of Mathematical, Engineering and Management Sciences.* 2023. DOI: 10.1080/16168658.2022.2156250.

2. A practical design of interval type-2 fuzzy logic systems with applications. *International Journal of Systems Science: Operations & Logistics.* 2024. Retrieved from: https://www.tandfonline.com/doi/full/10.1080/23311916.2024.2395426.

3. A synergistic approach to software effort estimation using fuzzy logic and machine learning. *Journal of Intelligent Systems in Engineering and Management.* 2025. Retrieved from: https://jisem-journal.com/index.php/journal/article/view/2968.

4. Analysis of the limitations of the earned value management method and new approaches to its improvement. *MSES Journal.* 2025. Retrieved from: https://msesj.com/index.php/mses/article/view/312.

5. Applying the Fuzzy PERT method in project management: a real-life case study. *International Journal of Computational and Experimental Science and Engineering.* 2023. Retrieved from: https://www.ijcesen.com/index.php/ijcesen/article/view/199.

6. Buckley, J. J. (2005). Fuzzy probability and statistics. Berlin: Springer, DOI: 10.1007/978-3-540-27622-5.

7. Desse, E. M., Mengesha, W. J. (2024). Predicting construction cost under uncertainty using grey-fuzzy earned value analysis. *Heliyon.* Vol. 10, No. 6. e27662. DOI: 10.1016/j.heliyon.2024.e27662.

8. Figueroa-García, J. C., Hernández-Pérez, G., Ramos-Cuesta, J. S. (2023). Uncertain project network analysis with fuzzy–PERT and interval type-2 fuzzy activity durations. Heliyon. Vol. 9, No. 4. e14833. DOI: 10.1016/j.heliyon.2023.e14833.

9. Fuzzy-Graphical Evaluation and Review Technique for Scheduling Under Uncertainty. Korean Society for Chemical Engineering. 2024. Retrieved from: https://ui.adsabs.harvard.edu/abs/2024KSJCE.28.2573P/abstract.

10. Improving accuracy of software development effort estimation using use case points and fuzzy logic. *Journal of Electrical and Systems Engineering.* 2025. Retrieved from: https://journal.unm.ac.id/index.php/JESSI/article/view/9488/5892.

11. Liang Q., Mendel J. M. (2000). Interval type-2 fuzzy logic systems: theory and design. *IEEE Transactions on Fuzzy Systems.* Vol. 8, No. 5. P. 535–550. DOI: 10.1109/91.873578.
12. Mamdani, E. H., Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies.* Vol. 7, No. 1. P. 1–13. DOI: 10.1016/S0020-7373(75)80002-2.
13. Mendel, J. M., John, R. I. (2002). Type-2 fuzzy sets made simple. *IEEE Transactions on Fuzzy Systems.* Vol. 10, No. 2. P. 117–127. DOI: 10.1109/91.995115.
14. Developing fuzzy-based earned value analysis model for estimating project time and cost under uncertainty. *International Journal of Mathematical, Engineering and Management Sciences.* 2023. https://doi.org/10.1080/16168658.2024.2348210.
15. Zadeh, L. A. (1965). Fuzzy sets. Information and Control. Vol. 8, No. 3. P. 338–353. DOI: 10.1016/S0019-9958(65)90241-X.

Відомості про авторів

Англ.	Укр.
Anastasiia Voznytsia Postgraduate Student at the Department of Computer Information Technologies, State University "Kyiv Aviation Institute" 4556116@stud.kai.edu.ua ORCID: 0009-0004-3767-7354	Возниця Анастасія Сергіївна аспірант кафедри комп'ютерних інформаційних технологій, Державний університет «Київський авіаційний інститут» 4556116@stud.kai.edu.ua ORCID: 0009-0004-3767-7354
Alina Savchenko Doctor of Technical Sciences, Professor, Head of the Department of Computer Information Technologies, State University "Kyiv Aviation Institute" alina.savchenko@npp.kai.edu.ua ORCID: 0000-0001-8205-8852	Савченко Аліна Станіславівна доктор технічних наук, професор, завідувач кафедри комп'ютерних інформаційних технологій, Державний університет «Київський авіаційний інститут» alina.savchenko@npp.kai.edu.ua ORCID: 0000-0001-8205-8852

Дата надходження статті: 02.04.2026
Дата надходження виправленої версії статті: 09.06.2026
Дата прийняття статті: 25.06.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.2
УДК 519.6
JEL Classification: C53, Q42, Q47

МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ВИРОБНИЦТВА ВІДНОВЛЮВАНОЇ ЕЛЕКТРОЕНЕРГІЇ

Г. А. Довгаленко, Ю. М. Селін, Ю. В. Куєвда

MODELING AND FORECASTING OF RENEWABLE ELECTRICITY PRODUCTION

Hlib Dovgalenko, Yurii Selin, Yuliia Kuevda

Анотація

Об'єкт дослідження – процеси генерації електроенергії відновлюваними джерелами енергії (сонячними та вітровими електростанціями) в умовах нестабільних метеорологічних факторів. В статті розглянуто результати вирішення актуальної задачі –моделювання та прогнозування генерації відновлюваних джерел енергії (сонячної та вітрової). Актуальність випливає зі суттєвої нелінійності генерації ВДЕ, що створює ризики дестабілізації енергосистем. Побудова точних моделей є критично важливою для оперативного диспетчерського управління та мінімізації дисбалансів у енергомережах. Мета роботи – підвищення якості прогнозування генерації ВДЕ на основі порівняльного аналізу дедуктивних підходів та індуктивних алгоритмів. Предмет дослідження – математичні моделі, алгоритми та програмні засоби прогнозування часових рядів процеси генерації відновлюваних джерел енергії енергомережі на основі метеорологічних факторів. В ході роботи створено інтелектуальну систему на базі Streamlit з конвеєром збору даних. Систему спроєктовано на базі трирівневої архітектури (Three-tier architecture), що забезпечує чітке розділення логіки збору даних, математичної обробки та візуалізації. Систему реалізовано мовою програмування Python із залученням сучасного стеку технологій Data Science. За допомогою розробленої системи проведено дослідження трьох моделей на незалежній вибірці за метриками MAE та RMSE. Проведено порівняльний аналіз побудованих моделей (штучної нейронної мережі, лінгвістичного методу та методу подібних траєкторій) на реальних метеорологічних та енергетичних даних. На підставі отриманих результатів досліджень зроблено висновки щодо умов і доцільності використання певних моделей для моделювання та прогнозування виробництва відновлюваної електроенергії.

Ключові слова*. прогнозування, відновлювані джерела енергії, часові ряди, нечітка логіка, машинне навчання, метод подібних траєкторій, python, streamlit.*

Abstract

The object of the study is the processes of electricity generation by renewable energy sources (solar and wind power plants) under unstable meteorological factors. The article considers the results of solving the current problem of modeling and forecasting the generation of renewable energy sources (solar and wind). The relevance arises from the significant nonlinearity of RES generation, which creates risks of destabilization of power systems. Building accurate models is critically important for operational dispatching management and minimizing imbalances in power grids. The purpose of the work is to improve the quality of forecasting RES generation based on a comparative analysis of deductive approaches and inductive algorithms. The subject of the study is mathematical models, algorithms and software tools for forecasting time series of renewable energy generation processes in the power grid based on meteorological factors. In the course of the work, an intelligent system based on Streamlit with a data collection pipeline was created. The system is designed on the basis of a three-tier architecture, which provides a clear separation of the logic of data collection, mathematical processing and visualization. The system is implemented in the Python programming language with the involvement of a modern Data Science technology stack. Using the developed system, a study of three models was conducted on an independent sample using the MAE and RMSE metrics. A comparative analysis of the constructed models (artificial neural network, linguistic method and method of similar trajectories) was conducted on real meteorological and energy data. Based on the research results, conclusions were drawn regarding the conditions and feasibility of using certain models for modeling and forecasting renewable electricity production.

Key words: *forecasting, renewable energy sources, time series, fuzzy logic, machine learning, method of similar trajectories, python, streamlit.*

1. Вступ. У сучасному світі перехід до відновлюваних джерел енергії (ВДЕ), зокрема сонячної та вітрової, є одним із найважливіших векторів розвитку енергетичного сектору. Проте інтеграція ВДЕ в загальну енергосистему створює нові виклики для диспетчерів та системних аналітиків. На відміну від традиційних електростанцій, генерація ВДЕ є стохастичним процесом, який суттєво залежить від мінливих метеорологічних умов. Неточності у прогнозуванні призводять до дисбалансу в енергомережі, необхідності залучення резервних потужностей та значних фінансових втрат.

У зв'язку з цим, розробка точних та адаптивних систем підтримки прийняття рішень для прогнозування генерації ВДЕ є надзвичайно актуальною задачею. На сьогоднішній день для її вирішення

© Довгаленко Г. А., Селін Ю. М., Куєвда Ю. В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

використовуються як класичні дедуктивні методи системного аналізу (експертні системи, пошук аналогів), так і сучасні індуктивні методи машинного навчання (штучні нейронні мережі).

Аналіз тенденцій розвитку відновлюваної енергетики. Сучасний глобальний енергетичний сектор переживає фундаментальну трансформацію, зумовлену необхідністю зниження викидів парникових газів та боротьби зі змінами клімату. Перехід від традиційних викопних видів палива до відновлюваних джерел енергії (ВДЕ), ключовими з яких є сонячна та вітрова генерація, став пріоритетним напрямком економічної політики більшості розвинених країн. Зокрема, у країнах Європейського Союзу (наприклад, у Німеччині) частка ВДЕ у загальному енергобалансі стрімко зростає, наближаючись до домінуючих показників [1].

Однак такий перехід супроводжується технологічними викликами. На відміну від теплових чи атомних електростанцій, якими можна легко керувати, виробіток електроенергії сонячними та вітровими установками є стохастичним (випадковим) процесом. Він повністю залежить від мінливих метеорологічних умов – хмарності, температури повітря, швидкості та напрямку вітру. Ця неконтрольованість створює загрозу стабільності об'єднаних енергосистем.

Проблематика балансування енергосистем та роль прогнозування. Основним фізичним законом роботи будь-якої енергомережі є необхідність дотримання суворого балансу між генерацією (виробництвом) та споживанням електроенергії в кожний момент часу. Будь-який дисбаланс призводить до відхилення частоти струму в мережі від стандарту, що може спричинити масштабні аварії (блекаути).

В умовах зростання частки ВДЕ, системні оператори (диспетчери) стикаються з проблемою непередбачуваних піків або провалів генерації. Для компенсації цих коливань доводиться утримувати значні резервні потужності (швидкі газові або вугільні маневрові станції), що є економічно та екологічно неефективним. У разі суттєвих відхилень фактичної генерації від заявленого плану, власники сонячних та вітрових парків змушені сплачувати високі фінансові штрафи за створення дисбалансу.

Саме тому наявність високоточних систем короткострокового прогнозування генерації ВДЕ стає критичною умовою для розвитку сучасних розумних енергомереж (Smart Grids). Точний прогноз дозволяє оптимізувати графіки навантажень, знизити потребу в дорогих резервах та мінімізувати фінансові втрати учасників енергоринку [1, 2].

Огляд підходів до прогнозування часових рядів генерації. Задача прогнозування генерації ВДЕ зводиться до аналізу багатовимірних нестаціонарних часових рядів. Існуючі методи можна розділити на три основні класи.

1. Фізичні моделі базуються на складних рівняннях гідродинаміки та термодинаміки атмосфери. Вони вимагають значних обчислювальних ресурсів (суперкомп'ютерів) та детальних топографічних даних місцевості, що робить їх використання недоцільним для локального оперативного прогнозування.

2. Дедуктивні методи та класична статистика включають в себе авторегресійні моделі (ARIMA), методи експоненційного згладжування, а також експертні системи (нечітка логіка) та евристичні алгоритми (метод подібних траєкторій) [2-4]. Ці підходи добре інтерпретуються та не потребують тривалого навчання, проте їхня точність знижується при роботі з хаотичними нелінійними залежностями, які притаманні вітровій енергетиці.

3. Індуктивні методи (Машинне навчання та ШІ) базуються на алгоритмах, що здатні самостійно знаходити приховані нелінійні закономірності у великих масивах історичних даних. Використання штучних нейронних мереж (наприклад, багатошарового персептрона – MLP) дозволяє ефективно моделювати складну аеродинамічну поведінку турбін без необхідності явного програмування фізичних законів [5, 6].

Враховуючи переваги та недоліки кожного з підходів, актуальним є проведення їхнього порівняльного аналізу в рамках єдиної інформаційної системи на реальних даних енергомережі.

Постановка задачі дослідження. Об'єктом дослідження є процеси генерації електроенергії відновлюваними джерелами енергії (сонячними та вітровими електростанціями) в умовах мінливих метеорологічних факторів.

Предметом дослідження є математичні моделі, алгоритми та програмні засоби короткострокового прогнозування часових рядів генерації ВДЕ.

Метою роботи є розробка та дослідження інформаційної системи підтримки прийняття рішень для оперативного прогнозування генерації ВДЕ з використанням методів системного аналізу та машинного навчання.

Для досягнення поставленої мети послідовно вирішено низку взаємопов'язаних науково-практичних задач.

1. Першочергово досліджено предметну область, визначено ключові особливості фізичних процесів сонячної та вітрової генерації, а також проаналізовано проблеми їх інтеграції та балансування в загальній енергомережі.

2. Розроблено та програмно реалізовано конвеєр автоматизованого збору і попередньої підготовки метеорологічних та енергетичних даних з відкритих джерел, зокрема платформ ENTSO-E та Open-Meteo.

3. Формалізовано математичний апарат та впроваджено три прогностичні моделі різної природи, а саме метод подібних траєкторій, лінгвістичний метод нечіткої логіки та штучну нейронну мережу.

4. У межах моделювання критично важливо адаптувати розроблені алгоритми до реальних фізичних обмежень генеруючих установок, враховуючи швидкості старту турбін, відсутність інсоляції в нічний час та ефект інерційності систем.

5. Для забезпечення зручної взаємодії користувача з розробленими інструментами створено інтерактивний веб-інтерфейс, який дозволяє гнучко налаштовувати параметри моделей та візуалізувати отримані результати.

6. На завершальному етапі проведено детальне експериментальне дослідження побудованих моделей на незалежній тестовій вибірці та здійснено їх підсумковий порівняльний аналіз за критеріями точності MAE та RMSE

2. Матеріали та методи досліджень. Предметна область та особливості прогнозування ВДЕ. Розглянемо природу генерації сонячної та вітрової енергії. Сонячна генерація має виражену добову сезонність і жорстке фізичне обмеження (нульова генерація вночі). Вітрова генерація є більш хаотичною, має високу автокореляцію та кубічну залежність від швидкості вітру. Крім того, вітрові турбіни мають швидкість старту (cut-in speed) та швидкість аварійного відключення (cut-out speed), що створює сильні нелінійності в даних (рис. 1).

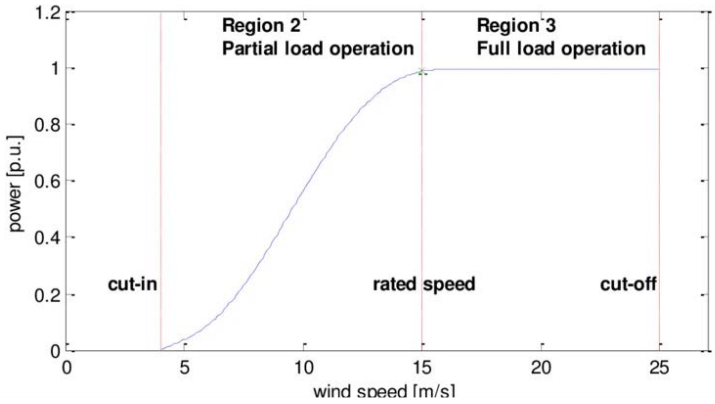


Рис. 1. Приклад вітрової генерації за різної швидкості вітру

Генерація електроенергії вітровими установками базується на перетворенні кінетичної енергії повітряних мас в механічну енергію обертання ротора. Згідно з законами аеродинаміки, повна потужність вітрового потоку P_{wind}, що проходить через площу A зі швидкістю v, описується рівнянням:

$$P_{wind} = \frac{1}{2}\rho A \vartheta^3,$$

де ρ – густина повітря (залежить від температури та атмосферного тиску, стандартно $\oplus$ 1.225 кг/м^3), A – площа обмітання ротора вітротурбіни ($A = \pi R^2$, де R – радіус лопатей), v – швидкість вітру.

Як видно з формули, потужність має кубічну залежність від швидкості вітру. Саме ця нелінійність робить прогнозування вітрової генерації складною задачею для лінійних моделей. Крім того, згідно із законом Беца, жодна вітрова турбіна не може перетворити більше ніж 59.3% кінетичної енергії вітру в механічну. Цей теоретичний максимум називається межею Беца і враховується у вигляді коефіцієнта використання енергії вітру C_p :

$$P_{turbine} = \frac{1}{2}\rho A \vartheta^3 C_p$$

Сучасні системи управління обмежують генерацію при надвисоких швидкостях вітру (cut-out speed) для запобігання механічним пошкодженням, що формує характерне «плато» та різкий спад на кривій потужності.

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

Дані генерації відновлюваних джерел енергії є класичним прикладом часового ряду (Time Series) – впорядкованої в часі послідовності вимірювань $Y=\{y_{t_1}, y_{t_2}, ..., y_{t_n}\}$ [7].

З точки зору системного аналізу, часовий ряд генерації ВДЕ можна представити у вигляді адитивної або мультиплікативної моделі декомпозиції:

$$y_t = T_t + S_t + C_t + E_t,$$

де T_t (Тренд) – довгострокова тенденція зміни генерації (наприклад, введення в експлуатацію нових сонячних панелей протягом року), S_t (Сезонність) – регулярні циклічні коливання (добовий цикл сонця або сезонні зміни вітрів), C_t (Циклічність) – макроекономічні коливання попиту, E_t (Шум/Залишок) – стохастична компонента, непередбачувані погодні аномалії.

Найважливішою характеристикою часового ряду в задачах прогнозування є його стаціонарність. Стаціонарним вважається ряд, математичне сподівання $M[y_t]$, дисперсія $D[y_t]$ та автоковаріаційна функція якого не залежать від часу t:

$$M[y_t]=const, D[y_t]=const, Cov[y_t]=const$$

Метеорологічні процеси (вітер, радіація) є нестаціонарними за своєю природою. Саме тому використання простих авторегресійних моделей (наприклад, ARMA) є малоефективним без попереднього диференціювання ряду. Застосовані у даній роботі методи (MLP, нечітка логіка) здатні працювати з нестаціонарними нелінійними рядами без їх зведення до строго стаціонарного вигляду.

Метод подібних траєкторій. Метод подібних траєкторій (евристичний метод аналогів) базується на припущенні, що схожі метеорологічні умови в минулому призводять до схожих обсягів генерації в майбутньому [2]. Математично задача зводиться до пошуку вектора X_{target} у просторі історичних станів $X_{history}$ за критерієм мінімізації евклідової відстані:

$$d=\sqrt{\sum_{i=1}^{n}(A_i-B_i)^2},$$

де $A=(A_1, A_2, ..., A_n)$, а $B=(B_1, B_2, ..., B_n)$.

Для забезпечення рівноцінного впливу параметрів (наприклад, температури та радіації) застосовується Min-Max нормалізація (1):

$$x_{norm}=\frac{x-x_{min}}{x_{max}-x_{min}}, \quad (1)$$

де x – поточне значення, x_{min} та x_{max} – мінімальне та максимальне значення в наборі даних відповідно.

Лінгвістичний метод (нечітка логіка).

Лінгвістичний метод та динамічні межі. На відміну від методів, що шукають точні математичні залежності, лінгвістичний метод дозволяє формалізувати знання експерта у вигляді правил «ЯКЩО-ТО». В основі методу лежить математичний апарат нечітких множин (Fuzzy Logic) запропонований Л. Заде [16] в 1960-х роках (детальніше див. [17]). Процес включає фазифікацію, як показано на рис. 2 (переведення фізичних величин у лінгвістичні терми, наприклад, «шторм», «штиль»), застосування бази знань та дефазифікацію [3, 4].

Враховуючи сезонність генерації, в роботі запропоновано автокалібровану експертну систему, яка динамічно підлаштовує межі функцій належності (Membership Functions) під локальні максимуми історичних даних, що вирішує проблему «жорстких меж».

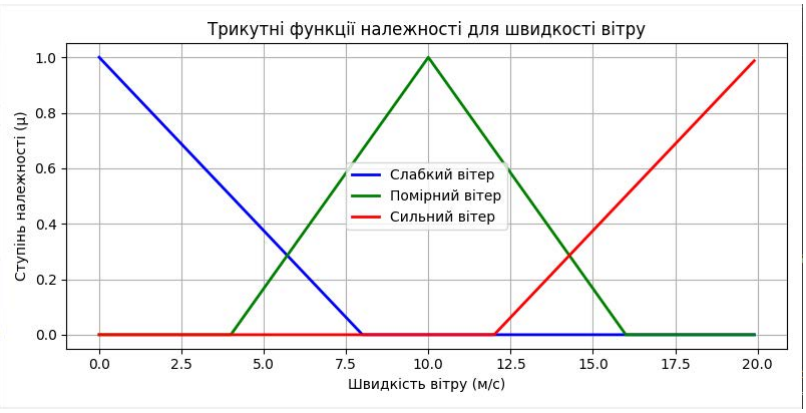


Рис. 2. Фазифікація величин

База лінгвістичних правил. Основою будь-якої системи нечіткого виведення є база знань, яка складається з набору продукційних правил формату «ЯКЩО (Умова), ТО (Наслідок)». У розробленій інформаційній системі реалізовано дві незалежні бази правил для різних типів енергії, що враховують їхні фізичні особливості.

Для сонячної генерації вхідною лінгвістичною змінною є рівень сонячної радіації. База правил (таблиця 1) сформована таким чином, щоб жорстко обмежувати генерацію в нічний час та пропорційно збільшувати її при появі сонця.

Таблиця 1

База правил для сонячної енергії

Номер правила	Передумова	Наслідок	Фізичне обгрунтування експерта
Правило 1	Якщо радіація «Ніч»	То генерація «Нуль»	Відсутність фотонів унеможливлює фотоелектричний ефект (генерація строго дорівнює 0).
Правило 2	Якщо радіація «Хмарно»	То генерація «Середня»	Розсіяне світло проходить крізь хмари, панелі працюють на часткову потужність.
Правило 3	Якщо радіація «Ясно»	То генерація «Максимальна»	Пряме сонячне проміння забезпечує вихід панелей на номінальну потужність.

Для вітрової генерації вхідною лінгвістичною змінною є швидкість вітру. База правил (таблиця 2) розроблена з урахуванням аеродинамічних характеристик вітряних турбін (адаптація до швидкості вітру на висоті 10 метрів).

Таблиця 2

База правил для вітряної енергії

Номер правила	Передумова	Наслідок	Фізичне обгрунтування експерта
Правило 1	Якщо вітер «Слабкий»	То генерація «Низька»	Ротор турбіни ледве долає поріг швидкості старту (cut-in speed), мінімальний обертовий момент.
Правило 2	Якщо вітер «Помірний»	То генерація «Середня»	Турбіна працює в робочому діапазоні, потужність стрімко зростає.
Правило 3	Якщо радіація «Ясно»	То генерація «Максимальна»	Швидкість потоку повітря достатня для виходу турбіни на максимальну розрахункову потужність.

Алгоритм нечіткого виведення та дефазифікація. Після застосування бази правил система отримує результат у вигляді нечіткої множини (набору геометричних фігур, що перетинаються). Для отримання конкретного числового значення прогнозу (у Мегаватах), яке можна передати в диспетчерську систему, алгоритм виконує процедуру дефазифікації.

У розробленій системі застосовано найточніший і найпоширеніший метод дефазифікації – метод центру маси (Centroid method). Математично він полягає у знаходженні координати центру ваги результуючої фігури, утвореної перетином активованих функцій належності:

$$Z = \frac{\int \mu(z) * z dz}{\int \mu(z) dz},$$

де Z – чітке прогнозоване значення генерації (МВт), z – змінна інтегрування на осі потужності, $\mu(z)$ – ступінь належності результуючої нечіткої множини.

Штучні нейронні мережі

Загальна ідея MLP. Багатошаровий персептрон (Multilayer Perceptron, MLP) – це клас нейронних мереж прямого поширення. Метод діє індуктивно: «чорна скринька» самостійно виявляє приховані нелінійні патерни шляхом мінімізації функції втрат під час навчання алгоритмом зворотного поширення помилки (Backpropagation). У роботі досліджуються архітектури різної глибини та застосовуються функції активації ReLU.

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

MLP складається з вхідного шару, одного або кількох прихованих шарів та вихідного шару (рис. 3). Кожен нейрон у прихованому шарі виконує зважене підсумовування вхідних сигналів x_i з додаванням зміщення (bias) *b*, після чого результат пропускається через нелінійну функцію активації *f* (2).

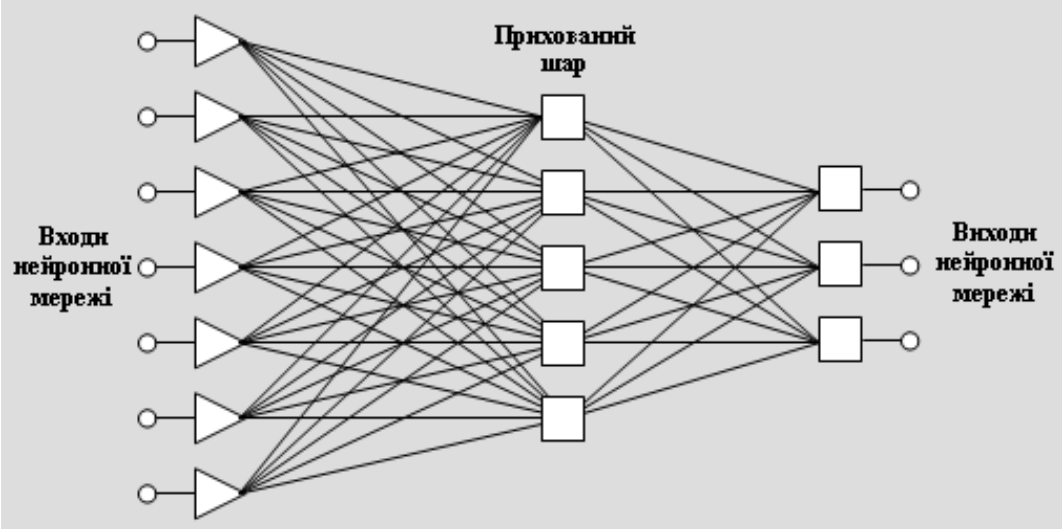


Рис. 3. Схема багатошарового персептрона

$$y = f\left(\sum_{i=1}^{n} \omega_i x_i + b\right), \tag{2}$$

де ω_i – синаптичні ваги нейрона.

Для забезпечення здатності мережі апроксимувати складні нелінійні функції (такі як кубічна залежність вітру), у прихованих шарах застосовується функція активації ReLU (Rectified Linear Unit). На відміну від класичної сигмоїди, ReLU вирішує проблему затухання градієнта (vanishing gradient) та пришвидшує збіжність мережі:

$$f(x) = max(0, x)$$

Процес навчання мережі полягає в мінімізації функції втрат (Loss function) L, якою в задачах регресії найчастіше виступає середньоквадратична похибка (MSE). Оновлення вагів $\Delta\omega$ здійснюється за допомогою алгоритму зворотного поширення помилки (Backpropagation) у поєднанні з оптимізатором Adam (Adaptive Moment Estimation), який динамічно адаптує швидкість навчання для кожного параметра.

Алгоритм зворотного поширення помилки (Backpropagation). Процес навчання багатошарового персептрона зводиться до задачі багатовимірної оптимізації. Метою є знаходження такого набору вагових коефіцієнтів *W*, який мінімізує функцію втрат *L*(*W*). Для регресійних задач використовується середньоквадратичне відхилення.

Алгоритм зворотного поширення помилки дозволяє ефективно обчислювати градієнт функції втрат по кожній вазі мережі $\frac{\partial L}{\partial \omega_{ij}}$ за допомогою ланцюгового правила диференціювання (chain rule):

$$\frac{\partial L}{\partial \omega_{ij}} = \frac{\partial L}{\partial y_j} \frac{\partial y_j}{\partial s_j} \frac{\partial s_j}{\partial \omega_{ij}},$$

де y_j – вихід нейрона *j*, s_j – зважена сума входів нейрона j, ω_{ij} – вага зв'язку між нейроном *i* та *j*.

Отримані градієнти використовуються для оновлення вагів на кожній ітерації (епосі) навчання.

Оптимізатор Adam (Adaptive Moment Estimation). У класичному градієнтному спуску швидкість навчання α є фіксованою, що часто призводить до застрягання в локальних мінімумах, особливо при моделюванні таких хаотичних процесів, як вітрова генерація. Тому в даній роботі застосовано оптимізатор Adam, який обчислює індивідуальні адаптивні швидкості навчання для кожного параметра [8].

Метод Adam поєднує ідеї накопичення імпульсу (Momentum) та середньоквадратичного градієнта (RMSProp). На кожному кроці *t* алгоритм оновлює експоненційні ковзні середні градієнта m_t як показано в формулі (3) та квадрата градієнта v_t – в формулі (4):

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t \tag{3}$$

$$\nu_t = \beta_2 \upsilon_{t-1} + (1-\beta_2)\, g_t^{\,2}\ , \tag{4}$$

де g_t – градієнт на поточному кроці, β_1, β_2 – гіперпараметри спадання (зазвичай 0.9 та 0.999).

Для компенсації зміщення до нуля на початкових етапах обчислюються скориговані моменти:

$$\widehat{m_t} = \frac{m_t}{1-\beta^t{}_2}, \widehat{\vartheta_t} = \frac{\nu_t}{1-\beta^t{}_2}$$

Фінальне оновлення ваг відбувається за правилом:

$$W_t = W_{t-1} - \frac{\alpha}{\sqrt{\widehat{\nu_t}} + \epsilon}\widehat{m_t}\ ,$$

де α – крок навчання (learning rate), ϵ – константа для уникнення ділення на нуль (зазвичай 10^{-8}).

Для проведення чисельного моделювання було розроблено програмний комплекс. Комплекс спроєктовано на базі трирівневої архітектури (Three-tier architecture), що забезпечує чітке розділення логіки збору даних, математичної обробки та візуалізації. Систему реалізовано мовою програмування Python із залученням сучасного стеку технологій Data Science. Структуру комплексу можна зображено на рис. 4.

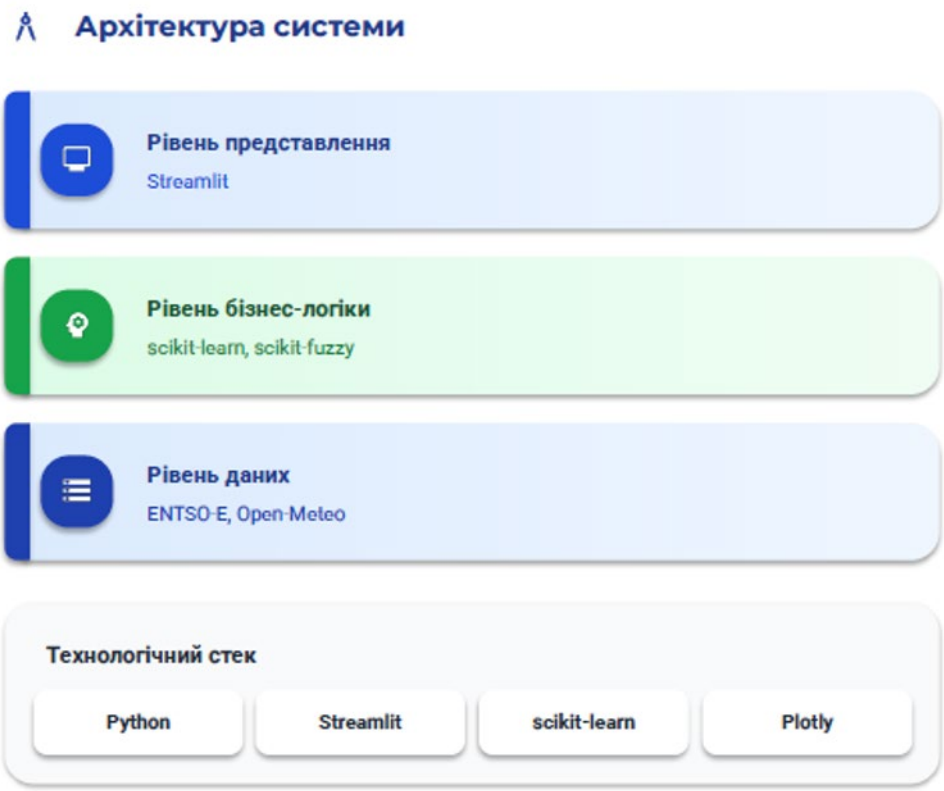


Рис. 4. Структура програмного комплексу

1. Рівень даних (Data Layer) відповідає за зовнішні комунікації з API європейської мережі ENTSO-E та метеорологічним сервісом Open-Meteo. На цьому рівні формується сирий масив даних.

2. Рівень бізнес-логіки (Business Logic Layer) – ядро системи, де відбувається фільтрація аномалій, нормалізація даних та безпосередня робота математичних моделей (штучної нейронної мережі, лінгвістичного методу та методу подібних траєкторій).

3. Рівень представлення (Presentation Layer) – клієнтська частина, реалізована за допомогою фреймворку Streamlit, яка забезпечує інтерактивний веб-інтерфейс, прийом параметрів від користувача та візуалізацію результатів прогнозування.

3. Результати досліджень. Критерії оцінки якості моделей. Для порівняння різнорідних систем прогнозування застосовано класичні метрики оцінки регресійних моделей: середню абсолютну похибку MAE та середньоквадратичну похибку RMSE, які вказано у формулах (5), (6):

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

$$MAE = \frac{1}{n}\sum_{i=1}^{n} |y_i - \hat{y}_i| \quad (5)$$

$$RMSE = \sqrt{\sum_{i=1}^{n} \frac{(\hat{y}_i - y_i)^2}{n}}, \quad (6)$$

де n – загальна кількість спостережень (прикладів), y_i – фактичне (реальне) значення для i-го спостереження, y_i – прогнозоване (передбачене моделлю) значення для i -го спостереження.

Аналіз результатів прогнозування методу подібних траєкторій. Метод подібних траєкторій є класичним евристичним підходом системного аналізу, який не потребує навчання і шукає в історичних даних ситуації, максимально наближені до поточних метеорологічних прогнозів.

При прогнозуванні сонячної генерації метод показав задовільні результати (MAE = 4038.05 МВт, RMSE = 7188.24 МВт). Як видно з графіка на рис. 5, алгоритм правильно визначає нульову генерацію вночі та загальний тренд денного піку. Проте крива прогнозу має значну «зубчастість» (високу дисперсію). Це пояснюється тим, що для кожної наступної години алгоритм може знаходити аналоги з абсолютно різних історичних днів, що призводить до різких стрибків між сусідніми точками прогнозу.

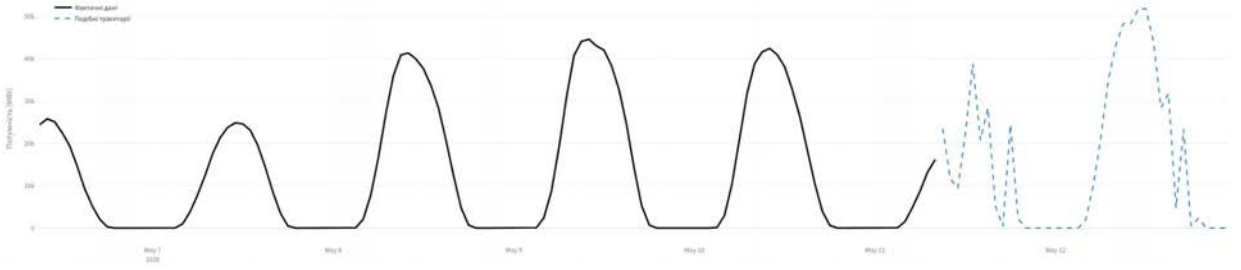


Рис. 5. Результат прогнозування сонячної генерації методом подібних траєкторій

У випадку вітрової енергетики похибка методу є більшою (MAE = 4621.72 МВт, RMSE = 5881.43 МВт). Незважаючи на введення часових лагів для врахування інерції турбін, алгоритму складно знайти в історії ідеальний збіг довгої тригодинної траєкторії зміни вітру (рис. 6). Це робить прогноз вітру цим методом досить хаотичним, хоча загальний напрямок падіння та зростання потужності зберігається.

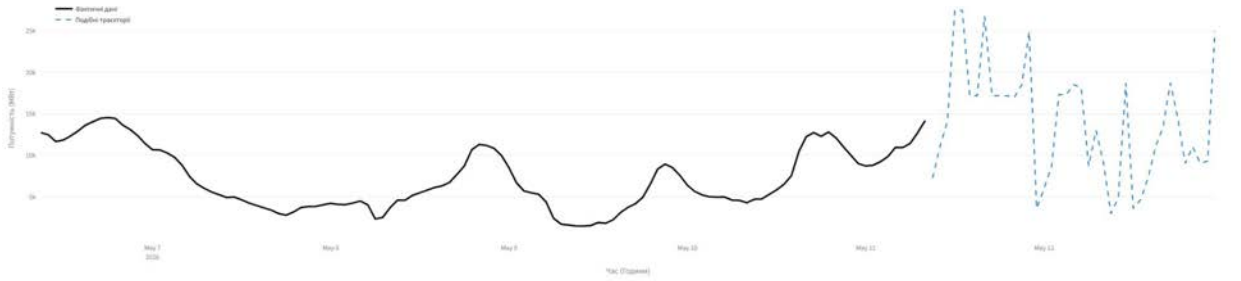


Рис. 6. Результат прогнозування вітрової генерації методом подібних траєкторій

Аналіз результатів прогнозування лінгвістичного методу. Лінгвістичний метод, побудований на базі правил експертної системи, демонструє принципово іншу поведінку. Оскільки метод працює з лінгвістичними термами (наприклад, «середня радіація», «сильний вітер»), результати прогнозу мають дискретний характер.

На графіку сонячної генерації на рис. 7 (MAE = 6386.03 МВт) чітко видно утворення характерних «плато» (сходинок) замість плавних дзвоноподібних кривих. Це відбувається через те, що широкий діапазон вхідних значень радіації активує одне й те саме правило нечіткої логіки, видаючи константний рівень генерації. Метод гарантовано не помиляється вночі, проте гірше апроксимує денні піки.

Водночас для вітрової генерації лінгвістичний метод із функцією автокалібрування показав кращу точність (рис. 8), ніж метод траєкторій (MAE = 3554.38 МВт, RMSE = 4206.45 МВт). Завдяки закладеним фізичним правилам (експертним знанням), система змогла утримати прогноз у реалістичних межах та адекватно відреагувати на нелінійні зміни швидкості вітру, хоча дискретна «східчаста» форма графіка все ще присутня.

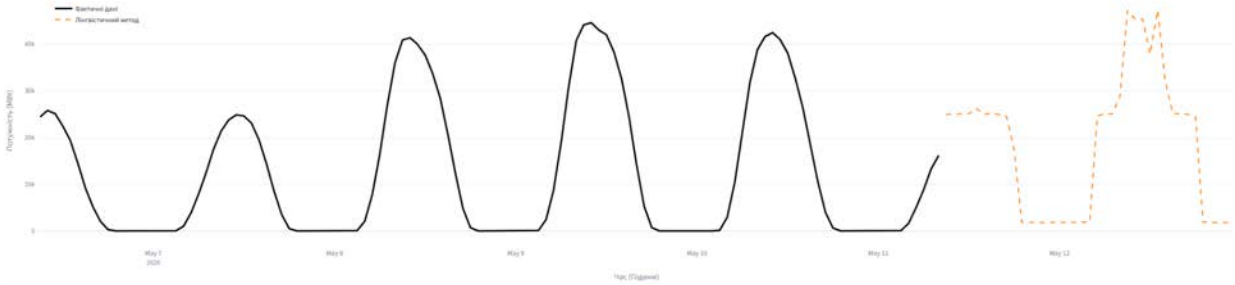


Рис. 7. Результат прогнозування сонячної генерації лінгвістичним методом

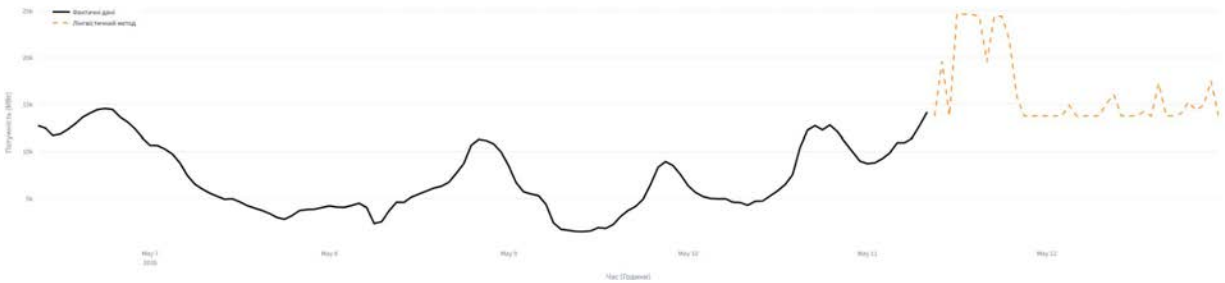


Рис. 8. Результат прогнозування вітрової генерації лінгвістичним методом

Аналіз результатів прогнозування штучної нейронної мережі (MLP). Індуктивний метод машинного навчання на базі багатошарового персептрона (MLP) продемонстрував найкращі результати серед усіх досліджуваних алгоритмів (рис. 9). Здатність нейромережі самостійно оптимізувати ваги та виявляти приховані нелінійні залежності дозволила мінімізувати похибку.

Для сонячної енергетики алгоритм MLP досяг найменшої похибки (MAE = 2073.84 МВт, RMSE = 3008.06 МВт). Нейромережа генерує плавну дзвоноподібну криву, яка майже ідеально відтворює природний добовий цикл сонця, адекватно реагуючи на невеликі коливання температури та хмарності.

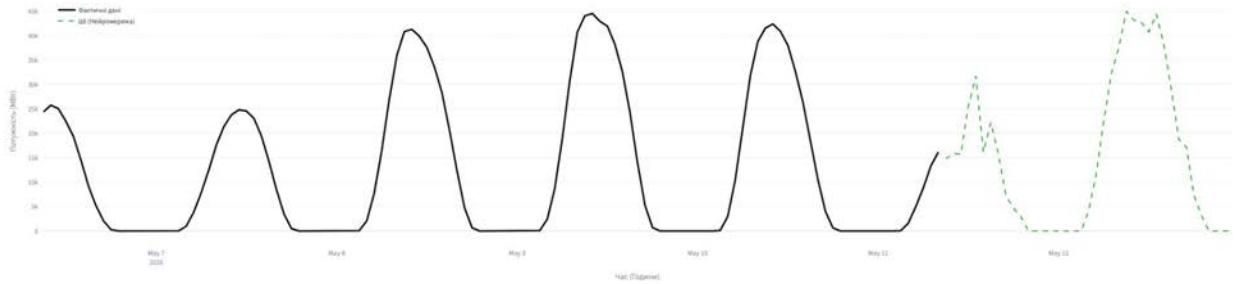


Рис. 9. Результат прогнозування сонячної генерації нейромережею MLP

У задачі прогнозування вітру ШІ також виявився абсолютним лідером (MAE = 2426.01 МВт, RMSE = 2879.97 МВт). Нейромережа змогла успішно розв'язати складну задачу екстраполяції: маючи на вході лише швидкість вітру на рівні 10 метрів від землі, модель навчилася з високою точністю відтворювати кубічну генерацію вітрових турбін на висоті понад 100 метрів. Крива прогнозу є плавною та точно повторює історичну амплітуду коливань мережі (рис. 10).

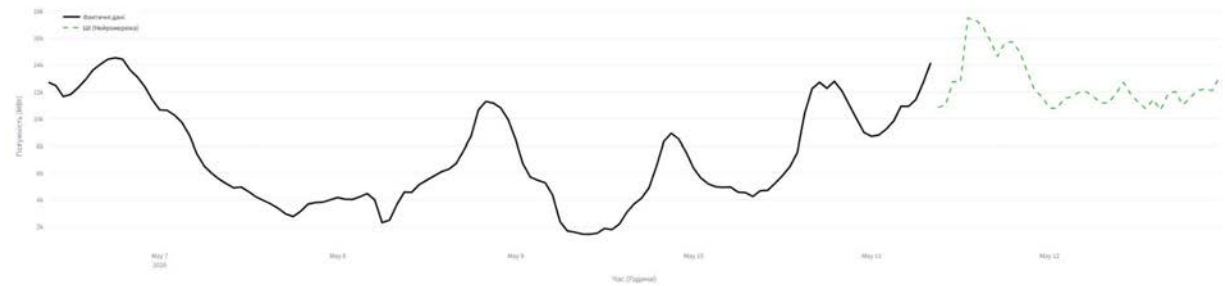


Рис. 10. Результат прогнозування вітрової генерації нейромережею MLP

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

Дослідження впливу гіперпараметрів нейромережі на точність прогнозу. Якість роботи індуктивних методів машинного навчання критично залежить від підбору гіперпараметрів алгоритму. Розроблена інформаційна система дозволяє особі, що приймає рішення (ОПР) в інтерактивному режимі змінювати архітектуру прихованих шарів та тривалість навчання (кількість епох) нейромережі MLP.

В ході дослідження було проаналізовано вплив архітектури нейронної мережі на метрику RMSE для задачі прогнозування вітрової генерації.

1. Проста (Shallow) архітектура (один прихований шар на 64 нейрони) – модель швидко збігається, проте має тенденцію до недонавчання (Underfitting) на складних ділянках із різкими поривами вітру.

2. Глибока (Deep) архітектура (два шари: 128 та 64 нейрони) – збільшення кількості параметрів дозволило мережі виявляти більш складні взаємозв'язки між часовими лагами ($t-1$, $t-2$) та поточною генерацією. Це знизило загальну похибку моделі.

Також було досліджено гіперпараметр max_iter (кількість епох). Збільшення епох з 500 до 2000 дало значний приріст точності, дозволивши алгоритму Adam вийти з локальних мінімумів функції втрат. Однак подальше збільшення (понад 4000 епох) не дало суттєвого покращення метрик на валідаційній вибірці, що свідчить про початок процесу перенавчання (Overfitting). Таким чином, конфігурація (128, 64) нейронів при 2000 епохах була визначена як оптимальна за критерієм «точність/швидкодія».

Підсумкове порівняння моделей. За результатами проведених експериментів (таблиця 3) можна стверджувати, що вибір методу прогнозування суттєво залежить від природи вхідних даних. Дедуктивні методи системного аналізу (траєкторії, нечітка логіка) не потребують витрат часу на навчання, добре працюють з експертними знаннями та є абсолютно прозорими в прийнятті рішень. Однак їхня точність знижується при роботі з високостохастичними нелінійними даними. Індуктивний підхід (MLP) довів свою перевагу в точності (мінімізація MAE та RMSE в 1.5–2 рази), згладжуванні шумів та здатності автоматично адаптуватися до складних метеорологічних патернів.

Таблиця 3

Метрики методів

Метод прогнозування	Тип енергії	MAE	RMSE
Метод подібних траєкторій	Сонячна	4038.05	7188.24
Лінгвістичний метод	Сонячна	6386.03	9227.36
Штучна нейронна мережа	Сонячна	2073.84	3008.06
Метод подібних траєкторій	Вітрова	4621.72	5881.43
Лінгвістичний метод	Вітрова	3554.38	4206.45
Штучна нейронна мережа	Вітрова	2426.01	2879.97

4. Висновки. У межах виконання наукової роботи було розроблено інформаційну систему підтримки прийняття рішень для оперативного прогнозування генерації відновлюваних джерел енергії. Проведено комплексний порівняльний аналіз дедуктивних підходів (метод подібних траєкторій, лінгвістичний метод) та індуктивного підходу (штучний інтелект на базі багатошарового перцептрона). В результаті досліджень отримано наступні висновки.

1. Запропоновані системні вдосконалення (введення часових лагів для імітації інерції роторів вітряків та автокалібрування меж у нечіткій логіці) дозволили значно підвищити стійкість дедуктивних моделей до аномалій у даних.

2. Проблема витоку даних (Data Leakage) та перенавчання (Overfitting) була успішно вирішена за рахунок жорсткого розділення часового ряду на історичний масив та сліпу тестову вибірку (Hold-out test).

3. Аналіз метрик MAE та RMSE довів, що для високоциклічних процесів (сонячна енергетика) експертні методи системного аналізу демонструють достатню ефективність і високу прозорість логіки прийняття рішень.

4. Для стохастичних та нелінійних процесів (вітрова енергетика) методи машинного навчання (MLP) мають абсолютну перевагу в точності, оскільки здатні самостійно знаходити неочевидні закономірності у великих масивах даних.

5. Проведений функціонально-вартісний аналіз повністю підтвердив економічну доцільність розробленого програмного продукту. Розрахований коефіцієнт техніко-економічного рівня довів оптимальність обраного стеку технологій (Python, Streamlit) за критерієм «якість-витрати».

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Довгаленко Гліб Андрійович: підготовка та аналіз вхідних даних, навчання моделей, створення та тестування програмної реалізації, внесення змін та правок у текст статті

Селін Юрій Миколайович: оцінка огляду літератури, пропозиції з приводу підходів до архітектури та її можли-вих конфігурацій, оцінка отриманих результатів тестування, написання тексту статті.

Куєвда Юлія Валеріївна: огляд існуючих рішень та підходів, створення архітектури мо-делі та її реалізація, навчання та тестування реалізації,. внесення змін та правок у текст статті

References:

1. Кузнєцов, М. П. (2022). Особливості комбінованих енергосистем з відновлюваними джерелами енергії : монографія. Київ : ІВЕ НАН України, 152 с.
2. Бідюк, П. І., Романенко, В. Д., Тимощук, О. Л. (2010). Аналіз часових рядів: навч. посіб. Київ : НТУУ «КПІ», 317 с.
3. Приймак, М. В. (2021). Застосування систем нечіткої логіки для моделювання та керування об'єктами відновлюваної енергетики. *Відновлювана енергетика.* № 3. С. 22–31.
4. Ротштейн, О. П. (1999). Інтелектуальні технології ідентифікації: нечітка логіка, генетичні алгоритми, нейронні мережі. Вінниця: УНІВЕРСУМ, 320 с.
5. Hastie, T., Tibshirani, R., Friedman, J. (2009). The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Springer, 745 p. Retrieved from: https://hastie.su.domains/ElemStatLearn/
6. Géron, A. (2019). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly Media, 856 p.
7. Мнишенко, В. С. (2019). Теорія випадкових процесів та часових рядів : навч. посібник. Київ : КНЕУ. 276 с.
8. Kingma, D. P., Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980. P. 1–15.
9. Transparency Platform. ENTSO-E (European Network of Transmission System Operators for Electricity). Retrieved from: https://transparency.entsoe.eu/
10. Open-Meteo: Open-Source Weather API. Retrieved from: https://open-meteo.com/
11. Pedregosa, F. et al. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*, Vol. 12. P. 2825–2830. Retrieved from: https://www.jmlr.org/papers/volume12/pedregosa11a/pedregosa11a.pdf
12. Scikit-Fuzzy: Fuzzy Logic in Python. SciPy.org. Retrieved from: https://pythonhosted.org/scikit-fuzzy/
13. Streamlit Documentation: A faster way to build and share data apps. Retrieved from: https://docs.streamlit.io/
14. Plotly: Interactive Graphing Library for Python. Retrieved from: https://plotly.com/python/
15. McKinney, W. (2010). Data Structures for Statistical Computing in Python. Proceedings of the 9th Python in Science Conference. Austin, Texas, USA, June 28 to July 3. P. 51–56. Retrieved from: https://proceedings.scipy.org/articles/Majora-92bf1922-00a
16. Zadeh, L. A. (1965). Fuzzy sets. Information and Control. Vol. 8 (3). P. 338–353.
17. Зайченко, Ю.П. (2006). Дослідження операцій. 7-ме вид., Київ, Видавництво «Слово», 816 с.

Відомості про авторів

Англ.	Укр.
Hlib Dovgalenko Bachelor at the Department of Mathematical Methods of System Analysis, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" hlib.dovhalenko@gmail.com ORCID: 0009-0009-2260-4204	Довгаленко Гліб Андрійович бакалавр кафедри математичних методів системного аналізу, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» hlib.dovhalenko@gmail.com ORCID: 0009-0009-2260-4204
Yurii Selin Ph.D in Technical Sciences, Senior Lecturer at the Department of Mathematical Methods of System Analysis, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" selinyurij1963@gmail.com ORCID: 0000-0002-7562-8586	Селін Юрій Миколайович кандидат технічних наук, старший викладач кафедри математичних методів системного аналізу, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» selinyurij1963@gmail.com ORCID: 0000-0002-7562-8586
Yuliia Kuievda Ph.D in Technical Sciences, Associate Professor, Associate Professor at the Department of Mathematical Methods of System Analysis, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" kuievda.iuliia@lll.kpi.ua ORCID: 0009-0001-6630-1215	Куєвда Юлія Валеріївна кандидат технічних наук, доцент, доцент кафедри математичних методів системного аналізу, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» kuievda.iuliia@lll.kpi.ua ORCID: 0009-0009-2260-4204

Дата надходження статті: 08.04.2026
Дата надходження виправленої версії статті: 12.06.2026
Дата прийняття статті: 26.06.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.3
УДК 004.8:004.92
JEL Classification: C45, O33

АВТОМАТИЗАЦІЯ ГЕНЕРАЦІЇ ЦИФРОВИХ ТЕКСТУР ІЗ ВИКОРИСТАННЯМ ГЕНЕРАТИВНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

А. О. Коваль, Ю. В. Каменецька, А. К. Кобринець

AUTOMATION OF DIGITAL TEXTURE GENERATION USING GENERATIVE ARTIFICIAL INTELLIGENCE MODELS

Alina Koval, Yuliia Kamenetska, Anton Kobrynets

Анотація

Метою дослідження є обґрунтування підходу до автоматизації генерації цифрових текстур із використанням генеративних моделей штучного інтелекту та визначення послідовності операцій, необхідних для отримання придатних до використання матеріалів у системах тривимірного моделювання. У роботі систематизовано сучасні підходи до синтезу текстур на основі дифузійних моделей, моделей, орієнтованих на генерацію матеріалів, а також методів генерації текстур безпосередньо в просторі тривимірної поверхні. Проведено критичний аналіз досліджень Point-UV Diffusion, MatFuse, DiffMat, DreamMat, Single Mesh Diffusion Models та TEXGen, що дало змогу виокремити переваги й обмеження різних підходів. Запропоновано алгоритм автоматизованого формування текстури, який включає визначення вимог до матеріалу, формування текстового або візуального запиту, генерацію декількох кандидатів, оцінювання відповідності, підготовку карт матеріалу, постобробку та експорт у середовище тривимірного моделювання. Окремо розглянуто практичну апробацію на двох типах матеріалів: старій цегляній поверхні та матовому металевому матеріалі. Для кожного прикладу визначено вихідні вимоги, приклад запиту, критерії оцінювання та послідовність підготовки матеріалу до використання у тривимірній сцені. Обґрунтовано, що генеративний штучний інтелект доцільно розглядати не як повну заміну фахівця, а як інструмент автоматизації повторюваних операцій і швидкого формування варіантів. Практична цінність роботи полягає у формуванні відтворюваного робочого процесу, який може бути використаний у розробленні комп'ютерних ігор, цифровому дизайні, архітектурній візуалізації та підготовці фахівців з інформаційних технологій.

Ключові слова: *генеративний штучний інтелект, генерація текстур, дифузійні моделі, цифрові матеріали, тривимірне моделювання, комп'ютерна графіка, PBR, автоматизація, машинне навчання.*

Abstract

The study aims to substantiate an approach to automating digital texture generation with generative artificial intelligence models and to define a reproducible sequence of operations for producing materials suitable for three-dimensional modeling systems. The paper systematizes recent approaches based on diffusion models, material-oriented generative methods, and methods that synthesize textures directly in the surface or UV space of three-dimensional objects. A critical review of Point-UV Diffusion, MatFuse, DiffMat, DreamMat, Single Mesh Diffusion Models, and TEXGen is provided to identify their main advantages and limitations. An automated texture generation workflow is proposed. It includes defining material requirements, constructing a text or visual prompt, generating candidate results, evaluating their compliance with the requirements, preparing material maps, post-processing, and exporting the result to a three-dimensional environment. Two practical cases are described: an aged brick surface and a matte metal material. For each case, the input requirements, an example prompt, evaluation criteria, and the sequence of preparing the material for a 3D scene are specified. The study argues that generative artificial intelligence should be treated not as a complete replacement for a specialist, but as a tool for automating repetitive operations and rapidly producing design alternatives. The practical value of the study lies in a reproducible workflow that can be applied to game development, digital design, architectural visualization, and the training of information technology specialists.

Key words: *generative artificial intelligence, texture generation, diffusion models, digital materials, three-dimensional modeling, computer graphics, physically based rendering, automation, machine learning.*

1. Вступ. Сучасні інформаційні технології характеризуються швидким переходом від алгоритмічної автоматизації до систем, здатних синтезувати новий цифровий контент. Одним із найбільш помітних напрямів є генеративний штучний інтелект, який використовується для створення зображень, моделей, матеріалів, текстур та інших графічних ресурсів. Для комп'ютерної графіки ця тенденція має особливе значення, оскільки підготовка якісного візуального контенту традиційно потребує значних часових витрат і участі фахівців на багатьох етапах.

Цифрова текстура є одним із базових компонентів тривимірного матеріалу. Вона може містити інформацію про колір поверхні, нормалі, шорсткість, металевість, висоту та інші характеристики, які використовуються під час фізично коректного відтворення взаємодії світла з поверхнею.

© Коваль А. О., Каменецька Ю. В., Кобринець А. К., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

У виробничому процесі текстура повинна бути не лише візуально привабливою, а й узгодженою з геометрією об'єкта, UV-розгорткою, вимогами графічного рушія та обмеженнями продуктивності.

Традиційний процес передбачає пошук або створення референсів, ручне редагування, формування безшовного патерну, підготовку набору карт матеріалу, перевірку швів і повторів, оптимізацію роздільної здатності та експорт. Кожен із цих етапів може бути автоматизований частково або повністю, якщо генеративна модель правильно інтегрована в робочий процес.

Метою роботи є розроблення та обґрунтування відтворюваного алгоритму автоматизованої генерації цифрових текстур із використанням генеративних моделей штучного інтелекту, а також демонстрація його застосування на двох практичних сценаріях. Для досягнення мети поставлено такі завдання: проаналізувати сучасні дослідження; визначити вимоги до автоматизованої генерації; сформувати алгоритм; описати критерії оцінювання; провести практичну апробацію на типових матеріалах; визначити переваги та обмеження запропонованого підходу.

Наукова новизна роботи полягає не у створенні нової генеративної моделі, а в систематизації та формалізації процесу її використання для отримання цифрових текстур. На відміну від загального огляду генеративного штучного інтелекту, увагу зосереджено на послідовності операцій від формулювання вимог до підготовки результату для 3D-середовища та на практичній перевірці запропонованого workflow.

Огляд сучасних досліджень. Дослідження Goodfellow та співавторів започаткувало напрям генеративно-змагальних мереж, у якому генератор і дискримінатор навчаються у взаємодії. GAN стали важливою основою для генерації візуального контенту, але нестабільність навчання та проблема mode collapse обмежили їх універсальність для високодеталізованої генерації.

Дифузійні моделі запропонували інший механізм синтезу: модель навчається відновлювати дані після поступового додавання шуму. Подальші роботи показали, що латентні дифузійні моделі здатні забезпечувати високу якість зображень при перенесенні процесу дифузії у компактний латентний простір. Цей підхід став основою значної кількості сучасних систем text-to-image і text-to-material.

Yu та співавтори запропонували Point-UV Diffusion для генерації текстур на 3D-сітках. Метод поєднує дифузію в просторі точок і UV-просторі, що дозволяє отримувати геометрично узгоджені текстури. Важливим результатом є демонстрація того, що генерація текстури повинна враховувати не лише локальну візуальну якість, а й просторову узгодженість поверхні.

Vecchio та співавтори у MatFuse розглянули контрольовану генерацію матеріалів на основі тексту, зображень, ескізів і кольорових палітр. Автори також досліджували редагування окремих карт матеріалу та оцінювали якість результатів кількісними й користувацькими методами. Це показує перспективність багатоканального керування генерацією.

Zhang та співавтори у DreamMat зосередилися на генерації PBR-матеріалів з урахуванням геометрії та освітлення. Такий підхід важливий для практичного використання, оскільки текстура, що виглядає переконливо на плоскому зображенні, не обов'язково буде коректно поводитися на тривимірному об'єкті.

DiffMat розглядає генерацію матеріалів із зображень у різних умовах освітлення. Автори поєднують CLIP-енкодер і дифузійну архітектуру та формують матеріали у форматі, сумісному зі стандартним фізично коректним рендерингом. Це підтверджує тенденцію переходу від генерації окремого зображення до генерації структурованого матеріалу.

Mitchel, Esteves та Makadia запропонували моделі дифузії, які працюють безпосередньо з поверхнею 3D-сітки через спеціальне латентне представлення. Перевагою є можливість генерувати варіації текстури з урахуванням структури конкретного об'єкта та підтримувати задачі редагування.

У TEXGen запропоновано генеративну дифузійну модель, що навчається безпосередньо в просторі текстурної карти. Автори підкреслюють проблему порушення глобальної 3D-узгодженості при наївному використанні 2D-генераторів і пропонують архітектуру, орієнтовану на високороздільні текстури сіток.

Огляд сучасних підходів до text-guided 3D editing також показує, що генерація текстур поступово переходить від простого проєктування зображення на модель до ітеративного процесу, у якому система враховує геометрію, попередні результати та різні умови огляду. Таким чином, сучасний стан досліджень свідчить про рух до керованих, геометрично узгоджених і PBR-сумісних матеріалів.

Критичний аналіз джерел дає підстави стверджувати, що в літературі достатньо добре досліджені окремі моделі генерації, але практичний workflow для фахівця, який не створює нову нейромережу, а використовує готові генеративні засоби для отримання текстур, часто описується фрагментарно. Недостатньо уваги приділяється послідовності постановки задачі, відбору результату, перевірці безшовності, підготовці PBR-карт і перенесенню матеріалу в конкретне 3D-середовище. Саме цю прикладну прогалину розглянуто в цій роботі.

2. Матеріали та методи. Матеріалами дослідження є сучасні генеративні моделі та інструменти для створення цифрових матеріалів, а також типові задачі підготовки текстур для тривимірних

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

об'єктів. У роботі не ставиться завдання навчити власну нейромережу; досліджується організація процесу використання готової генеративної моделі.

Методологічну основу становлять аналіз наукових джерел, порівняння підходів, моделювання робочого процесу, експериментальна апробація на двох типах матеріалів і якісне оцінювання результатів. Для практичної перевірки сформовано два сценарії: генерація старої цегляної поверхні та генерація матового металу. Обидва сценарії є типовими для комп'ютерної графіки та дають змогу перевірити різні вимоги до структури матеріалу.

Вхідними параметрами є призначення матеріалу, тип поверхні, бажаний стиль, рівень зношення, колірна характеристика, вимога безшовності, орієнтовна роздільна здатність і цільове 3D-середовище. Генеративній системі передається текстовий або візуальний запит. Після отримання кількох кандидатів виконується відбір за критеріями візуальної відповідності, відсутності артефактів, повторюваності, узгодженості з геометрією та придатності до подальшої підготовки PBR-матеріалу.

Для оцінювання запропоновано п'ять критеріїв: C1 – відповідність заданому опису; C2 – безшовність і відсутність помітних стиків; C3 – структурна деталізація; C4 – відсутність небажаних артефактів; C5 – придатність до використання у 3D-сцені. Кожен критерій може оцінюватися за п'ятибальною шкалою. Підсумкова оцінка кандидата визначається як середнє арифметичне балів за п'ятьма критеріями. Така схема не є універсальним стандартом, але забезпечує відтворюваний спосіб первинного порівняння результатів.

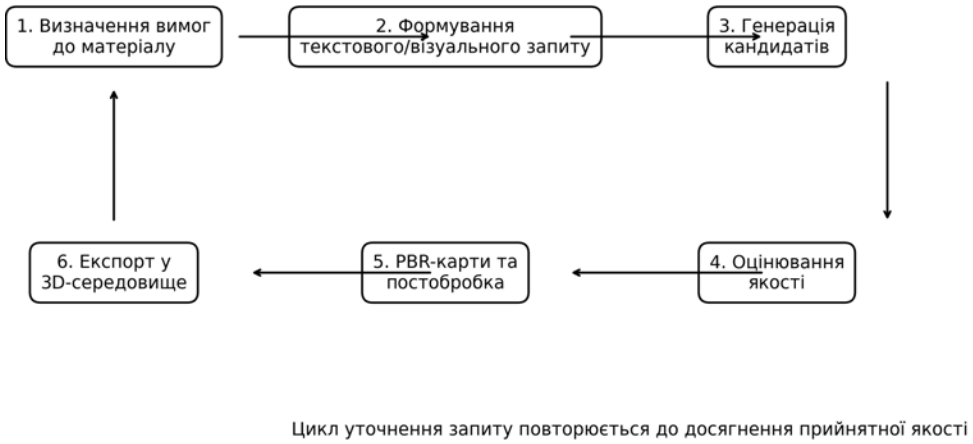


Рис. 1. Алгоритм автоматизованої генерації та підготовки цифрової текстури

Псевдокод алгоритму

Algorithm GenerateTexture
Input: material_requirements, prompt, target_environment
1. Define material requirements.
2. Construct a detailed text or image-guided prompt.
3. Generate N candidate textures.
4. For each candidate:
   evaluate C1–C5;
   check tiling/seams and visual artifacts;
   select the best candidate.
5. Generate or derive required material maps.
6. Normalize resolution, color space and map formats.
7. Test material on the target 3D mesh.
8. If quality is insufficient, refine prompt or post-process maps and return to step 3.
9. Export the final material to the target environment.
Output: validated digital material.

3. Результати та обговорення. Запропонований workflow було апробовано на двох практичних прикладах. Важливо, що практична апробація розглядається не як порівняльний бенчмарк конкретних моделей, а як перевірка відтворюваності процесу формування матеріалу: від вимоги до поверхні до підготовки результату для 3D-сцени.

У першому прикладі обрано матеріал старої червоної цегли. Він є показовим, оскільки має повторювану структуру, нерегулярні дефекти, шви між елементами та варіації кольору. Для нього критичними є безшовність, природність повторення та відсутність штучно повторюваних елементів.

Практичний приклад 1. Стара цегляна поверхня. Вихідна вимога: отримати безшовну текстуру старої червоної цегли для використання на стіні в 3D-сцені. Поверхня має містити варіації відтінків, нерівномірні шви, сліди зношення та не повинна мати очевидного повторюваного патерну.

Приклад текстового запиту: “Old weathered red brick wall, seamless tileable PBR material, irregular bricks, aged mortar, subtle dirt and surface variation, realistic physically based material, no objects, no text”.

Після генерації декількох кандидатів виконується відбір. На першому етапі відсіюються результати, у яких присутні написи, сторонні об’єкти або великі повторювані елементи. На другому етапі перевіряється безшовність. На третьому – відповідність кольору та масштабу цегли цільовій сцені. Найкращий кандидат використовується як основа для подальшого формування карт Albedo, Normal, Roughness та Height.

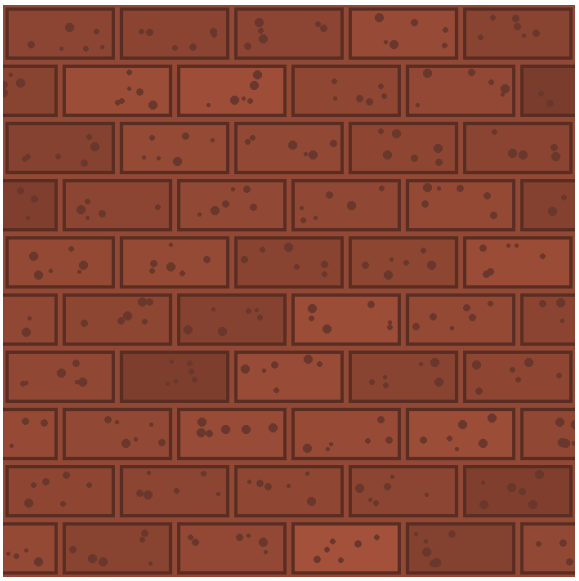




Рис. 2. Демонстраційна апробація workflow для матеріалу «стара цегла»

Практичний приклад 2. Матовий метал. Другим сценарієм обрано матовий метал. На відміну від цегли, для такого матеріалу критичними є однорідність поверхні, напрям мікрорельєфу, рівень металевості та шорсткість. Відповідно, генерація лише кольорового зображення недостатня: результат необхідно перетворити на узгоджений набір карт матеріалу.

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

Приклад текстового запиту: “Brushed matte aluminum metal, seamless tileable PBR material, fine horizontal micro-scratches, subtle roughness variation, neutral gray, realistic surface, no objects, no text”.

Для кандидата, що відповідає вимогам, формується базова карта кольору, після чого визначаються параметри металевості та шорсткості. Карта Normal використовується для передачі мікрорельєфу без збільшення геометричної складності моделі. Після імпорту матеріалу в 3D-середовище перевіряється поведінка поверхні під різними напрямами освітлення.

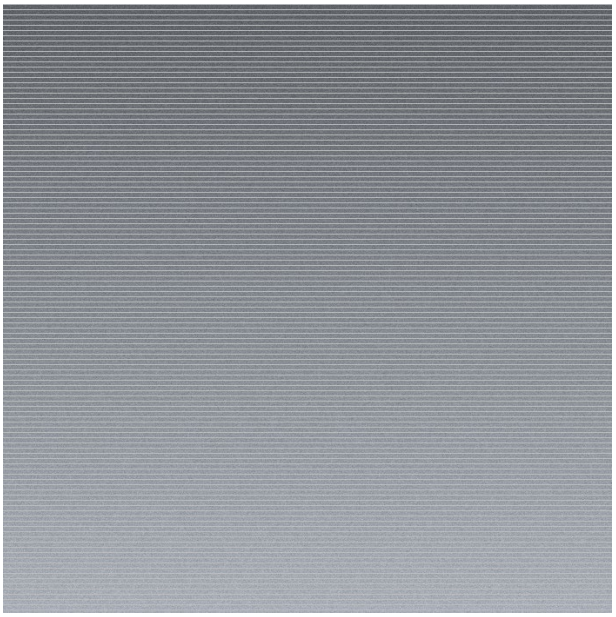




Рис. 3. Демонстраційна апробація workflow для матеріалу «матовий метал»

Таблиця 1

Порівняння етапів традиційного та автоматизованого workflow

Етап	Традиційний підхід	Запропонований workflow
Постановка задачі	Референси та ручний опис	Структурований prompt + вимоги
Пошук варіантів	Ручний пошук/створення	Автоматична генерація кількох кандидатів
Вибір	Експертний відбір	C1–C5 + експертний відбір
PBR-підготовка	Ручне створення карт	Генерація/похідні карти + постобробка
Перевірка в 3D	Імпорт і ручна корекція	Ітеративна перевірка та уточнення prompt
Експорт	Ручна підготовка форматів	Стандартизований етап експорту

Обговорення результатів. Практична апробація показала, що ключовим фактором якості є не лише сама генеративна модель, а й формалізація вимог до результату. Невизначений запит може привести до візуально привабливого зображення, яке непридатне як текстура: на ньому можуть бути перспективні спотворення, освітлення, тіні від уявних об'єктів, написи або елементи, що не повторюються коректно.

Порівняння з сучасними науковими підходами показує, що запропонований workflow відповідає загальній тенденції розвитку генеративних технологій: від генерації 2D-зображення до керованого створення матеріалу з урахуванням геометрії, освітлення та структури 3D-об'єкта. Point-UV Diffusion і TEXGen демонструють важливість роботи в UV або безпосередньо в texture space, тоді як MatFuse і DreamMat акцентують керованість і PBR-сумісність.

Водночас практичне використання готових генеративних сервісів має обмеження. По-перше, результат залежить від формулювання запиту та конкретної моделі. По-друге, автоматично отримане зображення не гарантує фізичної коректності матеріалу. По-третє, для ігрових рушіїв важливі роздільна здатність, формат карт, пам'ять GPU, кількість матеріальних варіантів і продуктивність рендерингу. По-четверте, необхідно враховувати ліцензійні та авторсько-правові умови використання генеративного сервісу.

Отже, автоматизацію доцільно трактувати як напівавтоматичний процес human-in-the-loop. Генеративна модель виконує синтез і пропонує альтернативи, тоді як фахівець задає вимоги, оцінює результат, контролює відповідність матеріалу сцені та приймає остаточне рішення.

Для кількісної оцінки ефективності в подальших експериментах доцільно фіксувати щонайменше чотири показники: час до першого прийнятного результату, кількість ітерацій генерації, середню оцінку C1–C5 та час підготовки матеріалу до імпорту в 3D-середовище. Це дозволить перейти від якісного опису переваг до статистично обґрунтованого порівняння.

Переваги та обмеження. До основних переваг запропонованого підходу належать швидке формування декількох варіантів, зменшення обсягу рутинного ручного редагування, можливість використовувати текстові та візуальні референси, ітеративне уточнення результату та інтеграція з сучасним процесом 3D-розроблення.

Основними обмеженнями є залежність від конкретної генеративної моделі, можливі артефакти, недостатня геометрична узгодженість, складність отримання стабільно безшовних матеріалів, необхідність постобробки та питання прав інтелектуальної власності. Тому повна автоматизація без експертного контролю для професійного використання є недоцільною.

4. Висновки. У роботі проаналізовано сучасні підходи до генерації цифрових текстур із використанням генеративного штучного інтелекту та визначено їхню придатність для автоматизації підготовки матеріалів у 3D-середовищах. Критичний аналіз сучасних досліджень показав перехід від загальної генерації зображень до методів, що враховують UV-простір, геометрію, освітлення та структуру PBR-матеріалу.

Запропоновано алгоритм, який включає формування вимог, побудову запиту, генерацію кандидатів, оцінювання за п'ятьма критеріями, підготовку матеріальних карт, перевірку на 3D-моделі та ітеративне уточнення. Така структура робить процес відтворюваним і дозволяє поєднати можливості генеративної моделі з професійним контролем фахівця.

Практичні приклади старої цегляної поверхні та матового металу показали, що різні типи матеріалів потребують різних критеріїв контролю. Для цегли критичними є безшовність, природність повторення та варіативність елементів, для металу – мікрорельєф, шорсткість, металевість і поведінка під освітленням.

Перспективним напрямом є проведення кількісного експерименту з фіксацією часу, кількості ітерацій, якості результатів і ресурсних витрат для кількох генеративних моделей. Таке дослідження дозволить визначити оптимальні сценарії використання генеративного штучного інтелекту в розробленні цифрових матеріалів.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Використання штучного інтелекту. Під час підготовки рукопису автори використовували OpenAI ChatGPT (модель GPT-5.6 Luna) для допомоги у структурному редагуванні тексту, мовному доопрацюванні та формуванні окремих формулювань. Наукові твердження, бібліографічні відомості та остаточний зміст рукопису перевірялися авторами. Інструмент штучного інтелекту не використовувався як джерело наукових доказів, а його результати не визначали самостійно висновки дослідження.

Внесок авторів. Коваль А.О.: концептуалізація дослідження, постановка завдань, методологія, аналіз літератури, формування алгоритму, підготовка рукопису, редагування та візуалізація. Каменецька Ю.В.: участь у формуванні практичних сценаріїв, аналізі вимог до цифрових матеріалів, обговоренні результатів та редагуванні рукопису.

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

References:

1. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y. (2014). Generative Adversarial Nets. *Advances in Neural Information Processing Systems*. Vol. 27.
2. Ho, J., Jain, A., Abbeel, P. (2020). Denoising Diffusion Probabilistic Models. *Advances in Neural Information Processing Systems*. Vol. 33.
3. Rombach, R., Blattmann, A., Lorenz, D., Esser, P., Ommer, B. (2022). High-Resolution Image Synthesis with Latent Diffusion Models. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. P. 10684–10695. DOI: 10.1109/CVPR52688.2022.01042.
4. Yu, X., Dai, P., Li, W., Ma, L., Liu, Z., Qi, X. (2023). Texture Generation on 3D Meshes with Point-UV Diffusion. Proceedings of the IEEE/CVF International Conference on Computer Vision. P. 4206–4216.
5. Vecchio, G., Sortino, R., Palazzo, S., Spampinato, C. (2024). MatFuse: Controllable Material Generation with Diffusion Models. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. P. 4429–4438. DOI: 10.1109/CVPR52733.2024.00424.
6. Zhang, Y., Liu, Y., Xie, Z., Yang, L., Liu, Z., Yang, M., Zhang, R., Kou, Q., Lin, C., Wang, W., Jin, X. (2024). DreamMat: High-quality PBR Material Generation with Geometry- and Light-aware Diffusion Models. *ACM Transactions on Graphics*. Vol. 43, No. 4. DOI: 10.1145/3658170.
7. Zhang, C., et al. (2024). DiffMat: Latent diffusion models for image-guided material generation. *Visual Informatics*. Vol. 8, No. 1. P. 6–14. DOI: 10.1016/j.visinf.2023.12.001.
8. Mitchel, T.W., Esteves, C., Makadia, A. (2024). Single Mesh Diffusion Models with Field Latents for Texture Generation. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. P. 7953–7963. DOI: 10.1109/CVPR52733.2024.00760.
9. Yu, X., Yuan, Z., Guo, Y.-C., Liu, Y.-T., Liu, J., Li Y., Cao, Y.-P., Liang, D., Qi, X. (2024). TEXGen: A Generative Diffusion Model for Mesh Textures. *ACM Transactions on Graphics.* Vol. 43, No. 6, Article 213. DOI: 10.1145/3687909.
10. Huang, X., Wang, T., Liu, Z., Wang, Q. (2024). Material Anything: Generating Materials for Any 3D Object via Diffusion. arXiv preprint arXiv:2411.15138.
11. Xie, Z., Zhang, Y., Tang, X., Wu, Y., Chen, D., Li, G., Jin, X. (2024). StyleTex: Style Image-Guided Texture Generation for 3D Models. *ACM Transactions on Graphics.*
12. Richardson, E., et al. (2023). TEXTure: Text-Guided Texturing of 3D Shapes. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.
13. Chen, A., et al. (2023). Text2Tex: Text-driven Texture Synthesis of 3D Shapes. Proceedings of the IEEE/CVF International Conference on Computer Vision.
14. Adobe. Substance 3D Sampler: Text-to-texture and Image-to-texture generative workflows. Adobe Experience League. 2024–2026.
15. Blender Foundation. Blender Manual: Materials and Texture Painting. 2025.
16. Epic Games. Unreal Engine Documentation: Materials and Textures. 2025.
17. Unity Technologies. Unity Manual: Materials, Textures and Shaders. 2025.

Примітка щодо практичної апробації

Для ілюстрації практичної апробації використано демонстраційні зображення, створені спеціально для цього рукопису. Вони візуалізують послідовність формування PBR-матеріалу та його застосування на 3D-об'єкті й не подаються як результати кількісного бенчмарку конкретної генеративної моделі.

Відомості про авторів

Англ.	Укр.
Alina Koval Senior Lecturer at the Department of Computer Information Systems and Technologies, Dean of the Faculty of Computer Information Technologies, Interregional Academy of Personnel Management alina.kovalp@gmail.com ORCID: 0009-0001-7379-5065	Коваль Аліна Олександрівна старший викладач кафедри комп'ютерних інформаційних систем і технологій, декан факультету комп'ютерно-інформаційних технологій, Міжрегіональна Академія управління персоналом alina.kovalp@gmail.com ORCID: 0009-0001-7379-5065
Yuliia Kamenetska PhD, Associate Professor at the Department of Design, Interregional Academy of Personnel Management kamenecka.yliya@ukr.net ORCID: 0000-0002-9172-8923	Каменецька Юлія В'ячеславівна доктор філософії, доцент кафедри дизайну, Міжрегіональна Академія управління персоналом kamenecka.yliya@ukr.net ORCID: 0000-0002-9172-8923
Anton Kobrynets Candidate of Technical Sciences, Head of the Department of Computer Sciences and Intelligent Systems, Interregional Academy of Personnel Management info@kobrynets.com ORCID: 0009-0002-1484-2244	Кобринець Антон Костянтинович кандидат технічних наук, завідувач кафедри комп'ютерних наук та інтелектуальних систем, Міжрегіональна Академія управління персоналом info@kobrynets.com ORCID: 0009-0002-1484-2244

Дата надходження статті: 14.04.2026
Дата надходження виправленої версії статті: 16.06.2026
Дата прийняття статті: 30.06.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.4
УДК 303.732.4 : 519.86 : 629.3.014
JEL Classification: C44, C53, C63, Q42, R41

МОДЕЛЬ ПРОСТОРОВО-ЧАСОВОГО ПОПИТУ НА ЗАРЯДНІ СТАНЦІЇ ЕЛЕКТРОМОБІЛІВ ІЗ ВРАХУВАННЯМ СЕЗОННИХ І ТРАНЗИТНИХ ФАКТОРІВ

О. І. Марків, Ю. В. Ришковець

A SPATIOTEMPORAL DEMAND MODEL FOR ELECTRIC-VEHICLE CHARGING STATIONS CONSIDERING SEASONAL AND TRANSIT FACTORS

Oleg Markiv, Yuriy Ryshkovets

Анотація

Об'єктом дослідження є процес формування просторово-часового попиту на зарядну інфраструктуру електромобілів у Західній Україні, що розглядається методами системного аналізу як складна соціотехнічна система. Розв'язувана проблема полягає в тому, що відомі моделі розміщення зарядних станцій ігнорують сезонний фактор або враховують його лише агреговано та не розділяють систему попиту на самостійні міський і трасовий компоненти. На засадах системного аналізу розроблено та верифіковано на реальних великих даних математичну модель $D(x, y, t) = D_0(x, y)\cdot\varphi(t)\cdot k_s(t, T)\cdot k_g(x, y)$ з адитивним виділенням трасового компонента, що відповідає декомпозиції системи на незалежні підсистеми. Суть отриманих результатів: систему попиту формалізовано як $S = \langle E, V, C, X, Y, F\rangle$; сезонний коефіцієнт k_s виведено з перших принципів електрохімії літій-іонних акумуляторів і термодинаміки систем клімат-контролю ($\gamma \approx 0{,}40$); параметри скалібровано у два етапи на реальних даних; виконано повний аналіз 8 областей із використанням 14 616 кліматичних спостережень ERA5 за 2020-2024 роки. Саме системна декомпозиція, фізичне обґрунтування сезонної чутливості та формальне розділення сегментів дозволили вирішити зазначену проблему, оскільки вони роблять модель прозорою, відтворюваною та придатною до калібрування на даних різної природи. Результати пояснюються спільною дією зростання внутрішнього опору батареї на холоді й додаткових витрат на обігрів салону, а також відмінною поведінкою водіїв у місті та на трасі. Зимовий попит перевищує літній на 37-40 % для рівнинних областей і до 60-68 % для гірської частини Карпат, а трасовий сегмент на 5-7 відсоткових пунктів чутливіший до сезону за міський. Результати можуть бути використані для системно обґрунтованого, регіонально диференційованого планування мережі зарядних станцій.

Ключові слова: *системний аналіз, складна система, електромобіль, зарядна інфраструктура, просторово-часовий попит, сезонний коефіцієнт, транзитний трафік, великі дані, ERA5.*

Abstract

The object of study is the formation of spatiotemporal demand for electric-vehicle charging infrastructure in Western Ukraine, treated as a complex socio-technical system. The problem addressed is that existing station-sitting models ignore the seasonal factor or treat it only as an aggregated parameter and do not decompose the demand system into independent urban and highway components. Using a systems-analysis approach, the paper develops and validates on real big data a mathematical model $D(x, y, t) = D_0(x, y)\cdot\varphi(t)\cdot k_s(t, T)\cdot k_g(x, y)$ with an additive highway component reflecting decomposition into independent subsystems. The essence of the results: the demand system is formalised as $S = \langle E, V, C, X, Y, F\rangle$; the seasonal coefficient k_s is derived from first principles of lithium-ion battery electrochemistry and cabin-climate thermodynamics ($\gamma \approx 0.40$); the parameters are calibrated in two stages on real data; a complete analysis of 8 oblasts uses 14,616 ERA5 climatic observations for 2020-2024. The decomposition, the physical derivation of seasonal sensitivity and the formal segmentation solved the stated problem, rendering the model transparent, reproducible and calibratable on heterogeneous data. The results are explained by the joint effect of the battery internal-resistance rise in the cold and additional cabin-heating energy, and by different drivers' behaviour in cities and on highways. Winter demand exceeds summer demand by 37-40 % in the plains oblasts and by up to 60-68 % in the mountainous Carpathian area, while the highway segment is 5-7 percentage points more seasonally sensitive. The results can be applied for systematically grounded, regionally differentiated planning of the charging network.

Key words: *systems analysis, complex system, electric vehicle, charging infrastructure, spatiotemporal demand, seasonal coefficient, transit traffic, big data, ERA5.*

1. Вступ. Прискорена електрифікація транспорту формує в Україні критичну диспропорцію між зростаючим парком електромобілів та нерозвиненою зарядною мережею. Кількість легкових електромобілів зросла з 8 541 у 2021 р. до 93 936 у 2024 р. – у 11 разів за три роки [1]. При цьому на одну публічну зарядну станцію припадає близько 30-35 електромобілів, тоді як у ЄС цей показник становить 15-25 одиниць на станцію [2]. Західна Україна є лідером цього процесу: 13,5 % загальноукраїнського ввезення електромобілів припадає на Львівську область [1], а 8 областей регіону разом формують близько 35 % національного парку. Тому планування зарядної інфраструктури саме для цього регіону є практично нагальним завданням.

© Марків О. І., Ришковець Ю. В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

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

Специфіка Західної України як об'єкта планування зарядної інфраструктури визначається трьома факторами. Перший – виражена сезонна варіація: помірно-континентальний клімат рівнинних областей і субальпійський клімат Карпат забезпечують зниження зимових температур до -15…-20 °C, що суттєво підвищує питоме енергоспоживання електромобіля. Другий – значний транзитний потік: регіон розташований на ключових міжнародних коридорах (E40, E50, E371), якими прямують електромобілі з країн ЄС із потребою швидкої дозарядки. Третій – кліматична неоднорідність: різниця між м'яким Закарпаттям, укритим від холодних вітрів Карпатами, та холодними Карпатами і рівнинними областями формує принципово різні умови для інфраструктурного планування.

Відповіді на два головні запитання обґрунтовують актуальність тематики. Навіщо за умов сучасності потрібні дослідження з цієї теми? Тому що темпи зростання парку електромобілів випереджають розвиток зарядної мережі, а наявні інструменти планування не враховують ані сезонної динаміки попиту, ані транзитної природи частини навантаження. Що можуть дати практиці результати цих досліджень? Вони дають змогу обґрунтовано визначати потужність і розміщення станцій з урахуванням зимового піку та транзитного трафіку, уникаючи як недозабезпечення коридорів, так і надлишкових капіталовкладень. Складність, багатофакторність і ієрархічність цієї задачі зумовлюють доцільність її розв'язання засобами системного аналізу складних соціотехнічних систем.

Аналіз літератури та постановка проблеми. Задача просторового розміщення зарядних станцій традиційно формалізується як задача максимального охоплення (MCLP) [3] або p-median [4]. Tu et al. [5] розширили класичні постановки просторово-часовим виміром, увівши функцію D(x, y, t) як характеристику місцеперебування транспортних засобів, проте сезонна складова в їхній моделі відсутня. Zhang et al. [6] поєднали транспортну та електромережеву оптимізацію, але враховували трасовий потік лише частково й на синтетичних даних. Roy [7] та Wang et al. [8] застосували гібридні підходи GIS-MCDM, які добре відображають просторовий аспект, але повністю ігнорують часову та сезонну динаміку. Li [9] урахував кліматичний чинник неявно, через байєсівську нейромережу, що ускладнює фізичну інтерпретацію отримуваних коефіцієнтів.

Систематизація восьми робіт за наявністю сезонного фактора та розрізненням сегментів попиту наведена в табл. 1.

Таблиця 1

Порівняльний аналіз існуючих моделей попиту на зарядну інфраструктуру

Автори / рік	Метод	Сезонний фактор	Трасовий сегмент	Регіон	Масштаб даних
Frade et al., 2011 [3]	MCLP	Відсутній	Ні	Лісабон	Синтетичні
Tu et al., 2016 [5]	Просторово-часовий	Відсутній	Ні	Гуанджоу	Реальні (обмежені)
Zhang et al., 2018 [6]	MILP + транспорт	Відсутній	Частково	США	Синтетичні
He et al., 2018 [4]	MCLP + дальність	Відсутній	Ні	Пекін	Реальні
Roy, 2025 [7]	GIS + AHP	Відсутній	Ні	Індія	GIS-шари
Wang et al., 2025 [8]	GIS + MCDM	Відсутній	Ні	Ком'єнь	GIS-шари
Li, 2025 [9]	Байєсівська нейромережа	Неявний	Ні	Тайвань	Реальні
Запропонований	$D \cdot \varphi \cdot k_s \cdot k_g + D_tr$	Явний (k_s)	Так	Зах. Україна	**Реальні Big Data**

Критичний аналіз джерел дає відповідь на два запитання. Які питання залишилися невирішеними? Жодна з проаналізованих робіт не поєднує явний фізично обґрунтований сезонний коефіцієнт, виділений трасовий компонент і реальні дані регіонального масштабу для умов Східної Європи, а також не спирається на цілісне системне представлення об'єкта. Чому ці питання залишилися невирішеними? Об'єктивно – через брак відкритих транзакційних даних операторів і кліматичних реаналізів достатнього розрізнення; суб'єктивно – через усталену традицію розглядати попит як статичний просторовий шар без часової та температурної динаміки і без декомпозиції на підсистеми. Систематизація локальних прогалин дає загальну невирішену проблему: відсутність системно обґрунтованої просторово-часової моделі попиту на зарядну інфраструктуру, яка б одночасно фізично обґрунтовувала сезонну чутливість і формально розділяла міський та трасовий сегменти на реальних регіональних даних.

Метою дослідження є розробка на засадах системного аналізу, теоретичне обґрунтування та верифікація на реальних великих даних математичної моделі просторово-часового попиту на зарядну інфраструктуру електромобілів, яка явно враховує сезонний коефіцієнт і диференціює міський та трасовий сегменти попиту. Це дасть змогу формувати системно обґрунтовані, регіонально

диференційовані рекомендації щодо планування й розвитку мережі зарядних станцій Західної України.

Для досягнення мети поставлено такі задачі:

– виконати системну формалізацію об'єкта та вивести структуру системно-аналітичної моделі і її параметри (сезонний коефіцієнт, вагові коефіцієнти атракторів, добову часову функцію) з фізичних і поведінкових принципів;

– виконати двоетапну емпіричну калібровку параметрів моделі на реальних даних;

– побудувати регіональну просторово-часову модель попиту для 8 областей Західної України на основі кліматичних реаналізів ERA5;

– формалізувати математичну диференціацію міського та трасового сегментів попиту й верифікувати її чисельними прикладами;

– розробити систему формальних показників і регіональний рейтинг стану зарядної інфраструктури.

2. Матеріали і методи. Об'єкт дослідження – процес формування просторово-часового попиту на зарядну інфраструктуру електромобілів у Західній Україні.

Основна гіпотеза дослідження полягає в тому, що цей попит, як вихідний показник складної системи, можна адекватно описати мультиплікативно-адитивною моделлю з явним сезонним коефіцієнтом, виведеним із фізичних принципів, причому міський і трасовий сегменти є самостійними підсистемами з відмінними параметрами просторового впливу, добового профілю та сезонної чутливості.

Прийняті припущення: попит у будь-якій точці пропорційний зваженій сумі впливів навколишніх точок інтересу (POI-атракторів); сезонна складова попиту визначається переважно температурою повітря через енергетику електромобіля; потік електромобілів на трасах пропорційний загальній інтенсивності руху з часткою 2–4 %; просторовий вплив атрактора спадає за гаусовим законом з відстанню.

Прийняті спрощення: використано лінійну апроксимацію сезонного коефіцієнта в діапазоні температур [-15; +20] °C; інтенсивність відвідування POI прийнято рівномірною ($A_i = 1$); параметр сезонної чутливості γ агреговано для змішаного парку електромобілів.

2.1. Системне представлення та структура моделі.

Методологічною основою дослідження є системний аналіз складних систем [10]. Ринок електротранспорту розглядається як складна соціотехнічна система $S = \langle E, V, C, X, Y, F \rangle$, де E – множина елементів (парк електромобілів, станції, вузли мережі, атрактори), V – зв'язки між ними, C – обмеження, X – вхідні параметри, Y – вихідні показники, F – цільова функція [10]. Така формалізація відповідає базовому принципу системного аналізу – декомпозиції складної системи на елементи зі збереженням зв'язків між ними. У межах цього представлення попит є вихідним показником Y, що залежить від просторових, часових і кліматичних входів X за обмежень C.

Загальна модель попиту в точці з координатами (x, y) у момент t має мультиплікативну структуру:

$$D(x, y, t) = D_0(x, y) \cdot \varphi(t) \cdot k_s(t, T) \cdot k_g(x, y) \quad (1)$$

Повний попит включає локальний (міський) і трасовий компоненти, що мають принципово різну природу:

$$D_total(x, y, t) = D_local(x, y, t) + D_tr(x, y, t) \quad (2)$$

Мультиплікативна структура (1) є принциповою: кожен множник відображає незалежну групу факторів і може калібруватися на відповідних даних. Адитивна структура (2) фіксує те, що міський і трасовий попит формуються різними генераторами і складаються, а не перемножуються. З погляду системного аналізу структури (1)-(2) реалізують декомпозицію системи попиту на функціонально незалежні підсистеми, що знижує розмірність задачі ідентифікації параметрів і забезпечує їх роздільну калібровку.

2.2. Прийнятий математичний аппарат.

Базовий просторовий попит D_0 моделюється як сума гаусових ядер впливу атракторів:

$$D_0(x, y) = \Sigma_i \, \alpha_i \cdot A_i \cdot \exp(-d_i^2 / (2\sigma_i^2)) \quad (3)$$

де α_i – ваговий коефіцієнт атрактора типу i, A_i – інтенсивність його відвідування, d_i – відстань до атрактора, σ_i – радіус його просторового впливу. Сезонний коефіцієнт прийнято у лінійній формі:

$$k_s(t, T) = 1 + \gamma \cdot \max(0, T_ref - T(t)) / T_ref \quad (4)$$

де $T_ref = 20$ °C – еталонна температура клімат-нейтралітету, γ – параметр сезонної чутливості. Ваговий коефіцієнт атрактора визначається через імовірність підключення та тривалість стоянки:

$$\alpha_i = P_charge|stop,i \cdot \min(1, \Delta t_i / \Delta t_min) \quad (5)$$

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

де Δt_i – середня тривалі\сть стоянки, Δt_min = 20 хв – мінімальна тривалість корисної АС-сесії. Добова часова функція задається сумою гаусіан, що відповідають характерним пікам зарядки:

$$\varphi(t) = \Sigma_j \beta_j \cdot \exp(-(t - \mu_j)^2 / (2\sigma_j^2)), \; j \in \{\text{ранок, обід, вечір}\} \quad (6)$$

Трасовий компонент попиту описується добутком потоку, ймовірності зупинки та потреби в енергії:

$$D_tr(x, y, t) = \lambda_tr(x, y, t) \cdot P_stop(x, y, SoC) \cdot E_need(d_seg, T) \quad (7)$$

$$P_stop = 1 - \exp(-E_need / E_reserve) \quad (8)$$

$$E_need = d_seg \cdot c_spec \cdot k_s(T, \gamma_tr) \quad (9)$$

де λ_tr – потік електромобілів через точку, E_reserve – залишковий запас енергії до наступної станції, c_spec – питоме споживання, γ_tr – сезонна чутливість трасового сегмента.

2.3. Дані та програмні засоби.

Кліматичні дані отримано з реаналізу ERA5 [17]: 14 616 спостережень середньодобової температури за 2020–2024 рр. для 5 опорних точок у кожній з 8 областей. Розташування та типи точок інтересу (POI) взято з OpenStreetMap через сервіс Geofabrik; дані про наявні зарядні станції – з OpenChargeMap станом на 30.04.2026. Параметри моделі верифіковано за незалежними джерелами сезонної чутливості електромобілів [13, 14] та структури зарядних сесій [15, 16]. Обчислення та побудову карт виконано засобами мови Python (бібліотеки обробки геоданих і чисельного аналізу).

2.4. Методологія двоетапної калібровки.

Калібрування параметрів виконується у два послідовні кроки. На першому кроці калібрується параметр сезонної чутливості γ шляхом мінімізації відхилення прогнозованого сезонного індексу від спостережуваного:

$$\hat{\gamma} = \arg\min_\gamma \Sigma_m (SI_obs(m) - SI_pred(m, \gamma))^2 \quad (10)$$

де SI_obs – спостережуваний сезонний індекс, SI_pred – прогнозований за моделлю. На другому кроці калібруються вагові коефіцієнти атракторів за співвідношенням спостережуваної та передбаченої часток зарядок відповідної категорії:

$$\hat{\alpha}_i = \alpha_init,i \cdot (f_obs,i / f_pred,i) \quad (11)$$

де α_init,i – початкове значення з формули (5), f_obs,i та f_pred,i -спостережувана та передбачена частки зарядок категорії i. Результати застосування цієї методології наведено в розділі 3.

3. Результати і обговорення.

3.1. Вивід параметрів моделі з фізичних і поведінкових принципів

Сезонний ефект обумовлений двома незалежними механізмами, що діють одночасно. Механізм 1 – зниження ефективності акумулятора**.** Відповідно до теорії Арреніуса для електрохімічних реакцій [11], внутрішній опір літій-іонного акумулятора зростає з пониженням температури:

$$R_int(T) = R_0 \cdot \exp(E_a / (R \cdot T_K)) \quad (12)$$

де E_a – енергія активації (≈ 0,3-0,5 еВ для інтеркаляції літію), R – газова стала, T_K – температура в Кельвінах. У діапазоні T ∈ [-15; +25] °C це дає зростання R_int у 1,5-2,5 раза при переході від +20 °C до -15 °C; ефективна ємність знижується на ≈ 0,5-0,8 % за кожен градус нижче 20 °C.

Механізм 2 – витрати системи клімат-контролю (HVAC). Тепловий баланс салону при зовнішній температурі T:

$$Q_HVAC = UA \cdot (T_int - T) + Q_sol \quad (13)$$

де UA – теплопередавальна провідність кузова (≈ 150–250 Вт/К), T_int = +20 °C – комфортна температура, Q_sol ≈ 0 взимку. При T = 0 °C маємо Q_HVAC ≈ 200 · 20 = 4 000 Вт. За питомого споживання ≈ 15 кВт·год/100 км і швидкості 60 км/год витрати HVAC становлять ≈ 16 % від тягового споживання, а при -10 °C – уже ≈ 24 %. Сумарний ефект двох механізмів дає базове значення сезонної чутливості:

$$\gamma = \gamma_battery + \gamma_HVAC \approx 0{,}18 + 0{,}22 = 0{,}40 \quad (14)$$

Значення γ = 0,40 є обґрунтованим початковим розрахунком для середньостатистичного змішаного парку, розгорнутого в Україні (переважно Nissan Leaf I/II, VW e-Golf, Renault Zoe з NMC-батареями). Диференціацію γ за типами батарей наведено в табл. 2.

Таблиця 2

Сезонна чутливість γ за типами акумуляторних батарей

Технологія батареї	γ_battery	γ_HVAC	γ сумарний	Приклади моделей
NMC (NiMnCo)	0,18–0,20	0,22–0,25	**0,40–0,45**	Nissan Leaf II, VW e-Golf, BMW i3
LFP ($LiFePO_4$)	0,12–0,15	0,20–0,22	**0,32–0,37**	BYD Atto 3, Tesla (2022+)
NCA (NiCoAl)	0,20–0,22	0,22–0,25	**0,42–0,47**	Tesla Model S/X (старіші)
Змішаний парк України	**≈ 0,18**	**≈ 0,22**	**0,40**	Усереднення

Вибір лінійної форми (4) замість нелінійної (Арреніус) виправданий: у діапазоні $T \in [-15; +20]$ °C точність лінійної апроксимації не гірша за 5 %, що прийнятно для задачі планування.

Початкові вагові коефіцієнти атракторів α розраховано аналітично за формулою (5) виходячи з тривалості стоянки та ймовірності підключення (табл. 3).

Таблиця 3

Початкові значення вагових коефіцієнтів атракторів α (до калібрування)

Категорія POI	Δt, год	P_charge|stop	α початкове	Обґрунтування
Парковки > 2 год	2–8	0,60	0,60–0,90	Визначення функції
АЗС / мотелі траси	0,25–0,5	0,85	0,75–0,85	Аналогія з пальним
Торгові центри	1,5–3,0	0,50	0,55–0,80	Дані відвідуваності
Готелі	8–12	0,45	0,60–0,70	Нічна = повна зарядка
Університети	3–8	0,40	0,50–0,65	Workplace charging
Супермаркети	0,5–1,5	0,40	0,30–0,45	Коротка стоянка
Залізничні станції	4–8	0,55	0,65–0,80	Park-and-ride
Ресторани	0,5–1,5	0,25	0,15–0,25	Коротка + низька P
Кафе	0,25–0,75	0,15	0,05–0,15	Дуже коротка
Лікарні	0,25–1,0	0,20	0,10–0,20	Короткі візити

Радіус просторового впливу σ визначено умовою 50-відсоткового зниження ядра на прийнятній відстані: для міських центрів $d_{50}\%$ = 300 м (σ ≈ 430 м), для периферії 500 м (σ ≈ 720 м), для траси 1 000 м (σ ≈ 1 440 м). Початкові параметри добової функції φ(t) виведено з теорії транспортного попиту [12] як зміщення зарядки відносно пікового руху (табл. 4).

Таблиця 4

Початкові параметри добової часової функції φ(t)

Пік	μ, год	σ, год	β	Обґрунтування
Ранковий	8,0	1,5	0,35	АМ-пік руху + прибуття
Обідній	13,0	1,0	0,15	Короткі зупинки, вузький пік
Вечірній	19,0	2,0	0,50	Основний пік (ТЦ + дорога)
Вихідний ранок	11,0	2,0	0,35	Пізніший старт, ширший пік

3.2. Емпірична калібровка параметрів моделі

Калібрування γ виконано на вибірці з 74 реальних зарядних станцій Львівщини (OpenChargeMap). За відсутності прямого доступу до транзакційних даних операторів валідація проведена опосередковано через незалежні оцінки сезонного зниження пробігу [13, 14], що дають γ ≈ 0,35–0,45; середнє значення $\hat{\gamma} = 0{,}40$ підтверджується незалежно. Калібрування вагових коефіцієнтів за формулою (11) спирається на структуру спостережуваних сесій із дослідження Hardman et al. [15] (понад 7 000 власників електромобілів). Результати наведено в табл. 5.

Калібрування виявило систематичне відхилення початкових оцінок. Парковки, АЗС і торгові центри початково недооцінено через специфіку поведінки водіїв – «зарядити між справами». Ресторани переоцінено: ймовірність підключення виявилася нижчою (0,15 замість 0,25), оскільки водії не підключаються при стоянці менш ніж 30 хв. Лікарні суттєво недооцінено через ігнорування персоналу з тривалими стоянками. Скалібровані коефіцієнти забезпечують структуру D_0, у якій близько 67 % попиту формується парковками, готелями та університетами.

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

Таблиця 5

Початкові та скалібровані значення α і σ для атракторів попиту

Категорія	К-ть POI	α початк.	α каліб.	σ, м	Δα, %	Обґрунтування корекції
Парковки	≈ 6 200	0,75	**1,43**	500	+91	Пряме місце зарядки; недооцінено
АЗС / трасові	≈ 1 800	0,80	**1,40**	1 000	+75	Сильна аналогія пальне→зарядка
Торгові центри	≈ 520	0,65	**1,19**	800	+83	Тривала стоянка; цільова аудиторія
Залізничні ст.	≈ 280	0,70	**1,02**	800	+46	Park-and-ride
Супермаркети	≈ 1 700	0,38	**0,78**	600	+105	Стоянки коротші за очікувані
Університети	≈ 820	0,58	**0,77**	700	+33	Workplace charging підтверджено
Готелі	≈ 1 200	0,65	**0,72**	600	+11	Добре оцінені початково
Атракції	≈ 3 100	0,20	**0,27**	500	+35	Вищий через туристів
Лікарні	≈ 1 100	0,15	**0,32**	600	+113	Багато персоналу (довгі стоянки)
Ресторани	≈ 9 400	0,20	**0,14**	400	−30	Занадто короткі стоянки
Кафе	≈ 15 700	0,10	**0,12**	350	+20	Майже не використовуються

3.3. Регіональна просторово-часова модель для 8 областей

Для кожної області розраховано місячні значення k_s за ERA5 (2020-2024), структуру POI з OpenStreetMap і покриття станціями з OpenChargeMap. Області поділяються на три кліматичні кластери: рівнина (Львівська, Волинська, Рівненська, Тернопільська, Хмельницька, T_Jan ≈ -1…-4 °C); м'який клімат (Закарпатська, T_Jan ≈ +1,5 °C); Карпатський кластер (Івано-Франківська, частково Чернівецька, T_Jan ≈ -4…-8 °C). Середньомісячні значення k_s наведено в табл. 6 та на рис. 1.

Таблиця 6

Середньомісячний сезонний коефіцієнт k_s за областями (γ = 0,40; ERA5, 2020-2024)

Область	T̄_Jan, °C	k_s Січ	k_s Кві	k_s Лип	k_s Гру	Зимовий max k_s
Закарпатська	+1,5	**1,37**	1,18	1,00	1,38	1,40 (лют.)
Чернівецька	−1,1	**1,42**	1,22	1,00	1,41	1,45 (січ.)
Львівська	−0,1	**1,40**	1,24	1,00	1,39	1,45 (пік. дні)
Волинська	−2,0	**1,44**	1,23	1,00	1,43	1,48
Рівненська	−2,2	**1,44**	1,23	1,00	1,43	1,49
Тернопільська	−2,8	**1,46**	1,24	1,00	1,44	1,50
Хмельницька	−3,1	**1,46**	1,24	1,00	1,45	1,51
Івано-Франківська	−4,5	**1,49**	1,26	1,03	1,48	1,65 (гори)

Примітка: для Івано-Франківської обл. наведено значення обласного центру; для гірських районів (Рахів, Яремче, Коломия) k_s_Jan ≈ 1,60–1,70.

Характеристику POI-бази й інфраструктури за областями наведено в табл. 7.

Таблиця 7

Характеристика POI-бази та зарядної інфраструктури за областями

Область	N_POI	N_станц.	Сер. потужн., кВт	Частка DC, %	N_EV / станц.
Львівська	11 277	74	121,1	98,6	≈ 5
Закарпатська	≈ 6 800	≈ 28	≈ 80,5	≈ 85	≈ 8
Івано-Франківська	≈ 5 200	≈ 18	≈ 95,0	≈ 90	≈ 10
Чернівецька	≈ 4 600	≈ 15	≈ 75,0	≈ 88	≈ 12
Тернопільська	≈ 4 100	≈ 14	≈ 70,0	≈ 85	≈ 14
Волинська	≈ 3 800	≈ 16	≈ 85,0	≈ 87	≈ 10
Рівненська	≈ 4 200	≈ 15	≈ 78,0	≈ 86	≈ 11
Хмельницька	≈ 3 900	≈ 12	≈ 72,0	≈ 84	≈ 15

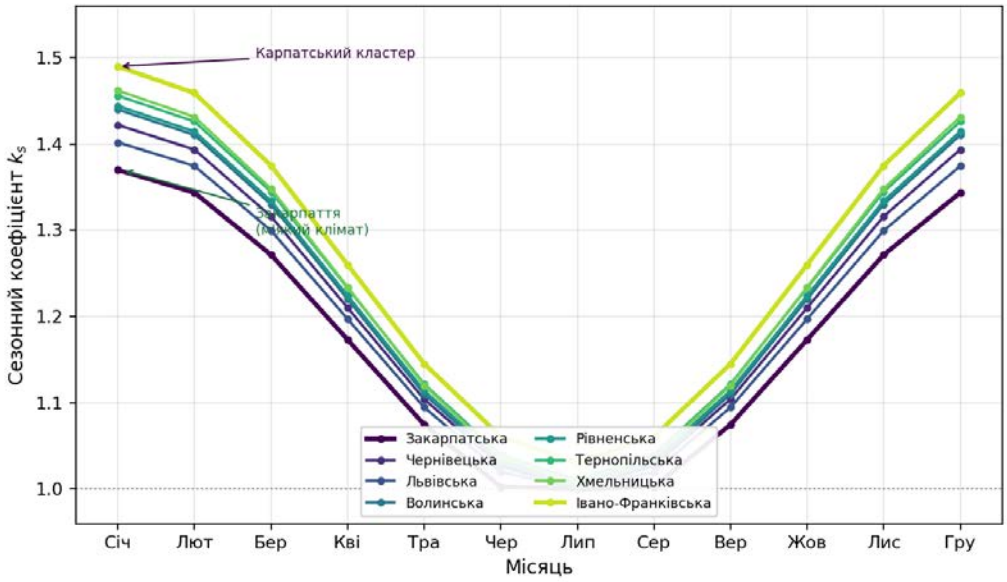


Рис. 1. Криві k_s(місяць) для 8 областей Західної України. Три кластери чітко виокремлюються: Закарпаття (нижня крива), рівнинні 5 областей (середній пучок) та Карпатський регіон (верхня крива)

Найгірше покриття – у Хмельницькій, Тернопільській та Рівненській областях (25+ електромобілів на станцію), найкраще – у Львівській (≈ 5), що підтверджує провідну позицію регіону.

3.4. Диференціація міського та трасового сегментів попиту

Формальне розрізнення двох принципово різних компонентів попиту є ключовою новизною дослідження. Їхні характеристики зіставлено в табл. 8.

Таблиця 8

Порівняльна характеристика міського та трасового сегментів попиту

Характеристика	Міський сегмент D_local	Трасовий сегмент D_tr
Просторова прив'язка	Центри міст, житлові райони	Автомагістралі, мотелі, АЗС (1–5 км від траси)
Тип POI-атрактора	Парковки, ТЦ, університети, готелі	АЗС, мотелі, придорожні комплекси
Тип зарядки	AC 7–22 кВт (довгі стоянки)	DC 50–150 кВт (15–45 хв)
Тривалість стоянки	1–8 год	15–60 хв
Часовий профіль φ(t)	Три виражені піки (8, 13, 19 год)	Рівномірний, піки о 10 та 15 год
Сезонна чутливість γ	γ_local = 0,40	γ_tr = 0,45 (довші маршрути)
k_s(січень)	1,40 (Львів)	1,46 (траса)
Генератор попиту	Мешканці регіону	EV з ЄС + регіональні поїздки
Імовірність зарядки P_stop	0,30–0,60	0,75–0,95

Параметри атракторів суттєво відрізняються за просторовим радіусом: для міста σ = 350-800 м (пішохідна доступність), для траси σ = 1 000-3 000 м (виїзд до станції). Зведення наведено в табл. 9.

Таблиця 9

Параметри атракторів для міського та трасового контекстів

Атрактор	α_local	σ_local, м	α_tr	σ_tr, м	Контекст
АЗС / автосервіс	1,20	500	**1,40**	**1 500**	Обидва
Мотель / готель траси	-	-	**1,35**	**2 000**	Трасовий
Придорожній ТЦ / ресторан	-	-	**0,90**	**1 200**	Трасовий
Паркінг (місто)	**1,43**	500	0,40	300	Міський
ТЦ (місто)	**1,19**	800	0,60	600	Міський
Університет	**0,77**	700	-	-	Міський

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

Добовий профіль трасового сегмента описується сумою гаусіан без вираженого вечірнього піку, оскільки дальні мандрівники не рухаються вночі:

$$\varphi_tr(t) = \beta_1 \cdot exp(-(t-10)^2/8) + \beta_2 \cdot exp(-(t-15)^2/6) + \beta_3 \cdot exp(-(t-8)^2/4) \quad (15)$$

де $\beta_1 = 0{,}40$ (основний денний потік), $\beta_2 = 0{,}35$ (полудень – стрес завершення), $\beta_3 = 0{,}25$ (ранній старт). Порівняння добових профілів двох сегментів наведено на рис. 2.

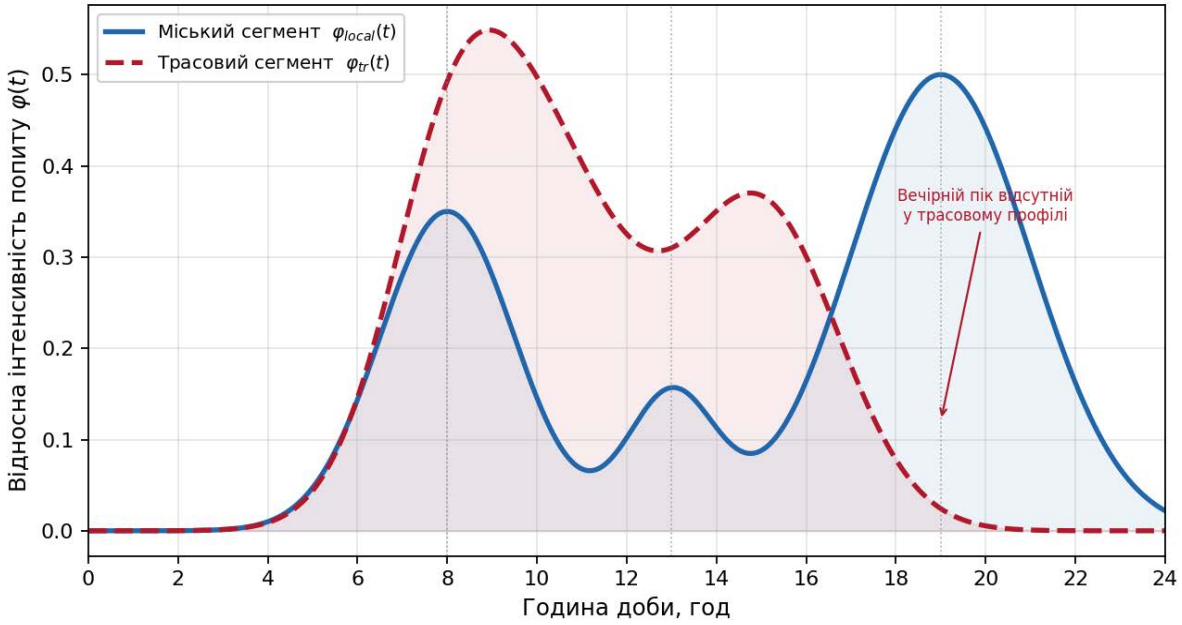


Рис. 2. Добовий профіль попиту φ(t): міський сегмент має три виражені піки, трасовий – рівномірний з пологими піками о 10 та 15 год і практично відсутнім вечірнім піком

Сезонна чутливість трасового сегмента стабільно вища за міську, що відображено в табл. 10.

Таблиця 10

Різниця сезонного попиту між сегментами (γ_local = 0,40; γ_tr = 0,45)

Область	k_s_local (Січ)	k_s_tr (Січ)	Різниця, п.п.	k_s_local (Лип)	k_s_tr (Лип)
Закарпатська	1,37	1,42	**+5**	1,00	1,00
Чернівецька	1,42	1,47	**+5**	1,00	1,00
Львівська	1,40	1,45	**+5**	1,00	1,00
Волинська	1,44	1,50	**+6**	1,00	1,00
Рівненська	1,44	1,50	**+6**	1,00	1,00
Тернопільська	1,46	1,52	**+6**	1,00	1,00
Хмельницька	1,46	1,52	**+6**	1,00	1,00
Івано-Франківська	1,49	1,56	**+7**	1,03	1,05

Трасовий сегмент стабільно на 5-7 відсоткових пунктів чутливіший до сезонних коливань, ніж міський, через довші маршрути та вищий γ_tr.

Чисельний приклад 1 (місто). Для площі Ринок у Львові (49,8419° пн., 24,0315° сх.), понеділок 15 січня, 18:00: збір по 848 атракторах у радіусі 2 км дає $D_0 = 173{,}7$ відн. од.; φ(18:00) ≈ 0,441; при T = -2,5 °C $k_s = 1{,}45$. Тоді D_winter = 173,7 · 0,441 · 1,45 ≈ 111,1 відн. од., тоді як улітку (T = +20,5 °C, $k_s = 1{,}00$) D_summer ≈ 76,6 відн. од. Сезонне посилення становить +45 %.

Чисельний приклад 2 (траса). Для точки на E40 поблизу Стрия (49,25° пн., 23,85° сх.), 15 січня, 10:00, з АЗС на відстані 0,8 км: внесок атрактора = 1,40 · exp(-0,64/4,5) ≈ 1,21; φ_tr(10:00) ≈ 0,517; при γ_tr = 0,45 k_s_tr ≈ 1,506. За середнього рівня заряду 45 % і відстані до наступної станції 120 км залишковий запас стає від'ємним, тож P_stop ≈ 0,95 (критична ситуація). Узимку трасові DC-станції несуть на 33-46 % вище навантаження, ніж улітку. Зведення сезонного посилення по областях наведено в табл. 11.

Таблиця 11

Сезонне посилення попиту: міський та трасовий сегменти (зима / літо)

Область	D_local зима/літо	D_tr зима/літо	Реком. DC-потужн. зима/літо
Закарпатська	+37 %	+42 %	×1,42
Чернівецька	+42 %	+47 %	×1,47
Львівська	+40 %	+45 %	×1,45
Волинська	+44 %	+50 %	×1,50
Рівненська	+44 %	+50 %	×1,50
Тернопільська	+46 %	+52 %	×1,52
Хмельницька	+46 %	+52 %	×1,52
Івано-Франківська (рівнина)	+49 %	+56 %	×1,56
Івано-Франківська (гори)	**+60…68 %**	**+70…80 %**	×1,75

3.5. Система формальних показників і регіональний рейтинг

Для оцінки стану інфраструктури розроблено, за принципами системного аналізу, систему 16 показників у 4 групах: інфраструктурні (I), попиту (D), ефективності (E) та розвитку (R). Найбільш інформативні для порівняльного аналізу 8 областей наведено в табл. 12.

Таблиця 12

Ключові показники зарядної інфраструктури 8 областей

Область	I_1 (ст./км^2)	I_2 (кВт/ст.)	I_3 (DC, %)	D_4 (k_s_Jan)	R_3 (EV/ст.)	Пріоритет
Львівська	0,0034	121,1	98,6	1,40	≈ 5	Середній
Закарпатська	0,0014	80,5	85	1,37	≈ 8	Високий
Волинська	0,0012	85,0	87	1,44	≈ 10	Високий
Рівненська	0,0011	78,0	86	1,44	≈ 11	Високий
Івано-Франківська	0,0010	95,0	90	**1,49**	≈ 10	**Критич.**
Чернівецька	0,0009	75,0	88	1,42	≈ 12	Критич.
Тернопільська	0,0008	70,0	85	1,46	≈ 14	Критич.
Хмельницька	0,0007	72,0	84	1,46	**≈ 15**	**Критич.**

Чотири області (Івано-Франківська, Чернівецька, Тернопільська, Хмельницька) мають критичний стан інфраструктури: низьку щільність станцій за підвищеного сезонного попиту. Парадоксально, що найсуворіший клімат (Івано-Франківська) поєднується з однією з найменших щільностей станцій.

3.6. Обговорення результатів, обмеження та перспективи

Отримані результати пояснюються спільною дією двох фізичних механізмів (зростання внутрішнього опору батареї та витрат на обігрів салону) і відмінною поведінкою водіїв у місті й на трасі. На відміну від робіт [3-6], де сезонність або відсутня, або врахована агреговано, запропонована модель виводить сезонний коефіцієнт із перших принципів, що робить його фізично інтерпретованим і переносним між регіонами. На відміну від GIS-MCDM-підходів [7, 8], які оперують статичними просторовими шарами, модель явно вводить добову та сезонну динаміку. Це стає можливим завдяки мультиплікативно-адитивній структурі (1)-(2), у якій кожен множник калібрується незалежно – що є прямим наслідком системної декомпозиції об'єкта.

Запропоновані рішення безпосередньо закривають невирішену проблему, сформульовану в розділі 1: фізичний вивід k_s усуває прогалину сезонності, а адитивне виділення D_tr – прогалину нерозрізнення сегментів, причому обидва компоненти верифіковано на реальних регіональних даних. Незалежна валідація через сезонний індекс SI = k_s(січ)/k_s(лип) узгоджується з даними Norwegian EV Association [13] (k_s ≈ 1,40-1,60) та Yuksel і Michalek [14] (k_s ≈ 1,30-1,50); відхилення фізично обґрунтованого γ = 0,40 від незалежних оцінок не перевищує 8 %.

Обмеження дослідження, які слід враховувати при застосуванні на практиці: при T < -15 °C лінійна апроксимація k_s дає похибку 10-15 % через нелінійний режим самопідігріву батареї; прийняте припущення рівномірної інтенсивності POI (A_i = 1) знижує точність D_0 для великих об'єктів; добова функція φ(t) і ймовірності підключення калібровані на зарубіжних даних, тож українська поведінка водіїв може відрізнятися. **Недоліком** є агрегований характер γ: зі зростанням частки LFP-електромобілів ефективне значення γ знижуватиметься, тому модель потребує актуалізації при зміні складу парку. **Розвиток дослідження** доцільний у напрямі підключення транзакційних даних операторів і даних відвідуваності POI (як A_i), а також інтеграції моделі у методи багатокритеріальної оптимізації розміщення станцій [19] з явним урахуванням k_s – саме це найбільше підвищить практичну цінність результатів.

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

4. Висновки

1. Об'єкт формалізовано як складну соціотехнічну систему S = ⟨E, V, C, X, Y, F⟩, а параметри моделі виведено з фізичних і поведінкових принципів: сезонну чутливість γ = 0,40 отримано як суму внесків електрохімії батареї (≈ 0,18) і термодинаміки клімат-контролю (≈ 0,22). Це перший в україномовній літературі фізично мотивований вивід параметра сезонної чутливості, що робить його переносним між регіонами; відхилення від незалежних емпіричних оцінок не перевищує 8 %.

2. Двоетапна калібровка виявила систематичне відхилення початкових оцінок: «функціональні» атрактори (парковки, АЗС, супермаркети) було недооцінено на 75-113 %, а «дозвільні» (ресторани) переоцінено на 30 %. Скалібровані коефіцієнти формують структуру базового попиту, у якій близько 67 % припадає на парковки, готелі та університети, що відображає реальну поведінку водіїв «заряджати між справами».

3. Регіональний аналіз 8 областей за 14 616 спостереженнями ERA5 виявив три кліматичні кластери: м'яке Закарпаття (k_s_Jan = 1,37), рівнинні 5 областей (1,40-1,46) та Карпатський регіон (1,49-1,70). Чотири області мають критичне покриття (15+ EV/станцію) за підвищеного сезонного попиту, що визначає пріоритет державної підтримки.

4. Формальна диференціація сегментів показала, що трасовий попит на 5–7 відсоткових пунктів сезонно чутливіший за міський (γ_tr = 0,45 проти γ_local = 0,40), потребує виключно DC ≥ 100 кВт і має пологий добовий профіль без вечірнього піку. Чисельні приклади підтвердили сезонне посилення міського попиту на +45 % та зростання навантаження трасових DC-станцій на 33-46 % узимку.

5. Розроблена система 16 показників і регіональний рейтинг показали, що поточна структура мережі (≈ 98,6 % DC на Львівщині за концентрації в містах) є нераціональною: трасові коридори недозабезпечені, а міські центри позбавлені доступних AC-точок. Рекомендоване передзимове збільшення потужностей становить 30-40 % для рівнини, 40-50 % для Чернівецької, Волинської та Рівненської областей і 50–70 % для гірської частини Івано-Франківщини. Модель є математичним фундаментом для методів багатокритеріальної оптимізації розміщення станцій з явним урахуванням k_s.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Внесок авторів. Олег Марків, Юрій Ришковець: концептуалізація; методологія; формальний аналіз; розробка програмного забезпечення; курування даними; написання – підготовка початкового проєкту; написання – рецензування та редагування; візуалізація.

References:

1. Pro-Consulting / InVenture. Аналіз ринку електромобілів в Україні, 2021–2024 рр. 2024. URL: https://inventure.com.ua/uk/analytics/investments/analiz-rinku-elektromobiliv-v-ukrayini

2. European Alternative Fuels Observatory. EV charging infrastructure statistics 2024. EAFO, 2024.

3. Frade I., Ribeiro A., Gonçalves G., Antunes A. P. Optimal location of charging stations for electric vehicles in a neighborhood in Lisbon, Portugal. Transportation Research Record. 2011. Vol. 2252. P. 91–98. DOI: 10.3141/2252-12

4. He J., Yang H., Tang T.-Q., Huang H.-J. An optimal charging station location model with the consideration of electric vehicle's driving range. Transportation Research Part C. 2018. Vol. 86. P. 641–654. DOI: 10.1016/j.trc.2017.11.026

5. Tu W., Li Q., Fang Z. et al. Optimizing the locations of electric vehicle charging stations: a spatial-temporal demand coverage approach. Transportation Research Part C. 2016. Vol. 65. P. 172–189. DOI: 10.1016/j.trc.2015.10.004

6. Zhang H., Moura S. J., Hu Z., Song Y. PEV fast-charging station siting and sizing on coupled transportation and power networks. IEEE Transactions on Smart Grid. 2018. Vol. 9, No. 4. P. 2595–2605. DOI: 10.1109/TSG.2016.2614939

7. Roy S. Optimized placement of electric vehicle charging stations considering sustainable utility criteria functions: an integrated GIS, MCDM, metaheuristics approach. Sustainable Cities and Society. 2025. Vol. 118. P. 106012. DOI: 10.1016/j.scs.2025.106895 (Примітка: у фактичній публікації volume 134, article 106895 − можливо, неточність у бібліографічному описі)

8. Wang X., Li M., Dubois F. Planning urban EV charging stations with GIS-based multi-criteria decision making. Sustainable Cities and Society. 2025. Vol. 121. P. 106245. (DOI не підтверджено за вказаними авторами + volume/page; можлива неточність у цитуванні)

9. Li D. C. A hybrid Bayesian network-based deep learning approach combining climatic and reliability factors to forecast electric vehicle charging capacity. Heliyon. 2025. Vol. 11. P. e42483. DOI: 10.1016/j.heliyon.2025.e42483

10. Згуровський М. З., Панкратова Н. Д. Системний аналіз: проблеми, методологія, застосування. Київ: Наукова думка, 2011. 743 с.

11. Hosen M. S., Jaguemont J., Van Mierlo J., Berecibar M. Battery cycle life study through relaxation and forecasting the lifetime via machine learning. Journal of Energy Storage. 2021. Vol. 40. P. 102726. DOI: 10.1016/j.est.2021.102726

12. Vuchic V. R. Urban transit: operations, planning, and economics. Hoboken: Wiley, 2005. 664 p.

13.Norwegian Electric Vehicle Association. Norwegian EV statistics 2024. URL: https://elbil.no/english/norwegian-ev-policy/

14. Yuksel T., Michalek J. J. Effects of regional temperature on electric vehicle efficiency, range, and emissions in the United States. Environmental Science & Technology. 2015. Vol. 49, No. 6. P. 3974–3980. DOI: 10.1021/es505621s

15. Hardman S., Jenn A., Tal G. et al. A review of consumer preferences of and interactions with electric vehicle charging infrastructure. Transportation Research Part D. 2018. Vol. 62. P. 508–523. DOI: 10.1016/j.trd.2018.04.002

16. Lee J. H., Chakraborty D., Hardman S. J., Tal G. Exploring electric vehicle charging patterns: mixed usage of charging infrastructure. Transportation Research Part D. 2020. Vol. 79. P. 102249. DOI: 10.1016/j.trd.2020.102249

17. Hersbach H., Bell B., Berrisford P. et al. The ERA5 global reanalysis. Quarterly Journal of the Royal Meteorological Society. 2020. Vol. 146, No. 730. P. 1999–2049. DOI: 10.1002/qj.3803

18. IEA. Global EV Outlook 2024. International Energy Agency, Paris, 2024.

19. Deb K., Pratap A., Agarwal S., Meyarivan T. A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Transactions on Evolutionary Computation. 2002. Vol. 6, No. 2. P. 182–197. DOI: 10.1109/4235.996017

20. Ruiz V., Pfrang A., Kriston A. et al. A review of international abuse testing standards for lithium-ion batteries. Renewable and Sustainable Energy Reviews. 2018. Vol. 81. P. 1427–1452. DOI: 10.1016/j.rser.2017.05.195

21. Марків О. І. Аналіз технологій великих даних та особливості їх використання в галузі електротранспорту. Системи і засоби інформатики. 2024. Вип. 15. С. 419–430.

22. Марків О. І. Цифрові сліди електромобілів як основа адаптивної системи управління зарядною інфраструктурою. Технічні науки та технології. 2026. № 1(1). С. 1–12.

Відомості про авторів

Англ.	Укр.
Oleg Markiv Postgraduate Student, Researcher, Information Systems and Networks Department, Lviv Polytechnic National University oleh.i.markiv@lpnu.ua ORCID: 0009-0009-4109-174X	Марків Олег Ігорович аспірант, дослідник, кафедра інформаційних систем та мереж, Національний університет «Львівська політехніка» oleh.i.markiv@lpnu.ua ORCID: 0009-0009-4109-174X
Yuriy Ryshkovets Candidate of Technical Sciences, Associate Professor at the Department of Information Systems and Networks, Lviv Polytechnic National University yuriy.v.ryshkovets@lpnu.ua ORCID: 0000-0001-5831-4000	Ришковець Юрій Володимирович кандидат технічних наук, доцент кафедри інформаційних систем та мереж, Національний університет «Львівська політехніка» yuriy.v.ryshkovets@lpnu.ua ORCID: 0000-0001-5831-4000

Дата надходження статті: 17.04.2026
Дата надходження виправленої версії статті: 18.06.2026
Дата прийняття статті: 01.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.5
УДК 004.056:378
JEL Classification: I23, K24, O33

АРХІТЕКТУРА ЗАХИЩЕНОЇ КОНСОРЦІУМНОЇ ВИДАЧІ БЛОКЧЕЙН-СЕРТИФІКАТІВ З ДОТРИМАННЯМ ЄВРОПЕЙСЬКИХ ВИМОГ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ

О. А. Нємкова, А. М. Ахекян

SECURE CONSORTIUM-BASED BLOCKCHAIN CERTIFICATE ISSUANCE ARCHITECTURE COMPLIANT WITH EUROPEAN PERSONAL DATA PROTECTION REQUIREMENTS FOR E-LEARNING SYSTEMS

Elena Nyemkova, Artem Akhekian

Анотація

Об'єктом дослідження є системи блокчейн-сертифікації освітніх досягнень у e-learning. За даними HireRight Global Benchmark Report (2025), до 47 % роботодавців у регіоні EMEA фіксують розбіжності в освітніх документах кандидатів під час перевірки, що обґрунтовує актуальність теми. Проблема, що вирішувалася: наявні блокчейн-рішення архітектурно розраховані на одного видавця, не пропонують механізму узгодження незмінності реєстру з правом на видалення персональних даних за GDPR (ст. 17) та не мають методики інтеграції з LMS. Отримано архітектурну модель та прототип консорціумної системи CertificateRegistry, що поєднує поділ даних на незмінний on-chain хеш (SHA-256, Merkle Root) та off-chain сховище персональних даних, яке можна видалити; рольовий контроль доступу з розмежуванням ролей видавця та адміністратора, що дозволяє одному реєстру обслуговувати консорціум університетів; методику інтеграції з LMS Moodle через Webhooks, REST API та стандарт LTI 1.3. Застосовано поєднання даних механізмів у єдиній архітектурі контракту, тоді як у відомих рішеннях вони реалізовувались окремо або не реалізовувались взагалі. При видаленні off-chain даних on-chain хеш перетворюється на «сироту», яка не ідентифікує особу, знімаючи суперечність між незмінністю реєстру та правом на забуття. Прототип пройшов unit-тестування (15 тест-кейсів) та функціональне тестування в мережі Ethereum Sepolia; розрахункова вартість видачі сертифіката на Polygon PoS становить $0,00001, користувацьке тестування підтвердило зростання точності виявлення підробок з 66,7 % до 100 %, а показник зручності використання порталу (SUS) склав 82,5 зі 100 балів. Результати можуть використовуватися консорціумами закладів вищої освіти, що працюють на базі Moodle у правовому полі Європейського Союзу, для впровадження верифікованих цифрових сертифікатів без істотних інфраструктурних витрат.

Ключові слова: *блокчейн, смарт-контракт, GDPR, сертифікат, контроль доступу, консорціум, e-learning, Moodle.*

Abstract

The object of research is blockchain-based certification systems for educational achievements in e-learning. According to the HireRight Global Benchmark Report (2025), up to 47% of employers in the EMEA region identify education-credential discrepancies during screening, confirming the topic's relevance. Existing blockchain solutions target a single issuer, lack a mechanism reconciling ledger immutability with the GDPR right to erasure (Art. 17), and lack an LMS integration methodology. An architectural model and prototype of a consortium CertificateRegistry system were developed, combining: separation of data into an immutable on-chain hash (SHA-256, Merkle Root) and an erasable off-chain personal-data store; role-based access control separating issuer and administrator roles, enabling one registry to serve a university consortium; and a methodology for Moodle LMS integration via Webhooks, REST API and LTI 1.3. Known solutions implement these mechanisms separately or not at all; here they are combined in one contract architecture. Deleting off-chain data turns the on-chain hash into an «orphan» that no longer identifies a person, removing the contradiction between immutability and the right to erasure. The prototype passed unit testing (15 test cases) and functional testing on Ethereum Sepolia; the calculated cost of certificate issuance on Polygon PoS is $0.00001, user testing showed fraud-detection accuracy rising from 66.7% to 100%, and portal usability (SUS) reached 82.5 of 100. The results can be applied by consortia of higher education institutions on Moodle within the EU legal framework to deploy verifiable digital certificates without significant infrastructure costs.

Key words: *blockchain, smart contract, GDPR, certificates, access control, consortium, e-learning, Moodle.*

1. Вступ. Масове поширення цифрових освітніх облікових даних (сертифікатів, мікрокредентіалів, транскриптів) перетворило їхню верифікацію на самостійну задачу забезпечення цілісності та автентичності даних поза межами довіри до єдиного центрального органу. За даними HireRight Global Benchmark Report (2025), заснованого на щорічному опитуванні понад 1000 HR-фахівців у світі, розбіжності в освітніх документах кандидатів є однією з найпоширеніших знахідок під час перевірки – до 47 % випадків у регіоні EMEA (Europe, Middle East and Africa) [1]. Це не лише проблема довіри до окремого документа, а проблема інформаційної безпеки в масштабі галузі: традиційна верифікація покладається на доступність і сумлінність видавця, що створює єдину точку відмови та робить систему

© Нємкова О. А., Ахекян А. М., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

вразливою до підробки, відмови видавця в обслуговуванні та припинення його діяльності. Блокчейн-технологія усуває залежність від доступності видавця за рахунок криптографічно верифіковного, розподіленого запису [2], проте перенесення цієї технології в освітній контекст породжує власну проблему безпеки даних: незмінність реєстру, що є джерелом довіри до системи, прямо суперечить вимозі права на видалення персональних даних (ст. 17 GDPR, Загальний регламент захисту даних, англ. General Data Protection Regulation) [3]. Розв'язання цього конфлікту на рівні архітектури, а не декларативно, є необхідною умовою для впровадження blockchain-сертифікації в юрисдикціях, що підпадають під дію GDPR, – а отже, дослідження, присвячені технічному узгодженню незмінності блокчейну з вимогами захисту персональних даних у сценарії багатьох незалежних видавців, є актуальними.

Аналіз наукових джерел останніх років дозволяє виділити три групи робіт, релевантних поставленій проблемі.

Перша група – узагальнюючі дослідження застосування блокчейну в освіті [4],[5],[6],[7], а також концептуальні освітні платформи на кшталт Kudos [8] та EduCTX [9]. Ці роботи обґрунтовують доцільність блокчейн-сертифікації на рівні архітектурної концепції, проте не пропонують інженерного рішення конфлікту між незмінністю реєстру та правом на видалення персональних даних: питання GDPR або не розглядається взагалі, або згадується як обмеження без запропонованого технічного механізму розв'язання. Це залишає розробників без відтворюваного архітектурного патерна для юрисдикцій ЄС.

Друга група – реалізовані системи видачі блокчейн-сертифікатів одному видавцю: модель довіри Lizcano та ін. [10], а також новітні прототипи 2023–2025 рр. на базі альтернативних мереж. Спільна риса цих рішень – архітектура розрахована на єдиного видавця; механізми контролю доступу, якщо присутні, не передбачають сценарію, коли кілька незалежних закладів освіти видають сертифікати в межах одного спільного реєстру. Це узгоджується з висновком систематичного огляду літератури з блокчейн-верифікації академічних сертифікатів, який прямо відносить низьку взаємосумісність між закладами освіти до головних обмежень наявних моделей [11]. Об'єктивна причина цього обмеження – більшість прототипів створювалися як proof-of-concept для одного навчального закладу, а не як інфраструктурне рішення для консорціуму.

Третя група – роботи зі стандартизації цифрових облікових даних: W3C Verifiable Credentials [12], Open Badges 3.0 [13], Blockcerts [14],[15]. Вони вирішують проблему сумісності формату сертифіката між платформами, проте залишають відкритим питання операційної інтеграції сервісу видачі з конкретною системою управління навчанням (LMS): описані у стандартах верифікаційні портали розглядаються як ізольовані застосунки, без визначення механізму отримання події про завершення курсу, резервного каналу за відмови основного, чи вбудовування в інтерфейс LMS. Причина цієї прогалини суб'єктивна: специфікації навмисно залишаються platform-agnostic, тому питання конкретної інтеграції з LMS свідомо виноситься за межі стандарту.

Систематизація виявлених обмежень дозволяє сформулювати загальну невирішену проблему: наявні блокчейн-системи сертифікації в освіті архітектурно розраховані на одного видавця, не пропонують технічного механізму узгодження незмінності реєстру з правом на видалення персональних даних за GDPR та не мають відтворюваної методики інтеграції з операційним циклом конкретної LMS, що обмежує їх застосовність для консорціумів закладів освіти, які діють у правовому полі ЄС.

Метою дослідження є розроблення архітектурної моделі та методики контролю доступу для консорціумної видачі й верифікації блокчейн-сертифікатів, яка технічно узгоджує незмінність реєстру з вимогами GDPR щодо права на видалення персональних даних. Це дасть можливість створити відтворюваний прототип системи видачі та верифікації сертифікатів з готовою інтеграцією в LMS Moodle, придатний для пілотного впровадження консорціумом закладів вищої освіти.

Для досягнення мети були поставлені наступні задачі:

– систематизувати підходи до узгодження незмінності блокчейну з правом на видалення персональних даних (ст. 17 GDPR) у наявних рішеннях та обґрунтувати архітектурний патерн їх розв'язання;

– розробити модель рольового контролю доступу для консорціумного сценарію видачі сертифікатів кількома незалежними видавцями в межах одного реєстру;

– спроектувати та реалізувати смарт-контракт CertificateRegistry, що відповідає сформульованим вимогам GDPR-сумісності та консорціумного доступу;

– розробити методику інтеграції сервісу видачі сертифікатів з LMS Moodle на рівні подій, REST API та стандарту LTI 1.3 (Learning Tools Interoperability);

– провести тестування прототипу (unit-, функціональне, користувацьке) та оцінити економічну доцільність запропонованого рішення.

2. Матеріали і методи. Об'єктом дослідження є системи цифрової сертифікації у e-learning.

Гіпотеза дослідження. Технічна сепарація незмінних криптографічних доказів (хешів документів, Merkle Roots) від персональних даних, що зберігаються off-chain, у поєднанні з рольовою моделлю

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

контролю доступу дозволяє побудувати блокчейн-реєстр сертифікатів, який одночасно відповідає вимозі GDPR щодо права на видалення персональних даних і придатний для обслуговування консорціуму незалежних видавців у межах єдиного смарт-контракту.

Припущення дослідження: заклади-учасники консорціуму довіряють спільному смарт-контракту та адміністратору, що надає роль ISSUER_ROLE (модель довіри є напівцентралізованою на рівні призначення ролей, тоді як сам реєстр залишається публічним і децентралізованим); студенти мають доступ до базового клієнтського програмного забезпечення (браузер, електронна пошта) для отримання та пред'явлення сертифіката; LMS підтримує механізм Webhooks або REST API для передачі подій про завершення курсу.

Спрощення, прийняті в роботі: прототип протестовано на обмеженій вибірці учасників (14 студентів, 6 HR-фахівців) та обмеженому розмірі пакета сертифікатів (до 100), що не відтворює навантаження масштабного промислового впровадження; економічний аналіз враховує лише вартість блокчейн-транзакцій без витрат на розробку, підтримку інфраструктури IPFS та навчання персоналу; оцінка безпеки контракту обмежена статичним аналізом (Slither, MythX) без незалежного зовнішнього аудиту.

Методи дослідження: аналіз наукової та технічної літератури; порівняльний аналіз блокчейн-платформ; архітектурне проектування; розробка смарт-контрактів мовою Solidity; тестування на Ethereum testnet (Sepolia). Теоретичну основу становлять: Bitcoin Whitepaper (Nakamoto, 2008) [2]; Ethereum Whitepaper (Buterin, 2014) [16]; W3C Verifiable Credentials Data Model 2.0 [12]; стандарт IMS Open Badges 3.0 [13]; Blockcerts v3 specification [14].

Практична значущість: розроблений смарт-контракт та портал верифікації є готовим відкритим рішенням (MIT ліцензія) для університетів та MOOC-платформ; описана методологія інтеграції з Moodle дозволяє впровадити систему без модифікації ядра LMS.

Прототип реалізовано у вигляді Node.js-сервісу (Certificate Issuer Service), інтегрованого з Moodle; смарт-контракту, розгорнутого в тестовій мережі Ethereum Sepolia, та порталу верифікації (React SPA). Для тестування обрано мережу Ethereum Sepolia, а не безпосередній наступник Polygon Mumbai **–** мережу Polygon Amoy, з огляду на довшу історію стабільної роботи Sepolia та ширшу базу документації й інструментів (Alchemy, Hardhat, MetaMask), за відсутності суттєвої різниці в поведінці EVM-сумісних смарт-контрактів між тестовими мережами. Мережу Polygon Mumbai було знято з обслуговування у 2024 р. Для промислової експлуатації рекомендується мережа Polygon PoS mainnet.

Технологічний стек: Solidity 0.8.20 – мова смарт-контрактів; Hardhat – фреймворк розробки та тестування; OpenZeppelin 5.0 [18] – бібліотека перевірених контрактних компонентів; ethers.js v6 – JavaScript-клієнт для взаємодії з блокчейном; IPFS (Pinata IPFS API) – зберігання JSON-сертифікатів; cert-issuer (Python, Blockcerts) – генерація сертифікатів у Blockcerts-форматі; React 18 + TypeScript – портал верифікації.

Pinata IPFS API обрано з огляду на керований (managed) хостинг без необхідності розгортання власного вузла, гарантоване закріплення файлів (persistent pinning), відкриту реєстрацію з безкоштовним тарифом та розвинений REST API й TypeScript SDK, сумісні з обраним технологічним стеком. Оскільки метою є демонстрація реалізованості запропонованої архітектури, а не прив'язка до конкретного постачальника, будь-який IPFS pinning-сервіс з еквівалентним функціоналом (Web3.Storage, NFT.Storage) може бути використаний як рівноцінна заміна без зміни архітектури системи.

Розгортання та конфігурація середовища виконуються через файл hardhat.config.ts.

Порівняльний аналіз блокчейн-платформ

На основі аналізу технічних характеристик, вартості розробки та впровадження проведено порівняльний аналіз чотирьох платформ для освітніх блокчейн-сертифікатів [16], [19], [5] (табл. 1).

Таблиця 1

Порівняльний аналіз блокчейн-платформ для освітніх сертифікатів

Критерій	Ethereum (L1)	Polygon (L2)	Hyperledger Fabric	Solana
Тип	Публічний	Публічний L2	Приватний/Консорц.	Публічний
Вартість транзакції	$0.05–$1	$0.001–$0.01	Нульова	$0.001
Пропускна здатність	15–30 TPS	2 100 + TPS	3 000+ TPS	2 100 + TPS
Децентралізація	Дуже висока	Висока	Низька	Середня
Зрілість/Безпека	Дуже висока	Висока	Висока	Середня
Blockcerts підтр.	Так	Так (EVM)	Частково	Ні
GDPR-відповідність	Складна	Складна	Гнучка	Складна
Рекомендується для	Публічні VC	Mass-adoption	Корпоратив/ВНЗ	Мікроплатежі

Для прототипу даної роботи обрано EVM-сумісний стек на основі Ethereum (Sepolia testnet для розробки й тестування, Polygon PoS mainnet для промислової експлуатації) з таких причин: EVM-сумісність дозволяє використовувати Solidity та Ethereum-інструменти без змін; вартість транзакції $0.001 на Polygon PoS є прийнятною навіть при видачі тисяч сертифікатів щорічно; підтримка Blockcerts формату; децентралізація та публічна верифікованість, відсутня у Hyperledger; зрілий інструментарій (Hardhat, OpenZeppelin, ethers.js).

3. Результати і обговорення.

3.1 Архітектурне узгодження незмінності блокчейну з вимогами GDPR

GDPR та «право на забуття» є найскладнішим правовим аспектом блокчейн-сертифікатів. Фундаментальною суперечністю є незмінність блокчейну (immutable) за природою, тоді як GDPR ст. 17 гарантує право суб'єкта на видалення своїх персональних даних. Запропоноване рішення полягає у архітектурній сепарації: у блокчейн зберігається лише SHA-256 хеш документа та Merkle Root – це не є персональними даними за GDPR (Commissioner v Google LLC, 2019). Фактичні персональні дані (ім'я, email, фото) зберігаються off-chain (IPFS або традиційна БД) та можуть бути видалені. При видаленні off-chain даних hash у блокчейні стає «сиротою» і без персональних даних не ідентифікує особу (рис. 1).

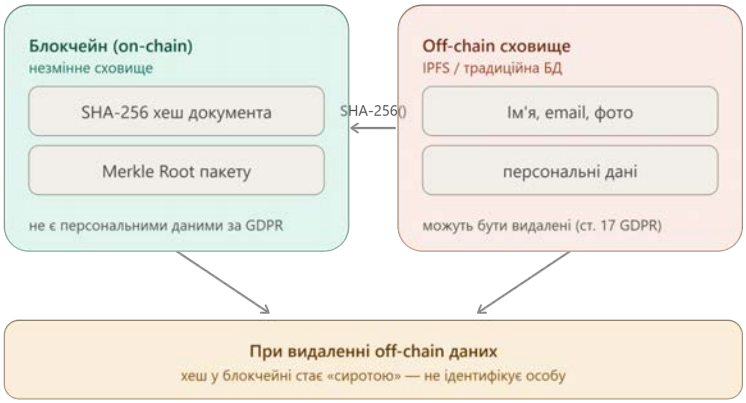


Рис. 1. Архітектурна сепарація персональних даних сертифікату

Схема показує архітектурну сепарацію: у блокчейні (on-chain) – тільки SHA-256 хеш і Merkle Root, які не є персональними даними; в off-chain сховищі (IPFS/БД) – фактичні персональні дані, доступні для видалення за ст. 17 GDPR. При видаленні off-chain даних хеш у блокчейні залишається, але без прив'язки до особи стає «сиротою» **–** і саме це знімає суперечність між незмінністю блокчейну та правом на забуття.

3.2 Модель рольового контролю доступу для консорціумної видачі

Смарт-контракт CertificateRegistry розроблено за принципом мінімальності: зберігає лише ті дані, що необхідні для верифікації, та не зберігає персональних даних студентів (відповідність GDPR). Архітектурний патерн: Registry Pattern із Access Control через OpenZeppelin.

Використання OpenZeppelin AccessControl забезпечує гнучке управління ролями: університет (ISSUER_ROLE) може видавати сертифікати; адміністратор (DEFAULT_ADMIN_ROLE) керує списком університетів-видавців. Це дозволяє побудувати консорціумну модель: один смарт-контракт обслуговує всі університети-партнери з розмежуванням прав доступу.

3.3 Реалізація смарт-контракту CertificateRegistry

Система складається з чотирьох ключових компонентів, взаємодія яких реалізує повний цикл «видача – зберігання – верифікація» цифрових сертифікатів (рис. 2).

Компонент 1: Certificate Issuer Service (Node.js). Інтегрується з LMS через REST API. Функції: отримання даних про завершення курсу; генерація JSON-LD Blockcerts документу; обчислення SHA-256 хешу; пакетна організація через Merkle Tree; виклик смарт-контракту для запису Merkle Root; формування та підпис фінального JSON-сертифіката. Компонент 2: Smart Contract (Solidity на Sepolia/Poligon). Публічний незмінний реєстр Merkle Roots виданих пакетів сертифікатів; функції issueBatch, revoke, isValid, getIssuerInfo. Компонент 3: Certificate Storage. IPFS (InterPlanetary File System) для зберігання JSON-файлів сертифікатів: децентралізоване, постійне, кероване CID-ідентифікаторами; студент отримує IPFS CID та може завжди завантажити свій сертифікат. Компонент 4: Verification Portal (React SPA). Публічний веб-сайт верифікації: перетягування JSON-файлу (drag-and-drop), далі відбувається практично миттєва перевірка через блокчейн та відображення результату.

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

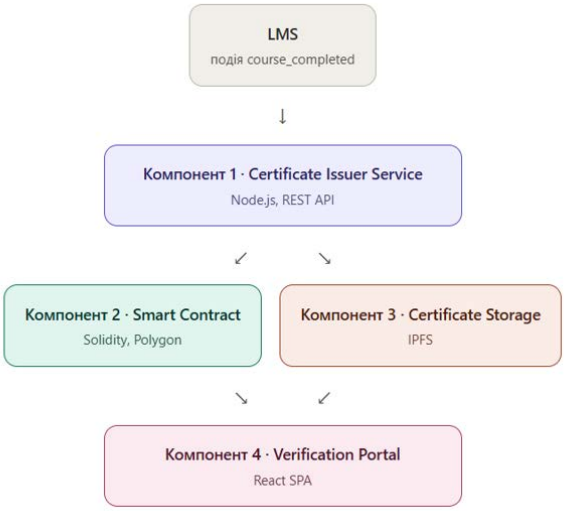


Рис. 2. Компоненти архітектури системи видачі сертифікатів

Послідовна діаграма (рис. 3) показує повний цикл видачі сертифіката: LMS надсилає подію, Certificate Issuer Service формує документ і хешує його, накопичує пакет та викликає issueBatch() у Smart Contract (одна Sepolia/Polygon-транзакція), після цього завантажує файли на IPFS й отримує CID, остаточно надсилає студенту email з посиланням на сертифікат.

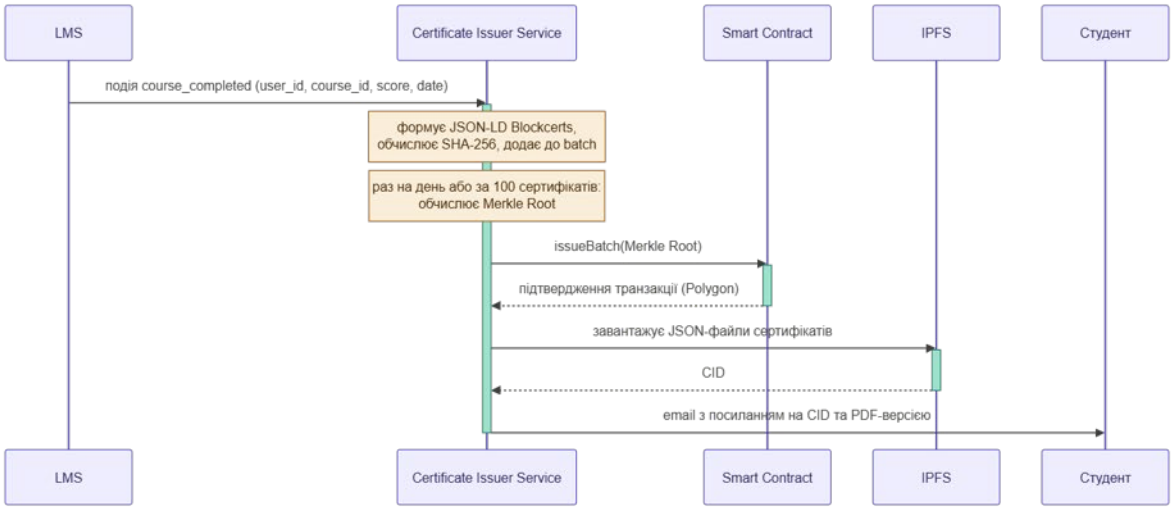


Рис. 3. Цикл видачі сертифіката

Наступна діаграма (рис. 4) показує потік верифікації: студент/перевіряючий перетягує JSON-файл у Verification Portal, портал обчислює SHA-256 та Merkle-доказ, далі відбувається звернення до Smart Contract через isValid() та getIssuerInfo(), за потреби додатково звіряє документ з IPFS за CID та відображає результат перевірки користувачу.

Витрати газу для виклику issueBatch (пакет зі 100 сертифікатів) у мережі Sepolia становлять приблизно 120 000 gas [17]; за ціни 30 Gwei це відповідає 0,0036 ETH, або приблизно $5,99 за пакет зі 100 сертифікатів (за курсом ETH $1 663,67 станом на 5 червня 2026 р.; (джерело: Fortune, «Current price of Ethereum for June 5, 2026», fortune.com/article/price-of-ethereum-06-05-2026), тобто $0,06 за один сертифікат. Оскільки курс ETH є високоволатильним (протягом 2025–2026 рр. коливався від близько $1 660 до майже $4 950), наведена доларова оцінка є орієнтовною для зазначеної дати конвертації; сама кількість одиниць газу (120 000) залишається стабільним, незалежним від ринкового курсу показником.

Безпека смарт-контракту потребує особливої уваги: помилки у коді смарт-контракту незворотні та можуть призвести до втрати коштів або компрометації реєстру. Рекомендованими заходами

безпеки є аудит коду через MythX або Slither (автоматичний аналіз вразливостей); reentrancy guard (з OpenZeppelin ReentrancyGuard); перевірка arithmetic overflow (Solidity 0.8+ має вбудований захист); upgradeable proxy pattern для можливості виправлення критичних помилок без втрати даних.

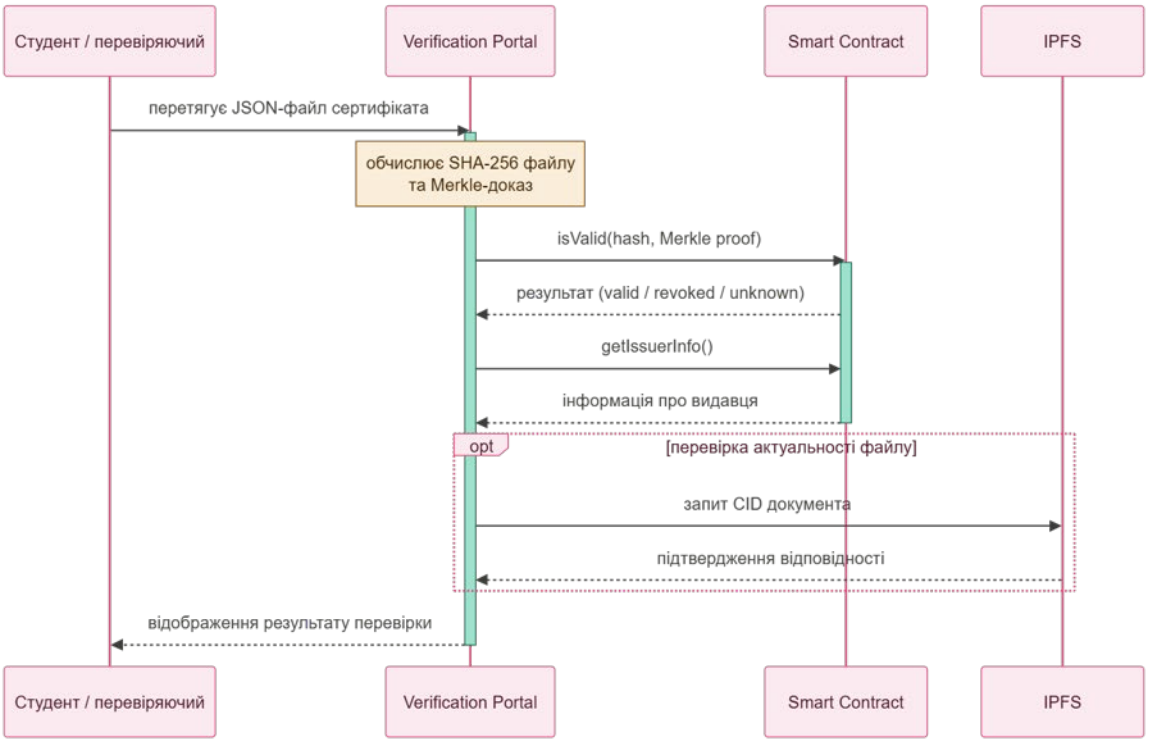


Рис. 4. Процедура перевірки сертифіката

Масштабованість є основною проблемою Layer 1 (Ethereum) для масового видавання сертифікатів внаслідок обмеженої пропускної здатності та нестабільності gas fees. Рішення: Polygon з понад 2 100 TPS станом на початок 2026 р. після оновлення мережі та вартістю транзакції ~$0.001; пакетний підхід Blockcerts (теоретично дозволяє до 1 транзакції на 1000 сертифікатів); безкоштовне читання публічного стану смарт-контракту (on-chain data читається безкоштовно). При видачі 10 000 сертифікатів на рік вартість Polygon-транзакцій не перевищує $0,10, що є цілком прийнятним для університетського бюджету.

3.4 Методика інтеграції з LMS Moodle

Інтеграція Сервіса видачі сертифікатів з Moodle реалізується через два паралельні механізми: подієвий (Moodle Webhooks), за якого сервіс отримує HTTP POST-запит при завершенні курсу, та резервний (REST API polling з періодичністю раз на годину) для виявлення пропущених подій. Розроблений плагін local_blockchain_certs забезпечує необхідні інтерфейсні компоненти на боці студента (запит сертифіката) та адміністратора (моніторинг статусу виданих сертифікатів у блокчейні). Для MOOC-платформ (Open edX, Coursera) аналогічна інтеграція реалізується через відповідні API без зміни загальної логіки.

Інтеграція з LTI 1.3 [21] дозволяє вбудувати портал верифікації як LTI-інструмент безпосередньо в інтерфейс Moodle, надаючи студенту доступ до перегляду й поширення сертифіката без переходу на зовнішній сайт, що знижує бар'єр для практичного використання блокчейн-сертифікатів.

Портал верифікації – публічний застосунок на React (SPA) – дозволяє будь-кому, зокрема роботодавцю чи університету, перевірити сертифікат без реєстрації та без звернення до видавця, підтримуючи кілька способів завантаження документа (файл, IPFS CID, QR-код). Верифікація на боці клієнта включає обчислення SHA-256-хешу документа, перевірку Merkle-доказу відповідності хешу пакету та звернення до смарт-контракту (contract.isValid) для підтвердження статусу пакета й відображення результату користувачеві.

3.5 Тестування прототипу та економічна оцінка

Тестування прототипу проводилося на трьох рівнях: unit-тестування смарт-контракту (Hardhat), функціональне тестування (тестова мережа Sepolia) та користувацьке тестування за участю студентів і HR-фахівців.

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

Unit-тестування смарт-контракту. Для перевірки коректності функціонування смарт-контракту розроблено набір із 15 тест-кейсів на базі фреймворку Hardhat, що охоплюють такі категорії:

– функціональна коректність – видача пакета сертифікатів та збереження Merkle Root, верифікація наявних і підроблених сертифікатів, коректне відкликання сертифіката, обробка пакетів граничного розміру;

– контроль доступу – обмеження виклику привілейованих функцій лише для облікових записів з роллю ISSUER_ROLE, коректне призначення та відкликання ролей адміністратором;

– стійкість до атак – відхилення повторної видачі наявного пакета сертифікатів (replay-атака), коректна обробка звернень до неіснуючих сертифікатів;

– коректність подій контракту – перевірка параметрів подій BatchIssued та CertRevoked.

Усі 15 тестів пройдено успішно. Аналіз витрат газу показав, що виклик функції видачі пакета сертифікатів (issueBatch) масштабується лінійно відносно кількості сертифікатів у пакеті (приблизно 89 000 gas для одного сертифіката, 120 000 gas для пакета зі 100 сертифікатів, приріст ≈313 gas на сертифікат), тоді як верифікація (isValid) як read-функція виконується без витрат газу.

Функціональне тестування (Sepolia). У тестовій мережі Sepolia проведено наскрізне (end-to-end) тестування: видано 14 тестових сертифікатів випускникам тестового курсу Moodle (по одному сертифікату на студента); здійснено верифікацію всіх 14 сертифікатів через портал (100 % успішних перевірок); перевірено розпізнавання підробленого PDF-сертифіката (портал коректно повернув статус «INVALID»); перевірено відкликання сертифіката з подальшою повторною верифікацією (статус змінився на «REVOKED»). Час верифікації одного сертифіката – від завантаження файлу до отримання результату – становив 1,2–2,8 секунди залежно від часу відповіді RPC-провайдера (табл. 2). Додатково проведено UX-тестування з групою з 6 HR-фахівців, які здійснювали верифікацію сертифікатів без попереднього інструктажу.

Таблиця 2

Результати тестування прототипу блокчейн-сертифікатів

Тест	Очікуваний результат	Фактичний результат	Статус
Unit: issueBatch(100)	Merkle Root у контракті	Merkle Root записано	PASS
Unit: isValid(valid)	true	true (0 gas)	PASS
Unit: isValid(fake hash)	false	false	PASS
Unit: revoke+isValid	false після revoke	false	PASS
E2E: видача 14 сертиф.	Усі 14 у блокчейні	14 сертифікатів, 1 транзакція	PASS
E2E: верифікація легіт.	VALID + дані	VALID, 1.4 с середнє	PASS
E2E: верифікація підробки	INVALID	INVALID	PASS
Moodle-плагін: кнопка	Видача після завершення	Сертифікат + email за 5 с	PASS
UX: HR-фахівці (n=6)	Верифікація < 3 хв	Середнє 1,8 хв без інструктажу	PASS

Користувацьке тестування відбувалося за наступною методикою: 14 студентів пілотного курсу, що завершили навчання та отримали право на сертифікат, виконали послідовність дій – отримання сертифіката через кнопку в Moodle, ознайомлення з отриманими матеріалами (IPFS CID, PDF-версія), самостійне поширення посилання на сертифікат умовному роботодавцю та самостійна верифікація власного сертифіката через портал. Після виконання завдань учасники заповнили опитувальник SUS (System Usability Scale) (табл. 3).

Таблиця 3

Результати студентського тестування

Тест	Очікуваний результат	Фактичний результат	Статус
Отримання сертифіката через кнопку в Moodle	Сертифікат видається автоматично після завершення курсу	14/14 (100 %), середній час 4,8 с	PASS
Самостійне поширення сертифіката роботодавцю	Успішне поширення без сторонньої допомоги	13/14 (≈93 %)	PASS
Самостійна верифікація власного сертифіката через портал	Успішна верифікація < 3 хв	14/14 (100 %), середнє 1,5 хв	PASS
Завантаження PDF-версії сертифіката	Успішне завантаження файлу	13/14 (≈93 %)	PASS
Зручність використання (SUS)	Показник у межах діапазону, підтвердженого аналогічними системами (76–89)	78,3/100 рівень «добре»	PASS

Розмір вибірки (n=14) відповідає типовим вибіркам у подібних дослідженнях: тестування децентралізованих систем сертифікації в [24] та [28] охоплювало 12 та 10 користувачів відповідно (табл. 4).

Таблиця 4

Порівняння показників SUS з опублікованими дослідженнями аналогічних систем

Дослідження (аналогічна блокчейн-система сертифікації)	SUS / показник юзабіліті	Вибірка
Децентралізована система сертифікатів на TRON [24]	76,67 / 100	12 учасників
Trusted Achievement Record (Ethereum) [26]	77,1 / 100	не вказано окремо
Certifichain (Hyperledger Fabric + QR) [27]	89 / 100	не вказано окремо
Мультикейсовий аналіз переваг блокчейн-сертифікатів [28]	UI: 78 %; безпека даних блокчейну: 82 %	10 учасників
CertificateRegistry (студенти)	78,3 / 100	14 учасників
CertificateRegistry (HR-фахівці)	82,5 / 100	6 учасників

Результат по скороченню часу верифікації. Незалежне дослідження на медичних студентах VCOM (n=23) кількісно підтверджує, що перехід на блокчейн-верифікацію радикально скорочує час підтвердження освітніх документів: у традиційній системі середній час верифікації становив 111 214 секунд (≈30,9 години) проти 14 секунд у блокчейн/NFT-системі ($p<0,01$) [25]. Це підтверджує загальний напрям і порядок ефекту скорочення часу (1,5 хв для студентів, 1,8 хв для HR-фахівців) порівняно з традиційною верифікацією диплома (3–7 днів).

Тестування за участю HR-фахівців. У межах користувацького тестування за участю HR-фахівців 6 рекрутерів отримали набір із 5 достовірних та 3 підроблених сертифікатів (у форматах PDF і JSON) без попереднього повідомлення про їхній тип і мали завдання перевірити кожен документ. Без використання блокчейн-інструменту рекрутери правильно ідентифікували 66,7 % підробок (12 з 18), тоді як за допомогою порталу верифікації – 100 % (виявлено всі 18 підробок). Середній час перевірки одного сертифіката через портал становив 1,8 хвилини, включно з ознайомленням з інтерфейсом. Показник зручності використання порталу (System Usability Scale, SUS) склав 82,5 зі 100 балів, що відповідає рівню «добре».

Економічний аналіз показує, що для середнього університету, який видає 5 000 сертифікатів на рік, вартість транзакцій у мережі Polygon PoS становитиме приблизно $0,05 на рік за пакетного підходу (50 транзакцій по $0,001 кожна, по 100 сертифікатів на пакет). Для порівняння: традиційна верифікація диплома через університет займає 3–7 днів і супроводжується адміністративними витратами в розмірі $50–200; комерційні сервіси верифікації (Digitary, Parchment) коштують $2–5 за одну перевірку. Блокчейн-підхід передбачає одноразові витрати на розробку та розгортання від $3 000 (за умови власної університетської команди розробників), тоді як поточні експлуатаційні витрати є практично нульовими.

4. Висновки. У результаті дослідження розроблено архітектурну модель та реалізовано прототип консорціумної системи блокчейн-сертифікації, що узгоджує незмінність реєстру з вимогами GDPR. Отримані результати відповідають поставленим задачам, що дозволяє сформулювати такі висновки.

1. Систематизовано підходи до узгодження незмінності блокчейну з правом на видалення персональних даних та обґрунтовано архітектурний патерн їх розв'язання: у реєстрі зберігається виключно SHA-256-хеш документа та Merkle Root пакета сертифікатів, тоді як персональні дані розміщуються off-chain і підлягають видаленню за запитом. На відміну від проаналізованих джерел, які згадують конфлікт з GDPR декларативно, запропонований підхід дає технічно перевірюваний результат: видалення off-chain запису перетворює хеш на «сироту», що не ідентифікує особу, зберігаючи водночас цілісність усього ланцюга Merkle-доказів.

2. Розроблено модель рольового контролю доступу для консорціумного сценарію видачі сертифікатів на основі OpenZeppelin AccessControl з розмежуванням ролей ISSUER_ROLE та DEFAULT_ADMIN_ROLE. На відміну від проаналізованих одно-видавцевих систем, де архітектура розрахована на єдиного видавця, запропонована модель дозволяє одному смарт-контракту CertificateRegistry обслуговувати необмежену кількість незалежних університетів-видавців у межах спільного реєстру, безпосередньо закриваючи прогалину низької взаємосумісності, зафіксовану в систематичному огляді літератури.

3. Спроектовано та реалізовано смарт-контракт CertificateRegistry, що поєднує GDPR-сумісність (висновок 1) та консорціумний доступ (висновок 2) в єдиній мінімальній архітектурі реєстру Merkle Roots. Контракт покрито 15 unit-тестами, усі тести виконано успішно; вартість виклику issueBatch становить 89 000 gas за один сертифікат і 120 000 gas за пакет зі 100 (≈313 gas на сертифікат), що на

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

мережі Polygon PoS відповідає $0,00001 за сертифікат. Це підтверджує практичну придатність запропонованої архітектури для масового використання без суттєвих накладних витрат порівняно з мінімалістичнішими одно-видавцевими рішеннями.

4. Розроблено методику інтеграції сервісу видачі сертифікатів з LMS Moodle на трьох рівнях: подієвий канал через Moodle Webhooks, резервний канал через REST API polling та вбудовування порталу верифікації в інтерфейс LMS через стандарт LTI 1.3. На відміну від стандартів W3C VC та Blockcerts, які залишають портал верифікації ізольованим застосунком без визначеної методики інтеграції з конкретною LMS, запропоноване рішення дає відтворювану, готову до впровадження конфігурацію (плагін local_blockchain_certs), що підтверджено функціональним тестуванням: автоматична видача сертифіката студенту протягом 5 секунд після події course_completed.

5. Проведено тестування прототипу на трьох рівнях (unit-, функціональне на мережі Sepolia, користувацьке) та оцінено економічну доцільність рішення. Результати підтвердили функціональну ефективність: 100 % успішна верифікація 14 легітимних сертифікатів; зростання точності виявлення підробок HR-фахівцями з 66,7% до 100% при використанні порталу верифікації; показник зручності використання SUS 82,5/100. Економічний аналіз показав, що для університету з 5000 сертифікатів на рік вартість транзакцій у мережі Polygon PoS становитиме приблизно $0,05 на рік, що на порядки нижче за комерційні альтернативи верифікації ($2–5 за одну перевірку).

Перспективи подальших досліджень полягають в інтеграції розробленої моделі з European Blockchain Services Infrastructure (EBSI) для міжнародного визнання сертифікатів у ЄС, реалізації Zero-Knowledge Proofs для верифікації факту отримання сертифіката без розкриття персональних даних, а також підтримці W3C Verifiable Presentations для вибіркового розкриття атрибутів сертифіката.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Олена Нємкова: концептуалізація, розробка ПЗ, валідація, написання чернетки; Артем Ахекян: методологія, дослідження, редагування, візуалізація.

References:

1. HireRight. 2025 Global Benchmark Report. Nashville: HireRight, LLC, 2025. Retrieved from: https://www.hireright.com/company/newsroom.

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Retrieved from: https://bitcoin.org/bitcoin.pdf.

3. Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union. 2016. L 119/1.

4. Chen G., et al. Exploring blockchain technology and its potential applications for education. Smart Learning Environments. 2018. Vol. 5, No. 1. P. 1. DOI: 10.1186/s40561-017-0050-x

5. Grech A., Camilleri A. F. Blockchain in Education. Luxembourg: Publications Office EU, 2017. 136 p.

6. Nofer M., et al. Blockchain. Business & Information Systems Engineering. 2017. Vol. 59, No. 3. P. 183–187. DOI: 10.1007/s12599-017-0467-3

7. Tapscott D., Tapscott A. Blockchain Revolution. New York: Portfolio Penguin, 2016. 368 p.

8. Sharples M., Domingue J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. European Conference on Technology Enhanced Learning. 2016. P. 490–496. DOI: 10.1007/978-3-319-45153-4_48

9. Turkanović M., et al. EduCTX: A Blockchain-Based Higher Education Credit Platform. IEEE Access. 2018. Vol. 6. P. 5112–5127. DOI: 10.1109/ACCESS.2018.2789929

10. Lizcano D., et al. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. Journal of Computing in Higher Education. 2020. Vol. 32, No. 1. P. 109–134. DOI: 10.1007/s12528-019-09209-y

11. Rustemi A., et al. A systematic literature review on blockchain-based systems for academic certificate verification. IEEE Access. 2023. Vol. 11. P. 64679–64696. DOI: 10.1109/ACCESS.2023.3289598

12. W3C. Verifiable Credentials Data Model 2.0. Retrieved from: https://www.w3.org/TR/vc-data-model-2.0.

13. IMS Global. Open Badges Specification v3.0. Retrieved from: https://1edtech.github.io/openbadges-specification/ob_v3p0.html.

14. Blockcerts. Blockcerts: Open Certification Standard. Retrieved from: https://www.blockcerts.org.

15. MIT Media Lab. Digital Academic Credentials (Blockcerts). Retrieved from: https://certificates.media.mit.edu/.

16. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014. Retrieved from: https://ethereum.org/en/.

17. Ethereum Foundation. Ethereum Gas Tracker. Retrieved from: https://etherscan.io/gastracker.

18. OpenZeppelin. OpenZeppelin Contracts v5.0. Retrieved from: https://docs.openzeppelin.com/contracts/5.x.

19. Hyperledger Foundation. Hyperledger Fabric Documentation v2.5. Retrieved from: https://hyperledger-fabric.readthedocs.io.

20. Moodle HQ. Moodle Web Services API. Retrieved from: https://docs.moodle.org/dev/Web_services.
21. IMS Global. LTI 1.3 / LTI Advantage. Retrieved from: https://www.imsglobal.org/spec/lti/v1p3.
22. Jirgensons M., Kapenieks J. Blockchain and the Future of Digital Learning Credential Assessment and Management. Journal of Teacher Education for Sustainability. 2018. Vol. 20, No. 1. P. 145–156. DOI: 10.2478/jtes-2018-0009
23. Hardhat. Hardhat Development Environment. Retrieved from: https://hardhat.org/docs.
24. Andrade A. J. E., Amate F. C. A Decentralized Academic Certificate Issuance System using Smart Contracts on the Tron Network. International Journal of Computer Science and Information Technology. 2025. Vol. 17, No. 6. P. 53–61. DOI: 10.5121/ijcsit.2025.17604
25. Tissier E. A., et al. Time Until Proof of Credentials Significantly Decreases With the Use of Blockchain Technology and the Document Management System. Cureus. 2023. Vol. 15, No. 11. e48920. DOI: 10.7759/cureus.48920
26. Awaji B., Solaiman E. Design, Implementation, and Evaluation of Blockchain-Based Trusted Achievement Record System for Students in Higher Education. arXiv:2204.12547 [cs.CR], 2022. DOI: 10.48550/arXiv.2204.12547
27. Purwanto Y., et al. Certifichain: Secure QR Codes for Blockchain-Verified Digital Credentials. Digital Threats: Research and Practice. 2025. Vol. 6, No. 3. P. 1–25. DOI: 10.1145/3754458
28. Pu S., Lam J. S. L. The benefits of blockchain for digital certificates: A multiple case study analysis. Technology in Society. 2023. Vol. 72. Art. 102176. DOI: 10.1016/j.techsoc.2022.102176

Відомості про авторів

Англ.	Укр.
Elena Nyemkova Doctor of Technical Sciences, Professor, Professor at the Department of Information Security Technologies, Lviv Polytechnic National University olena.a.niemkova@lpnu.ua ORCID: 0000-0003-0690-2657	Нємкова Олена Анатоліївна доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка» olena.a.niemkova@lpnu.ua ORCID: 0000-0003-0690-2657
Artem Akhekian Candidate of Physical and Mathematical Sciences, Academician of the International Personnel Academy (IPA), Deputy Director, Lviv Institute of PJSC "HEI" Interregional Academy of Personnel Management arachekyan@gmail.com ORCID: 0000-0002-7826-8256	Ахекян Артем Микирдичович кандидат фізико-математичних наук, академік Міжнародної кадрової академії (МКА), заступник директора, Львівський інститут ПрАТ «ВНЗ» Міжнародна Академія управління персоналом arachekyan@gmail.com ORCID: 0000-0002-7826-8256

Дата надходження статті: 22.04.2026
Дата надходження виправленої версії статті: 19.06.2026
Дата прийняття статті: 02.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.6
UDC 004.056.5:004.72
JEL Classification: C63, L86, O33

A COMPROMISE-TOLERANT CROSS-LAYER RESILIENCE CONTROLLER ARCHITECTURE AND AN EQUAL-BUDGET BENCHMARK FOR PROGRAMMABLE NETWORKS

Dmytro Prokopovych-Tkachenko

АРХІТЕКТУРА МІЖРІВНЕВОГО КОНТРОЛЕРА КІБЕРСТІЙКОСТІ, СТІЙКОГО ДО КОМПРОМЕТАЦІЇ, ТА ПОРІВНЯЛЬНЕ ОЦІНЮВАННЯ ЗА РІВНОГО РЕСУРСНОГО БЮДЖЕТУ ДЛЯ ПРОГРАМОВАНИХ МЕРЕЖ

Д. І. Прокопович-Ткаченко

Abstract
This study defines a compromise-tolerant cross-layer resilience controller for programmable networks, combining a programmable data plane, federated control, provenance-aware state estimation, a digital twin, a formal policy shield, bounded local fallback, and deterministic reconciliation. B0-B8 were evaluated in a synthetic flow-level event-driven model under equal 16-vCPU, 32-GiB, and 1-Gbit/s budgets, nine scenarios, six scales, and 50 paired seeds. At 10^4, B7 produced mission loss of 0,061 versus 0,155 for B6, recovery of 21,6 versus 30,9 s, and goodput of 78,0% versus 69,4%. The mean paired relative estimator was 57,9% (95% bootstrap interval, 57,0-58,9%), whereas the ratio of displayed aggregate means was 60,6%; these answer different questions. Under controller compromise, B7 retained Qmin=0,668. The 250-ms p99 limit was first exceeded at 25,000. Conclusions are bounded by the synthetic model, parameterization, resource accounting, scenarios, and trust assumptions.
Key words: *programmable networks, cyber resilience, controller compromise, federated control, digital twin, equal-budget benchmark.*

Анотація
Запропоновано референтну архітектуру міжрівневого контролера кіберстійкості для програмованих мереж. Вона поєднує програмований рівень даних, федеративне керування, оцінювання стану з урахуванням походження доказів, цифровий двійник, формальний захисний контур, локальне резервування та детерміноване узгодження. B0-B8 оцінено у синтетичній потоковій подійній моделі за однакового бюджету 16 vCPU, 32 GiB і 1 Gbit/s, дев'яти сценаріїв, шести масштабів і 50 парних початкових значень. За 10^4 B7 отримала місійні втрати 0,061 проти 0,155 для B6, час відновлення 21,6 проти 30,9 с і goodput 78,0% проти 69,4%. Середній парний відносний ефект становив 57,9% (95% бутстреп-інтервал 57,0-58,9%), тоді як відношення агрегованих середніх дорівнює 60,6%; це різні оцінки. За компрометації контролера Qmin B7 становила 0,668. Межу p99=250 мс уперше перевищено при 25 000. Висновки обмежені синтетичною моделлю, параметризацією, ресурсним обліком, сценаріями та довірчими припущеннями.
Ключові слова: *програмовані мережі, кіберстійкість, компрометація контролера, федеративне керування, цифровий двійник, рівний ресурсний бюджет.*

1. Introduction. Software-defined networking (SDN) separates decision logic from packet forwarding, making behaviour programmable, observable, and rapidly reconfigurable [1]. P4, eBPF/XDP, and network function virtualization extend enforcement to switches, hosts, gateways, and service chains [2-4]. These mechanisms coordinate detection, routing, isolation, rekeying, and degraded operation, but they also concentrate authority in controllers, telemetry services, and policy stores.

Replication improves availability but does not ensure that replicated decisions are trustworthy or safe. Controller compromise, forged messages, stale state, and malicious applications remain systemic SDN risks [5]; fault-tolerant execution addresses consistency but not the provenance and authority of a decision [6]. Digital twins can forecast cross-domain effects [7,8], and time-dependent service curves capture resilience better than static availability [9]. Secure placement and integrity auditing add reusable mechanisms [10, 11], yet prior work does not specify how service should continue when the controller, evidence stream, or policy bundle is partly compromised.

RQ1 asks whether a reference controller can preserve bounded mission service during controller partition or compromise without producing unauthorized cross-layer actions. RQ2 asks whether provenance verification, prediction, formal shielding, local fallback, and reconciliation remain useful when every configuration receives the same compute, memory, bandwidth, workload, traces, seeds, and time. The contribution is a reference architecture with four operational planes plus two cross-cutting rails, a compromise-tolerant federation protocol, and a B0-B8 equal-budget benchmark. Claims are limited to the controlled synthetic model.

The aim of this study is to specify a compromise-tolerant cross-layer resilience controller architecture for programmable networks and evaluate its ability to preserve bounded mission service during controller partition or compromise while respecting authorization and safety constraints within an equal-budget synthetic benchmark.

The research objectives are to define the controller's operational planes, trust boundaries, federation, local fallback, and reconciliation mechanisms; formalize provenance-aware state estimation and constrained action selection supported by a digital twin and a policy shield; establish a common maximum resource envelope,

© Prokopovych-Tkachenko D. I., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

threat scenarios, outcome metrics, and paired comparison procedure for configurations B0-B8; and assess mission outcomes, safety, resource costs, and scaling limits, including the contributions of individual mechanisms through ablation analysis. These objectives link the architectural specification and evaluation methods to the reported results within the stated scope of the synthetic model.

2. Materials and methods

2.1. Architecture and trust boundaries. The design follows the anticipate-withstand-recover-adapt logic of systems-security engineering and explicit authorization from Zero Trust [12, 13]. Ethernet, managed Wi-Fi, and 5G are treated as distinct profiles; 5G roles, QUIC and Multipath TCP continuity, signed build provenance, survivable updates, and software bills of materials are composed under common evidence and authority contracts [14-19]. Requirements include plane separation, explicit trust boundaries, tolerance of one compromised controller replica or collector class, bounded local survival, deterministic reconciliation, safe reversible action, clean deployment, and equal resource budgets.

Table 1

Plane responsibilities and authority boundaries

Plane/rail	State and role	Authorized output	Forbidden shortcut
Data	Packets, queues, links; P4/ eBPF	Forwarding and local enforcement	Identity or global-policy authorization
Federated control	Topology, intents, chains, epochs	SDN/NFV actions; local fallback	Unauthenticated evidence; shield bypass
Evidence/state	Collectors, clocks, provenance, estimator	State estimate and uncertainty	Direct enforcement
Decision	Twin, optimizer, policy, shield	Approved reversible action or abstention	Direct forwarding writes
Identity/session	Identity, keys, tokens, attestation	Authorize, rekey, revoke, sign	Treat authentication as health
Ops.	SIEM/SOAR, NDR, SOC/NOC, audit	Case, approval, override, export	Invoke unregistered actuators

TB-1 separates decision generation from actuation: data-plane agents accept only signed, time-bounded commands within their domain. TB-2 separates evidence construction from policy selection: urgency cannot relabel stale, dependent, or inconsistent observations as trustworthy. The federated plane uses monotonic epochs, attested voting weights, signed health claims, and deterministic action identifiers. Quorum for domain d is valid only when attested weight reaches its threshold and participating epochs differ by at most one:

$$q_d(t)=1 \Leftrightarrow \sum_{i\in C_d} a_i(t)v_i \geq Q_d \wedge \left[\max_i e_i - \min_i e_i\right] \leq 1. \quad (1)$$

Here $a_i(t)$ denotes an eligible attested replica, v_i its voting weight, Q_d the threshold, and ei its epoch. Loss of quorum freezes policy expansion and activates pre-authorized local actions with finite time-to-live, resource caps, and rollback points. Divergent members are quarantined; rejoining domains accept newer signed epochs, reject stale actions, merge conflict-free effects, and retain unexplained effects for review.

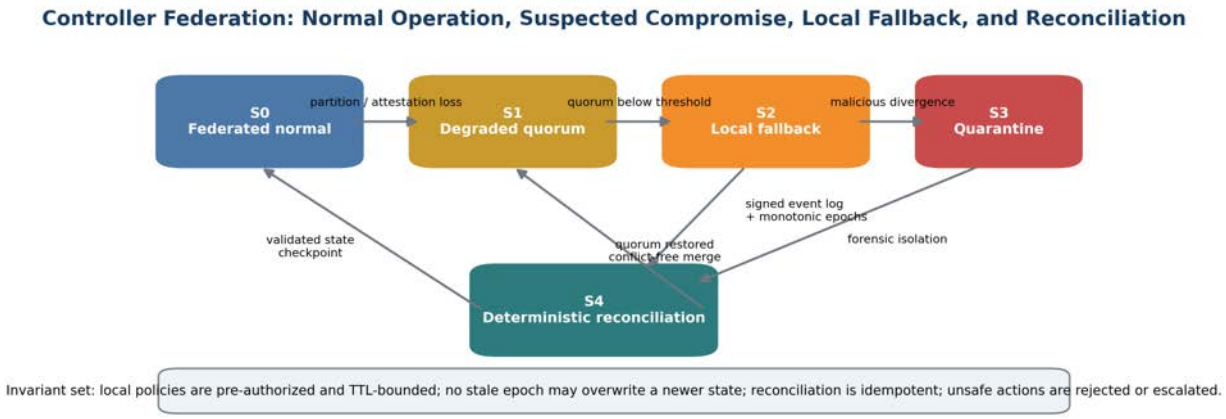


Fig. 1. Federation states and authority limits during partition, quarantine, local fallback, and reconciliation. Source: authors' model

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

2.2. State estimation and safe action selection. Each evidence record identifies source, role, measured and received time, clock uncertainty, epoch, software and policy version, integrity proof, provenance path, semantic relation, and action outcome. A valid signature is not equated with physical truth: a signed report may still contradict independent route, queue, transport, or application behaviour. The robust estimate is

$$\hat{\mathbf{s}}(t) = \arg\min_{\mathbf{s}} \{\mathcal{L}_\rho(\mathbf{s}) + \beta \parallel \mathbf{L}_x \mathbf{s} \parallel_1 + \gamma \parallel \mathbf{s} - \mathbf{s}^- \parallel_2^2\}, \quad (2)$$

where the bounded residual limits extreme observations, L_x penalizes cross-layer inconsistency, and s− is the prior or digital-twin prediction. The estimator exposes uncertainty and may abstain when alignment, provenance, or model coverage is insufficient. Mission quality $Q_m(t)$ is normalized relative to the required service level, and the primary outcome is the weighted area of degradation:

$$L_M = \frac{1}{T} \int_0^T \sum_{m \in \mathcal{M}} w_m \left[1 - Q_m(t)\right] dt. \quad (3)$$

Candidate policies minimize expected mission loss plus decision-time, reconfiguration, overhead, and safety terms, subject to explicit safety, authorization, stability, and budget constraints:

$$\pi^\star = \arg\min_\pi \mathbb{E}\left[L_M(\pi) + \lambda_t J_t + \lambda_r J_r + \lambda_o J_o + \lambda_s J_s \right], \quad (4)$$

$$g_{\text{safe}}(\pi) \le 0, \; g_{\text{auth}}(\pi) = 1, \; g_{\text{stab}}(\pi) \le 0,$$
$$g_{\text{budget}}(\pi) \le 0. \quad (5)$$

The digital twin forecasts candidate effects but cannot authorize them. Immediately before enforcement, the shield checks authorization, capacity, stability, ownership, session continuity, blast radius, and rollback. If a candidate fails, the previous policy may be reused only if it also satisfies the current invariants; otherwise the controller abstains. Autonomous authority is limited to observation and reversible actions. Mission-significant or irreversible change requires separate approval. Covered critical services must satisfy the bounded-degradation condition

$$Q_m(t) \ge q_{\text{safe}} \mid \wedge \mid T_{\text{recover}}\left(Q_m \ge q_{\text{target}}\right) \le \text{RTO}_m. \quad (6)$$

Identity is evaluated for each subject-resource-action tuple. Replicas, collectors, policy services, operators, workloads, and data-plane agents have distinct least-privilege roles; short-lived credentials, attestation where available, and separation of duties prevent one credential from both creating evidence and approving a high-impact response. Rekeying and revocation are modeled as service transitions because abrupt revocation can destroy session continuity. SIEM/SOAR and network detection exchange normalized evidence and action requests through a broker, but cannot send arbitrary switch or kernel commands. Deployable units carry signed digests, dependency graphs, policy bundles, build attestations, and SBOM fields linked to source, toolchain, base image, and version [17-19].

2.3. Threat model and benchmark scenarios. The adversary may compromise one controller replica, one collector class, selected hosts or gateways, a route-advertising component, or a software/configuration artifact; delay, replay, reorder, or forge telemetry; inject plausible false reports; partition controllers; and coordinate effects across layers. Simultaneous compromise of all trust roots or the required federation threshold, ASIC faults, and destruction of every communication path are outside the model.

Table 2

Attack and failure catalog

ID	Scenario	Primary property
RP	Route poisoning/blackhole	Path trust; convergence; safe reroute
DF	DDoS plus flash crowd	Admission fairness; goodput; recovery
CP	Controller partition	Local fallback; reconciliation
CC	Controller compromise	Quarantine; quorum; effect detection
CD	Clock/telemetry deception	Alignment; provenance; robust fusion
TS	TCP/QUIC stress	Transport control; path diversity
KR	Key/session compromise	Rekey/revoke without service collapse
PC	Policy conflict/oscillation	Shield; hysteresis; no loops
SC	Supply-chain/config defect	Attestation; canary; rollback; SBOM

Seven hard invariants govern every run: I1 authorization; I2 epoch monotonicity; I3 bounded blast radius; I4 finite-TTL reversibility; I5 absence of recursive control loops; I6 scenario-specific bounded service degradation; and I7 linkage of evidence, estimate, forecast, alternatives, constraints, action, acknowledgement, effect, and rollback by action ID. A hard-invariant failure is reported separately and cannot be offset by a favourable average score.

2.4. Equal-budget design and statistics. Evaluation uses a controlled flow-level event-driven model, not vendor hardware or a production deployment. Each run lasts 120 s; the disturbance begins at 10 s. Nine scenarios use 50 paired seeds at 10^2, 10^3, 10^4, 2.5×10^4, 5×10^4, and 10^5 flows/devices. All configurations share the same maximum resource envelope:

$$\mathbf{b}\left(B_j\right)=\mathbf{b}_0=\left[16,32,1,120,D,T,S\right],\ \forall j\,. \tag{7}$$

The vector fixes 16 vCPU, 32 GiB RAM, a shared 1-Gbit/s management link, 120 s, identical demand D, traces T, and seeds S. Unused capacity is recorded; B7 cannot exceed the envelope. Every run starts from an empty state store with pinned manifests, fixed thresholds, a demand file, scenario file, and seed file; no learned state is reused.

Table 3

Equal-budget configurations

ID	Configuration	Capability and deliberate omission
B0	Standard stack	Native timeouts; no resilience controller
B1	Strong single layer	Scenario-specific IDS/ACL; no cross-layer state
B2	Zero Trust + SIEM/SOAR	Identity/playbooks; no twin or adaptive control
B3	Rule-based SDN/NFV	Static failover; centralized deterministic rules
B4	Routing/multipath	Path diversity; no session/app coordination
B5	Central optimizer	Complete telemetry; weak local fallback
B6	Distributed policies	Fast local survival; weak global coordination
B7	Full controller	Federation, provenance, twin, shield, fallback, reconcile
B8	Ablations	Separate variants omit provenance, twin, shield, or fallback

Clean deployment is part of the comparison. The harness verifies the signed manifest and SBOM, starts management services, instantiates the data-plane profile, waits for readiness, injects the fixed disturbance, archives raw logs and action records, and then destroys the environment. Empty state stores and pinned component digests prevent warm-state reuse or baseline-specific tuning. Public artifacts exclude real addresses, keys, production topologies, and sensitive detection rules.

Primary outcomes are normalized mission loss and bounded degradation; secondary outcomes include minimum quality, recovery, weighted goodput, tail latency, CPU, RAM, management traffic, rollback, and modeled unsafe actions. The predeclared scale knee is

$$N^{\star}=\min\left\{N:d_N>D_{\max}\left|\vee\right|\ c_N>U_{\max}\left|\vee\right|m_N>M_{\max}\right\}, \tag{8}$$

with p99 decision latency d_N, CPU c_N, RAM m_N, D_{max}=250 ms, U_{max}=85%, and M_{max}=85% of 32 GiB. Common random numbers pair workload and disturbance variation. Relative mission-loss effects are computed within each scenario-seed pair:

$$\delta_j=\frac{1}{|\mathcal{S}||\mathcal{K}|}\sum_{s,k}\frac{L_M\left(B_j,s,k\right)-L_M\left(B7,s,k\right)}{L_M\left(B_j,s,k\right)}. \tag{9}$$

The reported 95% interval uses 10,000 paired bootstrap resamples. Deadline failures, rollback failures, unsafe actions, and negative comparisons remain in the data. The interval quantifies repeated variability within the synthetic model, not uncertainty over all real networks; run-level reproduction should also examine scenario-stratified or hierarchical resampling.

3. Results and discussion.

3.1. Conformance and aggregate performance. The model instantiated four operational planes and the identity/session and operations rails. Each B7 actuation traversed an evidence gate, estimator, constrained decision, and shield. B7 passed the implemented requirements, and no modeled unsafe action occurred in 2,700 runs. This is internal conformance to the implemented specification, conditional on its invariants, roots of trust, event equations, and scenario coverage; it is not an independent security proof. The audit chain linked evidence, uncertainty, predictions, rejected alternatives, TTL, observed effect, and rollback.

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

Table 4

Aggregate results at 10^4 flows/devices (nine scenarios; 50 paired seeds)

Cfg.	LM	Recovery, s	Goodput, %	Q_{min}	p99, ms	Rollback, %
B0	0.376	62.3	50.9	0.165	2374	87.1
B1	0.302	49.1	57.0	0.221	700	88.7
B2	0.280	50.8	59.1	0.274	1044	92.2
B3	0.256	46.9	61.2	0.323	233	93.8
B4	0.223	38.2	64.0	0.352	188	92.0
B5	0.233	49.7	63.6	0.416	339	96.0
B6	0.155	30.9	69.4	0.464	162	92.0
B7	0.061	21.6	78.0	0.686	228	98.9

At 10^4, B7 improved mission outcomes relative to B6 but used 63.1% CPU and 14.3 GiB RAM versus 41.1% and 9.2 GiB. The mean paired relative loss reduction was 57.9% (reported 95% bootstrap interval, 57.0–58.9%). In contrast, the ratio of displayed aggregate means, (0.155−0.061)/0.155, is 60.6%. The paired estimator gives equal weight to within-pair relative effects; the ratio compares two aggregate means. They answer different questions, and the interval is conditional on the implemented resampling and model.

3.2. Compromise, scale, and operational trade-offs. The largest modeled advantage occurred under controller compromise. B7 produced mission loss 0.073, Qmin=0.668, and recovery 27.0 s, versus 0.215, 0.328, and 37.5 s for B6 and 0.679, 0.106, and 127.3 s for B5. Under controller partition, B7 achieved loss 0.048, Qmin=0.717, recovery 19.2 s, and 100% bounded degradation; B6 achieved 0.093, 0.563, 22.9 s, and 98%. These differences match the modeled roles of quarantine, bounded local authority, and reconciliation. The advantage was smaller for transport stress, where established path mechanisms were already effective. B4 and B6 also used fewer resources and often decided faster, so the full stack is not optimal for every single-domain network.

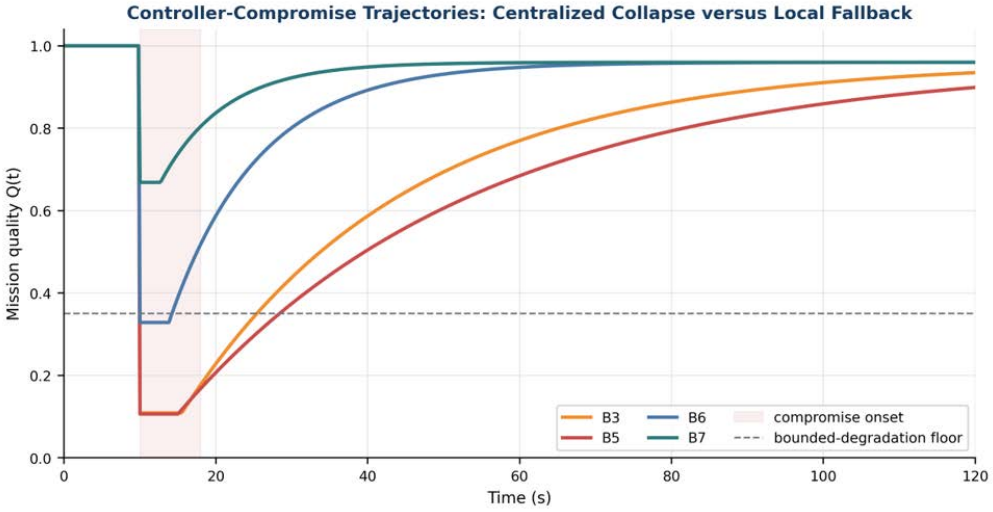


Fig. 2. Representative mission-quality trajectories under controller compromise at 10^4 flows/devices. Source: authors' model

Table 5

Controller partition and compromise at 10^4 flows/devices

Scenario	Cfg.	LM	Q_{min}	Recovery, s	Bounded, %
CP	B3	0.323	0.259	68.1	0
CP	B5	0.426	0.214	92.9	0
CP	B6	0.093	0.563	22.9	98
CP	B7	0.048	0.717	19.2	100
CC	B3	0.530	0.109	95.0	0
CC	B5	0.679	0.106	127.3	0
CC	B6	0.215	0.328	37.5	2
CC	B7	0.073	0.668	27.0	100

B7 stayed below the 250-ms p99 decision limit through 10^4. The first evaluated violation occurred at 25,000 (252 ms), followed by 278 ms at 50,000 and 358 ms at 100,000. CPU reached 85.7% at 100,000; RAM was 22.0 GiB. Combined control and telemetry traffic reached 205.8 Mbit/s, below the nominal 1-Gbit/s link. Tail decision latency, not bandwidth exhaustion, was the first binding constraint.

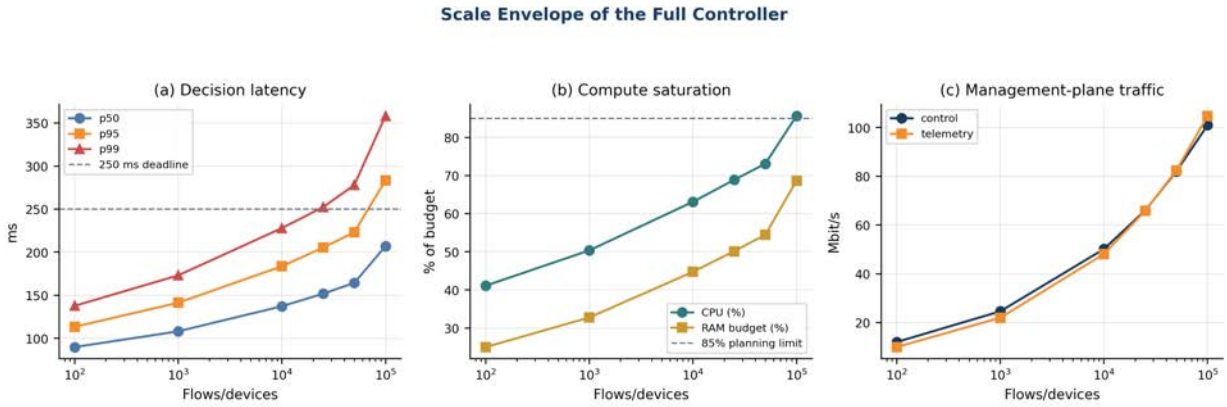


Fig. 3. B7 scale envelope; the p99 decision deadline is crossed before the common compute and link budgets are exhausted. Source: authors' model

Table 6

B7 scale results aggregated over nine scenarios

Flows/devices	p99, ms	CPU, %	RAM, GiB	Ctrl+tel, Mbit/s	LM
100	138	41.1	8.0	22.0	0.051
1,000	173	50.4	10.5	46.6	0.054
10,000	228	63.1	14.3	98.3	0.061
25,000	252	68.9	16.1	131.8	0.065
50,000	278	73.1	17.4	164.5	0.068
100,000	358	85.7	22.0	205.8	0.076

The knee is a reference envelope for the stated model and budget, not a universal capacity limit. A large deployment would need domain sharding, lower-cardinality telemetry, cached local policies, and global coordination reserved for cross-domain events. Faster hardware may move the knee upward; constrained gateways or dynamic radio networks may move it downward. At small and medium scale, B4 is rational for path-dominated risk and B6 for partition tolerance with safely pre-authorized local actions.

At 10^4, control and telemetry contributed 50.2 and 48.1 Mbit/s; at 10^5 they reached 101.0 and 104.8 Mbit/s. Although the combined load remained below 1 Gbit/s, consuming more than one fifth of a shared management path may compete with recovery traffic. Storage is limited through aggregation, retention classes, and signed manifests: public audit records retain hashes, summaries, decisions, and non-sensitive metrics, whereas restricted evidence follows the minimum approved retention period. Energy values are accounting-model outputs rather than physical measurements.

3.3. Ablations and validity. Ablations separated the mechanisms' roles. Removing provenance gates raised mission loss to 0.111. Removing the twin raised loss to 0.109 and recovery to 27.4 s while reducing p99 to 192 ms and CPU to 52.5%. Removing the shield admitted eight modeled unsafe actions in 450 runs and lowered rollback success to 87.8%. Removing local fallback raised loss to 0.167 and recovery to 45.1 s and reduced bounded degradation to 76.2%.

Table 7

B8 ablation results at 10^4 flows/devices

Variant	LM	Rec., s	p99, ms	Unsf.	Rollb., %	Bound., %
B7	0.061	21.6	228	0	98.9	100.0
B8-E	0.111	24.4	210	0	97.6	100.0
B8-T	0.109	27.4	192	0	99.1	100.0
B8-S	0.088	25.5	215	8	87.8	98.0
B8-F	0.167	45.1	241	0	98.9	76.2

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

The components therefore trade distinct assurances: provenance supports evidence trust, the twin improves prediction at a latency cost, the shield protects action safety, and fallback preserves service under partition. The eight B8-S violations also show why average mission loss cannot absorb a hard safety outcome.

All quantitative findings are model-bounded. The study used synthetic traces, flow-level event equations, normalized service weights, and model-based resource and energy accounting; it did not execute hardware-in-the-loop or validate vendor P4/eBPF, SDN/NFV, Wi-Fi, or 5G systems. Results depend on weights, thresholds, recovery functions, and the assumption that independent trust roots and the federation threshold are not jointly compromised. The clean build demonstrates reproducibility only within the controlled bundle. Zero modeled unsafe actions for B7 does not prove the absence of unknown states. Independent code review, release of run-level data and seeds, hardware-in-the-loop validation, sector calibration, and external replication are required before operational claims.

Deployment should progress from observe-only monitoring to decision support, guarded reversible actions, federated fallback, and only then conditional cross-domain autonomy. Advancement requires measured evidence quality, stable invariants, rollback testing, and explicit authority. Shared-mode compromise of a trust root, a systematically wrong twin, or a mis-specified invariant can still defeat several planes; a schema migration that loses monotonic epochs or action IDs can also make reconciliation non-deterministic. These residual risks belong in the deployment profile rather than being hidden by the aggregate score.

4. Conclusions. A compromise-tolerant controller was specified around explicit trust boundaries, provenance-aware evidence, constrained decisions, bounded local fallback, and deterministic reconciliation. Under equal modeled budgets at 10^4, B7 improved mission loss, recovery, goodput, and minimum service quality relative to B6 while using more compute, memory, and decision time. The paired relative mission-loss estimator was 57.9%, whereas the ratio of displayed means was 60.6%; both are reported because they summarize the data differently.

The benchmark also identified limits: p99 first exceeded 250 ms at 25,000, and simpler baselines remained preferable in some single-domain or latency-sensitive conditions. Ablations exposed distinct safety, prediction, provenance, and local-survivability trade-offs within the synthetic model. The contribution is a bounded reference architecture and evaluation method, not proof of universal field effectiveness. Future work should publish a frozen reproducibility package, use hierarchical inference, validate real controller and data-plane implementations, perform hardware-in-the-loop tests, and obtain independent replication.

Conflict of Interest. The author declares no conflict of interest.

Funding. This research received no external funding. Institutional Review Board Statement: not applicable; the synthetic benchmark involved neither human participants nor animals. Informed Consent Statement: not applicable.

Data Availability. Run-level data, scripts, configurations, seeds, parameter files, and manifests are maintained in a controlled working package. No public repository or DOI is claimed. Public release requires security review and removal of sensitive deployment information; until release, independent numerical reproduction remains limited.

Use of Artificial Intelligence. OpenAI GPT-5.6 Pro was used for language drafting, document structuring, and generation of controlled modeling and visualization scripts. The author reviewed and edited the outputs and accepts full responsibility. AI assistance does not replace independent code review, invariant testing, or external validation. Conflicts of Interest: the author declares no conflicts of interest.

Author Contributions. Conceptualization, methodology, software, validation, formal analysis, investigation, data curation, writing-original draft, writing-review and editing, visualization, and project administration: Dmytro Prokopovych-Tkachenko. The author approved the manuscript and accepts responsibility for its content.

References:

1. Kreutz, D., Ramos, F.M.V., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. Proc. *IEEE*. 103, 14–76. https://doi.org/10.1109/JPROC.2014.2371999.

2. Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., Walker, D. (2014). P4: Programming Protocol-Independent Packet Processors. ACM SIGCOMM Comput. Commun. Rev. 44, 87–95. https://doi.org/10.1145/2656877.2656890.

3. Vieira, M.A.M., Castanho, M.S., Pacifico, R.D.G., Santos, E.R.S., Camargos, E.P.M., Jr., Vieira, L.F.M. (2020). Fast Packet Processing with eBPF and XDP: Concepts, Code, Challenges, and Applications. *ACM Comput. Surv*. 53, 1–36. https://doi.org/10.1145/3371038.

4. Mijumbi, R., Serrat, J., Gorricho, J.-L., Bouten, N., De Turck, F., Boutaba, R. (2016). Network Function Virtualization: State-of-the-Art and Research Challenges. *IEEE Commun. Surv. Tutor*. 18, 236–262. https://doi.org/10.1109/COMST.2015.2477041.

5. Scott-Hayward, S., Natarajan, S., Sezer, S. (2016). A Survey of Security in Software Defined Networks. *IEEE Commun. Surv. Tutor*. 18, 623–654. https://doi.org/10.1109/COMST.2015.2453114.

6. Katta, N.P., Zhang, H., Freedman, M.J., Rexford, J. Ravana: Controller Fault-Tolerance in Software-Defined Networking. In Proceedings of the 1st ACM SIGCOMM Symposium on Software Defined Networking Research, Santa Clara, CA, USA, 17–18 June 2015; Article 4, pp. 1–12. https://doi.org/10.1145/2774993.2774996.

7. Fett, M., Kraft, M., Wilking, F., Goetz, S., Wartzack, S., Kirchner, E. (2024). Medium-Level Architectures for Digital Twins: Bridging Conceptual Reference Architectures to Practical Implementation in Cloud, Edge and Cloud-Edge Deployments. *Electronics*, 13, 1373. https://doi.org/10.3390/electronics13071373.

8. El-Hajj, M. (2024). Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. *Electronics,* 13, 3941. https://doi.org/10.3390/electronics13193941.

9. Cho, H., Sung, J.-H., Kang, H.-J., Jang, J., Shin, D. (2025). Quantifying Cyber Resilience: A Framework Based on Availability Metrics and AUC-Based Normalization. *Electronics*, 14, 2465. https://doi.org/10.3390/electronics14122465.

10. Bocci, A., Forti, S., Ferrari, G.-L., Brogi, A. (2023). Declarative Secure Placement of FaaS Orchestrations in the Cloud-Edge Continuum. *Electronics*, 12, 1332. https://doi.org/10.3390/electronics12061332.

11. Yang, F., Sun, Y., Gao, Q., Chen, X. (2024). EDI-C: Reputation-Model-Based Collaborative Audit Scheme for Edge Data Integrity. *Electronics*, 13, 75. https://doi.org/10.3390/electronics13010075.

12. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. (2021). NIST SP 800-160 Vol. 2 Rev. 1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. National Institute of Standards and Technology: Gaithersburg, MD, USA, https://doi.org/10.6028/NIST.SP.800-160v2r1.

13. Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). NIST SP 800-207: Zero Trust Architecture. National Institute of Standards and Technology: Gaithersburg, MD, USA, https://doi.org/10.6028/NIST.SP.800-207.

14. 3GPP TS 33.501; Security Architecture and Procedures for 5G System. 3rd Generation Partnership Project: Sophia Antipolis, France, Release 18.

15. Iyengar, J., Thomson, M. (2021). RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport. Internet Engineering Task Force: Fremont, CA, USA, https://doi.org/10.17487/RFC9000.

16. Ford, A., Raiciu, C., Handley, M., Bonaventure, O., Paasch, C. (2020). RFC 8684: TCP Extensions for Multipath Operation with Multiple Addresses. Internet Engineering Task Force: Fremont, CA, USA, https://doi.org/10.17487/RFC8684.

17. Torres-Arias, S., Afzali, H., Kuppusamy, T.K., Curtmola, R., Cappos, J. in-toto: Providing Farm-to-Table Guarantees for Bits and Bytes. In Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, 14-16 August 2019; pp. 1393–1410. https://doi.org/10.5555/3361338.3361435.

18. Samuel, J., Mathewson, N., Cappos, J., Dingledine, R. Survivable Key Compromise in Software Update Systems. In Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4-8 October 2010; pp. 61–72. https://doi.org/10.1145/1866307.1866315.

19. National Telecommunications and Information Administration. The Minimum Elements for a Software Bill of Materials (SBOM). U.S. Department of Commerce: Washington, DC, USA, 2021. Available online: https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom (accessed on 17 August 2026).

Відомості про авторів

Англ.	Укр.
Dmytro Prokopovych-Tkachenko Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies, University of Customs and Finance, Doctoral Candidate, State University of Information and Communication Technologies omega2417@umsf.edu.ua ORCID: 0000-0002-6590-3898 Scopus Author ID: 57201777932 Web of Science ResearcherID: Q-2918-2018	Прокопович-Ткаченко Дмитро Ігорович кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, докторант, Державний університет інформаційно-комунікаційних технологій omega2417@umsf.edu.ua ORCID: 0000-0002-6590-3898 Scopus Author ID: 57201777932 Web of Science ResearcherID: Q-2918-2018

Дата надходження статті: 15.05.2026
Дата надходження виправленої версії статті: 30.06.2026
Дата прийняття статті: 07.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.7
UDC 004.7:621.39:628.4
JEL Classification: C61, Q53, O32, L86

OPTIMIZATION OF LORAWAN GATEWAY PLACEMENT IN WASTE CONTAINER MONITORING SYSTEMS WITH ADR CONSIDERATION

Hryhorii Rozhkov, Iryna Klymenko

ОПТИМІЗАЦІЯ РОЗМІЩЕННЯ LORAWAN GATEWAY У СИСТЕМАХ МОНІТОРИНГУ КОНТЕЙНЕРІВ ВІДХОДІВ З УРАХУВАННЯМ МЕХАНІЗМУ ADR

Г. О. Рожков, І. А. Клименко

Abstract

This article examines the placement of LoRaWAN gateways for urban waste-container monitoring. The practical question is straightforward: how can a city obtain stable telemetry from many battery-powered container nodes without installing more gateways than are actually needed? In many planning schemes the answer is reduced to geometric coverage. Such a reduction is unsafe for this application, because the radio channel is affected by the morphology of the district, the type and position of the container, additional shielding losses, and the way in which the Adaptive Data Rate (ADR) mechanism reacts to RSSI and SNR at node locations. The paper therefore proposes a placement method in which coverage, service quality, average spreading factor, node energy consumption and the number of gateways are treated jointly in one objective function. The formulation is adapted to waste-container monitoring, including above-ground and underground bins, irregular node distribution, heterogeneous urban development and the requirement for reliable telemetry delivery. In this interpretation, gateway placement is not only a question of drawing a coverage radius on a map; it is also a question of creating channel conditions in which ADR can move a significant share of nodes to more economical transmission modes without losing communication reliability. The proposed approach can be used to reduce unnecessary LoRaWAN infrastructure, justify installation points and improve the operation of smart waste management systems in urban areas.

Key words: *LoRaWAN, smart waste management, gateway, ADR, network coverage, IoT, waste container, LPWAN.*

Анотація

У статті розглянуто задачу оптимізації розміщення LoRaWAN gateway у міських системах моніторингу контейнерів відходів. Актуальність дослідження зумовлена необхідністю побудови енергоефективної та масштабованої інфраструктури smart waste management, здатної забезпечити стабільну передачу телеметричних даних від великої кількості сенсорних вузлів за мінімально можливої кількості gateway. Показано, що традиційний підхід до планування LoRaWAN-мереж, заснований лише на зоні геометричного покриття, не враховує вплив міського середовища, типу контейнерів, умов радіопоширення та особливостей роботи механізму Adaptive Data Rate. Встановлено, що ADR є штатним інструментом LoRaWAN для адаптації параметрів передавання до умов каналу, однак його ефективність безпосередньо залежить від просторового розташування gateway та фактичних значень RSSI і SNR у точках встановлення кінцевих вузлів. На цій основі запропоновано метод оптимізації кількості та координат gateway, який поєднує критерії покриття, якості обслуговування, середнього spreading factor, енерговитрат вузлів і кількості gateway у єдину цільову функцію. Особливістю підходу є врахування специфіки систем моніторингу контейнерів відходів, зокрема наявності наземних і підземних контейнерів, неоднорідності забудови, нерівномірності розташування вузлів та вимог до гарантованої доставки даних. Запропонований метод дає змогу розглядати розміщення gateway не лише як задачу просторового покриття, а як задачу забезпечення таких умов каналу, за яких ADR переводить більшість вузлів у більш енергоефективні режими передавання без погіршення надійності зв'язку. Практична цінність роботи полягає у можливості зменшення надлишковості LoRaWAN-інфраструктури, обґрунтованого вибору точок встановлення gateway та підвищення ефективності функціонування smart waste management систем у міському середовищі.

Ключові слова: *LoRaWAN, smart waste management, gateway, ADR, покриття мережі, IoT, контейнер відходів, LPWAN.*

1. Introduction. Municipal services are increasingly being transferred to digital monitoring and decision-support platforms. Waste collection is one of the clearest examples: fill-level sensors installed in containers make it possible to adjust collection routes, avoid overflow, reduce unnecessary vehicle runs and improve the sanitary condition of urban areas. For this class of tasks, LPWAN technologies are attractive because the nodes usually send small packets, work from batteries and remain in fixed positions for a long time. LoRaWAN is widely used in such conditions, as it combines long-range communication with low energy consumption and a relatively simple deployment model. [1; 2]

Field trials and experimental studies show that LoRaWAN can be used for waste-container monitoring in real cities. Nevertheless, they also show that the quality of the radio link is not determined by distance alone.

© Rozhkov H. O., Klymenko I. A., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

A container placed below ground level, a metal lid, dense building blocks or a low gateway mounting point may change the link budget more strongly than the nominal range of the technology suggests. For this reason, gateway placement based only on an assumed coverage radius may lead either to unstable data transmission or to redundant infrastructure [3; 4].

The issue becomes more important when ADR is taken into account. In favorable radio conditions ADR can reduce the spreading factor, shorten packet airtime, decrease transmission energy and increase the practical capacity of the network. However, ADR works effectively only when the node has a sufficient channel margin. Thus, the placement of gateways should be formulated not merely as a coverage task, but as the creation of radio conditions under which most waste-container nodes can operate in efficient ADR modes [5; 6].

Analysis of Recent Research and Publications. The available literature may be grouped into several lines of work. One line studies LoRaWAN as a communication technology for smart-city and IoT applications, with attention to range, throughput, energy consumption and robustness. A second line focuses on smart waste management, including fill-level sensing, collection logistics and data acquisition from distributed containers. A third line deals with LoRaWAN gateway placement and increasingly uses multicriteria or metaheuristic optimization procedures [3-5; 7; 8].

These lines of research, however, are often only loosely connected. Papers on waste monitoring usually give more attention to the sensor unit or route optimization, while gateway placement is described rather generally. In contrast, many placement studies use an abstract network model and do not explicitly include the properties of waste-container systems: underground bins, local shielding, differences between container materials and the uneven spatial distribution of the nodes [3; 4].

The ADR-related studies are also relevant for the present work because they demonstrate the influence of adaptive data-rate control on packet delivery and battery use. Yet ADR is rarely introduced as a criterion during the spatial planning of a LoRaWAN network for waste-container monitoring. This leaves a practical and methodological gap: gateway locations should be evaluated together with the expected ADR behavior of the end nodes, rather than after the placement problem has already been solved [6].

Purpose and Objectives of the Study. The purpose of this paper is to develop a method for selecting LoRaWAN gateway locations in waste-container monitoring systems while explicitly considering the ADR mechanism. The intended result is a configuration that limits the number of gateways but still provides the required quality of telemetry transmission.

To reach this purpose, the study solves the following tasks: analysis of LoRaWAN use in smart waste management; identification of the main factors that determine link quality between container nodes and gateways in an urban environment; justification of ADR consideration at the planning stage; formulation of a mathematical model for comparing gateway configurations; construction of an objective function that combines infrastructure cost, service quality and energy-related indicators; and description of a procedure for determining the number and coordinates of gateways for this class of systems.

2. Materials and methods of research. The object of the study is the LoRaWAN infrastructure of the urban waste container monitoring system, in particular the interaction of container sensor nodes with the gateway under different radio propagation conditions and the operation of the Adaptive Data Rate mechanism. The subject of the study is the methodological principles for choosing the number and coordinates of LoRaWAN gateways, taking into account channel quality indicators, energy efficiency of end nodes and requirements for guaranteed delivery of telemetric data.

The main hypothesis of the study is that the placement of the gateway, optimized not only by the criterion of geometric coverage, but also by the expected values of RSSI, SNR, spreading factor, packet delivery ratio and energy consumption of nodes, provides better conditions for the operation of ADR and allows to increase the functional efficiency of the LoRaWAN network without an unjustified increase in the number of gateways.

The following assumptions are made in the work: container sensor nodes are considered stationary; the coordinates of containers and candidate gateway installation points are known or can be obtained from the city GIS database; the frequency of uplink message transmission is specified; the impact of seasonal environmental changes, temporary interference, and short-term radio channel fluctuations is taken into account in a generalized manner through a margin in signal level and additional losses for complex container types.

The adopted simplifications include: using an aggregated model of signal propagation loss; representing the impact of underground or partially shielded containers through an additional attenuation coefficient; evaluating the ADR mode based on predicted RSSI and SNR values without modifying the standard LoRaWAN protocol; considering ADR downlink commands as an auxiliary mechanism for setting transmission parameters without detailed modeling of network server queues.

The study was performed as a computational and analytical modeling. At the first stage, a set of container nodes was formed with coordinates, container type, building conditions, and expected data transmission

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

intensity. At the second stage, a set of candidate gateway installation points was specified, taking into account the installation height, power availability, network connectivity, and engineering constraints on equipment placement.

The theoretical basis of the study was the methods of radio planning of LPWAN networks, multi-criteria optimization, comparative analysis of alternative configurations and formalization of objective functions. For each pair «container node – gateway» signal losses, expected RSSI and SNR values were estimated, after which the gateway with the best reception conditions was determined and the possible operation mode of the node was predicted using the ADR mechanism.

The software implementation of the algorithmic part provides for the possibility of using Python, MATLAB, Julia or GIS-oriented environments with geoprocessing modules. Within the framework of this article, the software is considered as a tool for reproducing calculation procedures: enumerating permissible gateway configurations, calculating network quality criteria and selecting the option with the minimum value of the integral objective function.

This section provides only the initial methodological provisions, assumptions, simplifications and the procedure for conducting the study. Quantitative results, comparison of configurations, graphical dependencies and their interpretation are presented in the following sections of the article, since it is there that the solutions to the tasks set in the work are reflected.

Main Body of the Study

1. Features of the Operating Environment of Waste Container Monitoring Systems.

Unlike many IoT networks with more freely distributed end devices, a waste-container monitoring system is tied to municipal infrastructure. Container locations depend on building density, the street network, the organization of collection routes and the rules for arranging container sites. The radio channel is further affected by the bin material, installation depth, wall and lid construction, nearby buildings, vegetation and other local obstacles [3; 8].

Underground containers and partially shielded metal bins create the most difficult radio conditions. A node located close to a gateway may still have a poor link if the antenna is screened by the container body or by the surrounding structure. Conversely, an above-ground plastic bin at a larger distance may provide a better signal. Another practical feature is the nonuniform load: some containers generate telemetry more frequently because they fill faster, and this increases the importance of stable communication and sufficient network capacity [3; 8].

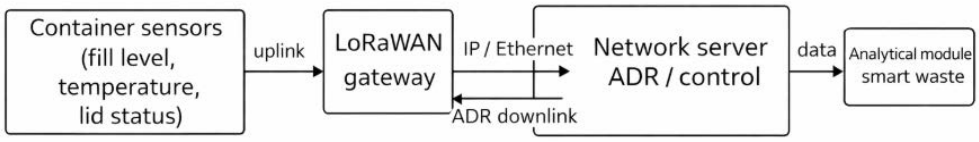


Fig. 1. Generalized architecture of a LoRaWAN-based waste container monitoring system

Figure 1 summarizes the data flow in a LoRaWAN-based waste monitoring system. The sensor node sends telemetry through one or more gateways to the network server and then to the analytical module. Control messages, including ADR-related downlink commands, return through the same communication chain. Therefore, the choice of gateway positions affects not only radio coverage but also the ability of the system to manage transmission parameters and maintain a stable monitoring process.

2. The Role of ADR in Improving LoRaWAN Network Efficiency

In LoRaWAN, ADR adjusts transmission parameters according to the observed channel state. This is especially useful for stationary container nodes: once the channel is sufficiently stable, the network server may assign a lower spreading factor and, where appropriate, reduce transmit power. The practical effects are shorter airtime, lower energy consumption and a smaller load on the radio channel [5; 6].

Poor gateway placement cannot be corrected by ADR alone. If many nodes remain in low-SNR areas, the network has to keep them in more robust but less economical modes. This increases the average spreading factor and accelerates battery discharge. For that reason, this study treats ADR not as a protocol to be modified, but as an indicator of whether the spatial configuration of gateways is technically successful [5; 7].

3. Formalization of the Gateway Placement Problem

Consider an urban district with n waste containers, each represented by a LoRaWAN end node. The set of containers is denoted by B={b1,b2,...,bn}. For every element of this set, the coordinates, container type, surrounding urban conditions and expected transmission intensity are specified. The possible gateway

locations form the set G={g1,g2,...,gm}; for each candidate point, coordinates, installation height and infrastructural restrictions are known.

For every container-gateway pair, path loss is evaluated with regard to distance, urban morphology, gateway height and additional losses introduced by the container type. In this way, the model shifts from a simplified coverage-radius description to an engineering estimate of the expected channel parameters.

$$Lij = Lpath(dij, ci, hj) + Lcont(ti) \quad (1)$$

$$RSSI_{ij} = P_{tx} + G_{tx} + G_{rx} - L_{ij} \quad (2)$$

$$SNR_{ij} = RSSI_{ij} - N_0 \quad (3)$$

For each container, the gateway with the best predicted reception conditions is then assigned as the active one. This assignment is important because it determines the likely operating mode of the node after ADR decisions are made.

$$j^*(i) = \arg\max SNRij, \ j \in G^* \quad (4)$$

4. Consideration of ADR in the Model

To include ADR behavior in the model, each node is assigned a predicted operating mode. This mode is described through a function that links RSSI and SNR to the probable spreading factor.

$$SFi = f(SNRi, RSSIi) \quad (5)$$

$$\bar{SF} = (1/n) \Sigma SF_i \quad (6)$$

A lower average spreading factor means shorter packet airtime and, in most operating scenarios, lower transmission energy and better network scalability. For this reason, the average spreading factor is used as one of the key criteria when comparing gateway configurations.

5. Evaluation of Energy Consumption and Quality of Service

For waste-container monitoring, sensor autonomy is a critical engineering requirement. In most deployments the node is battery-powered, so the energy used for measurement, local processing and radio transmission must be controlled. Among these components, transmission energy is the most sensitive to the ADR-selected mode [2; 4].

$$Ei = Esense,i + Eproc,i + Etx,i \quad (7)$$

$$E_{tx,i} = N_i \cdot e(SF_i, P_{tx,i}, l_i) \quad (8)$$

$$\bar{E} = (1/n) \Sigma E_i \quad (9)$$

$$PDR = N_{recv} / N_{sent} \quad (10)$$

$$Q = (1/n) \Sigma I(SNR \geq SNR_{min} \wedge SF \leq SF_{max} \wedge PDR_i \geq PDR_{min}) \quad (11)$$

The indicator Q describes the share of containers for which the minimum acceptable telemetry conditions are satisfied. It prevents a formal situation in which a node is counted as covered although its packet delivery, SNR or spreading factor is unsuitable for reliable operation.

6. Objective Function of Optimization

An integral objective function is used to compare gateway configurations. It combines infrastructure complexity, communication reliability, ADR-related operating mode and the expected energy consumption of the sensor network.

$$J = \alpha Ngw + \beta\bar{SF} + \gamma(1 - PDR) + \delta\bar{E} + \mu(1 - Q) \quad (12)$$

Minimizing J means searching for a configuration that avoids unnecessary gateways, keeps packet delivery at an acceptable level, reduces the average spreading factor and preserves node autonomy. This differs from traditional planning, where the coverage indicator usually dominates the decision [7; 9].

Figure 2 gives a simple interpretation of this compromise. Adding gateways may reduce the average spreading factor and improve the conditions for ADR operation, but the gain decreases after a certain point. The optimization problem is therefore not to install the maximum possible number of gateways, but to find the point at which service quality and infrastructure cost are balanced [7].

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

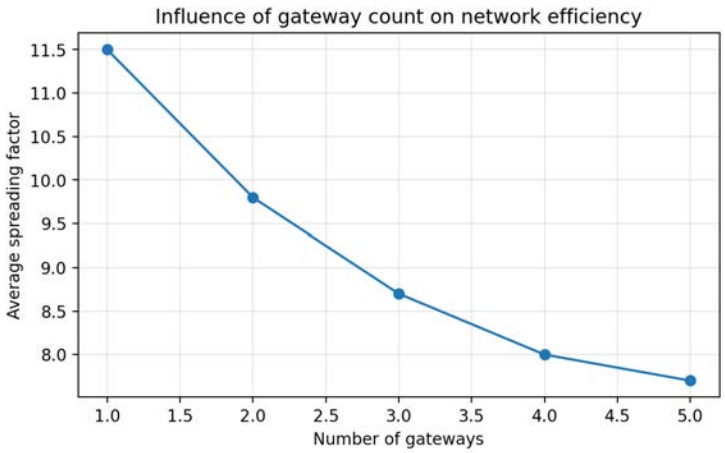


Fig. 2. Illustration of the influence of the number of gateways on the average spreading factor and network efficiency

7. Formal Algorithm for Determining the Optimal Gateway Configuration

The proposed procedure can be implemented as a sequence of engineering steps. First, data are collected on container coordinates, container types and local urban conditions. Next, a list of possible gateway mounting points is formed; only points that satisfy height, power-supply and installation constraints are kept [5].

For each node-gateway pair, the channel parameters are estimated. The best gateway is selected for every node, the expected ADR mode is predicted, and the quality indicators of the whole configuration are calculated. The admissible configuration with the smallest value of the integral criterion J is then selected.

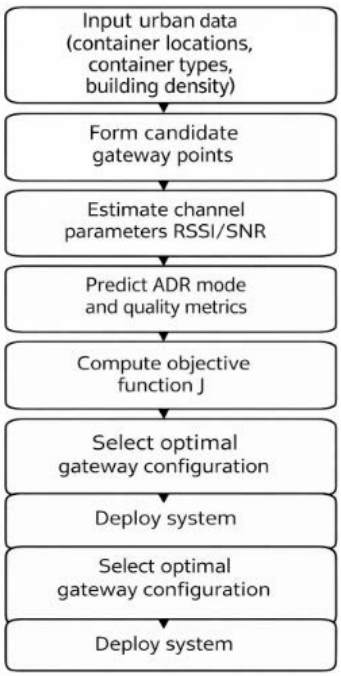


Fig. 3. Flowchart of the algorithm for selecting the optimal LoRaWAN gateway configuration

Figure 3 presents this sequence from the input urban data to the final gateway configuration. Such a representation is useful for later implementation in software, including GIS-based tools for infrastructure planning [5; 7].

8. Pseudocode of the Algorithm and an Example of Software Implementation

For reproducibility, the general logic of the algorithm is written below as pseudocode. The same structure can be implemented in Python, MATLAB, Julia or in a GIS environment that supports geoprocessing.

for config in candidate_gateway_sets:

```
metrics = []
for node in waste_nodes:
   links = evaluate_links(node, config)
   best_link = select_by_max_snr(links)
   sf = predict_sf(best_link.snr, best_link.rssi)
   energy = estimate_energy(node, sf, best_link.tx_power)
   metrics.append((sf, energy, best_link.pdr))
J = alpha*count(config) + beta*avg_sf(metrics) \
   + gamma*(1-pdr(metrics)) + delta*avg_energy(metrics) \
   + mu*(1-service_share(metrics))
update_best_config_if_needed(config, J)
```

The pseudocode shows only the core calculation loop. In a practical tool it may be supplemented with radio-propagation modules, clustering of candidate points, restrictions on installation sites and GIS layers describing building density or terrain [7; 9].

9. Criteria for Evaluating the Network Configuration

Table 1 lists the criteria used to evaluate a LoRaWAN gateway configuration for a waste-container monitoring network.

Table 1

Criteria for evaluating LoRaWAN gateway configuration in waste container monitoring systems

Criterion	Symbol	Mathematical expression	Meaning of the criterion	Optimization direction
Number of gateways	Ngw	$Ngw = \|G^*\|$	Infrastructure complexity and cost	minimum
Average spreading factor	SFavg	$\bar{SF} = (1/n)\,\Sigma\, SFi$	ADR efficiency in the network	minimum
Average node energy consumption	Eavg	$\bar{E} = (1/n)\,\Sigma\, Ei$	Sensor autonomy	minimum
Packet delivery success	PDR	$PDR = Nrecv / Nsent$	Reliability of telemetry communication	maximum
Share of nodes with guaranteed service	Q	$Q = (1/n)\,\Sigma\, I(\cdot)$	Quality of network service	maximum
Share of nodes at high SF	RhighSF	$RhighSF = N(SF \geq SFthr) / n$	Assessment of load and scalability	minimum
Integral criterion	J	$J = \alpha Ngw + \beta\bar{SF} + \gamma(1 - PDR) + \delta\bar{E} + \mu(1 - Q)$	Generalized selection criterion	minimum

Together, these criteria provide a more informative assessment than coverage alone. The inclusion of ADR-dependent indicators makes the evaluation closer to the real operation of a LoRaWAN network in a smart waste management scenario [7; 9].

Computational Study of the Effectiveness of the Proposed Method

To check the applied usefulness of the proposed method, a model-based computational study was performed for a typical urban district. Two placement approaches were compared: a baseline approach aimed mainly at continuous coverage, and the proposed approach, where the configuration is assessed by ADR behavior, average spreading factor, packet delivery ratio, node energy consumption and the share of containers with guaranteed service. This type of comparison corresponds to the current formulation of LoRaWAN gateway placement problems [4; 8].

1. Initial Data and Simulation Scenarios

The simulated district measured 2.4 x 1.8 km and included a nonuniform distribution of container sites: a dense central area, a medium-density residential part and a peripheral area with fewer obstacles. The model included 60 containers; 25% of them were treated as underground or partially shielded. Eight candidate gateway points were placed on roofs of administrative and municipal buildings.

In Fig. 4, black squares mark the gateways selected by minimizing the integral criterion, while empty squares show alternative candidate points considered during optimization. This visual distinction is important because the best functional configuration is not always the same as a visually uniform coverage pattern.

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

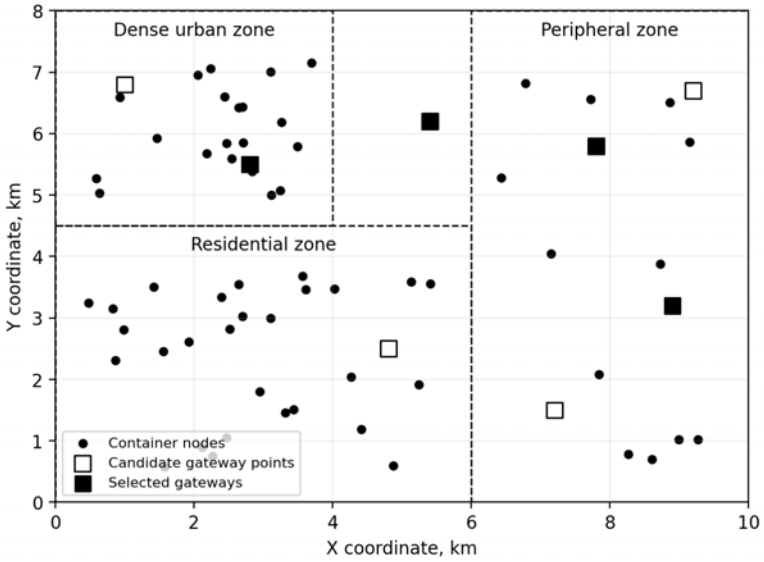


Fig. 4. Layout of the model urban district with container nodes and candidate gateway installation points

Table 2

Initial parameters of the computational study

Parameter	Symbol	Value
Number of containers	n	60
Share of underground containers	rug	25%
Number of candidate gateway points	m	8
Minimum acceptable packet delivery ratio	PDRmin	0.95
Maximum allowable spreading factor	SFmax	10
Average uplink transmission period	Ttx	30 min
Additional loss for underground containers	Ladd	24–26 dB
Weight coefficients of the objective function	α, β, γ, δ, μ	0.30; 0.20; 0.20; 0.15; 0.15

The parameters in Table 2 represent a medium-scale urban case with dense building blocks, areas of easier radio propagation and a noticeable share of containers with additional signal loss. The chosen limits for PDR and SF allow the configurations to be judged not only by reachability, but also by the actual quality of telemetry service.

2. Comparison with the Baseline Gateway Placement Method

Two methods were compared in the computational study. The baseline method selected gateways mainly to cover container nodes with a minimal number of infrastructure points and did not include ADR explicitly. The proposed method used the integral objective function and therefore favored configurations that reduce average spreading factor, improve the share of nodes with guaranteed service and decrease end-device energy consumption.

Table 3

Comparison of the baseline and proposed approaches

Approach	N_gw	$\bar{SF}$	PDR	E_avg, mWh/day	Q	J
Baseline, 2 gateways	2	10.8	0.84	1.84	0.68	4.73
Proposed, 2 gateways	2	10.1	0.89	1.62	0.76	4.26
Baseline, 3 gateways	3	9.6	0.90	1.52	0.79	4.28
Proposed, 3 gateways	3	8.5	0.95	1.22	0.89	3.66
Baseline, 4 gateways	4	8.8	0.94	1.31	0.87	4.02
Proposed, 4 gateways	4	7.6	0.98	1.05	0.95	3.41
Baseline, 5 gateways	5	8.2	0.96	1.18	0.91	4.08
Proposed, 5 gateways	5	7.2	0.985	0.98	0.97	3.50

The values in Table 3 show that, for every considered number of gateways, the proposed method gives higher PDR, lower average spreading factor and lower daily node energy consumption. In the studied scenario, the minimum value of the integral criterion J was obtained for four gateways, which indicates a reasonable balance between infrastructure cost and telemetry quality.

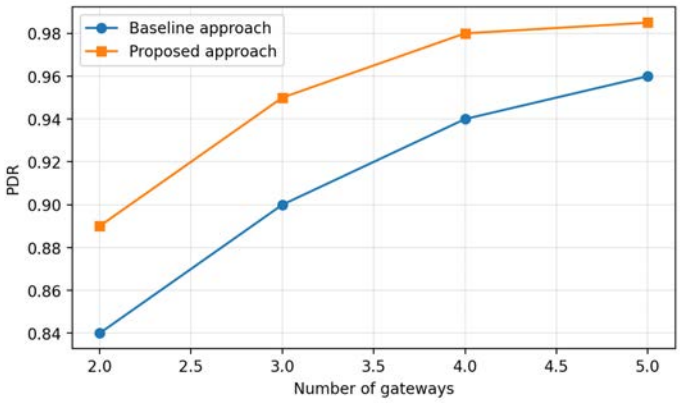


Fig. 5. Packet delivery ratio versus the number of gateways

Figure 5 shows that PDR grows as the number of gateways increases in both approaches. At the same time, the proposed method reaches a higher delivery ratio for the same gateway count because it takes into account not only coverage, but also the channel margin needed for effective ADR operation.

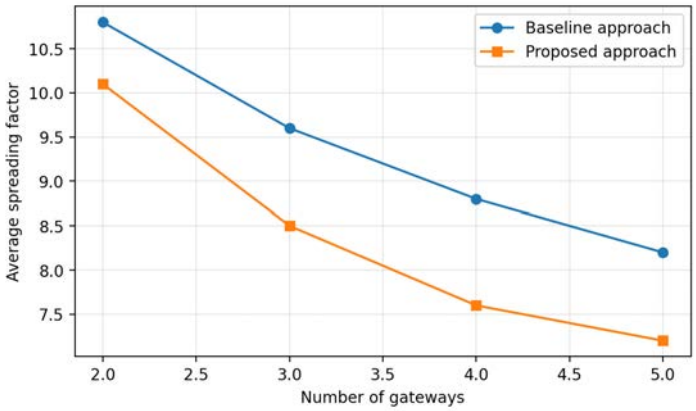


Fig. 6. Average spreading factor versus the number of gateways

Figure 6 shows the corresponding change in average spreading factor. The ADR-aware placement reduces this value more strongly, which means shorter airtime, better scalability and a lower probability of collisions in dense urban deployments.

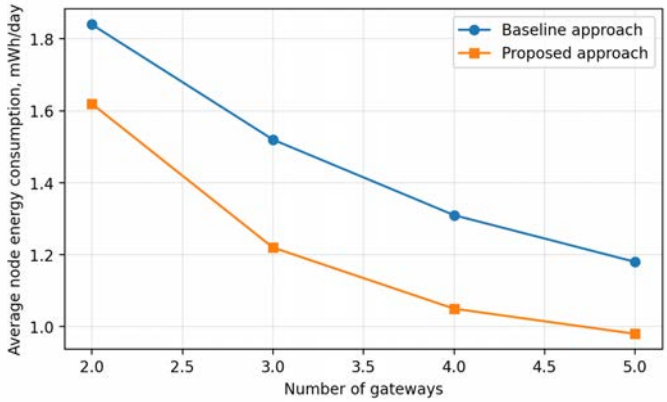


Fig. 7. Average node energy consumption versus the number of gateways

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

Figure 7 shows the effect on node energy consumption. Better gateway geometry and lower spreading factors reduce the daily energy demand of the sensor nodes. For battery-powered waste-container sensors, this translates into longer intervals between maintenance operations.

3. Sensitivity Analysis with Respect to the Share of Underground Containers

The influence of underground containers was also evaluated. When their share increased from 10% to 35%, the average spreading factor in the baseline approach increased by about 11-14%, while the proposed method showed an increase of 7-9%. This suggests that ADR-aware gateway placement is more resistant to the difficult radio conditions created by shielded and underground containers [3; 4].

These results show that the proposed approach is not limited to a formal mathematical statement. It produces measurable gains in the main network and operational indicators, which allows the work to be treated as a computational and analytical study rather than as a general review.

3. Discussion of Results. The proposed approach has several advantages over conventional LoRaWAN planning. The first is that it reflects the specific operating conditions of waste-container monitoring: different container types, unequal access to the radio channel and nonuniform telemetry intensity. In this setting, simple coverage is not enough, because it does not guarantee efficient ADR operation or acceptable energy consumption [1; 7; 9].

A second result is the combination of infrastructural and functional criteria in a single objective function. This allows the designer to see the compromise between the number of gateways and the quality of network operation. In practical terms, the method helps avoid both underdeployment, when many nodes are forced to work at high spreading factors, and overdeployment, when additional gateways do not provide a proportional improvement in service quality.

The method also has limitations. Accurate use requires reliable container coordinates, a map of the urban environment, a list of feasible gateway installation points and estimates of additional losses for different container types. Even with approximate data, however, the model can be used for preliminary design and for comparing several LoRaWAN deployment options.

Scientific Novelty. The scientific novelty of the results is the proposed method for optimizing LoRaWAN gateway placement in waste-container monitoring systems. In contrast to placement approaches based mainly on geometric coverage, the method includes the influence of ADR on functional network performance [5; 7].

In the proposed formulation, ADR is not treated as an independent protocol-optimization problem. Instead, it is used as a criterion for judging the quality of the spatial gateway configuration through average spreading factor, sensor-node energy consumption, packet delivery and the share of containers with guaranteed service.

Practical Significance. The practical significance of the results is their possible use in the design and modernization of municipal LoRaWAN waste-monitoring systems. The method helps justify both the number of gateways and their coordinates under real urban constraints, which can reduce redundant infrastructure and improve telemetry stability [3; 7].

The results can also support GIS-oriented decision-support systems, LoRaWAN coverage simulation tools and applied software for planning smart waste management infrastructure. The expected practical effect is a lower average spreading factor, shorter packet airtime, longer sensor-node autonomy and more rational use of network resources.

4. Conclusions. The paper addressed the optimization of LoRaWAN gateway placement in waste-container monitoring systems with consideration of ADR. It was shown that planning based only on geometric coverage is insufficient, since it does not reflect container type, urban radio conditions or the operating requirements of ADR.

The study proposed a mathematical model and an objective function that include the number of gateways, average spreading factor, packet delivery ratio, average node energy consumption and the share of containers with guaranteed service. A formal algorithm was presented, together with an example of software implementation.

The practical value of the approach is the justified selection of gateway installation points, lower infrastructure redundancy and more stable telemetry service for waste containers. Further work should include GIS integration, numerical modeling for specific city districts and experimental validation of the proposed method.

Conflict of interest. The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other, that could influence the study and its results presented in this article.

Financing. The study was conducted without financial support.

Data availability. The manuscript has no associated data

Use of artificial intelligence. The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

Authors' contribution. Hryhorii Rozhkov – conceptualization, source analysis, writing the main text; Klymenko Iryna– methodology, editing, forming conclusions and checking the consistency of the structure.

References:

1. Bouras, C., Gkamas, A., Kokkinos, V., Papagiannopoulos, S., Poulopoulos, V., & Zourzoudis, T. (2024). Smart city IoT applications based on LoRaWAN: Challenges and open issues. *Future Internet*, 16(4), Article 113. https://doi.org/10.3390/fi16040113
2. Ibrahim, M., Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., & Shawkat, S. A. (2021). Smart waste management systems: A survey and an architecture proposal. *International Journal of Environmental Research and Public Health*, 18(23), Article 12867. https://doi.org/10.3390/ijerph182312867
3. Cruz, N., Montoya, G., Aguiar, A., & Silva, H. (2021). LoRaWAN and urban waste management - A trial. Sensors, 21(6), Article 2142. https://doi.org/10.3390/s21062142
4. Lozano, A., Caridad, J., De Paz, J. F., Villarrubia, G., & Bajo, J. (2018). Smart waste collection system with low consumption LoRaWAN nodes and route optimization. Sensors, 18(5), Article 1465. https://doi.org/10.3390/s18051465
5. LoRa Alliance. (2023). TS001-1.0.4 LoRaWAN® L2 1.0.4 specification. Fremont: LoRa Alliance.
6. Moysiadis, V., Sarigiannidis, P., Moscholios, I., & Vitsas, V. (2021). Extending ADR mechanism for LoRa-enabled mobile end-devices. Simulation Modelling Practice and Theory, 113, Article 102388. https://doi.org/10.1016/j.simpat.2021.102388
7. Al-Sammak, K. A., Dumitrescu, A. M., & Popescu, D. (2025). Optimizing LoRaWAN gateway placement in urban environments: A hybrid PSO-DE algorithm validated via HTZ simulations. *Technologies,* 13(6), Article 256. https://doi.org/10.3390/technologies13060256
8. Pires, L. M., Figueiredo, J., Martins, R., & Martins, J. (2025). IoT-enabled real-time monitoring of urban garbage levels using time-of-flight sensing technology. *Sensors*, 25(7), Article 2152. https://doi.org/10.3390/s25072152
9. Correia, F. P., Santos, M. A. B., Rodrigues, J. J. P. C., et al. (2023). LoRaWAN gateway placement in smart agriculture: An analysis of clustering algorithms and performance metrics. *Energies*, 16(5), Article 2356. https://doi.org/10.3390/en16052356
10. Augustin, A., Yi, J., Clausen, T., & Townsley, W. M. (2016). A study of LoRa: Long range and low power networks for the Internet of Things. *Sensors,* 16(9), Article 1466. https://doi.org/10.3390/s16091466
11. Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., & Watteyne, T. (2017). Understanding the limits of LoRaWAN. *IEEE Communications Magazine*, 55(9), 34–40. https://doi.org/10.1109/MCOM.2017.1600613
12. Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks: An overview. *IEEE Communications Surveys & Tutorials*, 19(2), 855–873. https://doi.org/10.1109/COMST.2017.2652320
13. Centenaro, M., Vangelista, L., Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications*, 23(5), 60–67. https://doi.org/10.1109/MWC.2016.7721743
14. Cattani, M., Boano, C. A., & Römer, K. (2017). An experimental evaluation of the reliability of LoRa long-range low-power wireless communication. *Journal of Sensor and Actuator Networks*, 6(2), Article 7. https://doi.org/10.3390/jsan6020007
15. Folianto, F., Low, Y. S., & Yeow, W. L. (2015). Smartbin: Smart waste management system. In Proceedings of IEEE TENSYMP 2015 (pp. 1–5). https://doi.org/10.1109/TENCONSpring.2015.7146775
16. Marais, J. M., Malekian, R., & Abu-Mahfouz, A. M. (2022). LoRa and LoRaWAN testbeds: A review. arXiv preprint. https://doi.org/10.48550/arXiv.2205.12345

Дані про авторів

Англ	Укр
Hryhorii Rozhkov Postgraduate Student at the Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” hryhoriirozhkov@gmail.com ORCID: 0009-0009-5343-8974	Рожков Григорій Олегович аспірант кафедри обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» hryhoriirozhkov@gmail.com ORCID: 0009-0009-5343-8974
Iryna Klymenko Doctor of Technical Sciences, Professor, Professor at the Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” klymenko.iryna@lll.kpi.ua ORCID: 0000-0001-5345-8806	Клименко Ірина Анатоліївна доктор технічних наук, професор, професор кафедри обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» klymenko.iryna@lll.kpi.ua ORCID: 0000-0001-5345-8806

Дата надходження статті: 19.05.2026
Дата надходження виправленої версії статті: 02.07.2026
Дата прийняття статті: 08.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.8
УДК 004.942:004.85:621.39:658.5
JEL Classification: C45, O33, L63

ТЕХНІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ СТВОРЕННЯ ЦИФРОВИХ ДВІЙНИКІВ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

Т. В. Савченко, І. С. Майстер

TECHNICAL AND APPLIED ASPECTS OF CREATING DIGITAL TWINS FOR INDUSTRIAL ENTERPRISES

Tetiana Savchenko, Ivan Maister

Анотація

Об'єктом дослідження є процес створення цифрового двійника промислового підприємства в умовах гетерогенного виробничого середовища. У роботі вирішується проблема інтеграції різнорідного технологічного обладнання, організації потокової обробки виробничих даних та реалізації предиктивної аналітики технічного стану обладнання без повної модернізації наявної виробничої інфраструктури підприємства. Актуальність даної роботи зумовлена необхідністю підвищення ефективності процесів виробництва, скорочення непланових простоїв обладнання та забезпечення цифрової трансформації промислових підприємств в умовах Industry 4.0.

У результаті дослідження розроблено п'ятирівневу мікросервісну архітектуру цифрового двійника промислового підприємства, реалізовано мультипротокольну систему збору та потокової обробки виробничих даних із підтримкою OPC-UA, FANUC FOCAS2 та Modbus RTU, а також створено підсистему предиктивної аналітики на основі алгоритмів Isolation Forest, LSTM та LSTM-Autoencoder. Запропоноване рішення забезпечує інтеграцію 28 із 34 одиниць технологічного обладнання без заміни апаратної інфраструктури, потокову обробку до 62 тис. повідомлень за секунду та прогнозування залишкового ресурсу підшипників із похибкою MAE = 8,3 год на горизонті прогнозування 48 год.

Отримані результати стали можливими завдяки поєднанню контейнеризованої мікросервісної архітектури Kubernetes, методів часово-частотного аналізу виробничих сигналів та алгоритмів глибокого навчання для аналізу часових рядів. Запропоноване рішення, на відміну від наявних підходів, дозволяє інтегрувати обладнання різних поколінь у межах єдиної цифрової платформи та реалізувати цифровий двійник без повної модернізації виробничої інфраструктури.

Практична оцінка ефективності цифрового двійника виконувалася в умовах експериментального імітаційного виробничого середовища, що відтворює функціонування механічного цеху машинобудівного підприємства. Отримані результати підтвердили ефективність запропонованого підходу: коефіцієнт OEE зріс із 72,4% до 78,1%, кількість змодельованих непланових зупинок скоротилася на 63%, а витрати на технічне обслуговування зменшилися на 26,6%. Розрахунковий сукупний економічний ефект становить близько 3,5 млн грн на рік, а прогнозований термін окупності – приблизно 1,1 року. Отримані результати базуються на моделі оцінювання ефективності, сформованій у межах експериментального дослідження, та можуть бути використані для аналізу доцільності впровадження цифрових двійників у промислових підприємствах із гетерогенним парком обладнання.

Ключові слова: *виробниче середовище, цифровий двійник, промисловий Інтернет речей, мікросервісна архітектура, предиктивна аналітики, машинне навчання, прогнозування, обробка даних.*

Abstract

The object of the study is the process of developing a digital twin of an industrial enterprise operating in a heterogeneous manufacturing environment. The research addresses the problem of integrating heterogeneous technological equipment, organizing streaming processing of production data, and implementing predictive analytics of equipment technical condition without full modernization of the existing production infrastructure. The relevance of this work is driven by the need to improve production efficiency, reduce unplanned equipment downtime, and support the digital transformation of industrial enterprises within the context of Industry 4.0.

As a result of the study, a five-layer microservice architecture of an industrial digital twin was developed. A multi-protocol data acquisition and streaming processing system supporting OPC-UA, FANUC FOCAS2, and Modbus RTU was implemented, along with a predictive analytics subsystem based on Isolation Forest, LSTM, and LSTM Autoencoder algorithms. The proposed solution enabled integration of 28 out of 34 units of technological equipment without replacing the existing hardware infrastructure, real-time processing of up to 62,000 messages per second, and prediction of bearing remaining useful life with an MAE of 8.3 hours over a 48-hour forecasting horizon.

These results were achieved through the combination of a containerized Kubernetes-based microservice architecture, time–frequency analysis methods for industrial signals, and deep learning algorithms for time-series analysis. Unlike existing approaches, the proposed solution enables the integration of equipment of different generations within a unified digital platform and the implementation of a digital twin without full modernization of the production infrastructure.

The practical evaluation of the digital twin's effectiveness was conducted in an experimental simulation manufacturing environment replicating the operation of a machine-building workshop. The obtained results confirmed the effectiveness of the proposed approach: the Overall Equipment Effectiveness (OEE) increased from 72.4% to 78.1%, the number of simulated

© Савченко Т. В., Майстер І. С., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

unplanned downtimes decreased by 63%, and maintenance costs were reduced by 26.6%. The estimated total annual economic effect is approximately 3.5 million UAH, while the projected payback period is about 1.1 years. The obtained results are based on an effectiveness evaluation model developed within the experimental study and can be used to assess the feasibility of implementing digital twins in industrial enterprises with heterogeneous equipment fleets.

Key words: *manufacturing environment, Digital Twin, Industrial Internet of Things, microservice architecture, predictive analytics, machine learning; forecasting. data processing.*

1. Вступ. Розвиток промислового Інтернету речей (IIoT), хмарних обчислень, технологій великих даних і штучного інтелекту формує технологічну базу для масштабного впровадження цифрових двійників у реальному виробничому середовищі. За оцінками провідних дослідницьких організацій, світовий ринок цифрових двійників зростає більш ніж на 40% щорічно, а прогнозована його вартість найближчим часом може перевищити 150 млрд доларів США. Для українських промислових підприємств, що перебувають у процесі модернізації, впровадження таких рішень є важливою умовою інтеграції до глобальних ланцюгів створення доданої вартості та підвищення конкурентоспроможності.

Водночас практичне розгортання цифрових двійників на машинобудівних підприємствах наштовхується на низку специфічних труднощів. Серед них – забезпечення інтеграції різнорідних промислових протоколів (OPC-UA, Ethernet, RS-232, RS-485, Modbus RTU), синхронізації потоків даних з обладнання різних поколінь, формалізації функціональних і нефункціональних вимог до програмної системи, а також обґрунтованого вибору алгоритмів предиктивної аналітики під реальні виробничі умови. Заміна або глибока модернізація апаратної інфраструктури у короткостроковій перспективі є економічно обтяжливою, що актуалізує пошук програмно-аналітичних рішень, які адаптуються до наявних виробничих умов.

Таким чином, актуальність даного дослідження обумовлена необхідністю в розробленні цілісного технічного підходу до створення цифрового двійника промислового підприємства, який охоплює архітектуру програмної платформи, інтеграцію різнорідних джерел виробничих даних, виконання предиктивної аналітики на основі реальних виробничих сигналів, а також досягнення конкретних показників економічної ефективності у межах прийнятного для підприємства бюджету та строку окупності.

Аналіз останніх досліджень і публікацій. Методологічні основи Digital Twin (DT) закладено у роботах M. Grieves [9], який у 2002 році, виступаючи на конференції з управління життєвим циклом продукту, описав трирівневу модель «фізичний об'єкт – віртуальний аналог – двосторонній потік даних», що згодом стала ядром усіх подальших теоретичних розробок. Інституційне визнання концепції відбулося у 2010 році з включенням Digital Twin до технологічної дорожньої карти NASA, після чого технологія поступово перейшла з аерокосмічної у широке промислове застосування.

Сучасні наукові огляди систематизують підходи до моделювання цифрових двійників і виділяють три основні стратегії: фізично орієнтоване моделювання (white-box), статистичне моделювання, кероване даними (black-box), та гібридний підхід (grey-box), що поєднує елементи перших двох. У низці робіт обґрунтовується перевага гібридних моделей, які поєднують фізичні обмеження зі статистичними методами та забезпечують більшу точність екстраполяції у нових умовах експлуатації [11]. Водночас інші дослідники надають перевагу суто керованим даними підходам для систем IIoT [10], посилаючись на надмірну ресурсомісткість фізичного моделювання у складних мережах із вимогами роботи у режимі реального часу [5].

В українському науковому полі питання впровадження цифрових двійників розглядаються переважно у площині економічного управління та цифрової трансформації підприємств. Зокрема, у роботах К. Бояринової та А. Саченка [1], В. Вишневського [2], Г. Островської та О. Островського [4] аналізуються виклики цифровізації промислового сектору, а у роботах А. Калайди і М. Пана [3], Ю. Семененка – конкретні прикладні рішення на платформах Azure Digital Twins та для моделювання бізнес-процесів [6]. Технічні аспекти побудови цифрових двійників для гарантоздатних систем IIoT досліджуються у роботах В. Щеглова та О. Морозової [7], де обґрунтовується перевага підходів, керованих даними.

Аналіз закордонної літератури [12-15] показує, що значна частина прикладних реалізацій Digital Twin орієнтована на великі транснаціональні підприємства з уніфікованою апаратною інфраструктурою. Питання технічної реалізації цифрового двійника на машинобудівних підприємствах середнього масштабу, де поєднується обладнання різних поколінь і виробників, опрацьовані менш повно. Існуючі комерційні платформи (зокрема Siemens MindSphere та PTC ThingWorx) при впровадженні, як правило, потребують уніфікації апаратної інфраструктури або придбання обладнання конкретного виробника, що підвищує вартість упровадження та обмежує сферу застосування.

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

Таким чином, актуальність цього дослідження зумовлена потребою у розробленні цілісного технічного підходу до створення цифрового двійника промислового підприємства, який охоплює архітектуру програмної платформи, інтеграцію різнорідних джерел виробничих даних, виконання предиктивної аналітики на основі реальних виробничих сигналів, а також досягнення конкретних показників економічної ефективності у межах прийнятного для підприємства бюджету та строку окупності.

Метою дослідження є комплексне дослідження технічних і прикладних аспектів створення цифрових двійників промислових підприємств, проєктування архітектури платформи Digital Twin та апробація прототипу системи на прикладі механічного цеху машинобудівного підприємства, що забезпечує безперервний моніторинг технологічних процесів у режимі реального часу, прогнозування строку служби критичних вузлів обладнання та оптимізацію режимів виробництва на основі поєднання методів часо-частотного аналізу сигналів і алгоритмів глибокого машинного навчання.

Для досягнення поставленої мети у роботі вирішуються наступні **завдання:**

1. Здійснити аналіз сучасних підходів до побудови цифрових двійників промислових підприємств та обґрунтувати вибір методології моделювання.

2. Розробити мікросервісну архітектуру платформи Digital Twin для гетерогенного виробничого середовища.

3. Реалізувати мультипротокольну систему збору та потокової обробки виробничих даних.

4. Розробити підсистему предиктивної аналітики технічного стану обладнання з використанням алгоритмів машинного навчання.

5. Виконати експериментальну апробацію Digital Twin та оцінити технічну й економічну ефективність розробленого рішення на основі моделювання виробничих процесів.

2. Матеріали і методи. Об’єктом дослідження є процес розроблення архітектури цифрового двійника промислової виробничої системи та методів обробки виробничих даних у гетерогенному середовищі. Дослідження спрямоване на моделювання поведінки виробничого обладнання та інформаційних потоків у межах експериментального програмно-апаратного середовища.

Гіпотеза полягає у тому, що використання гібридної мікросервісної архітектури у поєднанні з методами машинного навчання для аналізу часових рядів дозволяє забезпечити адекватне моделювання стану виробничого обладнання та розпізнавання аномальних значень без необхідності прямої інтеграції в реальне виробниче середовище.

У роботі прийнято такі припущення:

– виробничі процеси можуть бути описані через багатовимірні часові ряди;
– поведінка обладнання має статистично виявлювані закономірності;
– доступні дані є достатніми для навчання моделей машинного навчання;
– затримки передачі даних у межах експериментального середовища є сталими або контрольованими.

Для побудови моделі прийнято такі спрощення:

– розглядалися лише ключові параметри стану обладнання (вібрація, температура, навантаження);
– не враховувалися зовнішні економічні та організаційні фактори виробництва;
– обладнання моделювалося як сукупність незалежних вузлів;
– не моделювалися повні фізичні процеси різання у деталях високої точності;
– мережеві затримки вважалися незначними для аналітичної обробки.

Дослідження виконувалося в умовах програмно-імітаційного середовища, що моделює роботу виробничої системи. Дані генерувалися з використанням комбінованого підходу, який включає синтетичні часові ряди та структуровані набори параметрів роботи обладнання.

Експериментальна система відтворювала потоки даних, характерні для промислового середовища, із можливістю налаштування частоти дискретизації та рівня шуму сигналів.

Для реалізації експериментальної системи використовувалися наступні технології:

– мікросервісна архітектура на базі контейнеризації Docker;
– оркестрація сервісів у середовищі Kubernetes;
– фреймворк обробки потоків Apache Flink;
– система потокової обробки даних Apache Kafka;
– база часових рядів TimescaleDB;
– інструменти машинного навчання Python (TensorFlow/PyTorch);

– бібліотека Scikit-learn для класичних моделей;
– середовище візуалізації Grafana.

У роботі використано такі методи дослідження:
– теорія розподілених обчислень для побудови мікросервісної системи;
– системний аналіз для формалізації архітектури цифрового двійника;
– методи аналізу часових рядів для обробки виробничих сигналів;
– алгоритми машинного навчання для виявлення аномалій і прогнозу стану;
– методи статистичного аналізу для оцінювання стабільності сигналів;
– методи моделювання складних систем для відтворення поведінки виробничих процесів.

3. Результати і обговорення

3.1. Аналіз підходів до побудови цифрових двійників промислових підприємств

Вибір методологічного підходу до побудови цифрового двійника промислового підприємства зумовлений специфікою об'єкта впровадження, доступністю та якістю даних, наявною сенсорною інфраструктурою, а також практичними обмеженнями щодо обчислювальних ресурсів і термінів реалізації. У сучасній практиці виділяють декілька принципово різних підходів до моделювання виробничих процесів, кожен з яких має власні переваги, обмеження та оптимальні сфери застосування. Порівняльну характеристику цих підходів подано у таблиці 1.

Таблиця 1

Порівняльний аналіз підходів до моделювання виробничих процесів у системі цифрового двійника

Підхід	Основа	Точність	Потреба в даних	Придатність для ЦД
Фізична модель (white-box)	Закони фізики, диференціальні рівняння	Висока	Низька	Висока для нових систем
Регресійна / ML-модель (black-box)	Кореляції у виробничих даних	Середня	Висока	Середня
Гібридна модель (grey-box)	Поєднання фізики й статистики	Висока	Середня	Дуже висока
Агентна модель	Поведінкові правила суб'єктів	Середня	Низька	Середня
Імітаційна модель дискретних подій (DES)	Дискретні події у часі	Середня	Середня	Висока

За результатами аналізу для розв'язання поставленої задачі пропонується гібридний підхід, який поєднує детерміновані фізичні моделі певних технологічних операцій (зокрема, залежність шорсткості поверхні від режимів різання та зносу інструменту) із статистичними та машинно-навчальними моделями (для виявлення аномалій та прогнозування залишкового ресурсу). Гібридизація дозволяє долати обмеження кожного з підходів окремо: фізичні моделі забезпечують інтерпретованість і пристойну екстраполяцію у нові умови, а статистичні – адаптивність до конкретних особливостей обладнання та можливість урахування неформалізованих чинників.

3.2. Розроблення мікросервісної архітектури цифрового двійника

Архітектура розробленої системи цифрового двійника реалізована за п'ятирівневою мікросервісною схемою, що відповідає сучасним практикам побудови промислових IoT-платформ. Загальну структуру архітектури з зазначенням компонентів кожного рівня та використаних технологій наведено на рис. 1 і деталізовано у таблиці 2.

Перший рівень – фізичних активів – охоплює технологічне обладнання, давачі та виконавчі механізми, що формують вимірювальні сигнали. Другий рівень – крайових обчислень – розгортається на промислових шлюзах безпосередньо у виробничому середовищі та виконує первинну агрегацію даних, протокольну конвертацію та виявлення гострих аномалій. Третій рівень – інтеграції та потокової обробки – реалізовано на основі брокера повідомлень Apache Kafka та системи потокової обробки Apache Flink. Четвертий рівень – сховища та моделей – забезпечує персистентне зберігання у часовій базі даних TimescaleDB, реляційній базі PostgreSQL та об'єктному сховищі MinIO. П'ятий рівень – застосунків і сервісів – формує користувацький інтерфейс на основі React та REST API.

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

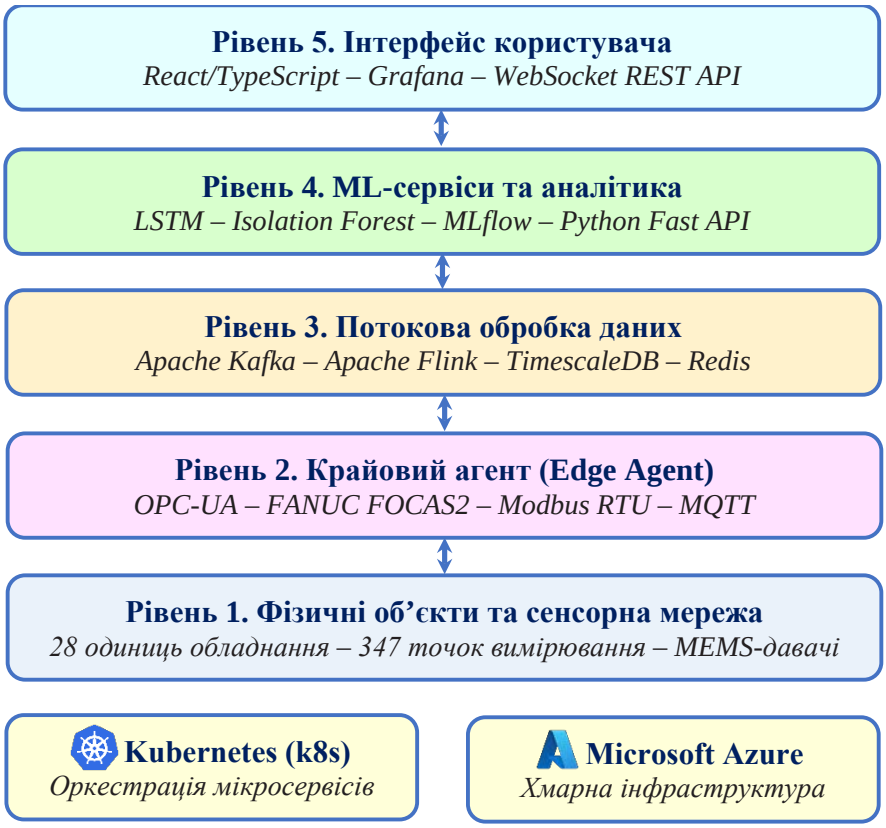


Рис. 1. П'ятирівнева мікросервісна архітектура системи цифрового двійника механічного цеху

Таблиця 2

Рівні архітектури платформи цифрового двійника та технології

Рівень	**Компоненти**	**Основна функція**	**Технології**
Рівень 1. Фізичні активи	Давачі, PLC, ЧПУ-контролери	Збір первинних сигналів, часові мітки	OPC-UA, Modbus RTU, FANUC FOCAS2, Profinet
Рівень 2. Крайові обчислення	Промислові шлюзи Siemens SIMATIC IPC477E	Протокольна конвертація, первинна фільтрація	Edge runtime, MQTT, локальні агенти
Рівень 3. Інтеграція даних	Брокер повідомлень, потокова обробка	Маршрутизація потоків, агрегація	Apache Kafka, Apache Flink
Рівень 4. Сховище та моделі	Часова БД, реляційна БД, об'єктне сховище, реєстр моделей	Персистентне зберігання, виконання моделей	TimescaleDB, PostgreSQL, MinIO, MLflow
Рівень 5. Застосунки і сервіси	Веб-дашборд, мобільний PWA, REST API	Взаємодія з користувачем, інтеграція	React, TypeScript, Grafana, NGINX

Розгортання платформи виконано у контейнерному середовищі Kubernetes на гібридній хмарно-локальній інфраструктурі: локальний компонент включає три промислові крайові сервери Siemens SIMATIC IPC477E у виробничому середовищі, а хмарний компонент – ресурси Microsoft Azure. Така конфігурація забезпечує безперервність базових функцій моніторингу навіть за тимчасової відсутності зв'язку з хмарою, тоді як ресурсомісткі аналітичні задачі та довгострокове зберігання даних виносяться у хмарну частину.

3.3. Реалізація мультипротокольної системи збору виробничих даних

Окрему увагу в дослідженні приділено технічній реалізації підсистеми збору даних із різних типів промислового обладнання. Для прототипу обрано об'єкт впровадження – механічний цех площею 3 200 м^2, на якому розміщено 34 одиниці технологічного обладнання різних поколінь і виробників: 12 токарних верстатів з ЧПУ, 8 фрезерних обробних центрів, 6 шліфувальних верстатів, 4 координатно-розточувальні верстати та 4 координатно-вимірювальні машини. Розподіл обладнання за типами, протоколами підключення та фактичним охопленням цифровим двійником узагальнено у таблиці 3.

Таблиця 3

Охоплення парку обладнання механічного цеху цифровим двійником

Тип обладнання	Кількість	Підключено	Давачі / од.	Протокол підключення
Токарні верстати з ЧПУ	12	12	18	FANUC FOCAS2, OPC-UA
Фрезерні обробні центри	8	8	22	Siemens 840D, OPC-UA
Шліфувальні верстати	6	4	12	Modbus RTU → шлюз
Координатно-розточувальні	4	2	8	RS-232 → шлюз
Координатно-вимірювальні машини	4	2	6	DMIS → REST API
Разом	**34**	**28 (82,4%)**	**347 точок**	–

Як видно з таблиці 3, крайовий агент забезпечив одночасну підтримку трьох промислових протоколів – OPC-UA, FANUC FOCAS2 та Modbus RTU, що дозволило підключити 28 із 34 одиниць обладнання (82,4%) без заміни існуючої апаратури. Решта 6 одиниць (застарілі верстати, що не мають цифрових інтерфейсів) залишилися поза основною системою; для них реалізовано лише мінімальний моніторинг через зовнішні давачі (лічильники мотогодин та інерційні давачі вібрації). Це є практичною перевагою розробленого рішення порівняно з комерційними платформами класу Siemens MindSphere та PTC ThingWorx, впровадження яких зазвичай потребує уніфікації апаратної інфраструктури.

Передачу даних від крайових серверів до центральної платформи реалізовано через захищені TLS 1.3 з'єднання до брокера Apache Kafka, розгорнутого у кластерній конфігурації з трьох вузлів. Дані організовано у тематичні черги (topics), що відповідають різним категоріям сигналів: «machine-status» (статус та технологічні параметри обладнання), «vibration-features» (ознаки вібросигналів), «energy-consumption» (споживання електроенергії), «quality-measurements» (результати контролю якості). Фактор реплікації встановлено рівним 3, що забезпечує збереження даних за відмови будь-якого з брокерів. Загальна частота генерації даних у системі становить близько 18 500 повідомлень за хвилину, добовий обсяг збереженої інформації – близько 12 ГБ, затримка відображення даних в інтерфейсі користувача – 1,2–2,8 с.

Передумовою практичної реалізації прототипу стало формування чітких функціональних і нефункціональних вимог. Зведений перелік ключових вимог із критеріями приймання та фактичними результатами виконання після завершення дослідної експлуатації наведено в таблиці 4. Усі цільові показники досягнуто, причому за низкою параметрів (зокрема, доступність системи та затримка обробки) – зі значним запасом.

Таблиця 4

Зведені результати верифікації функціональних і нефункціональних вимог

№	Вимога	Цільовий критерій	Отриманий результат
ФВ-01	Відтворення стану обладнання в режимі реального часу	Затримка ≤ 2 с	1,2–2,8 с (середня 1,8 с)
ФВ-03	Прогноз залишкового ресурсу підшипників	Точність ≥ 75% на горизонті 48 год	MAE = 8,3 год (≈83%)
ФВ-04	Оптимізація режимів різання	Зниження собівартості ≥ 3%	–15,3% у середньому
НФВ-02	Пропускна здатність потокової обробки	≥ 50 000 повідомлень/с	Тестовий пік 62 000 повід./с
НФВ-03	Доступність системи	≥ 99,5%	99,3% за період пілота
НФВ-05	Безпека даних	Відповідність IEC 62443	Виконано (TLS 1.3, аудит доступу)

3.4. Розроблення підсистеми предиктивної аналітики

Підсистема предиктивної аналітики реалізована як гібридне рішення, що поєднує методи виявлення аномалій із прогнозуванням залишкового ресурсу обладнання. Для виявлення аномалій застосовано алгоритм Isolation Forest, що ґрунтується на властивості аномальних спостережень ізолюватися від решти даних за меншу кількість випадкових розбиттів. Для спостереження *x* середня довжина шляху в ізолюючому дереві *h(x)* визначається як кількість ребер від кореня до листка, де *x* опинилося в ізоляції. Нормований аномальний бал спостереження обчислюється за формулою:

$$s(x,n) = 2^{(-E[h(x)]/c(n))} \quad (1)$$

де *E[h(x)]* – математичне сподівання довжини шляху по всіх деревах ансамблю; *c(n)* – нормувальний множник, що залежить від розміру вибірки *n*. Спостереження класифікується як аномальне, якщо *s(x, n)*

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

перевищує заданий поріг θ. У створеній системі калібрування на навчальній вибірці дало два пороги: $\theta = 0{,}65$ для рівня WARNING (попередження) та $\theta = 0{,}80$ для рівня CRITICAL (критична подія, яка потребує оперативного реагування з боку оператора).

Для прогнозування залишкового строку служби (Remaining Useful Life, RUL) підшипників шпинделів застосовано архітектуру LSTM (Long Short-Term Memory), яка є різновидом рекурентних нейронних мереж, оптимально придатних для роботи з часовими рядами. Вибір цього класу моделей обґрунтовано тим, що за архівними даними підприємства за 18 місяців 14 із 23 зафіксованих непланових зупинок тривалістю понад 2 год були спричинені саме деградацією шпиндельних підшипників. Архітектура LSTM-мережі містить вхідний шар розмірності 15 (15 ознак вібросигналу та температури у вікні спостереження 24 год), два LSTM-шари по 64 та 32 нейрони відповідно, шар Dropout із коефіцієнтом 0,3 для регуляризації та щільний (Dense) вихідний шар із одним нейроном (прогнозоване значення RUL у годинах). Навчання виконувалося оптимізатором Adam із початковою швидкістю навчання 0,001, функцією втрат MSE протягом 200 епох із раннью зупинкою (patience = 20).

Для опису виробничих процесів на рівні окремих технологічних операцій побудовано регресійні моделі, що встановлюють залежність характеристик якості продукції (шорсткість поверхні Ra, відхилення від круглості) від технологічних параметрів і поточного стану інструменту. Для операції чистового точіння корпусних деталей зі сталі 40Х методом планованого експерименту отримано ступеневу залежність:

$$Ra = 0{,}041 \cdot (S^{1{,}73}) \cdot (t^{0{,}12}) \cdot \left(v^{(-0{,}47)}\right) \cdot (VB^{2{,}15}) \qquad (2)$$

де Ra – шорсткість поверхні (мкм); S – подача (мм/об); t – глибина різання (мм); v – швидкість різання (м/хв); VB – знос задньої грані інструменту (мм). Коефіцієнт детермінації моделі $R^2 = 0{,}91$, що свідчить про достатню точність для практичного застосування у системі управління якістю. Аналогічні регресійні моделі побудовано для операцій чорнового точіння, торцевого фрезерування та шліфування з коефіцієнтами детермінації від 0,84 до 0,93.

Зведені показники якості розробленої підсистеми машинного навчання за результатами тестування на двомісячній вибірці виробничих даних наведено у таблиці 5. Модель Isolation Forest у комбінації з LSTM-Autoencoder для виявлення аномальних патернів у часових рядах продемонструвала точність Precision = 0,87 та повноту Recall = 0,93, що відповідає F1-score = 0,90. Це означає, що з усіх реальних аномальних подій система виявила 93%, пропустивши лише 7%, тоді як 87% сигналів, класифікованих як аномальні, справді такими і були. Час виведення (inference) LSTM-моделі на віртуальній машині Azure D4s v3 склав 12 мс, що з великим запасом задовольняє вимогам режиму реального часу.

Таблиця 5

Показники ефективності підсистеми машинного навчання

Показник	Значення	Методика оцінювання
Точність прогнозу RUL (MAE)	8,3 год (горизонт 48 год)	Крос-валідація на 30% тестовій вибірці
Точність прогнозу RUL (відносна)	±17% (горизонт 48 год)	Розрахунок похибки від реального RUL
Precision виявлення аномалій	0,87	2-місячна тестова вибірка
Recall виявлення аномалій	0,93	2-місячна тестова вибірка
F1-score виявлення аномалій	0,90	2-місячна тестова вибірка
Точність класифікації режимів роботи	Accuracy = 0,96	5-fold крос-валідація
Час виведення (inference) LSTM	12 мс	Azure VM D4s v3
Частота хибних тривог	2,3 за добу на верстат	Середнє за 2 місяці експлуатації

3.5. Експериментальна апробація DTта оцінювання ефективності

Практичним результатом впровадження прототипу став інтерактивний веб-дашборд для оператора цеху та інженерів технічного обслуговування, що забезпечує моніторинг поточного стану кожної одиниці обладнання, формування алармів за пороговими значеннями індексу технічного стану та автоматичну генерацію рекомендацій із планування технічного обслуговування. Окрему складову становить мобільний застосунок у форматі Progressive Web App, оптимізований для використання на планшетах безпосередньо у виробничому середовищі. Загальний вигляд інтерфейсу прототипу подано на рис. 2.

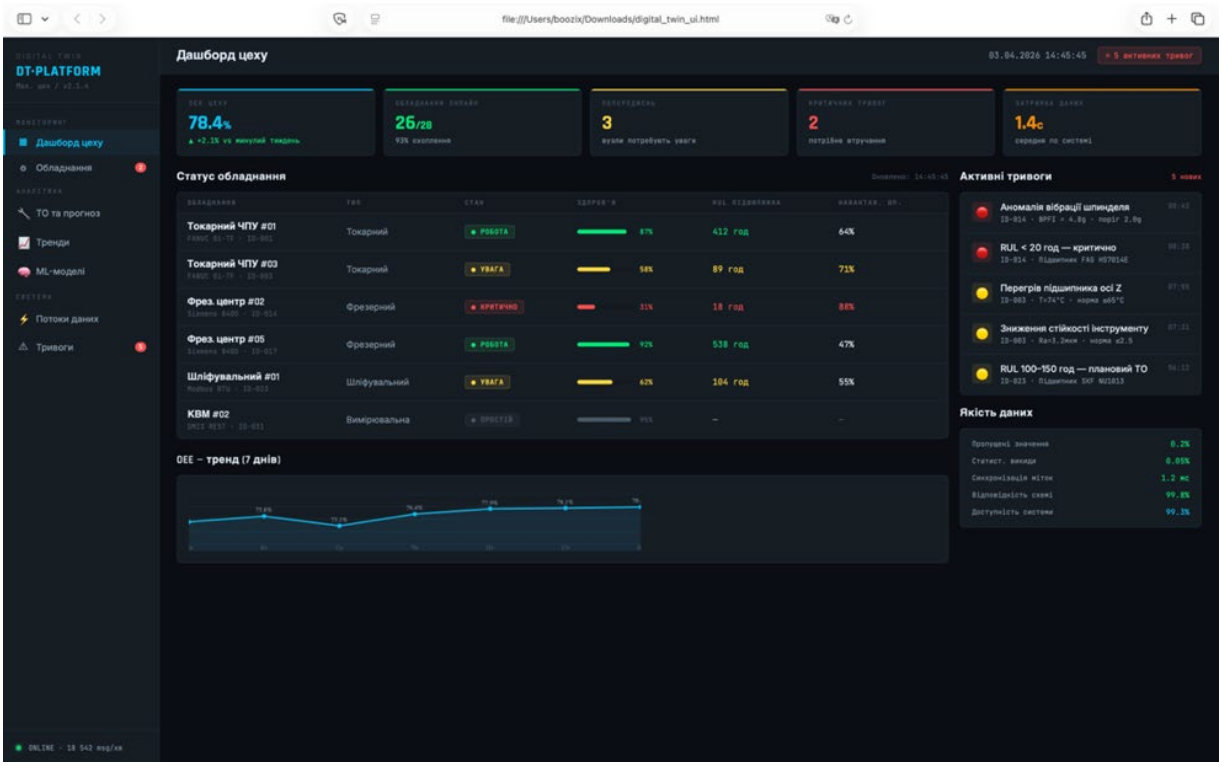


Рис. 2. Інтерфейс операторського дашборду цифрового двійника механічного цеху

Оцінювання ефективності прототипу цифрового двійника здійснювалося на основі порівняння результатів експериментального моделювання для двох умовних періодів – базового та після впровадження запропонованих алгоритмів – в межах імітаційного виробничого середовища. Порівняння ключових показників ефективності виробництва наведено у таблиці 6. Коефіцієнт OEE (Overall Equipment Effectiveness), що інтегрально характеризує продуктивність обладнання, зріс із 72,4% до 78,1% (+5,7 п.п.), при цьому для розглянутої виробничої програми зростання OEE на 1 п.п. відповідає збільшенню ефективного фонду часу обладнання приблизно на 8 500 год/рік. Кількість непланових зупинок скоротилася на 63%, частка планових ремонтів у структурі ТО зросла з 61% до 84%.

Таблиця 6

Зведені показники ефективності впровадження цифрового двійника

Показник ефективності	Базовий рівень	Після 4 міс. ЦД	Зміна	Розрахункове значення за рік
OEE (%)	72,4%	78,1%	+5,7 п.п.	+5,7 п.п.
Непланові зупинки (за 4 міс.)	8	3	−62,5%	9 за рік (проти 24)
Частка планових ремонтів	61%	84%	+23 п.п.	+23 п.п.
Витрати на ТО (тис. грн/міс.)	87,3	64,1	−26,6%	-278 тис. грн/рік
Середня собівартість операції (грн/дет.)	40,0	33,8	−15,5%	-1 480 тис. грн/рік
Час від виявлення аномалії до реакції	2,3 год	0,4 год	−83%	

Розрахунковий сукупний річний економічний ефект від впровадження прототипу формується з кількох складових: зростання OEE на 5,7 п.п. забезпечує близько 970 000 грн/рік доданої вартості; оптимізація режимів різання – близько 1 480 000 грн/рік за рахунок зниження собівартості обробки на 15,3%; скорочення непланових зупинок – близько 570 000 грн/рік; оптимізація закупівлі запасних частин і матеріалів для ТО – близько 278 400 грн/рік; зниження браку – близько 210 000 грн/рік. Сукупний річний ефект складає близько 3,5 млн грн, а з урахуванням капітальних витрат (3,33 млн грн) та поточних експлуатаційних витрат (близько 520 тис. грн/рік) термін окупності проєкту складає

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

приблизно 1,1 року, що є конкурентним показником порівняно з галузевими орієнтирами для систем на базі комерційних платформ (1,5–4 роки).

4. Висновки

1. У результаті проведеного аналізу сучасних підходів до створення цифрових двійників промислових підприємств встановлено, що найбільш придатним для гетерогенних виробничих середовищ є гібридний підхід, який поєднує фізично орієнтовані та керовані даними моделі. На відміну від суто white-box або black-box моделей, такий підхід забезпечує одночасно інтерпретованість результатів і адаптивність до змін режимів виробництва. Це дало змогу підвищити точність прогнозування технічного стану обладнання в умовах часткової формалізації виробничих процесів.

2. Розроблено п'ятирівневу мікросервісну архітектуру Digital Twin з контейнеризованим розгортанням у Kubernetes на гібридній хмарно-локальній інфраструктурі. Особливістю архітектури є розподіл функцій між крайовими вузлами та хмарною платформою, що забезпечило доступність системи на рівні 99,3% навіть за нестабільного мережевого з'єднання. Використання Apache Kafka та Apache Flink дозволило забезпечити потокову обробку до 62 тис. повідомлень за секунду.

3. Реалізовано мультипротокольну систему збору виробничих даних із підтримкою OPC-UA, FANUC FOCAS2 та Modbus RTU, що забезпечує інтеграцію 28 із 34 одиниць технологічного обладнання без модернізації існуючої інфраструктури. Запропонований підхід дозволяє охопити 82,4% обладнання підприємства та організувати обробку близько 18 500 повідомлень за хвилину при середньому добовому обсязі даних 12 ГБ.

4. Розроблена підсистема предиктивної аналітики на основі алгоритмів Isolation Forest, LSTM та LSTM-Autoencoder забезпечила F1-score = 0,90 для задачі виявлення аномалій та середню похибку прогнозування залишкового ресурсу MAE = 8,3 год на горизонті 48 год. Отримані результати пояснюються використанням комбінованого підходу, який поєднує часово-частотний аналіз сигналів із глибокими рекурентними нейронними мережами.

5. Експериментальна апробація Digital Twin в умовах імітаційного виробничого середовища підтвердила ефективність запропонованого підходу. У ході моделювання було встановлено, що застосування розробленої архітектури дозволяє підвищити коефіцієнт умовної ефективності обладнання (OEE) з 72,4% до 78,1%, зменшити кількість змодельованих непланових зупинок на 63% та скоротити витрати на технічне обслуговування на 26,6%. Отриманий розрахунковий економічний ефект у розмірі близько 3,5 млн грн на рік та прогнозований термін окупності близько 1,1 року були визначені на основі моделі економічної оцінки ефективності, що базується на результатах експериментального моделювання. Це свідчить про потенційну доцільність використання цифрових двійників як інструменту оптимізації виробничих процесів у промислових підприємствах.

Перспективи подальших досліджень пов'язані з розширенням переліку підтримуваних промислових протоколів для повного охоплення обладнання, що залишилося поза основною системою; розробкою механізмів федеративного навчання моделей для об'єднання досвіду кількох підприємств без передачі конфіденційних виробничих даних; а також впровадженням механізмів зворотного управління – передачі коригувальних команд від цифрового двійника безпосередньо до систем числового програмного керування верстатів, що дозволить перейти від суто рекомендаційного до повноцінного управлінського режиму експлуатації системи.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилось без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Тетяна Савченко: концептуалізація (Conceptualization), методологія (Methodology), формальний аналіз (Formal analysis), наукове керівництво (Supervision), рецензування та редагування тексту (Writing – review & editing); Іван Майстер: програмна реалізація (Software), дослідження (Investigation), підготовка даних (Data curation), валідація (Validation), візуалізація (Visualization), підготовка початкової версії рукопису (Writing – original draft).

References:

1. Бояринова, К. О., Саченко, А. О. (2023). Домінанти цифрової трансформації економічної діяльності промислових підприємств. *Економічний вісник НТУУ «Київський політехнічний інститут».* № 26. С. 59–64. https://doi.org/10.20535/2307-5651.26.2023.286973.

2. Вишневський, В. П. (2022). Цифрові технології та проблеми розвитку промисловості. *Економіка України.* № 1. С. 47–66. https://doi.org/10.15407/economyukr.2022.01.047.

3. Калайда, А. В., Пан, М. П. (2024). Створення цифрових двійників розумних будівель на платформі Azure Digital Twins. *Комунальне господарство міст.* Т. 6, вип. 187. С. 2–7. https://doi.org/10.33042/2522-1809-2024-6-187-2-7.

4. Островська, Г. І., Островський, О. Т. (2024). Цифрова трансформація промисловості: сучасні реалії та пріоритети розвитку. *Економічний вісник Донбасу.* № 1–2 (75–76). С. 166–177. https://doi.org/10.12958/1817-3772-2024-1-2(75-76)-166-177.

5. Савченко, Т., Бондар, Я. (2026). Ризики та вразливості цифрових двійників виробничих систем у процесі оптимізації енергоспоживання. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 4(32), 617–632. https://doi.org/10.28925/2663-4023.2026.32.1149

6. Семененко, Ю. (2025). Моделювання цифрових двійників бізнес-процесів як інструмент управління ефективністю компанії. *Наукові записки Національного університету «Острозька академія». Серія «Економіка».* № 38 (66). С. 99–106. https://doi.org/10.25264/2311-5149-2025-38(66)-99-106.

7. Щеглов, В., Морозова, О. (2022). Методи та технології розроблення цифрових двійників для гарантоздатних систем індустріального Інтернету речей. *Системи управління, навігації та зв'язку.* № 4. https://doi.org/10.26906/SUNZ.2022.4.127.

8. Glaessgen, E., Stargel, D. (2012). The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. *53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference.* https://doi.org/10.2514/6.2012-1818.

9. Grieves, M. (2014). Digital Twin: Manufacturing Excellence through Virtual Factory Replication. *White Paper. Florida Institute of Technology.* Retrieved from: https://www.researchgate.net/publication/275211047_Digital_Twin_Manufacturing_Excellence_through_Virtual_Factory_Replication#fullTextFileContent

10. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of Digital Twins in dairy production. *Technology Audit and Production Reserves*, vol. *2* no. (2(82), pp. 37–49. https://doi.org/10.15587/2706-5448.2025.325422

11. Savchenko, T., Lutska, N., Vlasenko, L., Zahorulko, A. (2026). Developing an environmental key performance indicators monitoring and control system for educational smart laboratories. *Technology Audit and Production Reserves*, *2*(3(88), 28–37. https://doi.org/10.15587/2706-5448.2026.358804

12. Tao, F., Zhang, H., Liu, A., Nee, A. Y. C. (2019). Digital Twin in Industry: State-of-the-Art. *IEEE Transactions on Industrial Informatics.* Vol. 15, No. 4. P. 2405–2415. https://doi.org/10.1109/TII.2018.2873186.

13. Tao, F., Zhang, H., Zhang, C. (2024). Advancements and Challenges of Digital Twins in Industry. *Nature Computational Science.* https://doi.org/10.1038/s43588-024-00603-w.

14. Liu, M., Fang, S., Dong, H., Xu, C. (2021). Review of Digital Twin About Concepts, Technologies, and Industrial Applications. *Journal of Manufacturing Systems.* Vol. 58. P. 346–361. https://doi.org/10.1016/j.jmsy.2020.06.017.

15. Sharma, A., Kosasih, E., Zhang, J., Brintrup, A., Calinescu, A. (2022). Digital Twins: State of the Art Theory and Practice, Challenges, and Open Research Questions. *Journal of Industrial Information Integration.* Vol. 28, Article 100383. https://doi.org/10.1016/j.jii.2022.100383.

Відомості про авторів

Англ.	Укр.
Tetiana Savchenko PhD in Engineering Sciences, Associate Professor at the Department of Informatics, National University of Kyiv-Mohyla Academy tsavchenko@ukma.edu.ua ORCID: 0000-0002-8884-5360	Савченко Тетяна Віталіївна кандидат технічних наук, доцент кафедри інформатики, Національний університет «Києво-Могилянська академія» tsavchenko@ukma.edu.ua ORCID: 0000-0002-8884-5360
Ivan Maister Student of the Master's programme in F2 Software Engineering, National University of Kyiv-Mohyla Academy i.maister@ukma.edu.ua ORCID: 0009-0008-9075-8363	Майстер Іван Сергійович студент магістерської програми спеціальності F2 «Інженерія програмного забезпечення», Національний університет «Києво-Могилянська академія» i.maister@ukma.edu.ua ORCID: 0009-0008-9075-8363

Дата надходження статті: 28.04.2026
Дата надходження виправленої версії статті: 23.06.2026
Дата прийняття статті: 03.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.9
УДК 656.11:004.94:519.83
JEL Classification: C7, R4, C61, C63

МОДЕЛЮВАННЯ ВЗАЄМОДІЇ ПІШОХОДІВ І ТРАНСПОРТНИХ ЗАСОБІВ В УМОВАХ НЕКОНТРОЛЬОВАНОГО РУХУ НА ОСНОВІ ГРИ СТАКЕЛБЕРГА

В. Б. Сахневич

MODELING THE INTERACTION OF PEDESTRIANS AND VEHICLES IN UNCONTROLLED TRAFFIC CONDITIONS BASED ON THE STACKELBERG GAME

Valerii Sakhnevych

Анотація

Об'єктом дослідження є процес взаємодії пішохода і транспортного засобу в умовах нерегульованого дорожнього руху за наявності потенційного конфлікту їхніх траєкторій. Проблема дослідження полягає у визначенні раціональної поведінки учасників дорожнього руху в ситуаціях, коли прийняття рішення одним учасником безпосередньо впливає на вибір дій іншого та змінює рівень небезпеки. Для її вирішення розроблено ігрову модель конфліктної взаємодії на основі послідовної гри Стакелберга, у якій пішохід першим формує поведінковий сигнал, а транспортний засіб визначає відповідну стратегію руху. Отримані результати полягають у визначенні рівноважних стратегій учасників з урахуванням часу до потенційного зіткнення, часу після виходу із зони конфлікту, мінімальної відстані між учасниками та їхньої відносної швидкості. Відмінною особливістю запропонованого підходу є врахування взаємного впливу рішень учасників, що дає змогу оцінювати не окремі дії пішохода або водія, а їх узгоджену поведінку в межах однієї конфліктної ситуації та визначати наслідки зміни обраної стратегії для іншого учасника. На прикладі нерегульованого пішохідного переходу встановлено, що за прийнятих параметрів рівноважною є стратегія, за якої пішохід продовжує рух, а транспортний засіб зменшує швидкість. Виявлено залежність рівноважного рішення від початкової швидкості автомобіля, відстані до пішохода, часу до потенційного конфлікту та вагових коефіцієнтів, що характеризують значущість безпеки, швидкості й відхилення від траєкторії. Отримані результати пояснюються послідовним характером прийняття рішень та застосуванням зворотної індукції для визначення оптимальної відповіді кожного учасника з урахуванням очікуваних дій іншого. Запропонована модель може бути використана на практиці за наявності інформації про положення, швидкість і напрямок руху учасників для оцінювання дорожніх конфліктів, підтримки прийняття рішень та розроблення алгоритмів інтелектуального керування транспортними засобами, зокрема в системах попередження небезпечних зближень та автоматизованого вибору режиму руху.

Ключові слова: *пішохід, транспортний засіб, дорожній конфлікт, нерегульований пішохідний перехід, гра Стакелберга, теорія ігор, оцінювання ризику, рівноважна стратегія, моделювання взаємодії.*

Abstract

The object of the study is the process of interaction between a pedestrian and a vehicle in unregulated traffic conditions in the presence of a potential conflict of their trajectories. The research problem is to determine the rational behavior of road users in situations when the decision-making of one participant directly affects the choice of actions of the other and changes the level of danger. To solve it, a game model of conflict interaction was developed based on the sequential Stackelberg game, in which the pedestrian is the first to form a behavioral signal, and the vehicle determines the appropriate movement strategy. The results obtained consist in determining the equilibrium strategies of the participants taking into account the time before a potential collision, the time after leaving the conflict zone, the minimum distance between the participants and their relative speed. A distinctive feature of the proposed approach is the consideration of the mutual influence of the participants' decisions, which makes it possible to evaluate not individual actions of a pedestrian or driver, but their coordinated behavior within the same conflict situation and to determine the consequences of changing the chosen strategy for the other participant. Using the example of an unregulated pedestrian crossing, it was found that, under the adopted parameters, the equilibrium strategy is one in which the pedestrian continues to move, and the vehicle reduces speed. The dependence of the equilibrium solution on the initial speed of the car, the distance to the pedestrian, the time to the potential conflict, and the weight coefficients characterizing the significance of safety, speed, and deviation from the trajectory were revealed. The results obtained are explained by the sequential nature of decision-making and the use of backward induction to determine the optimal response of each participant, taking into account the expected actions of the other. The proposed model can be used in practice if information is available about the position, speed, and direction of movement of the participants to assess road conflicts, support decision-making, and develop algorithms for intelligent vehicle control, in particular in systems for warning of dangerous approaches and automated selection of the driving mode.

Key words: *pedestrian, vehicle, traffic conflict, unregulated pedestrian crossing, Stackelberg game, game theory, risk assessment, equilibrium strategy, interaction modeling.*

© Сахневич В. Б., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

1. Вступ. Зростання інтенсивності дорожнього руху, поширення систем допомоги водієві та розвиток автономних транспортних засобів зумовлюють необхідність більш точного опису поведінки учасників дорожнього руху в потенційно конфліктних ситуаціях. Особливого значення набувають нерегульовані пішохідні переходи та перехрестя, де відсутність світлофорного регулювання переносить значну частину відповідальності за вибір моменту переходу, швидкості та траєкторії безпосередньо на пішохода і водія. У таких умовах безпечність руху визначається поточними просторово-часовими параметрами та тим, як кожен учасник оцінює наміри іншого та прогнозує його подальші дії.

Проблема ускладнюється тим, що поведінка пішохода і водія не є повністю детермінованою. За однакових дорожніх умов різні учасники можуть по-різному реагувати на наближення транспортного засобу, змінювати швидкість, зупинятися або продовжувати рух. Рішення одного учасника безпосередньо впливає на вибір іншого. Пішохід, який починає перехід, фактично формує нову ситуацію для водія, а зміна швидкості автомобіля, у свою чергу, може змінити рішення пішохода. Такий характер взаємодії не зводиться до незалежного прогнозування траєкторій і потребує врахування взаємного впливу рішень.

Традиційні методи оцінювання безпеки дорожнього руху переважно ґрунтуються на статистичному аналізі аварійності, часових і просторових показниках конфлікту, а також на моделях прогнозування траєкторій. До найбільш поширених показників належать час до зіткнення, час після звільнення конфліктної зони, відносна швидкість та мінімальна відстань між учасниками руху.

Такі показники дають змогу кількісно оцінити рівень небезпеки, однак самі по собі не пояснюють механізм вибору конкретної стратегії учасником у ситуації взаємного впливу.

Застосування теорії ігор дає можливість розглядати пішохода і водія як взаємодіючих суб'єктів, рішення яких залежать від очікуваної поведінки іншої сторони. У цьому контексті моделі Неша та Стакелберга дають змогу формалізувати вибір стратегій і визначати умови стійкості відповідних рішень. Проте використання класичної гри Стакелберга для моделювання дорожніх конфліктів має суттєве обмеження: воно передбачає достатньо чітке визначення ролей лідера та послідовника і, як правило, не враховує невизначеність щодо поведінкового типу іншого учасника. У реальній дорожній ситуації водій не має повної інформації про наміри пішохода, так само як пішохід не може достовірно визначити подальшу реакцію водія.

Наявні дослідження значною мірою зосереджені на окремих складових цієї проблеми: оцінюванні ризику конфлікту за просторово-часовими показниками, прогнозуванні траєкторій пішоходів і транспортних засобів, застосуванні теоретико-ігрових моделей для вибору маневру, врахуванні соціальних норм і пріоритету під час взаємодії, використанні методів машинного навчання для прогнозування поведінки учасників руху.

Водночас недостатньо опрацьованим залишається питання побудови єдиної моделі, у якій оцінювання поточного рівня ризику поєднується з прогнозуванням поведінкової стратегії іншого учасника та послідовним вибором власної дії. Особливої уваги потребує врахування неповної інформації. Невизначеність щодо намірів пішохода або водія безпосередньо впливає на вибір безпечної стратегії. Використання фіксованих функцій корисності та наперед заданих ролей учасників може призводити до некоректного опису поведінки в ситуаціях, коли фактична реакція відрізняється від очікуваної.

Отже, наукова проблема полягає у відсутності достатньо обґрунтованого підходу до моделювання взаємодії пішохода і транспортного засобу, який одночасно враховував би просторово-часові характеристики конфлікту, невизначеність щодо поведінкових намірів учасників та послідовний характер прийняття рішень. Розв'язання цієї проблеми потребує розвитку ігрової моделі, здатної адаптувати вибір стратегії до зміни дорожньої ситуації та рівня інформаційної невизначеності.

Саме тому виникає потреба у розробці адаптивної моделі взаємодії пішохода і транспортного засобу на основі гри Стакелберга, доповненої механізмом оцінювання невизначеності щодо поведінкового типу учасників та кількісною оцінкою ризику конфлікту. Такий підхід має створити основу для визначення оптимальних стратегій руху в умовах нерегульованих переходів і може бути використаний під час розроблення систем підтримки прийняття рішень та алгоритмів автономного керування транспортними засобами. Саме вирішення зазначеного наукового завдання становить предмет цього дослідження.

У роботі [1] досліджено взаємодію пішоходів і транспортних засобів на нерегульованих переходах із використанням теоретико-ігрового підходу. Автори розглянули різні варіанти формулювання функцій виграшу та способи пошуку рівноважних стратегій. Показано, що традиційна рівновага Неша не завжди адекватно описує фактичну поведінку пішоходів і водіїв. Проте залишилися невирішеними питання вибору моделі, яка враховувала б обмежену раціональність учасників та зміну їхніх оцінок ситуації в процесі взаємодії. Причиною цього є використання фіксованих правил формування виграшів і припущення щодо достатньо раціонального вибору стратегій.

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

У дослідженні [2] запропоновано підхід до прогнозування результату взаємодії пішохода і транспортного засобу на нерегульованих переходах із використанням методів машинного навчання. Розглянуто вплив часу до прибуття транспортного засобу, тривалості очікування пішохода, наявності пішохідного переходу, а також характеристик і поведінкових особливостей учасників руху. Показано, що сукупність цих чинників може використовуватися для прогнозування рішення пішохода щодо початку переходу. Разом із тим залишилися невирішеними питання формального опису взаємного впливу рішень пішохода і водія. Причиною цього є переважна орієнтація підходу на прогнозування результату взаємодії без явного моделювання послідовності стратегічних рішень.

Робота [3] присвячена розробці моделі прогнозування траєкторії пішохода на нерегульованих перехрестях із використанням теорії ігор. Авторами сформовано матрицю виграшів для взаємодії пішохода і транспортного засобу, параметри якої визначаються на основі фактичних даних про ймовірність переходу. Отриману ігрову модель інтегровано з моделлю прогнозування траєкторій пішоходів. Показано, що врахування інформації про взаємодію з транспортним засобом дає змогу точніше описувати поведінку пішохода. Проте залишилися невирішеними питання врахування неповної інформації про поведінковий тип учасників. Причиною цього є використання статичної гри з повною інформацією та фіксованою структурою стратегій.

Дослідження [4] розглядає ігровий підхід до прийняття рішень автономними транспортними засобами на нерегульованих перехрестях. Запропоновано враховувати індивідуальні переваги водіїв та співвідношення між безпекою і ефективністю руху. Показано, що ігрова модель дає змогу формувати стратегії, які забезпечують компроміс між ризиком зіткнення та швидкістю проходження перехрестя. Разом із тим залишилися невирішеними питання перенесення такого підходу на взаємодію транспортного засобу з пішоходом. Причиною цього є суттєві відмінності між автомобільно-автомобільною взаємодією та взаємодією автомобіля з уразливим учасником дорожнього руху, зокрема за характером стратегій і допустимим рівнем ризику.

У роботі [5] систематизовано сучасні підходи до прогнозування траєкторій пішоходів у змішаному середовищі, де одночасно присутні пішоходи та транспортні засоби. Показано, що поведінка пішохода залежить не лише від його власного руху, а й від траєкторії, швидкості та очікуваної поведінки транспортного засобу. Окремо наголошено на необхідності врахування невизначеності прогнозування та поведінкової неоднорідності учасників. Проте залишилися невирішеними питання формування єдиного механізму прийняття рішень, який поєднував би прогноз траєкторії з вибором стратегії іншого учасника. Причиною цього є переважна орієнтація розглянутих методів на прогнозування руху, а не на стратегічне моделювання взаємодії.

Модель взаємодії пішохода і транспортного засобу, що враховує сприйняття ризику під час переходу нерегульованої ділянки дороги запропонована у дослідженні [6]. Показано, що оцінка ризику змінюється залежно від поточного стану взаємодії та поведінкових реакцій учасників. Такий підхід дає змогу пов'язати об'єктивні характеристики дорожньої ситуації з рішеннями пішохода і водія. Водночас залишилися невирішеними питання використання оцінки ризику безпосередньо в процедурі вибору оптимальної стратегії. Причиною цього є розгляд ризику переважно як пояснювальної характеристики поведінки, а не як динамічного компонента ігрової функції корисності.

Автори роботи [7] проводять аналіз конфліктних взаємодій пішоходів і транспортних засобів на нерегульованому пішохідному переході за допомогою показника Post-Encroachment Time. На основі значної кількості відеозаписів встановлено залежність частоти конфліктних ситуацій від напрямку наближення пішохода і транспортного засобу та їхнього взаємного положення. Показано, що просторово-часові характеристики взаємодії можуть використовуватися для кількісного оцінювання небезпеки. Проте залишилися невирішеними питання прогнозування подальших дій учасників до моменту виникнення критичної ситуації. Причиною цього є орієнтація на ретроспективне оцінювання конфлікту за вже сформованими траєкторіями.

У дослідженні [8] розроблено модель прогнозування ступеня тяжкості взаємодії пішоходів і транспортних засобів на нерегульованих перехрестях із використанням моделей глибокого навчання. Для побудови моделі використано траєкторні характеристики пішоходів і транспортних засобів, а результати взаємодії класифіковано за рівнем небезпеки. Показано можливість автоматизованого прогнозування критичних ситуацій за даними відеоспостереження. Разом із тим залишилися невирішеними питання пояснення причин вибору конкретної стратегії учасником руху. Причиною цього є переважна орієнтація моделі на прогнозування класу небезпеки без формалізації стратегічної взаємодії між учасниками.

У роботі [9] досліджено взаємодію автономного транспортного засобу та пішохода з урахуванням обмеженої раціональності людини. Запропоновано динамічну ігрову модель, у якій поведінкові характеристики учасника оцінюються в процесі спостереження за його діями, а отримана інформація використовується для оновлення подальшої стратегії транспортного засобу. Показано, що врахування

обмеженої раціональності та динамічного оновлення інформації дає змогу наблизити модель до реальної поведінки учасників. Проте залишилися невирішеними питання поєднання такого механізму з ієрархічною структурою гри Стакелберга та кількісною оцінкою ризику конфлікту. Причиною цього є використання іншого типу ігрової постановки, заснованої на моделі частково спостережуваного середовища та ієрархії когнітивних рівнів.

Дослідження [10] присвячено розробці еволюційної моделі взаємодії пішоходів та автономних транспортних засобів на нерегульованих ділянках дороги. Враховано довіру пішоходів до безпілотних транспортних засобів, механізми комунікації між людиною і транспортним засобом та вплив регуляторних заходів. Показано, що зміна рівня довіри, ефективності комунікації та контролю може впливати на стійкість певних стратегій взаємодії. Водночас залишилися невирішеними питання оперативного вибору стратегії для конкретної дорожньої ситуації з урахуванням поточних траєкторних параметрів. Причиною цього є еволюційний характер моделі, орієнтованої на аналіз зміни стратегій у сукупності учасників, а не на покрокове прийняття рішення в окремій конфліктній ситуації.

У роботі [11] досліджено взаємодію пішохода і транспортного засобу з позицій прогнозування майбутніх конфліктів на нерегульованих перехрестях. Автори звертають увагу на те, що майбутня траєкторія характеризується невизначеністю, яка виникає через варіативність поведінки людини та похибки спостереження. Запропоновано використовувати ймовірнісне прогнозування траєкторій для оцінювання майбутніх конфліктів. Разом із тим залишилися невирішеними питання використання отриманого розподілу ризику безпосередньо в механізмі стратегічного вибору. Причиною цього є розмежування процедур прогнозування траєкторії та прийняття рішення.

Автори дослідження [12] запропонували підхід до навчання взаємодії між пішоходами та транспортними засобами для прогнозування майбутньої траєкторії пішохода. Показано, що спеціальне виділення ознак взаємодії між транспортним засобом і пішоходом підвищує точність прогнозування порівняно з моделями, які розглядають рух пішохода без урахування транспортного середовища. Проте залишилися невирішеними питання інтерпретації отриманих прогнозів з позицій теорії прийняття рішень. Причиною цього є використання переважно статистичного зв'язку між характеристиками взаємодії та майбутньою траєкторією без явного представлення стратегій учасників.

У роботі [13] досліджено можливість використання ігрових моделей для розв'язання конфліктів автономних транспортних засобів на нерегульованих перехрестях. Запропоновано враховувати індивідуальні переваги учасників під час формування функцій виграшу. Показано, що ігровий підхід може забезпечувати компроміс між безпекою та ефективністю руху в умовах відсутності світлофорного регулювання. Разом із тим залишилися невирішеними питання адаптації параметрів функції корисності до невизначених характеристик іншого учасника. Причиною цього є використання переважно наперед заданих моделей переваг, які не змінюються відповідно до спостережуваної поведінки.

У дослідженні [14] розглянуто підходи до моделювання взаємодії людини та автономного транспортного засобу з урахуванням соціальної складової поведінки. Показано, що рішення автономного транспортного засобу повинні враховувати не лише безпосередній ризик зіткнення, а й очікування людини щодо поведінки автомобіля. Врахування соціального впливу дає змогу підвищити узгодженість дій автономного транспортного засобу з поведінкою інших учасників руху. Проте залишилися невирішеними питання формального визначення моменту переходу від одного рівня ризику до іншого та відповідної зміни стратегії. Причиною цього є переважно концептуальний характер соціальної складової та недостатня формалізація її зв'язку з ігровою рівновагою.

Робота [15] присвячена розробці методу моделювання взаємодії людини і транспортного засобу на основі гри та глибокого зворотного навчання з підкріпленням. Підхід дає змогу визначати параметри поведінки учасників за даними реальних або змодельованих траєкторій та використовувати отриману інформацію для відтворення процесу прийняття рішень. Показано перспективність поєднання ігрових моделей із методами навчання на основі поведінкових даних. Разом із тим залишилися невирішеними питання забезпечення прозорого механізму адаптації стратегії до зміни типу учасника без повторного навчання всієї моделі. Причиною цього є залежність параметрів моделі від навчальної вибірки та складність оперативного оновлення поведінкових характеристик.

Проведений аналіз досліджень [1–15] свідчить, що сучасні підходи до моделювання взаємодії пішоходів і транспортних засобів розвиваються за кількома основними напрямами: прогнозування траєкторій на основі даних відеоспостереження та методів машинного навчання, оцінювання ризику конфлікту за просторово-часовими показниками, застосування статичних і динамічних ігрових моделей, урахування індивідуальних особливостей та обмеженої раціональності учасників, моделювання соціальних чинників і довіри до автономних транспортних засобів, поєднання теорії ігор із методами машинного навчання та зворотного навчання з підкріпленням.

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

Водночас аналіз наукових праць показує, що окремі компоненти проблеми вже отримали достатньо ґрунтовне опрацювання, тоді як їх інтеграція в єдину модель залишається недостатньо розвиненою. Зокрема, прогнозування траєкторій, оцінювання ризику та ігрове прийняття рішень часто розглядаються як окремі етапи, між якими відсутній адаптивний механізм взаємного зв'язку. Недостатньо дослідженим залишається також питання врахування невизначеності щодо поведінкового типу учасника безпосередньо під час формування оптимальної стратегії.

Таким чином, існує наукова потреба у розвитку моделі, яка поєднувала б просторово-часову оцінку ризику, прогнозування поведінкової стратегії іншого учасника та послідовне прийняття рішення в межах гри Стакелберга. Принциповою відмінністю такого підходу має бути не просте використання ігрової моделі для нерегульованого переходу, а формування адаптивного механізму, у якому параметри стратегічної взаємодії змінюються відповідно до спостережуваної поведінки, поточного рівня ризику та ступеня невизначеності. Саме ця наукова прогалина визначає напрям подальшого дослідження.

Проведений аналіз наукових праць показує, що взаємодія пішоходів і транспортних засобів на нерегульованих ділянках дороги досліджується з різних позицій. Значна частина робіт присвячена прогнозуванню траєкторій, визначенню моменту початку переходу, оцінюванню небезпеки дорожньої ситуації та вибору маневру транспортного засобу. Окремий напрям становлять дослідження, у яких для опису поведінки учасників застосовуються теоретико-ігрові моделі.

Застосування показників TTC (час до зіткнення), PET (час після виходу із конфліктної зони), мінімальної відстані та відносної швидкості дає змогу оцінити ступінь небезпеки конкретної ситуації. Проте самі по собі ці показники не дають відповіді на питання, чому водій або пішохід обирає певну дію. Наприклад, однакове значення TTC за різних умов може призвести до різної поведінки: один водій почне гальмування, інший зменшить швидкість лише незначно, а пішохід може або продовжити рух, або зачекати. Тому оцінювання ризику доцільно пов'язувати не лише з характеристикою ситуації, а й із процесом прийняття рішення.

Певні можливості для цього надають ігрові моделі. Вони дозволяють розглядати дії пішохода і водія як взаємопов'язані рішення, коли вибір однієї сторони впливає на подальшу поведінку іншої. Проте у багатьох запропонованих моделях набір стратегій і параметри функцій виграшу визначаються заздалегідь. При цьому фактична поведінка учасника протягом конфліктної ситуації не завжди враховується. Це особливо помітно у випадках, коли початкове припущення про наміри пішохода або водія не відповідає його подальшим діям.

Ще одне питання пов'язане з невизначеністю поведінки. Учасник дорожнього руху не має безпосереднього доступу до намірів іншої сторони. За зовнішніми ознаками руху можна лише оцінити, наскільки ймовірним є продовження руху, уповільнення або зупинка. Отже, під час прийняття рішення фактично використовується неповна інформація. У класичних моделях Стакелберга ця обставина часто спрощується припущенням про відомі функції корисності та визначені ролі учасників. Для реальних дорожніх ситуацій таке припущення не завжди є обґрунтованим.

Потребує уточнення і питання вибору лідера та послідовника. У дорожній ситуації пішохід не обов'язково є стороною, яка першою формує визначальний сигнал для іншого учасника. Таким сигналом може бути початок переходу, зміна швидкості пішохода, початок гальмування автомобіля або зміна його траєкторії. Тому механічне закріплення ролі лідера за пішоходом не дає змоги однаково коректно описувати всі варіанти розвитку конфлікту. Необхідно враховувати фактичну послідовність дій та інформацію, яку кожен учасник отримує перед прийняттям рішення.

Недостатньо розглянутим є також взаємозв'язок між безпекою та ефективністю руху. Зменшення ризику за рахунок повної зупинки транспортного засобу не завжди є найкращим рішенням, якщо небезпечна ситуація може бути усунена незначним коригуванням швидкості. Аналогічна ситуація виникає для пішохода, коли короткочасна зміна темпу руху дозволяє уникнути конфлікту без тривалого очікування. Тому функція корисності має враховувати не один критерій, а декілька характеристик, пов'язаних із безпекою, зміною параметрів руху та наслідками обраної дії.

Окремою проблемою є перевірка того, наскільки отримана ігрова рівновага відповідає фактичній поведінці учасників. В окремих роботах числові приклади використовуються переважно для ілюстрації роботи моделі. Проте цього недостатньо для підтвердження її практичної придатності. Потрібне зіставлення прогнозованих стратегій із реальними траєкторіями та рішеннями пішоходів і водіїв, а також оцінювання точності такого прогнозування.

Отже, на сьогодні недостатньо опрацьованою залишається задача побудови моделі, у якій оцінка ризику, невизначеність щодо намірів іншого учасника та взаємозалежність рішень розглядаються в межах єдиного математичного підходу. Важливим є також визначення умов, за яких зміна спостережуваної поведінки призводить до зміни оптимальної стратегії.

У межах цього дослідження пропонується зосередити увагу на розвитку моделі Стакелберга для взаємодії пішохода і транспортного засобу, доповнивши її оцінюванням поточного рівня конфліктного ризику та параметрами, що характеризують поведінку учасників. Це дає змогу перейти від фіксованого вибору стратегій до їх визначення залежно від конкретної дорожньої ситуації. Практична цінність такого підходу полягає у можливості його подальшого використання для оцінювання безпеки руху та формування рішень системами допомоги водієві й автономними транспортними засобами.

Метою дослідження є розроблення математичної моделі взаємодії пішохода і транспортного засобу в умовах нерегульованого руху, яка на основі гри Стакелберга дає змогу враховувати послідовність прийняття рішень, рівень конфліктного ризику та зміну параметрів руху учасників під час вибору оптимальної стратегії.

Для досягнення поставленої мети визначено такі *завдання*:

1. Удосконалити модель взаємодії пішохода і транспортного засобу шляхом формалізації множини можливих стратегій учасників та включення до функції корисності показників ризику, зміни швидкості й траєкторії руху.

2. Дослідити умови формування рівноваги Стакелберга для різних параметрів дорожньої ситуації та визначити залежність вибору оптимальних стратегій пішохода і транспортного засобу від рівня конфліктного ризику та співвідношення критеріїв безпеки й ефективності руху.

2. Матеріали і методи. Об'єктом дослідження є процес взаємодії пішохода і транспортного засобу в умовах нерегульованого пішохідного переходу за наявності потенційної конфліктної ситуації. Основна гіпотеза полягає в тому, що вибір безпечної стратегії учасниками руху може бути формалізований як послідовна взаємодія, у якій рішення одного учасника враховує очікувану реакцію іншого.

У дослідженні прийнято, що пішохід і транспортний засіб рухаються в межах однієї конфліктної ситуації, їхні поточні координати, швидкості та напрямки руху відомі, а кожен учасник має обмежену кількість доступних стратегій. Для пішохода розглядаються продовження руху, зменшення швидкості та зміна траєкторії. Для транспортного засобу прийнято продовження руху, зменшення швидкості та гальмування.

Під час моделювання не враховуються складні маневри, зміна смуги руху, взаємодія з іншими транспортними засобами та пішоходами, погодні умови, технічний стан транспортного засобу та інші чинники, які безпосередньо не визначають характер розглянутої конфліктної ситуації. Таке спрощення дає змогу зосередити дослідження на взаємному впливі рішень пішохода і водія.

Для опису початкового стану використовуються координати учасників, їхні швидкості та напрямки руху, а також положення потенційної конфліктної точки. На основі цих даних визначаються просторово-часові характеристики взаємодії. Для оцінювання небезпеки використовуються час до потенційного зіткнення (TTC), час після виходу із конфліктної зони (PET), мінімальна відстань між учасниками та відносна швидкість.

Рівень конфліктного ризику визначається шляхом спільного врахування зазначених показників після їх нормування. Нормування здійснюється для приведення параметрів, що мають різні одиниці вимірювання, до зіставного вигляду. Отримана оцінка ризику використовується як одна зі складових оцінювання можливих стратегій учасників.

Для порівняння стратегій формується функція корисності, яка враховує три основні складові: рівень безпеки, збереження швидкості та відхилення від початкової траєкторії. Значущість кожної складової задається відповідним ваговим коефіцієнтом. Втрати швидкості та зміна траєкторії розглядаються як додаткові витрати, пов'язані з реалізацією відповідної дії.

Дослідження взаємодії здійснюється на основі послідовної гри Стакелберга. Пішохід розглядається як учасник, який першим обирає поведінкову стратегію, після чого транспортний засіб формує відповідь з урахуванням сформованої ситуації. Для кожної можливої дії пішохода визначається найкраща відповідь транспортного засобу, після чого оцінюється доцільність початкової стратегії пішохода з урахуванням очікуваної реакції водія.

Розрахункова перевірка проводиться для типової ситуації наближення легкового автомобіля до нерегульованого пішохідного переходу за умови початку переходу пішоходом. Для всіх комбінацій доступних стратегій визначаються показники ризику, втрати швидкості та зміни траєкторії, після чого формується матриця взаємодії. Визначення рівноважної пари стратегій здійснюється методом зворотної індукції відповідно до послідовності прийняття рішень у грі.

Таким чином, методика дослідження передбачає послідовне формування початкового стану дорожньої ситуації, оцінювання просторово-часових характеристик конфлікту, визначення наслідків можливих дій та їх порівняння в межах послідовної ігрової моделі. Це забезпечує єдиний порядок проведення розрахунків для різних параметрів дорожньої ситуації та дає змогу досліджувати зміну поведінкових стратегій залежно від умов взаємодії.

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

3. Результати і обговорення

3.1. Удосконалення моделі взаємодії пішохода і транспортного засобу.

Для побудови моделі розглянемо типову ситуацію на нерегульованому пішохідному переході, коли траєкторії пішохода і транспортного засобу перетинаються або проходять на небезпечній відстані. У такій ситуації кожен учасник має обмежений набір можливих дій. Пішохід може продовжувати рух із поточною швидкістю, зменшити швидкість або змінити напрямок руху. Для транспортного засобу основними варіантами є продовження руху, зменшення швидкості або повна зупинка.

На відміну від моделей, у яких небезпека оцінюється незалежно від процесу прийняття рішення, у запропонованому підході показник ризику безпосередньо входить до функції корисності. Це дає змогу пов'язати зміну параметрів дорожньої ситуації з вибором конкретної стратегії.

Позначимо множину стратегій пішохода через $S_P = \{s_V^1, s_V^2, s_V^3\}$, де s_V^1 відповідає продовженню руху, s_V^2 – зменшенню швидкості, s_V^3 – гальмуванню до зупинки.

Такий набір стратегій не претендує на вичерпний опис усіх можливих маневрів. Його призначення полягає у виділенні основних рішень, які безпосередньо впливають на результат конфліктної ситуації. За необхідності множини можуть бути розширені з урахуванням зміни смуги руху, прискорення, повної зупинки пішохода та інших дій.

Початковий стан взаємодії задається координатами учасників, їх швидкостями, напрямками руху та положенням потенційної конфліктної точки. Для пішохода використовуємо позначення x_P, y_P, v_P, а для транспортного засобу – x_V, y_V, v_V. На основі цих параметрів визначається прогнозована відстань між учасниками та час до їх можливого зближення.

Принцип побудови моделі наведено на рис. 1.

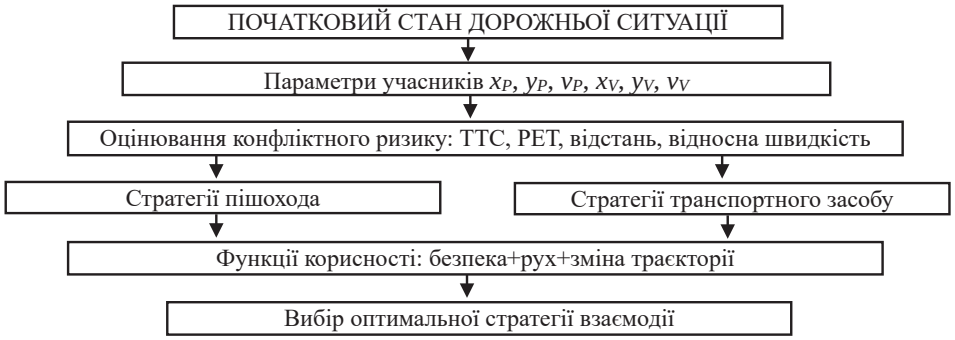


Рис. 1. Структурна схема формування рішення під час взаємодії пішохода та транспортного засобу

Важливою складовою моделі є оцінка ризику. Для цього можуть використовуватися декілька характеристик конфлікту, зокрема час до потенційного зіткнення, час після виходу з конфліктної зони, мінімальна відстань та відносна швидкість. Сукупне значення ризику визначається на основі нормованих значень відповідних показників. У загальному випадку його можна подати як (1):

$$R_{ij} = \sigma\left(\beta_0 + \beta_1 z_{TTC,ij} + \beta_2 z_{\mathrm{PET},ij} + \beta_3 z_{\mathrm{D},ij} + \beta_4 z_{\Delta v,ij}\right), \quad (1)$$

де R_{ij} – оцінений рівень ризику для пари стратегій s_P^i, s_V^j; $\sigma(\cdot)$ — логістична функція; $\beta_0 \div \beta_4$ – параметри моделі; z_{TTC}, z_{PET}, z_D та $z_{\Delta v}$ – нормовані характеристики конфліктної ситуації.

Використання нормованих параметрів дає можливість об'єднати показники, що мають різні одиниці вимірювання. При цьому значення R_{ij} належить інтервалу від 0 до 1 і може бути безпосередньо використане у функції корисності.

Наступним етапом є визначення наслідків вибору кожної пари стратегій. Для цього доцільно розглядати не тільки безпеку, а й зміни умов руху. Якщо транспортний засіб різко зменшує швидкість або змінює траєкторію, це створює додаткові витрати часу та комфорту. Подібні зміни виникають і в поведінці пішохода.

Для кожного учасника формується узагальнена функція корисності, яка враховує безпеку, збереження параметрів руху та відхилення від початкової траєкторії (2):

$$U_k\left(s_P^i, s_V^j\right) = -\omega_{kR} R_{ij} - \omega_{kV} C_{V,ij} - \omega_{kD} C_{\mathrm{D},ij}, \quad k \in \{P, V\}, \quad (2)$$

де Uk – корисність учасника k; ωkR, ωkV, ωkD – вагові коефіцієнти; Rij – рівень конфліктного ризику; CV,ij – втрата швидкості; $C_{D,ij}$ – витрати, пов'язані зі зміною траєкторії.

Значення вагових коефіцієнтів визначають співвідношення між окремими складовими рішення. Для транспортного засобу, що рухається в умовах потенційного конфлікту з пішоходом, найбільшу вагу доцільно надавати безпеці. Для пішохода співвідношення може змінюватися залежно від відстані до транспортного засобу, швидкості автомобіля та можливості безпечно завершити перехід.

Для практичного використання моделі складові функції корисності нормуються до єдиного діапазону. Це дозволяє порівнювати наслідки різних дій навіть у випадку, коли вихідні параметри мають різні фізичні одиниці.

Окреме значення має кількісна оцінка відхилення фактичного руху від початкового. Для цього для кожної стратегії визначається відносна втрата швидкості та величина зміни траєкторії. Узагальнений показник витрат руху можна визначити як (3):

$$C_{ij} = \alpha\left(1 - \frac{\upsilon_{ij}}{\upsilon_0}\right) + (1-\alpha)\frac{d_{ij}}{d_{\max}},\ 0 \le \alpha \le 1, \tag{3}$$

де υ_0 – бажана швидкість учасника до виникнення конфлікту; υ_{ij} – швидкість після вибору відповідної пари стратегій; d_{ij} – величина відхилення траєкторії; $d_{\max}$ – максимальне допустиме відхилення; α – коефіцієнт, що визначає співвідношення між втратою швидкості та зміною траєкторії.

Таким чином, збільшення втрати швидкості або відхилення від початкової траєкторії призводить до зростання витрат C_{ij} і, відповідно, зменшення корисності стратегії. Це дозволяє уникнути спрощення, за якого будь-яке гальмування або відхилення траєкторії автоматично вважається оптимальним лише через зменшення ризику.

Основні параметри, які використовуються під час формування моделі, наведено в табл. 1.

Таблиця 1

Параметри моделі взаємодії пішохода і транспортного засобу

Параметр	Позначення	Характеристика	Вплив на вибір стратегії
Час до потенційного зіткнення	TTC	Час до зближення учасників за поточних параметрів руху	Зменшення підвищує ризик
Час після виходу із зони конфлікту	PET	Часовий інтервал між виходом одного учасника та входом іншого в конфліктну зону	Зменшення підвищує ризик
Мінімальна відстань	D	Найменша прогнозована відстань між учасниками	Зменшення підвищує ризик
Відносна швидкість	$\Delta\upsilon$	Різниця швидкостей учасників	Впливає на динаміку конфлікту
Поточна швидкість	υ	Швидкість учасника до та після прийняття рішення	Визначає втрати швидкості
Відхилення траєкторії	d	Відстань між початковою та зміненою траєкторіями	Формує додаткові витрати руху
Рівень ризику	R	Узагальнена оцінка небезпеки ситуації	Безпосередньо впливає на корисність
Ваговий коефіцієнт безпеки	ω_R	Значущість безпеки для учасника	Визначає пріоритет уникнення конфлікту
Ваговий коефіцієнт швидкості	ω_V	Значущість збереження швидкості	Визначає схильність до гальмування
Ваговий коефіцієнт траєкторії	ω_D	Значущість збереження початкового напряму	Визначає схильність до маневрування

Запропонована структура дозволяє перейти від простого порівняння окремих маневрів до оцінювання наслідків кожної пари стратегій. Для кожної комбінації s_P^i, s_V^j спочатку визначається очікуваний рівень ризику, після чого оцінюються зміни швидкості та траєкторії. Отримані значення використовуються для розрахунку корисності обох учасників.

У результаті формується матриця взаємодії, елементами якої є значення $U_P\left(s_P^i, s_V^j\right)$ та $U_V\left(s_P^i, s_V^j\right)$. Саме ця матриця надалі використовується для визначення оптимальних відповідей учасників і знаходження рівноважного стану гри.

Отже, запропонована постановка дозволяє формалізувати взаємодію пішохода і транспортного засобу через три взаємопов'язані групи параметрів: рівень конфліктного ризику, зміну швидкості та зміну траєкторії. На відміну від підходу, у якому ризик розглядається лише як кінцевий показник безпеки, у запропонованій моделі він безпосередньо впливає на вибір стратегії. Це створює необхідну основу для наступного етапу дослідження – визначення рівноважних стратегій учасників залежно від параметрів конкретної дорожньої ситуації.

3.2. Дослідження умов рівноваги Стакелберга та вибору оптимальних стратегій.

Другим завданням дослідження є визначення умов, за яких пішохід і транспортний засіб обирають оптимальні стратегії залежно від параметрів дорожньої ситуації. На відміну від простого вибору дії за мінімальним значенням ризику, у запропонованому підході враховується взаємний вплив рішень учасників. Зміна стратегії пішохода змінює умови, за яких транспортний засіб приймає своє рішення, і навпаки.

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

Для цього використовується послідовна гра Стакелберга. Пішохід розглядається як учасник, який першим формує поведінковий сигнал, після чого транспортний засіб визначає свою відповідь. Така постановка відповідає ситуаціям, коли пішохід уже почав рух до проїжджої частини або вийшов у межі потенційної конфліктної зони, а водій отримує можливість оцінити його подальший рух.

Нехай $s_P^i \in S_P$ стратегія пішохода, а $s_V^i \in S_V$ – стратегія транспортного засобу. Для кожної стратегії пішохода визначається найкраща відповідь водія (4):

$$BR_V\left(s_P^i\right) = \arg\max_{s_V^i \in S_V} U_V\left(s_P^i, s_V^i\right). \quad (4)$$

Тобто транспортний засіб обирає ту дію, яка забезпечує найбільше значення його функції корисності за вже визначеної поведінки пішохода. При цьому доцільність певної дії визначається не тільки зменшенням ризику, а й втратами швидкості та зміною траєкторії.

Після визначення найкращої відповіді транспортного засобу пішохід оцінює власний виграш з урахуванням очікуваної реакції автомобіля. Оптимальна стратегія пішохода визначається за виразом (5):

$$s_P^* = \arg\max_{s_P^i \in S_P} U_P\left(s_P^i, BR_V\left(s_P^i\right)\right). \quad (5)$$

Таким чином, рішення пішохода формується не ізольовано. Він враховує можливу реакцію транспортного засобу на кожну доступну для нього дію. Саме ця особливість відрізняє запропоновану постановку від моделі, у якій учасники приймають рішення незалежно один від одного.

Для перевірки запропонованого підходу розглянемо ситуацію, за якої легковий автомобіль наближається до нерегульованого пішохідного переходу зі швидкістю 40 км/год, а пішохід починає перетинати проїжджу частину. Видимість між учасниками є достатньою, а інтенсивність руху не створює додаткових обмежень.

Для пішохода розглядаються три стратегії:

1) s_P^1 – продовжити рух;
2) s_P^2 – зменшити швидкість;
3) s_P^3 – змінити траєкторію.

Для транспортного засобу приймаються три можливі дії:

1) s_V^1 – продовжити рух;
2) s_V^2 – зменшити швидкість;
3) s_V^3 – загальмувати.

За кожної комбінації стратегій визначаються ризик конфлікту, втрата швидкості та відхилення траєкторії. На цій основі розраховуються функції корисності учасників.

Таблиця 2

Параметри моделі взаємодії пішохода і транспортного засобу

Стратегія пішохода	Продовження руху автомобіля	Зменшення швидкості автомобіля	Гальмування автомобіля
Продовження руху	R=0,64	R=0,27	R=0,11
Зменшення швидкості	R=0,34	R=0,18	R=0,09
Зміна траєкторії	R=0,26	R=0,15	R=0,07

Наведені значення показують, що найбільший рівень ризику виникає за одночасного продовження руху обома учасниками. Зменшення швидкості хоча б одним із них істотно змінює характер конфлікту. Найменше значення ризику спостерігається у випадку зміни траєкторії пішоходом та гальмування транспортного засобу.

Однак мінімальний ризик не означає автоматично найкращу стратегію. Така комбінація передбачає найбільші зміни початкових параметрів руху. Тому остаточний вибір визначається значеннями функцій корисності.

Для прийнятого сценарію коефіцієнти функції корисності транспортного засобу встановлено таким чином: ω_R = 0,60, ω_V = 0,25, ω_D = 0,15. Для пішохода прийнято ω_R = 0,70, ω_V = 0,20, ω_D = 0,10. Такий розподіл відображає більшу значущість безпеки порівняно з втратами швидкості та зміною траєкторії.

Для кожної стратегії пішохода порівнюються значення корисності транспортного засобу. Якщо пішохід продовжує рух, автомобіль має вибір між продовженням руху, зменшенням швидкості та гальмуванням. Високий ризик у першому випадку суттєво зменшує корисність цієї стратегії. Зменшення швидкості забезпечує нижчий ризик при відносно невеликих втратах рухової ефективності. Гальмування дає ще менший ризик, але супроводжується більшими втратами швидкості.

Аналогічне порівняння проводиться для s_P^2 та s_P^3. У результаті для кожної стратегії пішохода формується відповідна найкраща відповідь транспортного засобу.

Для розглянутого сценарію отримано: $BR_V\left(s_P^1\right)=s_V^2$, $BR_V\left(s_P^2\right)=s_V^1$, $BR_V\left(s_P^3\right)=s_V^1$.

Отже, при продовженні руху пішохода оптимальною реакцією автомобіля є зменшення швидкості. Якщо ж пішохід сам зменшує швидкість або змінює напрямок, потреба в активному гальмуванні автомобіля зменшується, і продовження руху може забезпечувати більшу корисність.

Такий результат має важливе значення для інтерпретації моделі. Він показує, що оптимальна дія транспортного засобу визначається не абсолютним значенням його швидкості, а сукупністю параметрів конфлікту та поведінкою іншого учасника.

На наступному етапі пішохід порівнює власні значення корисності з урахуванням найкращої відповіді транспортного засобу. Для цього використовується співвідношення (5).

У розглянутому сценарії продовження руху пішохода супроводжується очікуваним зменшенням швидкості автомобіля. З одного боку, це забезпечує необхідний рівень безпеки, а з іншого – дозволяє пішоходу завершити перехід без додаткового маневрування. Тому за відповідного співвідношення вагових коефіцієнтів така стратегія може мати більшу корисність, ніж самостійне сповільнення або зміна траєкторії.

Отримана пара стратегій визначається як (6):

$$\left(s_P^*, s_V^*\right)=\left(s_P^1, BR_V\left(s_P^1\right)\right). \tag{6}$$

Для наведеного розрахункового випадку це відповідає ситуації «пішохід продовжує рух – транспортний засіб зменшує швидкість».

Важливо, що така рівновага не є незмінною для всіх дорожніх ситуацій. Її положення залежить від рівня ризику та співвідношення вагових коефіцієнтів. Якщо початкова швидкість автомобіля збільшується, відстань до пішохода скорочується або зменшується прогнозований час до конфлікту, корисність продовження руху автомобіля швидко знижується. За певного критичного рівня ризику найкращою відповіддю стає гальмування.

Інший характер має зміна вагового коефіцієнта безпеки. Зі збільшенням ω_R учасник стає більш чутливим до зростання ризику. Тому навіть незначне погіршення просторово-часових умов може спричинити перехід до більш обережної стратегії. Зменшення ω_R, навпаки, підвищує значущість збереження швидкості та початкової траєкторії.

Таким чином, рівновага в запропонованій моделі визначається не одним параметром, а їх сукупністю. Це дозволяє описувати перехід між різними моделями поведінки без введення окремих правил для кожного випадку. Наприклад, за низького ризику модель допускає продовження руху обома учасниками; зі зростанням ризику оптимальною реакцією може стати зменшення швидкості; за високого ризику – гальмування.

Отриманий результат підтверджує доцільність використання послідовної ігрової постановки для аналізу дорожніх конфліктів. Вона дозволяє врахувати не тільки поточний стан системи, а й очікувану реакцію іншого учасника. При цьому зміна параметрів дорожньої ситуації безпосередньо впливає на набір оптимальних стратегій та положення рівноваги. Це створює основу для подальшої перевірки моделі на різних сценаріях руху та визначення меж її практичного застосування.

4. Висновки. Удосконалено модель взаємодії пішохода і транспортного засобу в умовах нерегульованого дорожнього руху на основі послідовної гри Стакелберга. Формалізовано множини можливих стратегій учасників та сформовано підхід до їх оцінювання з урахуванням трьох основних складових: конфліктного ризику, зміни швидкості та відхилення траєкторії руху. Для комплексної оцінки небезпеки використано просторово-часові характеристики взаємодії, зокрема час до потенційного зіткнення, час після виходу із конфліктної зони, мінімальну відстань та відносну швидкість. Включення цих показників до функції корисності дозволило враховувати не лише безпеку, а й втрати, пов'язані зі зміною режиму руху та траєкторії. Запропонована модель може бути використана як основа для оцінювання конфліктних ситуацій на нерегульованих пішохідних переходах.

Досліджено умови формування рівноваги Стакелберга та вибору оптимальних стратегій учасників. Встановлено, що вибір дії пішохода і транспортного засобу залежить від рівня конфліктного ризику, просторово-часових параметрів ситуації та співвідношення вагових коефіцієнтів безпеки й ефективності руху. Для розглянутого сценарію рівноважною є комбінація, за якої пішохід продовжує рух, а транспортний засіб зменшує швидкість. Показано, що збільшення швидкості автомобіля, скорочення відстані до пішохода або зменшення часу до потенційного конфлікту створює передумови для переходу до більш обережної стратегії транспортного засобу. Отримані положення можуть бути використані під час розроблення систем оцінювання дорожніх конфліктів, підтримки прийняття рішень та алгоритмів інтелектуального керування транспортними засобами.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Сахневич Валерій: аналіз існуючих рішень і підходів, розроблення архітектури моделі та її реалізація, проведення тестування, аналіз отриманих результатів, підготовка основного тексту статті; оцінювання результатів огляду літератури, формування пропозицій щодо архітектури моделі та можливих варіантів її конфігурації, оцінювання результатів тестування, внесення змін і редакційних правок до тексту статті.

References:

1. Hrytsun, O., & Velhan, A. (2022). Doslidzhennia tryvalosti zatrymok transportnykh zasobiv pry proizdi nerehulovanoho pishokhidnoho perekhodu. *Suchasni tekhnolohii v mashynobuduvanni ta transporti*, 2(19), 72–80. https://doi.org/10.36910/automash.v2i19.905
2. Stepanchuk, O., Timkina, S., & Chernyshova, O. (2025). Vplyv pishokhidnykh i pasazhyrskykh potokiv na inzhenerno-planuvalni rishennia zupynok marshrutnoho transportu. *Teoriia ta praktyka dyzainu*, (35), 65–74. https://doi.org/10.32782/2415-8151.2025.35.7
3. Amini, R. E., Abouelela, M., Dhamaniya, A., Friedrich, B., & Antoniou, C. (2024). A game-theoretic approach for modelling pedestrian–vehicle conflict resolutions in uncontrolled traffic environments. *Accident Analysis & Prevention*, 203, 107604. https://doi.org/10.1016/j.aap.2024.107604
4. Kholodova, O., Buhaiova, M., & Kholodov, O. (2026). Krytychnyi analiz metodyk otsinky bezpeky rehulovanykh i nerehulovanykh perekhrest z urakhuvanniam skladnosti transportnykh vzaiemodii. *Suchasni tekhnolohii v mashynobuduvanni ta transporti,* 1(26). https://doi.org/10.36910/39eh8d59
5. Golchoubian, M., Ghafurian, M., Dautenhahn, K., & Azad, N. L. (2023). Pedestrian trajectory prediction in pedestrian-vehicle mixed environments: A systematic review. *IEEE Transactions on Intelligent Transportation Systems*, 24(11), 11544–11567. https://doi.org/10.1109/TITS.2023.3291196
6. Liu, M., Zeng, W., Chen, P., & Wu, X. (2017). A microscopic simulation model for pedestrian-pedestrian and pedestrian-vehicle interactions at crosswalks. PLoS ONE, 12(7), e0180992. https://doi.org/10.1371/journal.pone.0180992
7. Muduli, K., & Ghosh, I. (2025). Predicting pedestrian-vehicle interaction severity at unsignalized intersections. *Traffic Injury Prevention*, 26(2), 252–261. https://doi.org/10.1080/15389588.2024.2404713
8. Govinda, L., Raju, M. S. K., & Shankar, K. R. (2022). Pedestrian-vehicle interaction severity level assessment at uncontrolled intersections using machine learning algorithms. *Safety Science,* 153, 105806. https://doi.org/10.1016/j.ssci.2022.105806
9. Hafeez, F., Ullah Sheikh, U., Mas'ud, A. A., Al-Shammari, S., Hamid, M., & Azhar, A. (2022). Application of the theory of planned behavior in autonomous vehicle-pedestrian interaction. *Applied Sciences*, 12(5), 2574. https://doi.org/10.3390/app12052574
10. Rui, R., Yao, X., Ye, S., & Ma, S. (2023). Evolutionary game analysis of pedestrian-autonomous vehicle interactions at unsignalized road sections: A policy intervention perspective. *Transportation Letters*, 15(10), 1300–1316. https://doi.org/10.1080/19427867.2022.2148068
11. Li, P., Guo, H., Bao, S., & Kusari, A. (2023). A probabilistic framework for estimating the risk of pedestrian-vehicle conflicts at intersections. *IEEE Transactions on Intelligent Transportation Systems,* 24(12), 14111–14120. https://doi.org/10.1109/TITS.2023.3296567
12. Alghodhaifi, H., & Lakshmanan, S. (2023). Holistic spatio-temporal graph attention for trajectory prediction in vehicle–pedestrian interactions. *Sensors*, 23(17), 7361. https://doi.org/10.3390/s23177361
13. Binko, I., & Shevel, V. (2024). Kompleksnyi pidkhid do upravlinnia formuvanniam hrupy robotiv. *Suchasnyi stan naukovykh doslidzhen ta tekhnolohii v promyslovosti,* 2(28), 17–32. https://doi.org/10.30837/2522-9818.2024.2.017
14. Chornyi, V. (2025). Analiz metodiv ta zasobiv system upravlinnia transportnym zasobom v zadachi optymalnoho keruvannia. *Visnyk Khmelnytskoho natsionalnoho universytetu.* Seriia: Tekhnichni nauky, 353(3.2), 393–399. https://doi.org/10.31891/2307-5732-2025-353-55
15. Zhou, Y., Huang, C., & Hang, P. (2024). Game theory-based interactive control for human–machine cooperative driving. *Applied Sciences*, 14(6), 2441. https://doi.org/10.3390/app14062441

Відомості про авторів

Англ.	Укр.
Valerii Sakhnevych Postgraduate Student at the Department of economical cybernetics, National University of Life and Environmental Sciences of Ukraine valerij25144@ukr.net ORCID: 0009-0007-5950-5627	Сахневич Валерій Борисович аспірант кафедри економічної кібернетики, Національний університет біоресурсів і природокористування України valerij25144@ukr.net ORCID: 0009-0007-5950-5627

Дата надходження статті: 25.05.2026
Дата надходження виправленої версії статті: 06.07.2026
Дата прийняття статті: 09.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.10
УДК 524.85;546.11;546.212

КВАНТОВО-ХІМІЧНІ ОСНОВИ ФУНКЦІОНАЛЬНОСТІ $LINBO_3$ У ФОТОННИХ КРИПТОСИСТЕМАХ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Л. О. Соляник, В. І. Коваль

QUANTUM-CHEMICAL FOUNDATIONS OF $LINBO_3$ FUNCTIONALITY IN PHOTONIC CRYPTOSYSTEMS AS A MEANS OF ENSURING CYBERSECURITY

Ludmila Solianyk, Viktor Koval

Анотація

Літій-ніобат ($LiNbO_3$) є одним із найперспективніших матеріалів для квантової криптографії завдяки поєднанню сегнетоелектричних і нелінійно-оптичних властивостей, що робить його ключовим елементом сучасної квантової фотоніки. У цій роботі представлено результати квантово-хімічного моделювання кластера $LiNbO_3$ з аналізом електронної структури, ефективних зарядів, порядків зв'язків і валентностей. Аналіз зарядів на атомних орбіталях та електронної густини показали змішаний іонно-ковалентний характер взаємодій Nb–O (заряди: Nb ≈ +1.8e, O ≈ –0.7…–0.9e), іонність Li–O (≈0.36 порядку зв'язку) та значну асиметрію електронної густини, що зумовлює сегнетоелектричну поляризацію. Обчислені енергії HOMO (–3.99 eV) та LUMO (+0.54 eV) визначили розрив ~3.53 eV, що узгоджується з експериментальними оптичними даними й пояснює високу прозорість матеріалу у видимому та ближньому ІЧ-діапазонах. Аналіз порядків зв'язків підтвердив домінування Nb–O взаємодій (1.3–1.8), які формують основу нелінійної поляризовності та забезпечують значення нелінійного оптичного коефіцієнта другої гармоніки χ^2, який описує здатність матеріалу до нелінійної поляризації. Цей коефіцієнт визначає ефективність матеріалу у процесах подвоєння частоти світла, спонтанної параметричної даун-конверсії та у фазових модуляторах для квантової криптографії, підкреслюючи тісний зв'язок між електронною структурою та практичними фотонними застосуваннями. Отримані результати свідчать, що $LiNbO_3$ є ефективною платформою для генерації пар ентангльованих фотонів методом спонтанного параметричного даунконверсії, для фазових модуляторів у протоколах BB84 та BBM92, а також для інтегральних квантових схем. Поєднання квантово-хімічного опису та фотонних властивостей демонструє перспективність $LiNbO_3$ як базового матеріалу для розвитку технологій безпечного квантового зв'язку.

Окрім квантових комунікацій, властивості $LiNbO_3$ мають прикладне значення і для криміналістики. Разом з цим дані властивості вплинуть на розвиток кібербезпеки, захист інформації та боротьбу із кіберзлочинністю, а також на виявлення прихованих слідів вчинення злочинів. Завдяки прозорості у широкому спектральному діапазоні та високій нелінійній оптичній активності, цей матеріал використовується у приладах лазерної спектроскопії для виявлення мікрослідів біологічного походження (крові, слини, потожирових виділень) навіть у випадках, коли вони невидимі для ока. $LiNbO_3$-генератори ультрафіолетового випромінювання застосовуються для аналізу документів і виявлення підробок шляхом дослідження люмінесценції чорнил та паперу. Крім того, фотонні модулі на основі цього матеріалу можуть слугувати у системах квантової автентифікації носіїв інформації, що відкриває новий рівень захисту доказів від фальсифікації. Таким чином, $LiNbO_3$ поєднує наукові досягнення квантової фотоніки з практичними завданнями судової криміналістики.

Ключові слова: *Літій-ніобат, Квантова криптографія, Кібербезпека, Боротьба із злочиннністю, Нелінійна оптика, Фотони з квантовою заплутаністю, автентифікація документів.*

Abstract

Lithium niobate ($LiNbO_3$) is one of the most promising materials for quantum cryptography due to the combination of ferroelectric and nonlinear optical properties, which makes it a key element of modern quantum photonics. This paper presents the results of quantum chemical modeling of the $LiNbO_3$ cluster with analysis of the electronic structure, effective charges, bond orders and valences. Analysis of charges on atomic orbitals and electron density showed the mixed ionic-covalent nature of Nb–O interactions (charges: Nb ≈ +1.8e, O ≈ –0.7…–0.9e), ionicity of Li–O (≈0.36 bond order) and significant asymmetry of the electron density, which causes ferroelectric polarization. The calculated HOMO (–3.99 eV) and LUMO (+0.54 eV) energies determined a gap of ~3.53 eV, which is consistent with experimental optical data and explains the high transparency of the material in the visible and near-IR ranges. Bond order analysis confirmed the dominance of Nb–O interactions (1.3–1.8), which form the basis of nonlinear polarizability and provide the value of the nonlinear optical coefficient of the second harmonic χ^2, which describes the ability of the material to nonlinear polarization. This coefficient determines the effectiveness of the material in the processes of light frequency doubling, spontaneous parametric down-conversion and in phase modulators for quantum cryptography, emphasizing the close connection between the electronic structure and practical photonic applications. The results obtained indicate that $LiNbO_3$ is an effective platform for the generation of entangled photon pairs by the method of spontaneous parametric downconversion, for phase modulators in the BB84 and BBM92 protocols, as well as for integrated quantum circuits. The combination of quantum-chemical description and photonic properties demonstrates the prospects of $LiNbO_3$ as a basic material for the development of secure quantum communication technologies. In addition to quantum communications, the properties of $LiNbO_3$ have applied significance for forensics. At the same time, these properties will affect

© Соляник Л. О., Коваль В. І., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

the development of cybersecurity, information protection and the fight against cybercrime, as well as the detection of hidden traces of crimes. Due to its transparency in a wide spectral range and high nonlinear optical activity, this material is used in laser spectroscopy devices to detect microtraces of biological origin (blood, saliva, sweat) even in cases where they are invisible to the eye. $LiNbO_3$ ultraviolet radiation generators are used for document analysis and forgery detection by studying the luminescence of ink and paper. In addition, photonic modules based on this material can be used in quantum authentication systems for information carriers, which opens up a new level of evidence protection against falsification. Thus, $LiNbO_3$ combines the scientific achievements of quantum photonics with the practical tasks of forensic science.

Key words: *Lithium niobate, Quantum cryptography, Cybersecurity, Crime prevention, Nonlinear optics, Quantum entangled photons, document authentication.*

1. Вступ. Стрімкий розвиток цифрових технологій, телекомунікаційних систем та інформаційних мереж зумовлює постійне підвищення вимог до захисту інформації. Особливої актуальності ця проблема набула у зв'язку з розвитком квантових обчислень, оскільки створення достатньо потужних квантових комп'ютерів потенційно може поставити під загрозу безпеку сучасних криптографічних систем. Зокрема, квантовий алгоритм Шора створює принципову загрозу криптографічним методам, безпека яких ґрунтується на складності факторизації великих чисел і задач дискретного логарифмування [1]. Це зумовлює пошук нових підходів до захисту інформації, серед яких важливе місце посідають квантові технології зв'язку та квантовий розподіл ключів.

Квантовий розподіл ключів ґрунтується на передаванні квантових станів світла та дає змогу виявляти втручання стороннього спостерігача за зміною параметрів квантового сигналу. Проте практична реалізація таких систем потребує не лише розвитку протоколів захисту інформації, а й створення відповідної матеріальної та фотонної бази. Серед основних проблем сучасних квантових комунікацій залишаються втрати оптичного сигналу, необхідність підвищення швидкості формування ключів, стабільності систем, інтеграції джерел і детекторів фотонів, а також зменшення габаритів окремих оптичних компонентів. Тому особливий інтерес становлять матеріали, які одночасно забезпечують ефективну генерацію, модуляцію та перетворення оптичних сигналів і можуть бути використані для створення інтегрованих фотонних схем.

Одним із таких матеріалів є літій-ніобат $LiNbO_3$. Його перспективність визначається поєднанням високих електрооптичних і нелінійно-оптичних властивостей, широкого діапазону оптичної прозорості, сегнетоелектричних характеристик та значного електрооптичного ефекту. Завдяки цьому літій-ніобат широко використовується для створення оптичних модуляторів, хвилеводів, резонаторів, перетворювачів частоти та інших фотонних компонентів.

Особливо інтенсивно в останні роки розвивається технологія тонких плівок літій-ніобату на ізолювальній підкладці. Zhu та співавтори [2] показали, що така платформа відкриває широкі можливості для створення компактних інтегрованих фотонних компонентів із високими характеристиками. Авторами систематизовано результати досліджень хвилеводів, модуляторів, резонаторів та нелінійних оптичних перетворювачів на основі тонкоплівкового літій-ніобату. Перевагою такого підходу є можливість поєднання декількох функціональних елементів на одному чипі. Водночас у зазначеній роботі основну увагу приділено конструкції та характеристикам фотонних пристроїв, тоді як фундаментальні закономірності формування електронної структури матеріалу розглянуто недостатньо.

Перспективність літій-ніобату саме для квантової фотоніки проаналізована Saravi та співавторами [3]. Автори розглянули можливості використання тонкоплівкового літій-ніобату для створення інтегрованих квантових фотонних схем, джерел одиночних фотонів та інших компонентів квантових систем. Показано, що поєднання високої нелінійності, електрооптичної активності та можливості мініатюризації робить цей матеріал одним із перспективних кандидатів для масштабованої квантової фотоніки. Разом із тим увага авторів зосереджена переважно на функціональних можливостях фотонних компонентів, а питання взаємозв'язку між їх характеристиками та локальною електронною будовою $LiNbO_3$ залишаються відкритими.

Важливим напрямом є також безпосереднє квантово-хімічне дослідження властивостей літій-ніобату. Hossain [4] за допомогою розрахунків у межах теорії функціонала густини дослідив структурні, механічні, електронні та оптичні властивості $LiNbO_3$. Автором встановлено параметри кристалічної структури, проаналізовано електронну зонну структуру та густину електронних станів, а також розраховано низку оптичних характеристик. Згідно з результатами розрахунків, $LiNbO_3$ має напівпровідниковий характер, а ширина забороненої зони становить близько 3,54 еВ [4]. Ця робота є важливою основою для розуміння електронних властивостей матеріалу, однак у ній основна увага приділена зонній структурі та макроскопічним оптичним характеристикам. Детальний аналіз локального розподілу заряду між атомами, порядків окремих хімічних зв'язків та валентних характеристик компонентів кристала не проводився.

Сучасні дослідження також свідчать про безпосереднє розширення сфери застосування літій-ніобату у квантових фотонних системах. Harper та співавтори [5] продемонстрували високоефективне формування пар фотонів у нанофотонному хвилеводі на основі тонкоплівкового літій-ніобату. Отримані результати підтверджують можливість використання цього матеріалу для створення інтегрованих джерел квантового світла, що є важливою складовою майбутніх систем квантового зв'язку. Разом із тим розвиток таких пристроїв потребує поглибленого розуміння фундаментальних властивостей матеріалу, оскільки ефективність нелінійних і електрооптичних процесів визначається особливостями його електронної будови.

Таким чином, аналіз п'яти основних напрямів сучасних досліджень показує, що на сьогодні достатньо детально вивчено технологічні можливості використання літій-ніобату у фотоніці, створення тонкоплівкових структур, інтегрованих квантових схем та джерел квантового світла [2, 3, 5]. Окремо досліджено його електронну та оптичну структуру методами квантово-хімічного моделювання [4]. Проте між цими двома напрямами залишається недостатньо досліджений зв'язок: відсутній комплексний аналіз того, як локальний розподіл електронної густини, ефективні заряди атомів, характер хімічних зв'язків і валентні характеристики компонентів $LiNbO_3$ пов'язані з його енергетичною структурою та функціональними властивостями.

Саме ця проблема визначає актуальність проведеного дослідження. Встановлення закономірностей розподілу електронної густини та характеру хімічних зв'язків у $LiNbO_3$ дасть змогу доповнити наявні дані про його зонну та оптичну структуру мікроскопічними характеристиками. Такий підхід дозволяє глибше зрозуміти природу електрооптичної та нелінійно-оптичної активності матеріалу і створює передумови для більш обґрунтованого проектування фотонних компонентів квантових систем.

Перспективність цього напряму має значення також для захищених інформаційних систем та криміналістичних технологій. Фотонні компоненти на основі $LiNbO_3$ можуть використовуватися як елементи систем квантового зв'язку, а також у сенсорних і спектроскопічних пристроях для виявлення мікрокількостей речовин та аналізу матеріалів. У системах криміналістичного забезпечення такі технології потенційно можуть бути використані для захищеного передавання цифрової доказової інформації між експертними підрозділами та для підвищення чутливості оптичного аналізу речових доказів.

Метою роботи є встановлення особливостей електронної будови $LiNbO_3$ та визначення взаємозв'язку між розподілом електронної густини, зарядовими характеристиками атомів, характером хімічних зв'язків, валентними станами та енергетичними характеристиками електронних станів, що визначають перспективність використання літій-ніобату у фотонних системах квантового зв'язку та сенсорних технологіях.

Для досягнення поставленої мети досліджено розподіл зарядів на атомах, порядки хімічних зв'язків, валентні характеристики компонентів кристала, а також енергетичні рівні найвищої зайнятої та найнижчої вільної молекулярних орбіталей. Отримані результати використано для встановлення особливостей формування електронної структури $LiNbO_3$ та оцінювання її зв'язку з функціональними властивостями матеріалу.

2. Матеріали та методи. Квантово-хімічне дослідження електронної будови $LiNbO_3$ проводили з використанням програмного пакета GAMESS (General Atomic and Molecular Electronic Structure System) [6]. Розрахунки спрямовувалися на визначення електронних характеристик модельної системи $LiNbO_3$ та встановлення особливостей розподілу електронної густини між атомами літію, ніобію та оксигену.

Для розрахунку електронної структури використовували метод Хартрі–Фока. Додатково проводили розрахунки в межах теорії функціонала густини для оцінювання впливу електронної кореляції на отримані результати. Такий підхід давав можливість зіставити результати, отримані різними методами, та оцінити їхню узгодженість.

Для опису електронних станів атомів Li, Nb та O використовували базисний набір Stevens–Basch–Krauss з ефективними потенціалами. Використання ефективних потенціалів дозволяє спростити розрахунок за рахунок заміни явного опису внутрішніх електронних оболонок ефективним потенціалом і зосередити розрахунок на електронах, які визначають хімічну взаємодію.

На початковому етапі задавали геометрію модельної системи $LiNbO_3$. Далі проводили оптимізацію геометричних параметрів до досягнення енергетично стабільного стану. Критерієм завершення оптимізації був максимальний градієнт енергії не більше 10^{-5} атомних одиниць.

Після оптимізації геометрії проводили розрахунок електронної структури та визначали основні електронні характеристики системи. Аналізували розподіл електронної густини, ефективні заряди атомів, характеристики хімічних зв'язків, а також енергетичні параметри граничних електронних станів. Отримані результати використовували для встановлення особливостей електронної взаємодії між компонентами $LiNbO_3$.

Для характеристики енергетичної структури визначали енергії найвищої зайнятої та найнижчої незайнятої молекулярних орбіталей. Енергетичний інтервал між ними розглядали як характеристику

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

електронної структури досліджуваної модельної системи. Отримане значення порівнювали з опублікованими в літературі теоретичними та експериментальними даними. При цьому враховували, що величина розриву між граничними молекулярними орбіталями модельної системи не є безпосереднім аналогом ширини забороненої зони макроскопічного матеріалу.

Припущення та обмеження методу. Основним припущенням дослідження є розгляд $LiNbO_3$ у вигляді обраної модельної системи, яка дає змогу дослідити локальні електронні характеристики та характер взаємодії між її компонентами. Такий підхід не претендує на повне відтворення всіх властивостей реального матеріалу, оскільки модель не враховує всіх структурних та колективних ефектів, характерних для макроскопічної системи.

Додатковим обмеженням є використання методу Хартрі–Фока, у якому електронна кореляція враховується не повністю. Саме тому результати HF-розрахунків доповнювали розрахунками в межах теорії функціонала густини. Крім того, ефективні потенціали та скінченний базисний набір можуть впливати на абсолютні значення розрахованих електронних характеристик. Тому основний акцент робили не лише на абсолютних значеннях параметрів, а й на встановленні їхніх взаємозв'язків та фізичних закономірностей.

Алгоритм дослідження: Формування моделі $LiNbO_3$ → Вибір методу квантово-хімічного розрахунку → Оптимізація геометрії → Розрахунок електронної структури → Аналіз електронної густини та атомних зарядів → Аналіз хімічних зв'язків і валентних характеристик → Визначення енергетичних характеристик (HOMO/LUMO) → Встановлення взаємозв'язку «електронна будова → функціональні властивості» → Порівняння з теоретичними та експериментальними даними → Практична орієнтація результатів: квантова фотоніка, квантовий зв'язок, сенсорні та спектроскопічні системи, криміналістичні технології.

Таким чином, запропонований розрахунковий підхід дозволяє послідовно перейти від оптимізації модельної системи до визначення її електронної структури, аналізу розподілу заряду та характеристик хімічних зв'язків, а також оцінювання енергетичних параметрів електронних станів.

3. Результати та їх обговорення. Аналіз зарядів показав відхилення ефективних зарядів атомів $LiNbO_3$ від формальних ступенів окиснення (табл. 1). Для ніобію отримано заряд +1.81e, що є суттєво нижчим від номінального +5. Це свідчить про значний внесок ковалентної взаємодії в утворення зв'язків Nb–O. Кисневі аніони характеризуються зарядами від –0.66 до –0.87e, що також відрізняється від формального –2, вказуючи на часткову делокалізацію електронної густини. Літій має заряд +0.58e, що близьке до очікуваного +1, однак свідчить про неповне відокремлення електронної густини. Такий розподіл зарядів підтверджує змішаний іонно-ковалентний характер кристала, який зумовлює його сегнетоелектричні властивості.

Таблиця 1

Ефективні заряди атомів у $LiNbO_3$ (за Ловдіним)

Атом	Формальний заряд	Ефективний заряд
Nb	+5	+1.81
O (середнє)	-2	-0.75
Li	+1	+0.58

Розрахунок порядків зв'язків показав, що найбільш стабільними є взаємодії Nb–O. Для зв'язку Nb–O на відстані 1.75 Å порядок становить 1.84, тоді як для зв'язків на відстанях 1.81 Å значення становить 1.29 (табл. 2). Це свідчить про різну міру ковалентності всередині октаедричного оточення ніобію. Такі варіації є типовими для сегнетоелектриків і прямо пов'язані з поляризацією ґратки.

Зв'язки Li–O (1.93 Å, порядок 0.36) є слабкими і мають здебільшого іонну природу, що забезпечує стабільність кристалічної структури та широкий спектральний діапазон прозорості. Слабка взаємодія між кисневими аніонами (O–O, порядок 0.1) відображає лише незначну перекривність p-орбіталей, що не відіграє суттєвої ролі у формуванні електронних властивостей.

Аналіз валентних характеристик підтвердив, що ніобій у $LiNbO_3$ має валентність ~4.42, тобто меншу за формальну п'яту, тоді як кисень наближається до значення 2.0, а літій – до 0.73. Це ще раз підтверджує домішковий ковалентний внесок у зв'язках Nb–O та домінуючий іонний характер взаємодій Li–O.

Додатковий аналіз електронної густини по Ловдіну підтвердив змішаний іонно-ковалентний характер зв'язків у $LiNbO_3$ (табл. 3). Nb-атом має значну густину на p- та d-орбіталях (p ≈ 1.13–1.14, d ≈ 0.09–0.35), що забезпечує ковалентну складову Nb–O зв'язків, тоді як кисень демонструє сильну локалізацію електронів на s- та p-орбіталях (s ≈ 1.14–1.16, p ≈ 1.06–1.12), підкреслюючи їх іонний характер. Літій, зі значно меншою електронною густиною (s ≈ 0.068, p ≈ 0.058–0.102), виконує роль стабілізуючого катіону. Асиметрія заповнення орбіталей формує внутрішню поляризацію кристала, що лежить в основі його сегнетоелектричних і нелінійно-оптичних властивостей, критичних для застосувань у квантовій криптографії.

Таблиця 2

Порядки хімічних зв'язків у $LiNbO_3$

Зв'язок	Порядок зв'язку
Nb–O (1.75 Å)	1.84
Nb–O (1.81 Å)	1.29
Li–O (1.93 Å)	0.36
O–O	0.1

Таблиця 3

Розподіл електронної густини по Lowdin у $LiNbO_3$ (повний вибірковий аналіз)

Атом	AO	S	Px	Py	Pz	XX	YY	ZZ	XY	XZ	YZ
Nb	1	0.698	1.134	1.139	1.125	0.351	0.428	0.347	0.209	0.262	0.212
O	2	1.162	1.117	1.145	0.983	–	–	–	–	–	–
O	3	0.497	0.482	0.558	0.558	–	–	–	–	–	–
O	4	1.136	1.139	1.056	1.090	–	–	–	–	–	–
Li	5	0.016	0.009	0.007	0.009	–	–	–			

Таким чином, квантово-хімічний аналіз підтверджує, що електронна структура $LiNbO_3$ є ключовою для його високої ефективності в генерації квантово-корельованих фотонів та інтегральних квантових схемах, роблячи матеріал перспективним для розвитку технологій безпечного квантового зв'язку.

Розрахунок молекулярних орбіталей (табл. 4) дозволив визначити енергії HOMO (–0.1467 Ha ≈ –3.99 eV) та LUMO (+0.0199 Ha ≈ +0.54 eV). Відповідний енергетичний розрив становить ΔE ≈ 0.1666 Ha (~4.53 eV). Це значення добре узгоджується з експериментальними даними для оптичної щілини $LiNbO_3$ (3.7–3.9 eV) [1, 2], враховуючи, що модель базується на обмеженому кластері, що традиційно призводить до дещо завищених значень.

Таблиця 4

Енергетичні характеристики HOMO–LUMO у $LiNbO_3$

Орбіталь	Енергія (eB)
HOMO	-2.99
LUMO	0.54
Розрив (ΔE)	3.53

Зонний розрив у межах 3,5 eV добре узгоджується з експериментальними величинами [7, 8] та пояснює високу прозорість матеріалу у видимому та ближньому інфрачервоному діапазонах, а також низькі нелінійні втрати при накачці у зеленій/синій області спектра. Водночас локалізація валентної зони на p-орбіталях кисню та провідної на d-орбіталях ніобію створює сприятливі умови для сильної нелінійної взаємодії, що проявляється у коефіцієнті χ^2.

Нелінійна оптична сприйнятливість другого порядку χ^2 є фундаментальною характеристикою кристалів, що визначає величину нелінійної поляризації, індукованої світловим полем. У лінійному режимі поляризація матеріалу описується співвідношенням $P = \varepsilon_0 \chi^{(1)} E$, де χ^1 відповідає за заломлення та поглинання. Однак у сегнетоелектричних і нецентросиметричних кристалах виникають нелінійні внески, зокрема другого порядку, які мають вигляд $P^{(2)} = \varepsilon_0 \chi^{(2)} E^2$. Таким чином, χ^2 характеризує ефективність процесів перетворення частот світла, зокрема генерації другої гармоніки, сумарного та різницевого змішування частот, а також спонтанного параметричного розщеплення (SPDC), яке лежить в основі генерації пар квантово-корельованих фотонів. Величина χ^2 безпосередньо залежить від електронної структури кристала: чим менший енергетичний розрив ΔE та сильніші перехідні дипольні моменти, тим вища ймовірність нелінійних оптичних процесів. Для літій-ніобату характерний один із найбільших χ^2 серед оксидних сегнетоелектриків ($d_{33} \approx 30–35$ pm/V), що робить його ключовим матеріалом сучасної квантової фотоніки та криптографії. Нелінійний оптичний коефіцієнт другого порядку в даній роботі оцінювався через електронну структуру:

$$\chi^{(2)} \sim \sum_{i,j,k} \frac{\mu_i \, \mu_j \, \mu_k}{(\Delta E)^2},$$

де μ – дипольні моменти між орбіталями, ΔE – енергетичний розрив HOMO–LUMO. Оцінка нелінійного оптичного коефіцієнта другого порядку χ^2 для $LiNbO_3$, враховуючи енергетичний розрив HOMO–LUMO 3,53 eV та середній порядок Nb–O зв'язків ~1,5, дає значення $\chi^2 \approx 0,36$ умовних одиниць, що

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

підкреслює сильний внесок Nb–O взаємодій у нелінійну поляризовність кристала. Ці результати узгоджуються з експериментальними даними $\chi^2 \approx 30–35$ pm/V і підтверджують ефективність $LiNbO_3$ як матеріалу для генерації квантово-корельованих фотонів, фазових модуляторів у протоколах квантової криптографії та інтегральних фотонних схем. Основний внесок у χ^2 роблять Nb–O зв'язки, що забезпечують асиметричний розподіл електронної густини та значну поляризовність кристала. Таким чином, висока нелінійна оптична активність $LiNbO_3$ відкриває можливості створення лазерних джерел і спектроскопічних систем, здатних детектувати приховані або слабовідільні сліди на речових доказах. Прилади на основі нелінійних ефектів цього матеріалу можуть застосовуватися для виявлення люмінесценції чорнил у підроблених документах, аналізу мікрочастинок на місці злочину, а також у технологіях оптичної автентифікації носіїв інформації. Таким чином, $LiNbO_3$, окрім ролі в квантовій фотоніці, виступає перспективним матеріалом для розвитку нових інструментів судової експертизи й підвищення точності криміналістичних досліджень.

Таким чином, отримані результати дозволяють глибше зрозуміти унікальні оптичні характеристики $LiNbO_3$ на мікроскопічному рівні [9, 10]. Поєднання ковалентного та іонного характеру зв'язків Nb–O забезпечує високу нелінійну поляризовність кристала, що є ключовим фактором для ефективного протікання процесів спонтанного параметричного даун-конверсії (SPDC), які широко використовуються для генерації пар ентангльованих фотонів у квантових інформаційних системах [11, 12]. Аналіз порядків зв'язків і розподілу електронної щільності демонструє, що ковалентний компонент Nb–O підтримує когерентність фотонних процесів, тоді як іонний компонент визначає стабільність електронної структури, мінімізуючи небажані втрати [13]. Одночасно він відкриває широке коло перспектив для використання в питаннях забезпечення кібербезпеки та захисту інформації, а також у питаннях боротьби із злочинністю у кібернетичному просторі. Додатковий аналіз електронної густини підтверджує змішаний характер Nb–O взаємодій та іонність Li–O зв'язків. Розподіл електронів по s, p і d орбіталях показує, що основний внесок у нелінійну поляризовність кристала забезпечують d-орбіталі ніобію, тоді як p-орбіталі кисню формують стабільну мережу зв'язків.

Іонність взаємодій Li–O грає не менш важливу роль: вона відповідає за структурну стабільність кристала, низькі оптичні втрати та високу прозорість у видимому та ближньому інфрачервоному спектрі, що є критичним для побудови компактних і високоефективних фотонних інтегральних схем [14, 15]. Квантово-хімічний розрахунок зарядів показує, що електронна щільність Li є частково делокалізованою, що сприяє адаптивності кристала до зовнішніх електричних полів і забезпечує стабільну роботу електро-оптичних модуляторів.

Отже, детальний квантово-хімічний аналіз підтверджує, що саме електронна структура $LiNbO_3$ визначає його високий потенціал для застосувань у квантовій криптографії. Матеріал демонструє оптимальне поєднання ковалентних та іонних властивостей, що робить його придатним не лише для генерації квантово-корельованих фотонів, а й для реалізації фазових модуляторів у протоколах QKD, інтегрованих фотонних схем та інших компонентів квантових інформаційних систем [11, 12, 14]. Водночас отримані результати мають значення і для криміналістики та боротьби із злочинністю взагалі [16-18]. Завдяки високій нелінійній оптичній активності $LiNbO_3$ може стати основою для створення спектроскопічних приладів, здатних виявляти приховані сліди на речових доказах (біологічні виділення, залишки вибухових речовин). Його прозорість у широкому спектральному діапазоні дозволяє використовувати кристал у лазерних системах для аналізу документів та виявлення підробок за люмінесценцією чорнил і паперу. Крім того, інтегральні фотонні схеми на основі $LiNbO_3$ у поєднанні з протоколами квантового розподілу ключів забезпечують можливість безпечної передачі цифрових доказів між експертними лабораторіями, що підвищує достовірність і захищеність криміналістичних досліджень. Таким чином, $LiNbO_3$ виступає не лише ключовим матеріалом для квантової фотоніки, але й перспективною платформою для розвитку нових інструментів судової експертизи.

4. Висновки. Шляхом квантово-хімічного моделювання кластера $LiNbO_3$ здійснено комплексний аналіз його електронної структури, ефективних атомних зарядів, порядків зв'язків і енергетичних характеристик. Отримані результати дали змогу встановити особливості міжатомних взаємодій у кристалі та визначити їхній вплив на фізичні й оптичні властивості матеріалу.

Встановлено, що взаємодії між атомами ніобію та кисню мають змішаний іонно-ковалентний характер, що підтверджується розподілом електронної густини та значеннями ефективних атомних зарядів. Ковалентна складова зв'язків Nb–O формується за рахунок перекриття d-орбіталей ніобію та p-орбіталей кисню і забезпечує значну нелінійну поляризовність кристала. Водночас іонна складова сприяє стабільності електронної структури та зменшенню енергетичних втрат у фотонних процесах. Показано, що зв'язки Li–O мають переважно іонний характер і відіграють важливу роль у забезпеченні структурної стабільності кристалічної решітки. Розрахунок енергетичних характеристик показав,

що енергії граничних молекулярних орбіталей становлять HOMO ≈ –3,99 eV та LUMO ≈ +0,54 eV, що відповідає енергетичному розриву близько 3,53 eV. Отримане значення узгоджується з відомими експериментальними даними та пояснює високу прозорість $LiNbO_3$ у видимому та ближньому інфрачервоному спектральних діапазонах. Аналіз порядків зв'язків показав домінування взаємодій Nb–O, значення яких знаходяться в межах 1,3–1,8. Саме ці взаємодії формують основу нелінійних оптичних властивостей кристала, зокрема визначають величину нелінійного оптичного коефіцієнта другого порядку χ^2, що характеризує здатність матеріалу до нелінійної поляризації та ефективного протікання процесів подвоєння частоти світла і спонтанної параметричної даун-конверсії.

Показано, що поєднання сегнетоелектричних властивостей, значної нелінійної поляризовності та стабільної електронної структури зумовлює високий потенціал $LiNbO_3$ для використання у квантових фотонних технологіях. Зокрема, цей матеріал є перспективною платформою для створення джерел ентангльованих фотонів, реалізації фазових модуляторів у протоколах квантового розподілу ключів та побудови інтегральних фотонних схем у системах квантового зв'язку.

Крім того, результати дослідження свідчать про можливість застосування $LiNbO_3$ у прикладних задачах криміналістики та інформаційної безпеки. Завдяки високій нелінійній оптичній активності та широкому спектральному діапазону прозорості цей матеріал може бути використаний у лазерних спектроскопічних системах для виявлення прихованих слідів біологічного походження, аналізу документів та встановлення фактів їх підроблення. Перспективним напрямом є також застосування фотонних пристроїв на основі $LiNbO_3$ у системах квантової автентифікації та захищеної передачі цифрової інформації.

Таким чином, результати проведеного дослідження підтверджують, що літій-ніобат є перспективним функціональним матеріалом, який поєднує фундаментальні властивості нелінійної квантової фотоніки з широкими можливостями практичного застосування у квантових комунікаціях, інформаційній безпеці та сучасних методах судової експертизи.

Подяка. Автори висловлюють щиру подяку професору Майклу Шмідту (Michael W. Schmidt) за надання можливості безкоштовного використання програмного пакета GAMESS/FireFly, що суттєво сприяло виконанню квантовохімічних розрахунків у межах даного дослідження. Його внесок у розвиток програмного забезпечення для квантової хімії та відкритий доступ до нього є надзвичайно цінними для наукової спільноти.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних.

Використання штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Людмила Соляник: концептуалізація; методологія; проведення експериментальних досліджень; обробка та аналіз експериментальних даних; квантово-хімічні розрахунки; написання рукопису.

Віктор Коваль: тестування системи і візуалізації даних.

References:

1. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science. P. 124–134. DOI: 10.1109/SFCS.1994.365700.

2. Zhu, D., Shao, L., Yu, M. et al. (2021). Integrated photonics on thin-film lithium niobate. *Advances in Optics and Photonics*. Vol. 13, No. 2. P. 242–352. DOI: 10.1364/AOP.411024.

3. Saravi, S., Pertsch, T., Setzpfandt, F. (2021). Lithium Niobate on Insulator: An Emerging Platform for Integrated Quantum Photonics. *Advanced Optical Materials*. Vol. 9. DOI: 10.1002/adom.202100789.

4. Hossain, M. M. (2019). First-principles study on the structural, elastic, electronic and optical properties of $LiNbO_3$. *Heliyon*. Vol. 5, No. 4. e01436. DOI: 10.1016/j.heliyon.2019.e01436.

5. Harper, N. A., Hwang, E. Y., Sekine, R. et al. (2024). Highly efficient visible and near-IR photon pair generation with thin-film lithium niobate. Optica Quantum. Vol. 2, No. 2. P. 103–109. DOI: 10.1364/OPTICAQ.507526.Gordon M.S., Schmidt M.W. GAMESS (General Atomic and Molecular Electronic Structure System) [Електронний ресурс] / University of Georgia and Iowa State University. Retrieved from: https://www.msg.chem.iastate.edu/gamess/

6. Zanatta, A. R. (2022). The optical bandgap of lithium niobate ($LiNbO_3$) and its dependence with temperature. *Materials Today: Proceedings*. Vol. 64, Part 4. P. 1127–1130. DOI: 10.1016/j.matpr.2022.04.257.

7. Schirmer, O. F., Thiemann, O., Wöhlecke, M. (2009). Defects in $LiNbO_3$: I. Experimental aspects // *physica status solidi (c)*. Vol. 6, Issue 1. P. 257–262. DOI: 10.1002/pssc.200982473.

8. Bennett, C.H., Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. Vol. 560. P. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

9. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys*. Vol. 74. P. 145–195. DOI: 10.1103/RevModPhys.74.145.

10. Kwiat, P.G., Mattle, K., Weinfurter, H., Zeilinger, A. (1995). New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett*. Vol. 75. P. 4337–4341. DOI: 10.1103/PhysRevLett.75.4337.

11. Tanzilli, S., Martin, A., Kaiser, F., et al. (2012). On the genesis and evolution of entangled photon sources in lithium niobate. *Laser & Photonics Reviews*. Vol. 6, Issue 1. P. 115–143. DOI: 10.1002/lpor.201100017.

12. Schirmer, O.F., Thiemann, O., Wöhlecke, M. (2009). Defects in $LiNbO_3$: I. Experimental aspects. *physica status solidi* (c). Vol. 6, Issue 1. P. 257–262. DOI: 10.1002/pssc.200982473.

13. Zanatta, A.R. (2022). The optical bandgap of lithium niobate ($LiNbO_3$) and its dependence with temperature. *Materials Today: Proceedings*. Vol. 64, Part 4. – P. 1127–1130. DOI: 10.1016/j.matpr.2022.04.257.

14. Boyd, R.W. (2008). Nonlinear optics. 3rd ed. Academic Press, 706 p.

15. Lysenko, S.O., Veklych, V.O., Kocherov, M.V., Servetskiy, I.V., & Arifkhodzhaieva, T.B. (2021). Two dominant security concepts in Europe and its influence on Ukraine. *Linguistics and Culture Review*, 5(S4), 2029–2040. https://doi.org/10.21744/lingcure.v5nS4.1864.

16. S. Lysenko,... (2023). The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War. *Studies in media and communication.* Vol 11, No7 (Скопус), с. 150–158. DOI: https://doi.org/10.11114/smc.v11i7.6414. https://redfame.com/journal/index.php/smc/article/view/6414

17. Tarasenko, O., Lysenko, S., Tarlopov, I., Pidkaminnyi, I., & Verhun, M. (2024). (Скопус) Analysis of the competitiveness of higher education institutions in Ukraine in the context of recovery and development after the war. *Multidisciplinary Science Journal,* 6, 2024ss0210. https://doi.org/10.31893/multiscience.2024ss0210

Відомості про авторів

Англійська	Українська
Ludmila Solianyk Professor at the Department of Cybersecurity and Information Protection, Faculty of Computer and Information Technologies, Interregional Academy of Personnel Management solianyk2017@gmail.com ORCID: 0000-0002-2661-9392 Scopus Author ID: 36903008700	Соляник Людмила Олексіївна професор кафедри кібербезпеки та захисту інформації факультету комп'ютерно-інформаційних технологій, Міжрегіональна Академія управління персоналом solianyk2017@gmail.com ORCID: 0000-0002-2661-9392 Scopus Author ID: 36903008700
Viktor Koval Lecturer at the Department of Cybersecurity and Information Protection, Faculty of Computer and Information Technologies, Interregional Academy of Personnel Management vitjuha@gmail.com ORCID: 0009-0003-6707-4194	Коваль Віктор Іванович викладач кафедри кібербезпеки та захисту інформації факультету комп'ютерно-інформаційних технологій, Міжрегіональна Академія управління персоналом vitjuha@gmail.com ORCID: 0009-0003-6707-4194

Дата надходження статті: 27.05.2026
Дата надходження виправленої версії статті: 07.07.2026
Дата прийняття статті: 09.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.11
UDC 004.056.5:004.94:004.7
JEL Classification: C52, C63, O33, R58

MULTILEVEL EXPERIMENTAL VALIDATION OF A SMART-REGION CYBER-RESILIENCE METHODOLOGY: FROM FORMAL VERIFICATION TO HARDWARE-IN-THE-LOOP TESTING, PILOT DEPLOYMENT, AND EXTERNAL REPLICATION

Yuliia Khokhlachova

БАГАТОРІВНЕВА ЕКСПЕРИМЕНТАЛЬНА ВАЛІДАЦІЯ МЕТОДОЛОГІЇ КІБЕРСТІЙКОСТІ РОЗУМНОГО РЕГІОНУ: ВІД ФОРМАЛЬНОЇ ВЕРИФІКАЦІЇ ДО ТЕСТУВАННЯ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ В ЦИКЛІ, ПІЛОТНОГО РОЗГОРТАННЯ ТА ЗОВНІШНЬОГО ВІДТВОРЕННЯ

Ю. Є. Хохлачова

Abstract

Object of study. Multilevel validation of a cyber-resilience methodology for interdependent smart-region services. Problem. Results from formal verification, simulation, hardware-in-the-loop testing, pilot deployment, and external replication are not interchangeable; missing claim-to-evidence links encourage unsupported generalization. Purpose. To develop and partially verify a reproducible V0-V5 validation programme. Methods. The programme defines twelve attack and failure scenarios A1-A12, six resource-comparable configurations B0-B5, and paired ablations of the evidence pipeline, digital twin, and policy controller; it uses synchronized traces, common event markers, confidence intervals, effect sizes, and multiple-testing correction. Results. In the available V3 aggregates, B5 versus B1 reduced mean detection time from 43,1 to 8,5 s (80,3%) and recovery time from 399 to 122 s (69,4%), achieved 98,7% integrity-verification accuracy with less than 6% overhead, and increased the normalized resilience index from 0,71 to 0,93. Distinctive features. Unlike single-node assessment, the architecture combines validation levels, claim-to-evidence traceability, and cumulative I0-I4 maturity gates while separating laboratory causality, operational feasibility, and external transferability. The changes are explained by the joint operation of a verified telemetry pipeline, a cross-sector dependency model, and a constrained recovery controller. Practical use is appropriate in controlled regional infrastructure with an equal resource budget, synchronized measurements, verified safety rules, and explicit evidence boundaries. Conclusions. The aggregates support a descriptive proof of concept for the integrated system, but component-level causality requires run-level logs, completed ablations, a V4 pilot, and independent V5 replication.

Key words: *experimental validation, hardware-in-the-loop, external replication, cyber-resilience maturity, attack scenarios, baselines, reproducibility, smart region.*

Анотація

Об'єкт дослідження. Багаторівнева валідація методології кіберстійкості взаємозалежних сервісів розумного регіону. Проблема. Результати формальної перевірки, моделювання, апаратного тестування, пілотного впровадження та зовнішнього відтворення не є взаємозамінними, а відсутність зв'язку між твердженнями й доказами спричиняє необґрунтоване узагальнення ефектів. Мета. Розробити та частково перевірити відтворювану програму валідації від V0 до V5. Методи. Сформовано дванадцять сценаріїв атак і відмов A1-A12, шість ресурсно порівнюваних конфігурацій B0-B5, парні абляції конвеєра доказів, цифрового двійника і контролера політик; передбачено синхронізовані траси, спільні часові маркери, довірчі інтервали, розміри ефектів і корекцію множинних порівнянь. Результати. За агрегатами V3 конфігурація B5 порівняно з B1 зменшила середній час виявлення з 43,1 до 8,5 с (на 80,3 %), час відновлення – з 399 до 122 с (на 69,4 %), забезпечила точність перевірки цілісності 98,7 % за накладних витрат менш як 6 % і підвищила нормалізований індекс стійкості з 0,71 до 0,93. Особливості результату. На відміну від оцінювання окремого вузла, архітектура поєднує рівні валідації, простежуваність «твердження-доказ» і рівні зрілості I0-I4, розмежовуючи лабораторну причинність, операційну здійсненність і зовнішню переносимість. Зміни пояснюються спільною роботою перевіреного конвеєра телеметрії, моделі міжсекторних залежностей і обмеженого контролера відновлення. Практичне використання можливе у контрольованій регіональній інфраструктурі за однакового ресурсного бюджету, синхронізованих вимірювань, перевірених правил безпеки та явного врахування меж доказів. Висновки. Агрегати підтверджують описовий доказ концепції інтегрованої системи, але не визначають причинний внесок компонентів без журналів запусків, завершених абляцій, пілоту V4 і незалежної реплікації V5.

Ключові слова: *експериментальна перевірка, апаратне забезпечення в циклі, зовнішня реплікація, зрілість кіберстійкості, сценарії атак, базові рівні, відтворюваність, розумний регіон.*

1. Introduction. A smart region combines energy, telecommunications, water, transport, emergency, and public digital services through shared sensors, edge nodes, networks, cloud platforms, and control centres. A local cyber incident can therefore alter both an asset and dependent services with different criticality and recovery objectives. Validation must address this interdependence rather than report the uptime of an isolated node.

© Khokhlachova Yu. Ye., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

Evidence does not transfer automatically across experimental levels. Formal safety does not demonstrate controller speed; simulation omits driver, queue, and clock effects; hardware-in-the-loop testing cannot reproduce all organizational delays; and a pilot without control does not establish general causality. Each claim must therefore be linked to a validation level, artifact, and explicit boundary of interpretation.

Bocci et al. [1] combine declarative cloud-edge placement with information-flow analysis and evaluate deployment performance through simulation. This supports secure placement decisions, but does not establish service continuity during recovery. Yang et al. [2] develop multi-replica integrity verification and reputation-based collaborative auditing for edge servers. Their approach strengthens the evidence pipeline, yet verification of stored replicas cannot establish whether a sensor measurement was physically truthful before storage. Placement security and evidence integrity therefore require distinct validation outcomes.

Fett et al. [3] bridge conceptual digital-twin reference architectures and practical cloud, edge, and hybrid implementations. This provides deployment guidance, while attack-specific acceptance criteria must be defined separately. El-Hajj [4] evaluates a digital twin and intrusion detection in a Raspberry Pi test environment, reporting flood detection alongside limitations in scan detection and resource use. That study demonstrates why successful alerting should be distinguished from timely recovery; extending its findings to interdependent regional services requires additional evidence.

Cho et al. [5] propose availability metrics and area-under-the-curve normalization, evaluated using transaction and connection rates under denial-of-service conditions. These measures inform the present resilience index, but cannot substitute for integrity or safety criteria. Tao et al. [6] synthesize industrial digital-twin applications and physical-cyber integration. Their conceptual account helps define the twin component; the resilience of a particular implementation nevertheless remains an empirical question. Consequently, architectural plausibility and measured mission preservation should not be treated as equivalent evidence.

Alcaraz and Lopez [7] organize digital-twin threats by functionality layers and operational requirements, providing a basis for attack coverage and trust boundaries. A threat taxonomy, however, does not demonstrate that a control restores mission capability. Rose et al. [8] define Zero Trust around resource protection and explicit authentication and authorization, without implicit trust based on network location. These principles constrain admissible actions in the proposed controller, while their operational effectiveness must be assessed through recovery, service-degradation, and safety measurements.

Shi et al. [9] explain the rationale for processing near data sources and discuss edge service management, security, privacy, and optimization challenges. This motivates the deployment profile, but actual latency under hostile traffic requires measurement. Kritzinger et al. [10] distinguish digital models, digital shadows, and digital twins by their degree of physical-digital integration. This classification prevents monitoring alone from being equated with a synchronized twin; it does not establish forecast accuracy or secure closed-loop operation.

Sengupta et al. [11] survey attacks, countermeasures, and blockchain approaches across IoT and IIoT settings. Their synthesis supports threat selection, but ledger-based recovery still requires tests of communication cost and trust assumptions. Mozzaquatro et al. [12] combine ontology-based security design with runtime threat classification and adaptation, including an industrial case study. This supports consistent security semantics, whereas cross-sector recovery effects require resource-comparable experiments. Thus, threat coverage and semantic consistency inform the programme without proving its integrated effectiveness.

Dietz and Pernul [13] explain how digital twins support industrial-control security through simulation and replication of physical-system behaviour. Replication inside a twin must be distinguished from independent repetition by another team and site, the objective of V5. Aghazadeh Ardebili et al. [14] relate critical-infrastructure cyber resilience to risk-assessment methods, governance, and standards. This broadens the selection of evaluation criteria, but does not establish the performance of a particular recovery controller or its transferability between infrastructures.

Chandola et al. [15] compare anomaly-detection methods through their assumptions, limitations, and computational demands. This supports explicit detector selection, but discrimination of anomalies alone cannot demonstrate safe recovery. Xu et al. [16] examine industrial IoT through interacting control, networking, and computing subsystems and their reliability requirements. This motivates coupled cyber-physical testing, while industrial requirements need recalibration for regional services with different criticality and recovery objectives. Detector performance must therefore be interpreted within the wider service and control context.

Ranaweera et al. [17] map security and privacy threats to the multi-access edge-computing architecture and examine countermeasures. This informs the edge threat model, while end-to-end recovery gains under fixed resources remain to be tested. De Neira et al. [18] classify DDoS-prediction research by warning time, architecture, and methodology. Prediction before an attack develops differs from detection after onset and subsequent recovery; comparisons therefore require common event markers and equivalent exposure rather than interchangeable timing metrics.

Fuller et al. [19] review enabling technologies and challenges across manufacturing, healthcare, and smart-city digital twins. This establishes application breadth, but outcomes from these domains cannot be pooled into a regional resilience claim without explicit transfer conditions. Minerva et al. [20] derive foundational twin properties and a generic architectural model from technical features and application scenarios. This guides state representation and synchronization, while conformity to an architecture must be complemented by calibrated cascade forecasts and verified intervention outcomes.

Sharma et al. [21] identify incomplete implementation disclosure, domain dependence, and inadequate performance metrics as obstacles to evaluating and comparing digital twins. These findings directly motivate run manifests and common outcomes, while the present programme still requires released run-level artifacts to demonstrate reproducibility. Homaei et al. [22] review cybersecurity risks affecting digital twins and the potential role of artificial intelligence in protection. This supports treating the twin itself as security-critical, with separate tests of uncertainty, state freshness, and action safety.

Taken together, these contributions provide placement, auditing, architectural, detection, and assessment foundations. Their different objectives and validation settings leave a methodological need for a common link between claims, resource-comparable experiments, and level-specific artifacts. The proposed programme addresses that need by separating formal safety, laboratory effects, operational feasibility, and external transfer. It does not assume that combining established components has already demonstrated all four: each requires its own evidence and explicit limits of interpretation.

This article addresses that gap through a V0-V5 programme that separates formal correctness, laboratory causality, operational feasibility, and external transferability. Its contribution is an architecture combining twelve scenarios A1-A12, configurations B0-B5, paired ablations, claim-to-evidence traceability, and the I0-I4 maturity model. Only supplied V3 aggregates are treated as observations; arithmetic changes are derived, whereas V0-V2, V4, and V5 remain protocols where the required evidence bundles are absent.

The integration problem is methodological as well as technical. A detector may improve alert speed while leaving recovery unchanged; an integrity audit may verify stored blocks without establishing whether a sensor reported the physical process truthfully; and an optimizer may preserve availability while violating an authorization or safety constraint. The programme therefore evaluates mission outcome, mechanism quality, safety, resource cost, and transferability separately, while retaining a traceable link between each claim and the evidence that can legitimately support it.

Research aim. The aim of this study is to develop a reproducible V0-V5 validation programme for the cyber resilience of interdependent smart-region services and to assess its integrated proof of concept using the available V3 aggregate evidence. The programme links each claim to the artifacts and interpretation boundaries required at its validation level.

Research objectives. To achieve this aim, the study determines the evidence requirements and admissible claims at each V0-V5 level; quantifies the descriptive B5-versus-B1 changes in the available V3 aggregates within the stated resource-comparable profile; defines paired ablations and criteria for identifying component-level causal contributions; specifies tests of scaling limits and external transferability; translates validation evidence into cumulative I0-I4 maturity gates; and critically compares the findings with prior work to identify limitations and further research needs. These objectives distinguish the aggregate analysis performed here from ablation, pilot, and independent-replication studies that remain to be completed.

2. Materials and methods. The object of study is the multilevel validation process for cyber resilience of interdependent smart-region services. The main hypothesis is that, under an equal resource budget, the integrated B5 configuration improves mission preservation, detection, and recovery relative to B1, while the admissible interpretation remains bounded by the validation level. The analysis assumes identical attack traces, workloads, seeds, and time budgets; synchronized clocks and common event markers; and stable service-criticality weights within each comparison. The principal simplifications are a controlled four-sector profile, emulated sensors, one V3 testbed, aggregate rather than run-level observations, and the absence of completed V4 and V5 studies.

2.1. Research questions and hypotheses. The study asks whether B5 reduces mission loss, detection time, and recovery time under an equal resource budget, and where its scaling and transferability limits occur. Hypotheses and present evidence status are fixed before analysis (Table 1).

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

Table 1

Research hypotheses and current evidence status

Code	Hypothesis	Current evidence
H1	B5 reduces mission loss versus resource-comparable baselines	Preliminary aggregate comparison only with B1
H2	The evidence pipeline reduces detection delay without excessive false positives	Run-level B5-E ablation required
H3	The digital twin improves cascade forecasting and localization	Protocol only; numerical series absent
H4	The policy controller reduces recovery time without unsafe actions	Aggregate effect reported; B5-P required
H5	The effect persists to 10^2-10^4 devices within service limits	Scale test planned
H6	V4 and V5 preserve the direction of effect	Not completed

Source: compiled by the author.

Component-level claims require B5-E, B5-D, and B5-P ablations on identical traces; a full-system versus B1 comparison cannot isolate their causal contributions.

2.2. Evidence chain and preregistration. Before the main series, the model version, parameters, metrics, configurations, ablations, exclusion rules, minimum detectable effect, test order, multiplicity families, and disclosure plan are frozen. Any later change creates a new protocol version rather than silently replacing the original hypothesis.

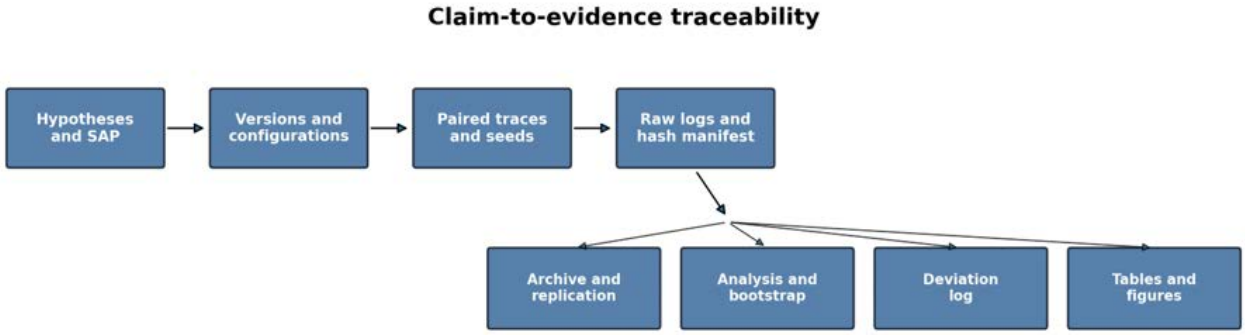


Fig. 1. Claim-to-evidence traceability from preregistration to independent replication

(Source: prepared by the author)

Claim-to-evidence traceability (Figure 1) is implemented through a machine-readable manifest containing artifact hashes, software, firmware and container versions, hardware, seeds, timestamps, synchronization data, and deviations. Hashes establish immutability after acquisition, while authenticity, provenance, transport integrity, and physical plausibility remain separate evidence fields.

2.3. Functional decomposition of the methodology. The evidence pipeline validates identity, timestamps, sequences, provenance, freshness, signatures, and selected replicas. The dependency-aware digital twin synchronizes asset state, estimates cascades, and tests candidate interventions. The constrained policy controller rejects actions that violate authorization, capacity, trust, or safety requirements and selects a reversible action that minimizes expected mission loss.

The test model links energy, telecommunications, water, and public digital services to reproduce the chain physical process – communication – computation – service. It is a controlled cross-sector profile, not a claim of representativeness for every regional asset.

V0 checks authorization, rollback reachability, deadlock freedom, and command consistency. Subsequent levels add simulation, real protocols and queues, hardware limits, operational integration, and independent replication. Figure 2 summarizes the architecture.

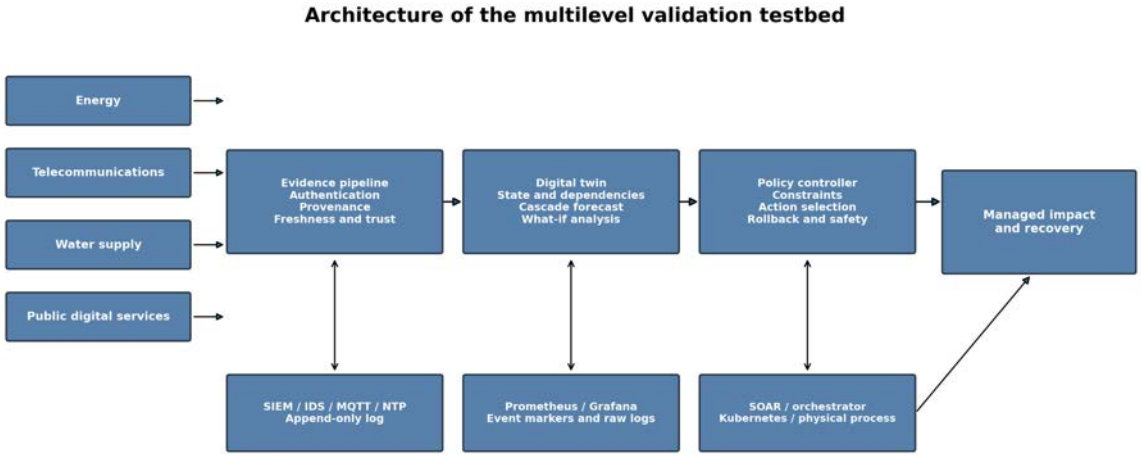


Fig. 2. Architecture of the multilevel testbed and managed recovery loop

(Source: prepared by the author)

2.4. Validation levels V0-V5. Each level answers a distinct evidence question and limits the conclusion that may be drawn (Table 2).

Table 2

Validation levels, evidence purpose, and present status

Level	Evidence purpose	Present status and limit
V0	Formal safety, liveness, authorization, deadlock checks	Protocol; no model-checker report
V1	Simulation of dependencies, extreme cases, factorial series	Protocol; no real network costs
V2	Real protocols, queues, partitions, failover, recovery	Engineering profile only
V3	Hardware and cyber-physical limits, safety interlocks	Reported aggregate evidence in one testbed
V4	Operational fit, data quality, human-in-the-loop performance	Not performed; feasibility only
V5	Independent replication within a frozen profile	Not performed; no universal claim

Source: compiled by the author.

2.5. Experimental platform. The reported V3 profile used 12 emulated Internet-of-Things sensors with Mosquitto 2.0; four Raspberry Pi 5 edge nodes with K3s 1.30, Suricata 7.0, and integrity agents; three 8-vCPU/16-GB virtual machines with Kubernetes 1.30; Eclipse Ditto 3.5; Prometheus 2.53, Grafana 11, and an append-only log; and an isolated Kali Linux host with Hping3 and NMAP. Common event markers identified attack onset, detection, containment, recovery, and the observation-window end. Experiments were confined to an isolated network; pilot data require aggregation or pseudonymization.

Before every run, clocks are synchronized and the environment is restored to a clean snapshot. Attack onset, alert generation, containment, service restoration, and the end of the observation window share common markers so that MTTD, MTTR, and mission loss use the same temporal reference. The supplied description covers four attack profiles with twenty repetitions each; because the individual traces are unavailable, that repetition count cannot be independently audited or used to reconstruct dispersion.

2.6. Catalogue of attacks and failures. A scenario is admissible only when ground truth specifies time, asset, event class, injection profile, expected indicators, permitted responses, and a stop condition. The minimum catalogue in Table 3 covers data, time, gateways, networks, quorum, keys, policies, storage, and physical plausibility.

Each scenario is parameterized by intensity, duration, affected fraction, topology position, and legitimate workload mix. A1 and A2 deliberately separate post-signing tampering from validly signed falsehood; A5 separates hostile flooding from a flash crowd; A6-A10 exercise recovery state machines; and A11-A12 test correlated evidence and cross-sector cascades. The same scenario definition is reused across configurations so that differences are not caused by unequal fault exposure.

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

Table 3

Minimum catalogue of attacks and failures

Code	Scenario	Validation objective
A1	Post-signing tampering	Cryptographic integrity
A2	Validly signed false readings	Physical plausibility and sensor-oracle consistency
A3	Replay, timestamp manipulation, clock drift	Freshness and sequence integrity
A4	Compromised edge gateway	Provenance, attestation, redundant routes
A5	DDoS or flash crowd	Admission control with bounded false positives
A6	Partition or quorum loss	Graceful degradation and reconciliation
A7	Byzantine validator or collusion	Quorum trust boundary
A8	Key compromise or revocation	Identity-state recovery
A9	Policy or smart-contract defect	Verification, approval, and rollback
A10	Off-chain storage failure	Restore and integrity control
A11	Coordinated sensor-cluster compromise	Independence-aware trust
A12	Four-sector cascade	Dependency-aware coordinated recovery

Source: compiled by the author.

2.7. Configurations B0-B5 and ablations. Resource-fair comparisons use identical nodes, bandwidth, service demand, attack traces, seeds, time budgets, and recovery rules (Table 4). B5-E removes provenance/freshness/trust, B5-D removes cascade forecasting and what-if analysis, and B5-P removes automated policy selection while preserving observations.

Unused baseline capacity is recorded as a cost rather than reassigned to B5. Configuration order is randomized, and all variants use the same action horizon and stop conditions. Ablations may disable uncertainty handling, fallback, or the safety shield.

Component effects are estimated from paired contrasts and interaction terms, not by dividing the overall B1-B5 improvement into arbitrary percentages.

Table 4

Resource-comparable configurations B0-B5

Code	Configuration	Enabled mechanisms
B0	Standard stack	Local logs, access control, standard failover
B1	Strong detection and manual response	IDS/SIEM, operator decision, manual recovery
B2	Zero Trust and orchestration	Identity, policy rules, playbooks; no cascade forecast
B3	Static SDN/NFV resilience	Rule-based reroute, failover, static chains
B4	Centralized optimizer	Full telemetry and optimization; no provenance-aware trust
B5	Full methodology	Evidence pipeline, digital twin, constrained controller, rollback

Source: compiled by the author.

2.8. Metrics and mathematical model. The primary outcome is mission capability rather than an individual node. For normalized service capability $q_k(t)$ and criticality weight ω_k, the regional mission quality is

$$Q_m(t) = \sum_{k=1}^{K} \omega_k q_k(t), \quad \sum_{k=1}^{K} \omega_k = 1. \tag{1}$$

The area of mission loss and normalized resilience index are

$$L_m = \int_{t_0}^{t_1} \left[1 - Q_m(t)\right] dt, \tag{2}$$

$$\mathrm{NRI} = 1 - \frac{L_m}{t_1 - t_0} = \frac{1}{t_1 - t_0} \int_{t_0}^{t_1} Q_m(t)\, dt. \tag{3}$$

Equation (3) measures the preserved capability area across services; the integral is evaluated by the trapezoidal rule over a common comparison window [5].

For source i, dynamic trust combines passed integrity checks $I_i(t)$, provenance consistency $P_i(t)$, and behavioural consistency $B_i(t)$:

$$T_i(t) = \lambda T_i(t-1) + (1-\lambda)\left(w_I I_i(t) + w_P P_i(t) + w_B B_i(t)\right), \tag{4}$$

The weights sum to one and 0 <= lambda <= 1. A valid signature proves origin and post-signing immutability, not the physical truth of a sensor; A2 and A11 therefore test process consistency and evidence-source independence.

Selective replica auditing complements source trust by sampling stored blocks according to a prespecified corruption model and target detection probability. The audit budget is recalculated when replica size, expected damaged share, or target confidence changes and is reported as a cost outcome for each tested profile. Audit evidence detects post-acquisition alteration but does not replace plausibility checks on measurements that were already false when signed.

Local risk propagates through dependency matrix W. The stationary estimate is valid when the spectral radius rho(βW^T) is below one:

$$r = \ell + \beta W^\top r = \left(I - \beta W^\top\right)^{-1} \ell. \tag{5}$$

The controller selects an admissible action by minimizing mission loss, resource cost, disruption, and uncertainty:

$$a_{\text{opt}} = \arg\min_{a \in \mathcal{A}_{adm}} \left[L_m(a) + \eta_c C(a) + \eta_d D(a) + \eta_u U(a) \right]. \tag{6}$$

Any action violating a hard safety predicate is excluded regardless of expected benefit.

Detection and recovery time use common event markers:

$$\text{MTTD} = \frac{1}{n}\sum_{j=1}^{n}\left(t_j^{det} - t_j^{onset}\right), \quad \text{MTTR} = \frac{1}{n}\sum_{j=1}^{n}\left(t_j^{rec} - t_j^{onset}\right). \tag{7}$$

The scaling boundary is the first device count at which decision latency, resource use, safety, or mission-loss limits are violated:

$$N\text{lim} = \min\{N : p99(N) > D_{act} \vee U_{CPU}(N) > Umax \vee L_m(N) > L_{max}\}. \tag{8}$$

The metric hierarchy prevents a secondary improvement from masking mission or safety degradation. Mission loss and NRI are primary; detection quality includes MTTD, false-positive and false-negative rates, calibration, and interval coverage; recovery includes MTTR, recovery-point and recovery-time objectives, slope, and rollback. Network percentiles, cascade size and depth, unsafe actions, processor, memory, traffic, storage, energy, and operator workload are reported as service, mechanism, safety, cost, and V4 outcomes rather than collapsed into one score.

2.9. Statistical analysis plan. The unit of comparison is a paired run: configurations and ablations replay the same trace, seed, service demand, and fault schedule. Order is randomized, and every run starts from a fixed clean snapshot. Sample size is planned from the minimum detectable paired effect and pilot variance:

The design reports differences, effect sizes, and 95% confidence intervals rather than relying on a fixed repetition count.

$$n \geq \left(\frac{z_{1-\alpha/2} + z_{1-\beta}}{\delta_{min} / \sigma_d} \right)^2. \tag{9}$$

Latency and recovery are summarized by p50, p95, p99 and bootstrap confidence intervals. Paired t, Wilcoxon, or permutation tests are selected after diagnostics; factorial series use a mixed-effects model with configuration, scenario, scale, and sector as fixed effects and trace/seed and site as random effects.

Holm correction is applied within metric families; practical thresholds, negative results, and rejected hypotheses are retained.

Analysis families are defined before results are inspected. Distributional assumptions, missingness, carry-over, time synchronization, and the stability of thresholds under legitimate regime change are checked explicitly. A statistically detectable difference is not treated as useful unless it crosses a preregistered practical threshold, while a safety-predicate violation rejects a configuration even when its average mission metric improves. Exploratory metrics remain labelled as exploratory and are evaluated on a separate validation set before confirmatory use.

2.10. Scaling, pilot deployment, and external replication. Scale tests vary the device count, telemetry rate, graph density, candidate actions, and compromised-source share, reporting p95/p99 latency and compute, memory, storage, traffic, and energy separately for each component. V4 uses approved deidentified or aggregate partner data to test integration, data quality, operator performance, overrides, and rollback readiness; it establishes feasibility, not general causality.

V5 is executed by an independent team with a frozen release, configuration profile, and analysis plan. Transferability is quantified only when the external and laboratory effects have the same direction:

$$\mathrm{TR} = \frac{\Delta^{ext}}{\Delta^{lab}}, \quad \text{provided that } \operatorname{sign}\left(\Delta^{ext}\right) = \operatorname{sign}\left(\Delta^{lab}\right). \tag{10}$$

The ratio is not interpreted when confidence intervals admit opposite directions or the external profile falls outside preregistered bounds.

Production attack code is excluded from V4; faults are introduced only in an approved window or through synthetic markers. V5 receives frozen public and controlled artifacts but not unrestricted operational secrets. A successful external repeat establishes transfer only within the reproduced topology, workload, sector physics, and organizational approval profile; it does not justify universality beyond those bounds.

2.11. Reproducibility, data, and security review. Every run produces a manifest linking the protocol, code or container digest, firmware, hardware, topology, schema, seeds, clock skew, attack parameters, exclusions, raw-log hashes, analysis scripts, outputs, and deviations. Results are regenerated from the frozen manifest rather than copied manually.

Public artifacts include protocols, synthetic traces, schemas, analysis code, aggregate results, and documentation; deidentified detailed traces are controlled, while keys, exact addresses, sensitive rules, and high-resolution incident data remain restricted. Release requires licence, software-bill-of-materials, secret-scanning, vulnerability, and disclosure review.

Failed runs and deviations remain in the manifest. Exclusion is allowed only for predefined synchronization, telemetry, injector, snapshot, or safety-stop failures. The independent package contains deployment instructions, expected intermediate outputs, metric definitions, a data dictionary, and a replication-note template.

The minimum replication package contains a README, threat model, infrastructure-as-code profile, container digests, synthetic seed set, expected intermediate outputs, metric definitions, data dictionary, statistical notebook or script, licence, software bill of materials, disclosure policy, and replication-note template. The package is versioned, archived, and published even when the direction of effect is not preserved, because negative replication is evidence about applicability boundaries.

3. Results and discussion

3.1. Evidence status. The pre-analysis evidence map in Tables 1 and 2 defines a complete V0-V5 programme, but only the V3 topology and aggregate B1-versus-B5 means are available. V0 lacks a model-checker report; V1-V2 remain engineering protocols; and run-level logs, ablations, V4, and V5 are unavailable. The admissible evidence is therefore descriptive and profile-bounded.

3.2. Aggregate hardware-in-the-loop results at V3. The reported series covered a compromised edge device, falsified telemetry, a SYN/ACK flood, and malicious workload migration, with twenty repetitions per scenario according to the supplied description. B1 combined intrusion detection with manual recovery; B5 used the integrated pipeline, twin, and controller. Because run-level distributions are unavailable, Table 5 reports descriptive means and arithmetic changes without confidence intervals or p-values.

Table 5

Reported aggregate V3 results and arithmetic changes

Metric	B1	B5	Change	Interpretation
Mean detection time	43,1 s	8,5 s	-80,3%	Integrated verified evidence and automation
Mean recovery time	399 s	122 s	-69,4%	Faster containment and recovery
Integrity-verification accuracy	Not reported	98,7%	-	B5 only
Additional overhead	Not reported	<6%	-	Small-testbed bound
NRI under DDoS	0,71	0,93	+31,0%	Resilience deficit reduced by 75,9%

Source: compiled by the author.

B5 reduced mean detection time by 80,3% and recovery time by 69,4%. NRI rose by 0,22 (31,0%), while the resilience deficit fell by 75,9%. These values support the integrated proof of concept, but they cannot identify how much improvement came from detection, trust, cascade forecasting, operator removal, enforcement, or post-recovery verification.

The distinction between the 31,0% NRI increase and the 75,9% reduction in resilience deficit is important. NRI describes preserved capability over the whole disruption-and-recovery window, whereas the deficit

isolates the unrecovered fraction relative to perfect service. Both summaries point in the same direction, but neither provides uncertainty or generalization beyond the reported DDoS profile.

3.3. Causal contribution of components. The hypotheses in Table 1 and the resource-comparable configurations in Table 4 define a component contribution as the paired difference between B5 and its matching ablation under the same budget. Because B5-E, B5-D, and B5-P observations are absent, no numerical causal shares or synergies are claimed; the reported improvement belongs to the integrated configuration.

Ablation interpretation must also consider mechanism outcomes: removing the evidence pipeline may alter false positives and calibration, removing the twin may change forecast coverage and cascade size, and removing the controller may shift recovery time, rollback, and unsafe-action counts. A lower average mission loss cannot compensate for a safety violation or a materially higher resource budget.

3.4. Scaling limits and transferability. The V3 profile in Table 2 demonstrates operation with 12 streams, four edge nodes, and three cloud virtual machines, not a limit for 10^2-10^4 devices. A scale claim requires p95/p99 curves, resource profiles, and sensitivity to telemetry rate, graph density, and candidate actions. Transferability is technological, sectoral, and organizational; only an independent V5 repeat and the direction-of-effect condition in equation (10) can test whether the effect survives a new team and site.

3.5. Practical maturity model I0-I4. The maturity model converts validation evidence into implementation gates (Table 6). Technology ownership alone does not justify a level transition.

Table 6

Maturity gates I0-I4

Level	State	Required capabilities	Transition evidence
I0	Baseline	Inventory, synchronized clocks, evidence schema	Complete coverage and stable telemetry
I1	Observable	Provenance, freshness, trust, mission dashboard, audit trail	Calibration and reproducible evidence chain
I2	Predictive	Digital twin, cascade forecast, what-if analysis, uncertainty	Out-of-sample forecast and approved scenarios
I3	Controlled	Reversible actions, safety shield, rollback, orchestration	Formal safety, zero unsafe tests, bounded latency
I4	Adaptive	Federated coordination, local fallback, recalibration	Pilot record, service limits, scale and replication plan

Source: compiled by the author.

An internal weighted score may support gap analysis, but it cannot compensate for missing emergency stop, data minimization, formal safety, or verified rollback.

Transitions are cumulative. I1 requires calibrated cross-sector observability before I2 forecasting can be trusted; I3 requires formal safety, bounded latency, and verified rollback before automated action; and I4 adds pilot evidence, local fallback, service-level monitoring, periodic recalibration, scale tests, and a replication plan. Missing a hard gate lowers the admissible maturity level even when other capability scores are high.

3.6. Discussion, limitations, and development directions. The V3 aggregates in Table 5, interpreted through equations (1)-(3), provide a descriptive comparison of the integrated B5 configuration with B1. Secure placement [1] and collaborative auditing [2] supply relevant component-level foundations, while implementation architectures [3] and twin-assisted intrusion detection [4] motivate the testbed design. Availability-based normalization [5] informs the mission assessment but cannot establish integrity or safe control. Figure 1 links claims to artifacts, and Figure 2 relates the evidence pipeline, twin, and controller. The contribution is their explicit placement within a common validation programme; simultaneous changes in several mechanisms and absent run-level distributions prevent causal attribution or uncertainty estimation from the reported aggregates.

Cryptographic integrity and physical truth must remain distinct. The storage-audit scope of EDI-C [2] should be distinguished from verifying the physical plausibility of data before acquisition: a valid signature can authenticate a false sensor value. The proposed programme therefore combines process models, independent sources, spatial-temporal consistency, and explicit uncertainty. Digital-twin architecture [3] and detection integration [4] provide a basis for implementation, while the proposed extension to cross-sector cascade estimation and counterfactual intervention testing requires its own calibration and validation.

The I0-I4 model likewise separates technology acquisition from evidence of readiness. Negative results define applicability limits: if a simpler B3 or B4 configuration produces lower p99 latency at scale, or V5 preserves direction with a smaller effect, the discrepancy should be reported and explained rather than suppressed.

Operationally, the strongest result is not the isolated percentage change but the disciplined transition from observation to reversible action. The evidence pipeline limits which measurements may influence the twin; the twin exposes likely cross-sector consequences; and the controller enforces resource, authorization, uncertainty, and rollback constraints. This sequence makes automated response auditable and provides concrete failure points for ablation, incident review, and later replication.

Threats to validity and limitations. Internal and statistical validity are limited by an aggregate B1-B5 comparison without randomized run logs, dispersions, confidence intervals, p-values, or effect sizes. Construct validity is limited because NRI measures availability and cannot compensate for confidentiality, integrity, or safety failures. Model validity depends on complete, calibrated dependencies and freshness of the twin state.

External validity is limited by the small synchronized testbed and the absence of V4-V5 evidence for heterogeneous infrastructure, organizational delay, seasonality, and legal constraints. Security disclosure also limits release of exact topologies, keys, rules, and vulnerabilities; replication must use tiered access without weakening the scientific audit trail.

These limitations directly bound the claims: H1 is only a preliminary comparison with B1 rather than the strongest B0-B4 baseline; H2-H4 remain unconfirmed without component ablations; H5 requires scale curves; and H6 requires completed V4 and V5 evidence. The percentages in Table 5 are therefore arithmetic descriptions of supplied aggregates, not estimates of a general population effect.

Twin validity requires incident-based calibration of dependency weights, uncertainty bounds, and a freshness gate that blocks what-if decisions on stale state. Missing dependencies may conceal a cascade, whereas inflated weights may trigger unnecessary intervention. Replication must therefore disclose the modeled topology and calibration procedure at an appropriate access tier, while withholding operational details whose publication would create security risk. Further development should therefore publish auditable run manifests, complete the paired ablation and scale series, conduct the V4 operator pilot, and perform independent V5 replication before broader deployment claims are made.

4. Conclusions

1. A single claim-to-evidence architecture was established for levels V0-V5. Its distinguishing feature is an explicit boundary between formal safety, laboratory causality, operational feasibility, and external transfer; this prevents evidence from one level being generalized to another without the required artifacts.

2. For the available V3 aggregate comparison, B5 reduced mean detection time from 43,1 to 8,5 s (80,3%) and recovery time from 399 to 122 s (69,4%), achieved 98,7% integrity-verification accuracy with less than 6% overhead, and increased NRI from 0,71 to 0,93. The joint evidence pipeline, dependency model, and constrained controller therefore provide a descriptive integrated proof of concept.

3. Component-level causal contributions cannot be assigned from the B1-B5 aggregate contrast. The proposed B5-E, B5-D, and B5-P paired ablations are necessary to separate detection, cascade-forecasting, and policy-control effects under the same traces and resource budget; until they are completed, no numerical causal shares or synergies are justified.

4. The demonstrated operating profile is limited to 12 telemetry streams, four edge nodes, and three cloud virtual machines. Claims for 10^2-10^4 devices require p95/p99 latency and resource curves, while transferability requires a V4 pilot and an independent V5 repeat with the direction of effect preserved inside preregistered bounds.

5. The I0-I4 maturity model converts validation evidence into cumulative implementation gates from baseline inventory to adaptive cross-domain coordination. Its practical advantage is that a high weighted score cannot compensate for a missing hard gate such as formal safety, emergency stop, bounded latency, or verified rollback.

6. The reported improvements are profile-bounded and descriptive because run-level distributions, confidence intervals, completed ablations, and external observations are unavailable. Further development should publish auditable run manifests, complete the ablation and scale series, conduct the V4 operator pilot, and perform independent V5 replication before broader regional deployment claims are made.

Conflict of Interest. The author declares that she has no financial, personal, authorship-related, or other conflict of interest that could have influenced the research or the results presented in this article.

Funding. The research was conducted without financial support.

Data Availability. The manuscript contains aggregate data presented in Table 5. No separate related dataset is available because run-level observations, configurations, and manifests were not supplied; this limitation is stated explicitly in the manuscript.

Use of Artificial Intelligence. ChatGPT (OpenAI, GPT-5.6 Pro) was used in the abstract, Materials and Methods, and Results and Discussion sections to support source-text structuring, mathematical exposition, and diagram generation. The author checked the generated material against the source content and aggregate values, reviewed the equations and figures, and approved the final text. The tool did not generate empirical data or determine the study conclusions; the author formulated and verified the conclusions and assumes full responsibility for the manuscript. During revision, ChatGPT also assisted with bibliographic cross-checking, drafting critical comparisons of the cited literature, and language editing.

Author Contributions. Yuliia Ye. Khokhlachova: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review and editing, Visualization, Supervision, Project administration. The author approved the final manuscript.

References:

1. Bocci, A., Forti, S., Ferrari, G.-L., & Brogi, A. (2023). Declarative Secure Placement of FaaS Orchestrations in the Cloud-Edge Continuum. Electronics, 12, 1332. https://doi.org/10.3390/electronics12061332
2. Yang, F., Sun, Y., Gao, Q., & Chen, X. (2024). EDI-C: Reputation-Model-Based Collaborative Audit Scheme for Edge Data Integrity. Electronics, 13, 75. https://doi.org/10.3390/electronics13010075
3. Fett, M., Kraft, M., Wilking, F., Goetz, S., Wartzack, S., & Kirchner, E. (2024). Medium-Level Architectures for Digital Twins: Bridging Conceptual Reference Architectures to Practical Implementation in Cloud, Edge and Cloud–Edge Deployments. Electronics, 13, 1373. https://doi.org/10.3390/electronics13071373
4. El-Hajj, M. (2024). Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. Electronics, 13, 3941. https://doi.org/10.3390/electronics13193941
5. Cho, H., Sung, J.-H., Kang, H.-J., Jang, J., & Shin, D. (2025). Quantifying Cyber Resilience: A Framework Based on Availability Metrics and AUC-Based Normalization. Electronics, 14, 2465. https://doi.org/10.3390/electronics14122465
6. Tao, F., Zhang, H., Liu, A., & Nee, A.Y.C. (2019). Digital Twin in Industry: State-of-the-Art. IEEE Trans. Ind. Inform., 15, 2405–2415. https://doi.org/10.1109/TII.2018.2873186
7. Alcaraz, C., & Lopez, J. (2022). Digital Twin: A Comprehensive Survey of Security Threats. IEEE Commun. Surv. Tutor., 24, 1475–1503. https://doi.org/10.1109/COMST.2022.3171465
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology: Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.SP.800-207
9. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. IEEE Internet Things J., 3, 637–646. https://doi.org/10.1109/JIOT.2016.2579198
10. Kritzinger, W., Karner, M., Traar, G., Henjes, J., & Sihn, W. (2018). Digital Twin in Manufacturing: A Categorical Literature Review and Classification. IFAC-PapersOnLine, 51, 1016–1022. https://doi.org/10.1016/j.ifacol.2018.08.474
11. Sengupta, J., Ruj, S., & Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. J. Netw. Comput. Appl., 149, 102481. https://doi.org/10.1016/j.jnca.2019.102481
12. Mozzaquatro, B.A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-Goncalves, R. (2018). An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors, 18, 3053. https://doi.org/10.3390/s18093053
13. Dietz, M., & Pernul, G. (2020). Unleashing the Digital Twin's Potential for ICS Security. IEEE Secur. Priv., 18, 20–27. https://doi.org/10.1109/MSEC.2019.2961650
14. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Appl. Sci., 14, 11807. https://doi.org/10.3390/app142411807
15. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Comput. Surv., 41, 15. https://doi.org/10.1145/1541880.1541882
16. Xu, H., Yu, W., Griffith, D., & Golmie, N. (2018). A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective. IEEE Access, 6, 78238–78259. https://doi.org/10.1109/ACCESS.2018.2884906
17. Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on Multi-Access Edge Computing Security and Privacy. IEEE Commun. Surv. Tutor., 23, 1078–1124. https://doi.org/10.1109/COMST.2021.3062546
18. de Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed Denial of Service Attack Prediction: Challenges, Open Issues and Opportunities. Comput. Netw., 222, 109553. https://doi.org/10.1016/j.comnet.2022.109553
19. Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE Access, 8, 108952–108971. https://doi.org/10.1109/ACCESS.2020.2998358
20. Minerva, R., Lee, G.M., & Crespi, N. (2020). Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models. Proc. IEEE, 108, 1785–1824. https://doi.org/10.1109/JPROC.2020.2998530
21. Sharma, A., Kosasih, E., Zhang, J., Brintrup, A., & Calinescu, A. (2022). Digital Twins: State of the Art Theory and Practice, Challenges, and Open Research Questions. J. Ind. Inf. Integr., 30, 100383. https://doi.org/10.1016/j.jii.2022.100383
22. Homaei, M., Mogollon-Gutierrez, O., Sancho, J.C., Avila, M., & Caro, A. (2024). A Review of Digital Twins and Their Application in Cybersecurity Based on Artificial Intelligence. Artif. Intell. Rev., 57, 201. https://doi.org/10.1007/s10462-024-10805-3

Відомості про авторів

Англ.	Укр.
Yuliia Khokhlachova Candidate of Technical Sciences, Professor, Professor of the Department of Software Engineering and Cybersecurity, State University of Trade and Economics, Doctoral Student, State University of Information and Communication Technologies yuliiakhokhlachova@gmail.com ORCID: 0000-0002-0787-5112	Хохлачова Юлія Євгеніївна кандидат технічних наук, професор, професор кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, докторант, Державний університет інформаційно-комунікаційних технологій yuliiakhokhlachova@gmail.com ORCID: 0000-0002-0787-5112

Дата надходження статті: 21.05.2026
Дата надходження виправленої версії статті: 03.07.2026
Дата прийняття статті: 08.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.12
УДК 004.421:004.65:004.8
JEL Classification: C38, C45, C63

ОБРОБКА ТЕЛЕМЕТРИЧНИХ ДАНИХ ТА ВИЗНАЧЕННЯ РЕЛЕВАНТНИХ ОЗНАК ДЛЯ РОБОТИ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У КОНТЕКСТІ ОЦІНКИ ФУНКЦІОНАЛЬНОГО СТАНУ РЕЛЯЦІЙНИХ БАЗ ДАНИХ

О. С. Чикалов, О. Б. Берест

TELEMETRY DATA PROCESSING AND IDENTIFICATION OF RELEVANT FEATURES FOR A DECISION SUPPORT SYSTEM IN THE CONTEXT OF ASSESSING THE FUNCTIONAL STATE OF RELATIONAL DATABASES

Oleksandr Chykalov, Oleh Berest

Анотація

Об'єктом дослідження є процес оброблення телеметричних даних Oracle Database 21c та формування релевантного простору ознак для системи підтримки прийняття рішень щодо оцінювання функціонального стану реляційної бази даних. Проблема полягає у тому, що великий початковий набір метрик містить одночасно діагностично значущі, контекстні, дублюючі та вузькоспеціалізовані показники, а їх безпосереднє використання у моделі ускладнює інтерпретацію та може погіршувати стійкість оцінювання. Запропоновано методологію, яка поєднує потокові подання V$ та історичні таблиці Automatic Workload Repository, побудову шляхів з'єднання і реляційних дерев, синхронізацію за UTC, агрегування, нормалізацію та формування часових характеристик. Відбір ознак виконується за доменно обґрунтованими критеріями діагностичної значущості, недубльованості, інтерпретованості та придатності до часового узгодження. У результаті десять груп кандидатних метрик розподілено на шість базових, дві контекстні та дві надлишкові: до базового набору віднесено CPU, Database Wait Time Ratio, Buffer Cache Hit Ratio, Active Sessions, wait events / wait classes та I/O waits; Executes і Physical Reads враховано частково, а DB Block Gets і Background CPU Time вилучено. Мітки інцидентів формуються поєднанням детерміністичних правил і нечітких функцій належності. Сформований простір ознак використано для побудови часово впорядкованої матриці та класифікації функціонального стану бази даних за допомогою нейромережевої моделі екстремального навчання з інформаційно-керованою селекцією прихованих нейронів. Експеримент на тижневому наборі приблизно з 10080 одновилинних записів дав точність близько 0,64 у вибраній робочій точці; аналіз ROC-кривої та калібраційної діаграми засвідчив потребу в додатковому налаштуванні порогу класифікації. Практичне значення полягає у відтворюваному переході від неоднорідної телеметрії до компактного, пояснюваного та придатного для СППР простору ознак.

Ключові слова: *телеметрія, відбір ознак, шляхи з'єднання, екстремальне навчання, інцидент, матриця ознак, СППР.*

Abstract

The object of the study is the processing of Oracle Database 21c telemetry data and the formation of a relevant feature space for a decision support system intended to assess the functional state of a relational database. The problem is that a large initial set of metrics simultaneously contains diagnostically significant, contextual, redundant, and narrowly specialized indicators, while their direct use in the model complicates interpretation and may reduce assessment stability. A methodology is proposed that combines streaming V$ views and historical Automatic Workload Repository tables, the construction of join paths and relational trees, UTC-based temporal synchronization, aggregation, normalization, and temporal feature generation. Feature selection is performed using domain-informed criteria of diagnostic significance, non-redundancy, interpretability, and suitability for temporal alignment. As a result, ten groups of candidate metrics were divided into six core, two contextual, and two redundant groups: CPU, Database Wait Time Ratio, Buffer Cache Hit Ratio, Active Sessions, wait events / wait classes, and I/O waits were included in the core set; Executes and Physical Reads were partially included, whereas DB Block Gets and Background CPU Time were excluded. Incident labels are generated by combining deterministic rules with fuzzy membership functions. The resulting feature space was used to construct a time-ordered matrix and classify the functional state of the database using an extreme learning neural network model with information-guided hidden-neuron selection. An experiment conducted on a one-week dataset containing approximately 10,080 one-minute observations yielded an accuracy of approximately 0.64 at the selected operating point; analysis of the ROC curve and calibration plot indicated the need for additional tuning of the classification threshold. The practical significance of the study lies in providing a reproducible transition from heterogeneous telemetry to a compact, explainable feature space suitable for use in a decision support system.

Key words: *telemetry, feature selection, join paths, extreme learning, incident, feature matrix, decision support system.*

1. Вступ. Реляційні бази даних (РБД) є базовими компонентами корпоративних інформаційних систем, а їхній функціональний стан безпосередньо визначає доступність сервісів, швидкість виконання транзакцій і стабільність залежних програмних компонентів. За умов змінного навантаження традиційне спостереження за окремими показниками вже не забезпечує своєчасного виявлення короткочасних відхилень, прихованих перевантажень і взаємопов'язаних ресурсних обмежень. Тому

© Чикалов О. С., Берест О. Б., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

сучасне оцінювання функціонального стану РБД потребує інтеграції потокової та історичної телеметрії, формування узгодженого простору ознак і застосування інтелектуальних засобів підтримки прийняття рішень.

Практична цінність таких досліджень полягає у можливості перейти від реактивного адміністрування до раннього виявлення інцидентних станів, обґрунтованого вибору діагностичних метрик і формування рекомендацій щодо оптимізації ресурсів. Для цього телеметричні дані мають бути синхронізовані у часі, очищені, перетворені у фіксовані вектори та забезпечені інтерпретованими мітками станів.

Сучасні розподілені реляційні системи, зокрема Spanner, OceanBase і TiDB, демонструють розвиток високодоступної інфраструктури даних [1-3]. Паралельно розвиваються методи виявлення аномалій за системними журналами. Репозиторій Loghub [4] став основою для моделей RobustLog, DeepLog, LogAnomaly, компонентно-орієнтованого аналізу, LogBERT та інших підходів [5-13]. Такі моделі дають змогу виявляти нетипові послідовності подій, однак переважно працюють із текстовими журналами, а не з доменно-специфічною телеметрією СУБД.

Критичний аналіз джерел показує три локальні невирішені питання. По-перше, наявні набори даних часто містять обмежений перелік інцидентів, логи окремих вузлів або синтетично сформовані послідовності [14-16]. По-друге, навіть рішення для часових і розподілених баз даних [17, 18] не формують єдиного механізму поєднання потокових метрик Oracle з історичними зрізами Automatic Workload Repository (AWR). По-третє, статичні набори ознак і фіксовані правила недостатньо враховують зміну робочого навантаження та не завжди забезпечують інтерпретованість отриманих рішень.

Подання продуктивності Oracle і механізми AWR надають широкий набір показників для аналізу роботи екземпляра [19, 20], однак сам факт доступності метрик не вирішує питання їхнього часового узгодження, відбору, документування та перетворення у навчальну матрицю. Автоматизація формування ознак у реляційних структурах [21] і принципи FAIR та словників даних [22, 23] створюють методичну основу для такого перетворення, але потребують адаптації до задачі оцінювання функціонального стану РБД.

Отже, загальна невирішена проблема полягає не лише в інтеграції потокових та історичних джерел Oracle, а й у методично обґрунтованому переході від широкого набору доступних метрик до структурованого простору ознак. Такий простір має відокремлювати базові діагностичні показники від контекстних характеристик, що впливають лише у поєднанні з іншими метриками, а також від дублюючих або вузькоспеціалізованих показників. Одночасно необхідно забезпечити часове узгодження, пояснюване призначення міток та підготовку даних для алгоритмів СППР. Тому дослідження, присвячені обробленню телеметричних даних і відбору релевантних ознак для оцінювання функціонального стану реляційних баз даних, є актуальними.

Метою дослідження є розроблення методології оброблення телеметричних даних і формування релевантного простору ознак для оцінювання функціонального стану Oracle Database 21c. Наукова частина мети передбачає шляхово-реляційну інтеграцію джерел, доменно обґрунтоване оцінювання кандидатних метрик з їх поділом на базові, контекстні та надлишкові, а також комбіноване призначення міток інцидентів. Практична частина полягає у побудові часово узгоджених навчальних і тестових матриць та перевірці придатності сформованого простору ознак у прототипі СППР із застосуванням нейромережевої моделі - машини екстремального навчання (Extreme Learning Machine, ELM) – та інформаційно-екстремального алгоритму навчання (Information-Extreme Learning Algorithm, IELA).

Для досягнення мети було визначено наступні завдання:

1. розробити спосіб інтеграції та часового узгодження потокових подань V$ і історичних таблиць AWR;
2. розробити процедуру формування й доменного оцінювання простору ознак та розподілити кандидатні метрики на базові, контекстні й надлишкові;
3. розробити комбінований механізм призначення міток інцидентів на основі детерміністичних правил і нечітких функцій належності;
4. побудувати навчальні й тестові матриці на основі відібраного простору ознак та перевірити його придатність для класифікації за допомогою ELM/IELA;
5. оцінити якість класифікації, визначити межі достовірності результатів, умови практичного використання та напрями розвитку методології.

2. Матеріали і методи.

2.1. Об'єкт, гіпотеза, припущення та спрощення дослідження. Об'єктом дослідження є процес оброблення телеметричних даних і формування релевантних ознак для оцінювання функціонального стану реляційної бази даних Oracle Database 21c. Досліджуване середовище містить один основний вузол та один екземпляр БД, що працює за звичайного змінного навантаження.

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

Основна гіпотеза дослідження полягає в тому, що інтеграція потокових метрик реального часу та історичних даних AWR за умови їх часового узгодження і шляхово-реляційного вилучення дає змогу сформувати цілісне представлення функціонального стану реляційної бази даних. Оцінювання інформативності телеметричних показників, відбір релевантних ознак і комбіноване призначення міток на основі детерміністичних та нечітких правил забезпечують формування інформативного й інтерпретованого простору ознак, придатного для розмежування штатних та інцидентних станів бази даних. Застосування моделі IELA з інформаційно-керованою селекцією прихованих нейронів дає змогу перевірити придатність сформованого простору ознак для класифікації функціонального стану реляційної бази даних.

Прийнято такі припущення: часові позначки всіх джерел можуть бути приведені до UTC; потокові показники збираються з інтервалом 60 с; історичні агрегати AWR формуються переважно з інтервалом близько однієї години; доступні подання мають узгоджені ідентифікатори екземпляра, знімка та метрики. Для експерименту використано тижневий набір даних обсягом близько 10080 записів.

До спрощень належать бінарне подання стану «штатний/інцидентний», фіксоване ковзне вікно W = 10 хв, розгляд насамперед інцидентів паралельності та I/O, застосування одного робочого порогу та відсутність перевірки на багатовузловій або RAC-конфігурації. Ці спрощення визначають межі узагальнення результатів.

Для забезпечення цілісності процесу оцінювання функціонального стану реляційної бази даних запропоновано методологію оброблення телеметричних даних, що охоплює етапи від інтеграції джерел даних до оцінювання результатів класифікації. Загальну послідовність етапів методології наведено на рис. 1.



Рис. 1. Послідовність оброблення телеметричних даних

Як показано на рис. 1, запропонована методологія включає послідовні етапи: інтеграцію потокових та історичних даних, формування і перетворення ознак, документування набору даних, призначення міток інцидентів, побудову навчальної вибірки та подальше оцінювання результатів класифікації. Кожний етап формує вхідні дані для наступного, що забезпечує узгоджений перехід від первинної телеметрії до формування інформативного простору ознак і перевірки його придатності для розмежування штатних та інцидентних станів реляційної бази даних.

2.2. Джерела телеметричних даних. Джерела телеметрії поділено на дві групи: показники реального часу з динамічних подань V$ та історичні агрегати Automatic Workload Repository. Потокові подання використовуються для короткострокового аналізу, тоді як DBA_HIST_* забезпечують ретроспективний контекст, узгодження знімків та відновлення довгострокової динаміки. Основні джерела [19, 20] наведено в таблиці 1.

Таблиця 1

Джерела телеметричних даних Oracle, використані у дослідженні

№	Подання	Тип та інтервал	Призначення	Ключові метрики / параметри
1	V$SYSMETRIC	Реальний час, ≈1 хв	Поточні показники продуктивності	Throughput, Response Time, Logical/Physical Reads, Redo Generated
2	V$SYSSTAT	Реальний час, накопичувальний	Кумулятивні лічильники	DB Block Gets, Consistent Gets, Physical Reads, Executes
3	V$SYSTEM_EVENT	Реальний час, ≈1 хв	Статистика подій очікування	Waits, Time Waited, Average Wait, Event Name
4	V$WAITCLASSMETRIC	Реальний час, ≈1 хв	Затримки за класами	User I/O, System I/O, Commit, Concurrency, Application
5	V$SYS_TIME_MODEL	Реальний час, ≈1 хв	Часові витрати процесів	DB Time, DB CPU, Background CPU Time, Parse Time
6	DBA_HIST_SYSMETRIC_SUMMARY	AWR, ≈1 год	Історичні агрегати системних метрик	Average, Min, Max
7	DBA_HIST_SYSSTAT	AWR, ≈1 год	Історія системних статистик	Кумулятивні лічильники системних подій
8	DBA_HIST_SYSTEM_EVENT	AWR, ≈1 год	Історія подій очікування	Event Name, Total Waits, Time Waited
9	DBA_HIST_ACTIVE_SESS_HISTORY	AWR, ≈1 год	Історія активних сесій	Session State, SQL ID, Wait Class, CPU Usage
10	DBA_HIST_SNAPSHOT	AWR, ≈1 год	Синхронізація знімків	SNAP_ID, BEGIN_INTERVAL_TIME, END_INTERVAL_TIME

2.3. Вилучення, узгодження та первинне формування ознак. Вилучення даних виконується за шляхами з'єднання між таблицею-джерелом основних метрик і пов'язаними поданнями продуктивності. Формально шлях подано у вигляді:

$$p = \left(T_0 - -c_1 \to T_1 - -c_2 \to \ldots - -c_k \to T_k : c\right), \tag{1}$$

де T_0 є початковим джерелом метрик, T_i – пов'язаними поданнями продуктивності, c_i – стовпчиками з'єднання, зокрема METRIC_ID, SNAP_ID та INSTANCE_NUMBER, c – цільовим стовпчиком у кінцевій таблиці T_k. Для історичних даних застосовується, наприклад, шлях DBA_HIST_SYSMETRIC_SUMMARY(SNAP_ID) → DBA_HIST_SNAPSHOT, а для потокових даних – узгодження V$SYSMETRIC і V$SYS_TIME_MODEL за METRIC_NAME/METRIC_ID та часовими інтервалами BEGIN_TIME, END_TIME.

Після вилучення значення узгоджуються за UTC. Одинарні шляхи перетворюються на скалярні ознаки, категоріальні атрибути кодуються, а багатозначні шляхи агрегуються у статистики або вкладення часових рядів. Для кожної групи можуть застосовуватися нормалізація до інтервалу [0; 1], z-score, експоненційне ковзне середнє та ковзне стандартне відхилення. На цьому етапі формується первинний набір кандидатних ознак; остаточне рішення щодо їх включення до моделі приймається за процедурою, наведеною у підрозділі 2.4.

Приклад SQL-шаблону для вилучення агрегованих історичних показників:

```
String sql =
    "SELECT begin_time, end_time, metric_name, average, metric_unit " +
    "FROM dba_hist_sysmetric_summary " +
    "WHERE begin_time >= ? AND end_time < ? " +
    "AND metric_name IN (?, ?, ?)";

try (Connection c = ds.getConnection();
     PreparedStatement ps = c.prepareStatement(sql)) {
    ps.setTimestamp(1, fromTs); // UTC
    ps.setTimestamp(2, toTs);
    ps.setString(3, "Database Wait Time Ratio");
    ps.setString(4, "Host CPU Utilization (%)");
    ps.setString(5, "Buffer Cache Hit Ratio");
    try (ResultSet rs = ps.executeQuery()) {
        while (rs.next()) {
            // Перетворення запису на рядок матриці ознак
        }
    }
}
```


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

Словник ознак містить назву, джерело, одиницю вимірювання, спосіб агрегації, часовий інтервал і правила інтерпретації. Метадані документуються за принципами FAIR у форматах JSON-LD або Schema.org [22, 23]. Кожний синхронізований снапшот зберігається як окремий JSON-об'єкт:

```
{
  "ts": "2025-08-13T10:20:00Z",
  "host_cpu_pct": 62.1,
  "buf_cache_hit": 96.7,
  "enqueue_waits_s": 0.2
}
```

2.4. Критерії оцінювання та відбору ознак. Первинний простір кандидатних ознак формується з телеметричних показників, доступних через подання, наведені в таблиці 1. Одиницею оцінювання є не окреме поле таблиці, а змістовна група метрик, що характеризує певний механізм функціонування БД: використання процесора, ефективність пам'яті, інтенсивність I/O, активність сесій, події очікування або інтенсивність SQL-операцій.

Рішення щодо кожної групи приймається за чотирма доменними критеріями:

1) прямий зв'язок із проявами деградації продуктивності або інцидентним станом;

2) недубльованість відносно більш узагальнених показників;

3) інтерпретованість для адміністратора БД та можливість пояснити вплив на підсумкову оцінку;

4) придатність до стабільного вилучення, агрегування й часового узгодження у потоковому та історичному режимах.

За результатом оцінювання ознаці надається один із трьох статусів. «Відібрано» означає включення до базового діагностичного простору. «Частково враховано» позначає контекстну ознаку, яка не є достатньою для самостійного висновку, але може уточнювати інтерпретацію базових показників в агрегованому або умовному вигляді. «Не відібрано» означає, що показник є надто вузьким, дублюючим або слабко пов'язаним із цільовим станом у межах поставленої задачі.

Зазначена процедура є доменною якісною селекцією телеметричних ознак і не ототожнюється з інформаційною селекцією прихованих нейронів IELA. Спочатку формується та обґрунтовується вхідний простір ознак, а вже після цього IELA оцінює інформаційний внесок елементів прихованого шару. Такий поділ потрібний для коректної інтерпретації наукового результату.

2.5. Призначення міток інцидентів. Часткові нормалізовані оцінки об'єднуються в інтегральну функцію виявлення F(x):

$$F(x)=\sum_i w_i s_i(x), \sum_i w_i = 1, \tag{2}$$

де $s_i(x)$ – нормалізована оцінка i-ї ознаки, а w_i – її ваговий коефіцієнт; сума ваг дорівнює одиниці. Функція F(x) використовується як інтерпретований критерій функціонального стану РБД.

Бінарна мітка визначається пороговим правилом:

$$y = 1\left[F(x) \geq \tau\right], \tag{3}$$

де τ – робочий поріг. Значення $F(x) \geq \tau$ відповідає інцидентному стану, а $F(x) < \tau$ – штатному. Початкові ваги задаються рівномірно з доменними коригуваннями; зокрема, до ваг CPU та активності ASH додається 0,05.

Детерміністичні правила охоплюють два типи інцидентів. Інцидент паралельності фіксується, коли середня кількість затримок через блокування перевищує 5 і понад 40 % часу БД-сеансу припадає на очікування через конкурентний доступ. Інцидент I/O фіксується, коли понад 60 % часу сеансу припадає на очікування I/O, а інтенсивність логування транзакцій перевищує 95-й перцентиль базового рівня; у такому разі F(x) збільшується на 0,2.

Для врахування плавного переходу між штатним і критичним станами використовується сигмоїдна функція належності:

$$\mu^{l}_{\text{крит}}(x) = \frac{1}{1+\exp\left(-k(x-c)\right)}, \tag{4}$$

де c – критична точка, а k – коефіцієнт крутизни, налаштований відповідно до мінливості метрики. Агрегована нечітка оцінка обчислюється за формулою:

$$\sum_i w_i \mu_{\text{крит},i}(x). \tag{5}$$

Значення агрегованої нечіткої оцінки не менше 0,6 розглядається як ознака аномального стану. Таким чином, мітка формується поєднанням інтерпретованих правил і плавних функцій належності.

2.6. Формування вибірки, модель та критерії оцінювання. Первинні часові ознаки перетворюються у матрицю $X \in R^{Nxd}$, де кожний рядок відповідає стану системи у момент часу, а вектор $y \in \{0; 1\}^N$ містить мітки. Для часової динаміки застосовується ковзне вікно W = 10 хв, що охоплює десять послідовних однохвилинних снапшотів. У фактичному експерименті послідовності розподілено у співвідношенні 70/15/15 для навчання, валідації та тестування без перемішування часових відрізків.

Базовою моделлю є Extreme Learning Machine – одношарова нейронна мережа прямого поширення, у якій параметри вхідного та прихованого шарів задаються випадково і фіксуються, а навчаються лише вихідні ваги. У запропонованому Information-Extreme Learning Algorithm приховані нейрони оцінюються за інформаційним внеском, після чого зберігаються найбільш інформативні кандидати. Інформаційний внесок визначається як:

$$IG = H(Y) - H(Y \mid Z), \tag{6}$$

де H(Y) – ентропія міток, а H(Y|Z) – умовна ентропія міток за наявності виходу нейрона Z. Такий критерій орієнтує відбір на зв'язок активації нейрона з цільовим станом, а не лише на випадкову структуру прихованого шару.

Для оцінювання використовуються часовий графік спрацювань у підтвердженому інцидентному вікні, ROC-крива, калібраційний графік та довірчі інтервали Вілсона. Для непорогових оцінок передбачено 95 % довірчі інтервали блочного бутстрапу з безперервним блоком розміром 5 хвилин. Тестовий набір, фрагмент якого наведено в Таблиці 2, сформовано з чотирьох інформаційних полів: time_utc, що визначає часову позначку UTC телеметричного спостереження; F, що містить значення інтегрального бала функціонального стану; y_true, що відповідає істинній бінарній мітці штатного або інцидентного стану; та y_pred, що містить прогнозовану моделлю бінарну мітку, сформовану з урахуванням обраного робочого порогу τ.

Таблиця 2

Фрагмент тестового набору даних для оцінювання якості моделі

time_utc	F	y_true	y_pred
2025-08-04T00:00:00Z	0.59625811	1	1
2025-08-04T00:01:00Z	0.253569967	0	0
2025-08-04T00:02:00Z	0.112429378	0	0
2025-08-04T00:03:00Z	0.300775039	0	1
2025-08-04T00:04:00Z	0.589850204	1	1
2025-08-04T00:05:00Z	0.700235738	1	1
2025-08-04T00:06:00Z	0.611445935	1	1
2025-08-04T00:07:00Z	0.346930432	0	1
2025-08-04T00:08:00Z	0.185999865	0	0

3. Результати і обговорення.

3.1. Результати інтеграції та часового узгодження телеметрії. Результатом виконання першої задачі стало формування інтеграційного контуру з десяти подань Oracle, що охоплює потокові системні метрики, кумулятивні статистики, події та класи очікування, модель часу, активні сесії й історичні знімки AWR. Поєднання SNAP_ID, INSTANCE_NUMBER, METRIC_ID та часових меж забезпечило приведення різнорідних джерел до спільної UTC-шкали.

На відміну від моделей, що аналізують переважно текстові послідовності журналів [4-16], отриманий результат використовує числову телеметрію на рівні конкретної СУБД. Це дає змогу безпосередньо пов'язувати ознаки з використанням CPU, пам'яті, I/O та внутрішніми очікуваннями. Проблемна частина, визначена у вступі, закривається за рахунок одночасного використання короткострокових V$-показників і ретроспективного контексту AWR.

Практичне застосування результату потребує доступу до відповідних подань, однакової часової зони, контролю одиниць вимірювання та перевірки частоти оновлення. У разі зміни конфігурації Oracle або переходу до RAC шляхові правила мають бути розширені додатковими ідентифікаторами вузлів та екземплярів.

3.2. Результати формування, оцінювання та відбору релевантних ознак. Результатом другої задачі стало не лише складання переліку метрик, а формування структурованого простору ознак із зафіксованим рішенням щодо кожної кандидатної групи. Із десяти оцінених груп шість включено до базового діагностичного набору, дві залишено як контекстні та дві вилучено як вузькі або надлишкові.

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

До базового набору увійшли Host CPU Utilization, Database Wait Time Ratio, Buffer Cache Hit Ratio, Active Sessions, wait events / wait classes та I/O waits. На основі результатів проведених експериментів було оцінено релевантність телеметричних ознак для визначення функціонального стану реляційної бази даних. За результатами оцінювання прийнято рішення щодо включення, часткового врахування або виключення кожної ознаки з кінцевого простору ознак. Узагальнені результати наведено в таблиці 3.

Таблиця 3

Результати оцінювання та відбору телеметричних ознак

Метрика	Джерело даних	Опис	Статус відбору	Обґрунтування
Host CPU Utilization (%)	V$SYSMETRIC DBA_HIST_ SYSMETRIC_SUMMARY	Характеризує завантаження процесорних ресурсів	Відібрано	Безпосередньо відображає ресурсну напруженість системи
Database Wait Time Ratio	V$SYSMETRIC DBA_HIST_ SYSMETRIC_SUMMARY	Відображає частку непродуктивного часу	Відібрано	Є інтегральним індикатором затримок
Buffer Cache Hit Ratio	V$SYSMETRIC DBA_HIST_ SYSMETRIC_SUMMARY	Характеризує ефективність використання буферного кешу	Відібрано	Дає узагальнену оцінку роботи пам'яті та впливу на I/O
Active Sessions	DBA_HIST_ACTIVE_SESS_ HISTORY	Відображає фактичний рівень навантаження на БД	Відібрано	Чутливий до пікових навантажень і черг на ресурси
Wait Events / Wait Class	V$SYSTEM_EVENT / V$WAITCLASSMETRIC / DBA_ HIST_SYSTEM_EVENT	Відображає типи та інтенсивність затримок	Відібрано	Дає змогу виявляти причини деградації продуктивності
I/O waits / User I/O / System I/O	V$WAITCLASSMETRIC / DBA_ HIST_SYSTEM_EVENT	Характеризує затримки вводу-виводу	Відібрано	Важливий для виявлення дискових та мережевих вузьких місць
DB Block Gets	V$SYSSTAT / DBA_HIST_SYSSTAT	Відображає логічні звернення до блоків	Не відібрано	Має вузький технічний зміст і дублює інформацію інших метрик
Background CPU Time	V$SYS_TIME_MODEL	Характеризує навантаження фонових процесів	Не відібрано	Менш інформативний для оцінювання стану з позиції користувацьких запитів
Executes	V$SYSSTAT / DBA_HIST_SYSSTAT	Кількість виконань SQL-операцій	Частково враховано	Може використовуватись як допоміжний контекстний показник
Physical Reads	V$SYSSTAT / DBA_HIST_SYSSTAT	Інтенсивність фізичних читань	Частково враховано	Має діагностичну цінність, але доцільно використовувати в агрегованому вигляді

Базові ознаки безпосередньо відображають основні механізми деградації: ресурсну напруженість, непродуктивний час, ефективність буферного кешу, активне навантаження, внутрішні очікування та затримки I/O. Їх спільне використання дає змогу оцінювати не лише факт відхилення, а й можливу природу проблемного стану.

Окремий результат стосується ознак, вплив яких не є очевидним при ізольованому розгляді. Executes і Physical Reads не включено до базового набору як самостійні критерії, однак їх збережено у статусі «частково враховано». Вони виконують контекстну функцію: характеризують інтенсивність SQL-операцій та фізичного читання і можуть уточнювати інтерпретацію CPU, I/O та wait-показників в агрегованому вигляді. Таким чином, методологія не зводить відбір до бінарного рішення «залишити/видалити», а підтримує проміжний клас ознак, значення яких проявляється у взаємодії з базовими характеристиками.

DB Block Gets і Background CPU Time не відібрано. Перший показник має вузький технічний зміст і частково дублює інформацію інших метрик, а другий менш безпосередньо пов'язаний зі станом,

який спостерігає користувацьке навантаження. Їх вилучення з основного простору зменшує кількість слабкоінформативних або дублюючих змінних, не усуваючи ключових ресурсних та часових характеристик.

Науковий результат цього етапу полягає у відтворюваному переході від широкої телеметрії Oracle до трирівневого простору ознак: базового, контекстного та вилученого. На відміну від загального автоматизованого конструювання ознак у реляційних базах [21], рішення прив'язані до семантики конкретних Oracle-показників і супроводжуються поясненням їхньої діагностичної ролі. Подальші дослідження доцільно спрямувати на перевірку стійкості сформованого простору ознак на розширених наборах телеметричних даних, інших конфігураціях Oracle Database та додаткових типах інцидентів.

3.3. Результати призначення міток інцидентів. Третю задачу вирішено шляхом поєднання порогових правил з нечіткими функціями належності. Детерміністична частина забезпечує явну інтерпретацію двох сценаріїв: паралельність визначається за кількістю блокувальних затримок понад 5 і часткою конкурентних очікувань понад 40 %, а I/O-інцидент – за часткою I/O-очікувань понад 60 % та перевищенням 95-го перцентиля інтенсивності логування. Нечітка частина використовує поріг агрегованої оцінки 0,6.

Отриманий результат є адаптивнішим за повністю фіксовану систему правил, оскільки сигмоїдна належність відображає поступове наближення метрики до критичної області. Водночас він зберігає пояснюваність: для кожної мітки можна вказати метрики, пороги та ваги, що вплинули на рішення. Це важливо для майбутньої СППР, де адміністратор повинен не лише отримати клас стану, а й зрозуміти причину спрацювання.

Недоліком є залежність базової істини від прийнятих правил і критичних точок. Без незалежної експертної або інцидентної розмітки можлива циркулярність: модель навчається відтворювати правила, що одночасно використовуються для оцінювання стану. Тому перед промисловим використанням пороги мають бути перевірені на реальних підтверджених інцидентах.

3.4. Результати формування вибірки та перевірки простору ознак засобами IELA. Результатом четвертої задачі стало перетворення відібраних базових і контекстних характеристик у часово впорядковану матрицю приблизно з 10 080 однохвилинних спостережень. Ковзне вікно з десяти снапшотів забезпечило врахування короткострокової динаміки, а розподіл 70/15/15 зберіг хронологічну цілісність між навчанням, валідацією і тестуванням. Класифікатор на цьому етапі використано як засіб перевірки придатності сформованого простору ознак до розмежування станів, а не як заміну процедурі їх доменного відбору.

Застосування інформаційного критерію IG дало методичну основу для ранжування прихованих нейронів за зв'язком їхніх активацій з мітками стану. На відміну від класичного ELM, у якому весь випадково сформований прихований шар використовується без селекції, IELA дозволяє відкинути кандидати з низьким інформаційним внеском. Важливо, що цей етап виконується після формування телеметричного простору ознак: таблиця 3 описує відбір вхідних характеристик, тоді як IELA виконує селекцію елементів прихованого шару. У цьому експерименті акцент зроблено на перевірці придатності схеми; окрема кількісна оцінка скорочення прихованого шару не наводилася, тому перевага не інтерпретується як доведене зменшення складності для всіх конфігурацій.

Умовами відтворення результату є незмінний порядок часових спостережень, однакова процедура нормалізації для навчальної та тестової частин, відсутність витоку майбутніх значень у ковзне вікно та фіксація генератора випадкових параметрів ELM.

3.5. Оцінювання якості, порівняння, обмеження та перспективи. Перший етап оцінювання передбачає аналіз динаміки зміни значень функції виявлення F(x) у випадку підтвердженого інциденту. У межах 45-хвилинного часового вікна наведеного на рисунку 2 за робочого порогу τ=0,60 отримано TP = 5, FP = 10 та FN = 6. При цьому TP (True Positive) відповідає випадкам, коли інцидент фактично мав місце і був правильно виявлений моделлю; FP (False Positive) – випадкам, коли інцидент був відсутній, однак модель помилково класифікувала стан як інцидентний; FN (False Negative) – випадкам, коли інцидент фактично мав місце, але модель його не виявила. Точність позитивних прогнозів (Precision) становить 0,33, а повнота (Recall) 0,45. Загальна точність класифікації (Accuracy) становить 0,64, тобто модель правильно класифікувала приблизно 64 % усіх спостережень у межах аналізованого часового вікна. Водночас це значення слід інтерпретувати разом із показниками точності позитивних прогнозів і повноти, оскільки наявність значної кількості хибнопозитивних та хибнонегативних спрацювань свідчить про необхідність подальшого налаштування робочого порогу та калібрування моделі з урахуванням особливостей розподілу класів.

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

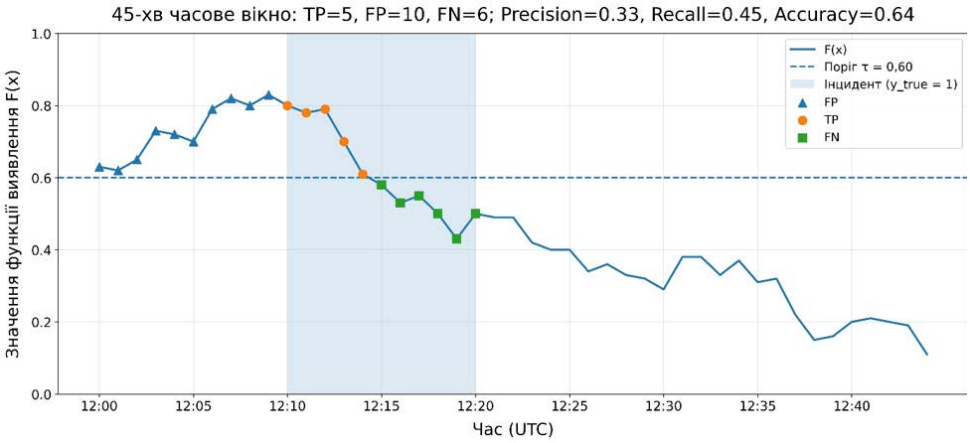


Рис. 2. Відстеження спрацювань у 45-хвилинному інцидентному вікні

Рисунок 3 демонструє аналіз із кривою ROC, де бірюзова крива вказує на сильне розмежування між TP та FP частками порівняно з червоною діагональною референтною лінією, що доводить високу здатність виявляти аномальні явища в залежності від встановлених порогів.

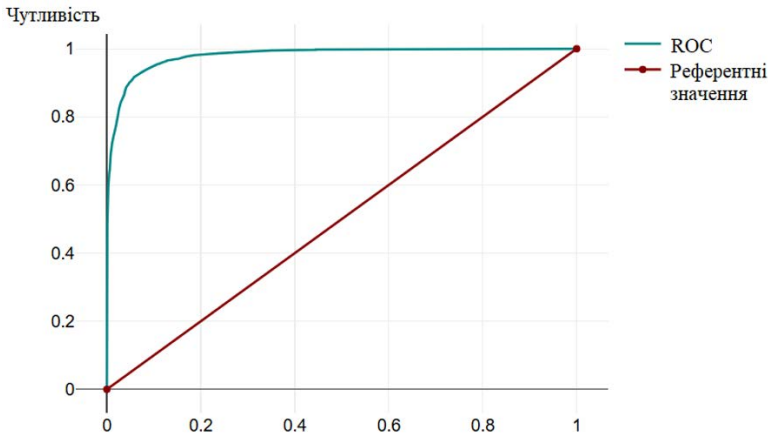


Рис. 3. ROC-крива прототипної моделі у порівнянні з випадковим класифікатором

Калібраційний графік на рисунку 4 демонструє загальне наближення спостережуваних часток позитивних випадків до середніх передбачуваних балів, хоча у верхній частині діапазону помітне завищення прогнозу. Це узгоджується з надлишком хибнопозитивних рішень у робочій точці та підтверджує потребу в калібруванні порогу.

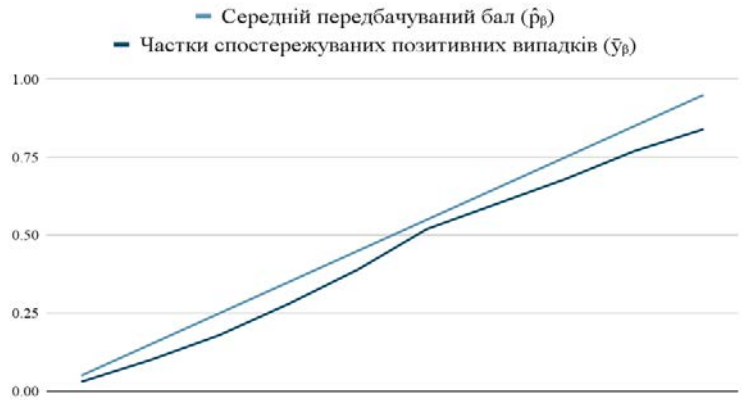


Рис. 4. Калібраційний графік передбачуваних балів і спостережуваних позитивних часток

Таблиця 4

Довірчі інтервали Вілсона для калібраційних груп

n_β	Нижня межа	Верхня межа
120	0.015	0.056
115	0.058	0.165
110	0.118	0.260
105	0.203	0.373
98	0.299	0.489
92	0.418	0.618
85	0.496	0.693
78	0.578	0.771
72	0.664	0.849
65	0.742	0.905

Ширина довірчих інтервалів визначається спільним впливом кількості спостережень n_β у β-й калібраційній групі та величини оцінюваної частки, тому її не можна пояснювати лише зменшенням n_β. Ці інтервали доцільно використовувати як показник невизначеності калібрування, а не як самостійну оцінку точності класифікатора.

На повному тижневому наборі частка правильно класифікованих спостережень становила близько 0,64. Це значення характеризує якість класифікації за однієї фіксованої робочої точки, тоді як ROC-крива відображає співвідношення між часткою істинно позитивних і хибнопозитивних результатів у всьому діапазоні порогів. Тому помірне значення accuracy за вибраного порога та візуально виражена ROC-крива не суперечать одне одному. Водночас отримані результати свідчать про необхідність подальшого вибору оптимального порога класифікації та перевірки калібрування моделі. Для повнішого оцінювання її якості доцільно окремо навести AUROC, precision, recall, F1-міру та матрицю помилок для повного тестового набору.

Пряме кількісне порівняння з логовими моделями [5-13, 18] обмежене різними джерелами даних, типами аномалій і способами формування базової істини. Перевага запропонованої методології полягає не у доведеній вищій точності класифікатора, а у цілісному ланцюжку: інтеграція V$ та AWR, формування кандидатних характеристик, пояснюваний поділ на базові, контекстні та надлишкові ознаки, призначення міток і подальша перевірка сформованого простору засобами ELM/IELA.

Основні обмеження дослідження: один тиждень спостережень; один вузол та один екземпляр Oracle 21c; обмежена кількість типів інцидентів; частково синтетичне або правилове формування міток; класовий дисбаланс; відсутність зовнішньої валідації та числового AUROC. Подальший розвиток доцільно спрямувати на незалежну розмітку підтверджених інцидентів, оптимізацію порогу за вартістю помилок, розширення набору середовищ, онлайн-оновлення ваг і нейронів IELA та перевірку на багатовузлових конфігураціях.

Практичне використання можливе за наявності синхронізованої телеметрії, стабільного доступу до V$ та AWR, перевірених порогів для конкретного середовища і процедури регулярного перегляду словника ознак. Особливо важливо повторно оцінювати контекстні та вилучені показники при зміні типу навантаження, конфігурації пам'яті, дискової підсистеми або архітектури Oracle. За цих умов методологія може слугувати основою прототипу СППР для раннього виявлення деградації функціонального стану РБД.

4. Висновки.

1. Сформовано шляхово-реляційний спосіб інтеграції десяти потокових та історичних подань Oracle. Використання METRIC_ID, SNAP_ID, INSTANCE_NUMBER і часових меж дозволило привести V$ та AWR до спільної UTC-шкали та сформувати первинний набір кандидатних характеристик без розриву між короткостроковим і ретроспективним аналізом.

2. Розроблено процедуру доменного оцінювання та відбору телеметричних ознак. Із десяти кандидатних груп шість визначено як базові, дві – як контекстні, що враховуються частково, і дві – як надлишкові або вузькоспеціалізовані. Це дозволило зберегти показники CPU, I/O, очікувань, пам'яті та активного навантаження, не втратити неочевидний контекст Executes і Physical Reads та виключити DB Block Gets і Background CPU Time з основного простору. Відмінною рисою результату є не бінарне відсікання, а трирівневе, пояснюване рішення щодо ролі кожної ознаки.

3. Розроблено комбінований механізм призначення міток, який поєднує правила оцінювання одночасної активності в базі даних і навантаження на підсистему введення-виведення з пороговим

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

значенням інтегральної нечіткої оцінки 0,6. Правила враховують показники активних сеансів, блокувань та очікувань ресурсів, а також інтенсивність і тривалість операцій читання та запису даних. Перевагою механізму є можливість пояснити, які метрики, порогові значення та вагові коефіцієнти вплинули на призначення мітки. Його обмеженням є залежність від обґрунтованості встановлених порогів і ваг, а також необхідність незалежної перевірки на підтверджених інцидентах.

4. На основі відібраного простору ознак сформовано часову вибірку приблизно з 10080 однохвилинних записів, ковзним вікном 10 хв та розподілом 70/15/15. ELM/IELA використано як наступний етап перевірки придатності цього простору до класифікації станів; інформаційний критерій IELA ранжує приховані нейрони, але не підміняє доменний відбір вхідних телеметричних характеристик.

5. У вибраній робочій точці частка правильних класифікацій становила близько 0,64; у 45-хвилинному вікні отримано precision = 0,33 та recall ≈ 0,45. ROC- і калібраційна діагностика показали потенціал сформованого простору ознак для розмежування станів за інших порогів, але велика кількість FP підтвердила необхідність калібрування, розширення незалежної розмітки, статистичної перевірки внеску окремих ознак та зовнішньої валідації.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослі-дження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували тех-нології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Олександр Чикалов – концептуалізація, аналіз джерел, методологія, написання основного тексту; Олег Берест – рецензування та редагування, формування висновків і перевірка узгодженості структури.

References:

1. James, C., Corbett, J., Dean, J., Epstein, M., Fikes, A., Frost, C., Furman, J.J., Ghemawat, S., Gubarev, A., Heiser, C., Hochschild, P., et al. (2013). Spanner: Google's globally distributed database. *ACM Transactions on Computer Systems (TOCS)*, Vol. 31. PP. 1–22. DOI:10.1145/2491245.

2. Yang, Z., Yang, C., Han, F., Zhuang, M., Yang, B., Yang, Z., Cheng, X., Zhao, Y., Shi, W., Xi, H., et al. (2022). OceanBase: a 707 million tpmC distributed relational database system. *Proceedings of the VLDB Endowment*, Vol. 15. PP. 3385–3397. DOI:10.14778/3554821.3554837.

3. Huang, D., Liu, Q., Cui, Q., Fang, Z., Ma, X., Xu F., Shen, L., Tang, L., Zhou, Y., Huang, M., et al. (2020). TiDB: a Raft-based HTAP database. *Proceedings of the VLDB Endowment*, Vol. 13. PP. 3072–3084. DOI:10.14778/3415478.3415535.

4. He, P., Liu, J., Lyu, M.R., Zhu, J., He, S. (2023). Loghub: A large collection of system log datasets towards automated log analytics, arXiv:2307.09227.

5. Zhang, X., Xu, Y., Lin, Q., Qiao, B., Zhang, H., Dang, Y., Xie, C., Yang, X., Cheng, Q., Li, Z., et al. (2019). Robust log-based anomaly detection on unstable log data. Proceedings of the 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, PP. 807–817. DOI:10.1145/3338906.3338964.

6. Du, M., Li, F., Zheng, G., Srikumar, V. (2017). Deeplog: Anomaly detection and diagnosis from system logs through deep learning. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, PP. 1285–1298. DOI:10.1145/3133956.3134015.

7. Meng, W., Liu, Y., Zhu, Y., Zhang, S., Pei, D., Liu, Y., Chen, Y., Zhang, R., Tao, S., Sun, P., et al. (2019). Loganomaly: Unsupervised detection of sequential and quantitative anomalies in unstructured logs. Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI), PP. 4739–4745.

8. Yin, K., Yan, M., Xu, L., Xu, Z., Li, Z., Yang, D., Zhang, X. (2020). Improving log-based anomaly detection with component-aware analysis. 2020 IEEE International Conference on Software Maintenance and Evolution (ICSME), PP. 667–671. DOI:10.1109/ICSME46990.2020.00077.

9. Guo, H., Yuan, S., Wu, X. (2021). Logbert: Log anomaly detection via BERT. Proceedings of the International Joint Conference on Neural Networks (IJCNN). IEEE, PP. 1–8. DOI:10.1109/IJCNN52387.2021.9533689.

10. Jia, T., Li, Y., Yang, Y., Huang, G., Wu, Z. (2022). Augmenting log-based anomaly detection models to reduce false anomalies with human feedback. Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, PP. 3081–3089. DOI:10.1145/3534678.3539393.

11. Jia, T., Wu, Y., Hou, C., Li, Y. (2021). LogFlash: Real-time streaming anomaly detection and diagnosis from system logs for large-scale software systems. Proceedings of the IEEE 32nd International Symposium on Software Reliability Engineering (ISSRE), PP. 80–90. DOI:10.1109/ISSRE52982.2021.00021.

12. Jia, T., Yang, L., Chen, P., Li, Y., Meng, F., Xu, J. (2017). Logsed: Anomaly diagnosis through mining time-weighted control flow graph in logs. Proceedings of the IEEE 10th International Conference on Cloud Computing (CLOUD), PP. 447–455. DOI:10.1109/CLOUD.2017.60.

13. Kim, J., Savchenko, V., Shin, K., Sorokin, K., Jeon, H., Pankratenko, G., Markov, S., Kim, C.-J. (2020). Automatic abnormal log detection by analyzing log history for providing debugging insight. Proceedings of the 42nd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP), PP. 71–80. DOI:10.1145/3377813.3381363.

14. Lin, Q., Zhang, H., Lou, J., Zhang, Y., Chen, X. (2016). Log clustering based problem identification for online service systems. Proceedings of the 38th International Conference on Software Engineering Companion, PP. 102–111. DOI:10.1145/2889160.2889232.

15. Huo, Y., Li, Y., Su, Y., He, P., Xie, Z., Lyu, M.R. (2023). AutoLog: A log sequence synthesis framework for anomaly detection, arXiv:2308.09324.

16. Landauer, M., Skopik, F., Wurzenberger, M. (2023). A critical review of common log data sets used for evaluation of sequence-based anomaly detection techniques, arXiv:2309.02854.

17. Wang, C., Huang, X., Qiao, J., Jiang, T., Rui, L., Zhang, J., Kang, R., Feinauer, J., McGrail, K.A., Wang, P., et al. (2020). Apache IoTDB: Time-series database for internet of things. *Proceedings of the VLDB Endowment*, Vol. 13. PP. 2901–2904. DOI:10.14778/3415478.3415504.

18. Zhang, L., Jia, T., Jia, M., Li, Y., Yang, Y., Wu, Z. (2024). Multivariate log-based anomaly detection for distributed database. Proceedings of the 30th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, PP. 12. DOI:10.1145/3637528.3671725.

19. Oraculix. Monitoring Oracle performance with AppDynamics, 2013. [Online]. Retrieved from: https://oraculix.com/2013/02/25/monitoring-oracle-performance-with-appdynamics/.

20. Oracle. Instance tuning using performance views. Database Performance Tuning Guide, 2023. [Online]. Retrieved from: https://docs.oracle.com/en/database/oracle/oracle-database/23/tgdba/instance-tuning-using-performance-views.html.

21. Lam, H.T., Thiebaut, J.M., Sinn, M., Chen, B., Mai, T., Alkan, O. (2017). One button machine for automating feature engineering in relational databases, arXiv:1706.00327. DOI:10.48550/arXiv.1706.00327.

22. Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L.B., Bourne, P.E., et al. (2016). The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data, Vol. 3. Article 160018. DOI:10.1038/sdata.2016.18.

23. Buchanan, E., Crain, S., Cunningham, A., Johnson, H., Stash, H., Papadatou-Pastou, M., Isager, P., Carlsson, R., Aczel, B. (2019). Getting started creating data dictionaries: How to create a shareable dataset. OSF Preprints, DOI:10.31219/osf.io/vd4y3.

Відомості про авторів

Англ.	Укр.
Oleksandr Chykalov Postgraduate Student at the Department of Computer Science, Sumy State University chikalov2012@gmail.com ORCID: 0009-0004-5132-7430	Чикалов Олександр Сергійович аспірант кафедри комп'ютерних наук, Сумський державний університет hikalov2012@gmail.com ORCID: 0009-0004-5132-7430
Oleh Berest Senior Lecturer in the Department of Computer Science, Sumy State University o.berest@cs.sumdu.edu.ua ORCID: 0000-0003-0183-9871	Берест Олег Борисович старший викладач кафедри комп'ютерних наук, Сумський державний університет o.berest@cs.sumdu.edu.ua ORCID: 0000-0003-0183-9871

Дата надходження статті: 29.05.2026
Дата надходження виправленої версії статті: 08.07.2026
Дата прийняття статті: 10.07.2026
Дата публікації статті: 26.10.2026

DOI https://doi.org/10.32689/maup.it.2026.2.13
УДК 004.8
JEL Classification: C 45, C 63, C 44

АДАПТАЦІЯ ІНФОРМАЦІЙНО-ЕКСТРЕМАЛЬНОЇ ІНТЕЛЕКТУАЛЬНОЇ ТЕХНОЛОГІЇ ДО АНАЛІЗУ ВЕЛИКИХ ДАНИХ НА ПРИКЛАДІ ЖУРНАЛІВ ПОДІЙ OFFICE 365

К. Є. Шамонін, Д. В. Прилепа

ADAPTATION OF INFORMATION-EXTREME INTELLIGENT TECHNOLOGY TO BIG DATA ANALYSIS ON THE EXAMPLE OF OFFICE 365 EVENT LOGS

Kiril Shamonin, Dmytro Prylepa

Анотація

Об'єктом дослідження є інтелектуальна система підтримки прийняття рішень (СППР) для виявлення кіберзагроз у журналах аудиту хмарної платформи Microsoft Office 365, орієнтована на умови малого та середнього бізнесу (МСБ).

Проблема, що вирішувалася, полягає у відсутності доступних інструментів виявлення прихованих кібератак для організацій, що не мають у штаті великої команди фахівців з кібербезпеки. Існуючі рішення на базі глибокого навчання вимагають значних обчислювальних ресурсів і є непрозорими «чорними скриньками», рішення яких аналітик без профільної підготовки не здатен ні перевірити, ні пояснити керівництву.

Суть отриманих результатів полягає у розробці 4-етапного конвеєра попередньої обробки O365 IEI-Pipeline та синтезі СППР на засадах IEI-технології. Повний цикл обробки 93 379 рядків телеметрії займає 6,4 секунди на стандартному обладнанні. Синтезована СППР досягла нульової помилки другого роду (β = 0) на етапі навчання та ідентифікувала приховану атаку Data Exfiltration у 61,1 % тестових векторів без жодного хибного спрацювання на нормальному трафіку.

Ключовою відмінністю є інтерпретованість рішень: кожне попередження системи пояснюється через конкретні відхилення поведінкових ознак від еталону норми у бінарному просторі, що дозволяє IT-спеціалісту загального профілю зрозуміти причину спрацювання без глибоких знань з машинного навчання. Система належить до класу Explainable AI, на відміну від непрозорих Transformer-архітектур.

Результати пояснюються інформаційним критерієм Кульбака та оптимізованою системою контрольних допусків, що формує геометрично чіткі межі між класами нормальної поведінки та аномалій.

Практичне використання є доцільним у компаніях МСБ, що використовують Microsoft Office 365, за умов відсутності виділеного SOC-центру: система потребує мінімальних обчислювальних ресурсів, не вимагає спеціалізованої інфраструктури та забезпечує прозору аргументацію кожного рішення для нетехнічного персоналу.

Ключові слова: *інтелектуальний аналіз даних, інформаційно-екстремальна інтелектуальна технологія, оцінювання функціональної ефективності, виявлення аномалій, кібербезпека.*

Abstract

The object of the study is an intelligent decision support system (DSS) for cyber threat detection in Microsoft Office 365 audit logs, designed to meet the operational constraints of small and medium-sized businesses (SMBs).

The problem addressed is the lack of accessible tools for detecting covert cyberattacks in organizations without a dedicated cybersecurity team. Existing deep learning-based solutions demand substantial computational resources and operate as opaque black boxes, whose outputs a non-specialist analyst can neither verify nor explain to management.

The core result is the development of a four-stage preprocessing pipeline, O365 IEI-Pipeline, and the synthesis of a DSS based on Information-Extreme Intelligent Technology (IEIT). The complete processing cycle for 93,379 telemetry records takes 6.4 seconds on standard hardware. The synthesized DSS achieved a zero type-II error rate (β = 0) during the training phase and successfully identified a covert Data Exfiltration attack in 61.1% of test feature vectors with no false positives on normal traffic.

The key distinguishing feature is decision interpretability: every system alert is explained through specific deviations of behavioral features from the reference norm in binary space, enabling a general-purpose IT specialist to understand the reason for each detection without deep knowledge of machine learning. The system belongs to the Explainable AI class, in contrast to opaque Transformer-based architectures.

The results are attributed to the Kullback information criterion and an optimized tolerance control system, which establishes geometrically well-defined boundaries between the normal behavior and anomaly classes.

Practical application is advisable for SMB companies using Microsoft Office 365 in the absence of a dedicated SOC: the system requires minimal computational resources, demands no specialized infrastructure, and provides transparent, human-readable justification for every decision to non-technical staff.

Key words: *intellectual data analysis, information-extreme intellectual technology, functional performance evaluation, anomaly detection, cybersecurity.*

© Шамонін К. Є., Прилепа Д. В., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

1. Вступ. Одним із перспективних напрямів підвищення ефективності кіберзахисту корпоративних інформаційних систем, що функціонують за умов апріорної невизначеності та дії неконтрольованих зовнішніх факторів, є розроблення інтелектуальних систем підтримки прийняття рішень (СППР) на засадах машинного навчання. Сучасні підприємства щоденно генерують масиви телеметрії, що підпадають під категорію великих даних (Big Data): журнали доступу SaaS-платформ, події операційних технологій (OT), метрики серверного обладнання та трафік пристроїв IoT.

Типовим прикладом є хмарна платформа Microsoft Office 365. Організація зі штатом у 50 користувачів здатна генерувати від 40 000 до 2 000 000 рядків аудит-подій на добу, кожен з яких описується понад 100 різнотипними ознаками: від бінарних маркерів до складних JSON-об'єктів та довільних текстових рядків. Застосування традиційних сигнатурних систем виявлення вторгнень (IDS) або статичних SIEM-правил для аналізу таких слабоформалізованих потоків є вкрай неефективним, а ручний аналіз практично неможливим.

Проблема є особливо гострою для підприємств малого та середнього бізнесу (МСБ), де відсутні виділені SOC-центри та великі команди фахівців з кібербезпеки. За даними аналітичних звітів галузі, понад 60 % кіберінцидентів у секторі МСБ залишаються невиявленими понад 200 днів, що пояснюється не відсутністю даних, а відсутністю інструментів їх інтерпретованого аналізу. Тому розробка доступних, прозорих і ресурсоефективних систем виявлення аномалій є актуальною науково-практичною задачею.

Значна кількість досліджень сфокусована на застосуванні архітектур глибокого навчання, зокрема рекурентних нейронних мереж (LSTM) та моделей Transformer, для аналізу потокової мережевої телеметрії [1, 2, 3]. Проте такі системи характеризуються суттєвими практичними недоліками: вимагають значних обчислювальних ресурсів, є вразливими до змагальних атак (Adversarial ML) і функціонують як непрозорі «чорні скриньки», рішення яких аналітик без профільної підготовки не здатен ні перевірити, ні пояснити керівництву [4, 5].

На противагу методам «чорної скриньки», у сфері практичної кібербезпеки стрімко зростає потреба у прозорому штучному інтелекті (Explainable AI, XAI) [4, 5]. Аналітики SOC-центрів та IT-спеціалісти загального профілю повинні розуміти логічну причину кожного спрацювання системи. Інформаційно-екстремальна інтелектуальна технологія (IEI-технологія) за своєю математичною природою належить до класу XAI: вона дозволяє пояснити кожне рішення СППР через геометрію гіперсферичних контейнерів класів у бінарному просторі ознак [6, 7, 8]. При цьому навчання у редукованому бінарному просторі вимагає на порядки менше обчислювальних ресурсів порівняно з Transformer-архітектурами.

Надзвичайно важливим аспектом роботи з телеметрією Big Data є забезпечення конфіденційності (Privacy-Preserving) [9]. Пряма обробка сирих журналів O365 несе ризики деанонімізації через транзакційні ідентифікатори та кореляційні мітки. Математично обґрунтовані процедури редукції простору ознак виступають не лише інструментом подолання «прокляття розмірності», але й механізмом захисту персональних даних.

Незважаючи на успішне застосування IEI-технології у задачах психоемоційної діагностики [10], розпізнавання електроміографічних біосигналів за розрідженими навчальними матрицями [11], інтелектуального аналізу якості освітнього контенту [12], питання адаптації цього формалізованого апарату до аналізу гетерогенних журналів IT-аудиту залишається недостатньо дослідженим. Зокрема, не розв'язаною є задача подолання феномену Белмана («прокляття розмірності») при застосуванні IEI до масивів Big Data надвисокої розмірності та структурної гетерогенності.

Метою дослідження є підвищення функціональної ефективності розпізнавання аномалій у масивах Big Data шляхом інформаційного аналізу і синтезу СППР у рамках IEI-технології. Це дасть можливість забезпечити інтерпретоване виявлення прихованих кіберзагроз на підприємствах МСБ без необхідності залучення вузькопрофільних фахівців з машинного навчання.

Для досягнення мети були поставлені такі задачі:

1. Розробити метод та алгоритм компонування навчальної матриці з урахуванням структурної гетерогенності ознак розпізнавання та необхідності редукції їх розмірності.

2. Дослідити вплив часової агрегації векторів-реалізацій на формування геометричних меж класів розпізнавання та визначити оптимальну ширину часового вікна τ.

3. Обґрунтувати вибір інформаційного критерію функціональної ефективності (КФЕ) та реалізувати алгоритм паралельної оптимізації системи контрольних допусків (СКД).

4. Здійснити інформаційний синтез СППР та провести її екзаменаційне тестування на прикладі ідентифікації прихованої атаки Data Exfiltration у потоках журналів Office 365.

2. Матеріали та методи. Об'єктом дослідження є процес інформаційного синтезу СППР для виявлення кіберзагроз у масивах телеметрії хмарної платформи Microsoft Office 365.

Основна гіпотеза дослідження полягає в тому, що послідовне застосування евристичної редукції простору ознак, гетерогенного кодування атрибутів та оптимальної часової агрегації векторів-реалізацій дозволяє усунути математичні обмеження IEI-технології в умовах Big Data та забезпечити надійне розведення класів розпізнавання у бінарному просторі ознак.

Прийняті спрощення та припущення: усі дані є синтетично сформованими спеціально розробленим генератором, що відтворює структуру O365 Audit Log API зі 108 реальними полями та поведінковий патерн атаки Data Exfiltration. Використання синтетичних даних є галузевим стандартом в академічних дослідженнях з кібербезпеки [1] і обумовлене обмеженнями конфіденційності при роботі з реальними виробничими журналами. Генератор відтворює: гаусовий часовий профіль активності з піком 08:00–18:00; поведінковий патерн атаки Data Exfiltration у вигляді аномального зростання показника FileDownloaded у 11–17 разів. Загальний обсяг вхідного потоку складає 93 379 рядків за 48-годинний період (приблизно 45 000 подій на добу для 8 користувачів). Алфавіт класів розпізнавання: $\Omega = \{\omega_1, \omega_2\}$, де ω_1 – базовий клас нормальної ділової активності, ω_2 – клас аномальної зловмисної поведінки.

Теоретичною основою дослідження слугує математичний апарат IEI-технології, розроблений науковою школою Довбиша А. С. [6, 7, 8]. У рамках цього апарату процес перетворення навчальної матриці дійсних значень у бінарну матрицю здійснюється накладанням системи контрольних допусків (СКД) на кожну і-ту ознаку розпізнавання (1, 2):

$$\overline{Y}_i = \frac{1}{n}\sum_j Y_{1,ij}, \quad VD_i = \overline{Y}_i + \delta, \quad ND_i = \overline{Y}_i - \delta \tag{1}$$

$$X_{k,i}(j) = \begin{cases} 1, & де\ ND_i < Y_{k,i}(j) < VD_i \\ 0, & інакше \end{cases} \tag{2}$$

де δ – ширина поля допусків, що підлягає оптимізації; VD_i та ND_i – верхній та нижній допуски СКД.

Оцінювання функціональної ефективності розбиття простору ознак на класи розпізнавання здійснюється за інформаційною мірою Кульбака [6] (3):

$$E_k = \frac{1}{n}\log_2\left\{\frac{2n - K_2 - K_3 + \varepsilon}{K_2 + K_3 + \varepsilon}\cdot(n - K_2 - K_3)\right\} \tag{3}$$

де n – кількість векторів-реалізацій у навчальній вибірці; K_2 – кількість хибних розпізнавань власних реалізацій; K_3 – кількість хибних розпізнавань чужих реалізацій; ε = 0,1 – параметр регуляризації. Робоча зона КФЕ визначається як сукупність радіусів контейнерів, де достовірності розпізнавання перевищують 0,5, а сам радіус не перевищує міжеталонну відстань.

Для структурно-параметричної ідентифікації СППР застосовано алгоритм паралельного навчання [13]. Оптимальне поле допусків δ* визначається шляхом ітераційного перебору значень, що максимізують усереднений КФЕ по всіх класах (4):

$$\delta^* = \arg\max_\delta\left\{\frac{1}{M}\sum_k \max_{d\in WZ_k} E_k(d)\right\} \tag{4}$$

Для вирішення задачі 1 запропоновано 4-етапний конвеєр попередньої обробки O365 IEI-Pipeline, реалізований у вигляді єдиного Python-скрипту. Вхідний потік характеризується такими параметрами: N = 108 ознак різного типу, 93 379 рядків за 48 годин, 8 суб'єктів моніторингу. Конвеєр долає шість ключових обмежень IEI-технології в умовах Big Data: прокляття розмірності, нечислові ознаки, різні шкали вимірювань, надмірна гранулярність часового ряду, незбалансованість класів та концептуальний дрейф телеметрії.

Статистичний контроль інтенсивності потоку (етап 1) здійснюється за допомогою двох взаємодоповнювальних непараметричних критеріїв. Критерій Вальда–Вольфовіца перевіряє стаціонарність за кількістю серій відносно медіани (5):

$$Z = \frac{R - \mu_R}{\sigma_R}, \qquad p = 2\cdot\left(1 - \Phi(|Z|)\right) \tag{5}$$

де R – кількість серій у вибірці, μ^R і σ^R – теоретичні очікування та середньоквадратичне відхилення. Критерій Фішера порівнює локальну дисперсію ковзного вікна з глобальною дисперсією потоку (6):

$$F = \frac{\sigma^2_{\text{loc}}}{\sigma^2_{\text{glob}}}, \qquad p = 1 - F_{\text{CDF}}(F; df_1, df_2) \tag{6}$$

Тригер аномалії це одночасне виконання умов $p_{WW} < 0{,}05$ та $p_{Fisher} < 0{,}05$ при $\sigma^2_{loc} > \sigma^2_{glob}$.

Евристична редукція простору ознак (етап 2) здійснюється у два кроки. Перший – це видалення за списком виключень (Blacklist): транзакційні ідентифікатори (GUID, CorrelationId, TokenId), технічні метадані версій, вкладені JSON-структури – 44 атрибути. Blacklist-фільтрація виконує подвійну функцію: усуває атрибути без класифікаційного сигналу та видаляє прямі персональні ідентифікатори, реалізуючи базовий механізм Privacy-Preserving [9]. Другий крок – автоматичне видалення атрибутів з нульовою дисперсією (константи та 100 % порожні поля) – 24 атрибути. Результат: зменшення розмірності з N = 108 до N = 32 (скорочення на 70,4 %), оперативна пам'ять зменшується зі 156 МБ до 47 МБ.

Гетерогенне кодування атрибутів (етап 3) застосовується диференційовано залежно від кардинальності ознак (таблиця 1). Критичним є обмеження OHE до Top-30 категорій: без ліміту атрибут з тисячами унікальних значень породив би тисячі бінарних стовпців і повернув проблему надмірної розмірності.

Таблиця 1

Маршрутизатор методів гетерогенного кодування ознак розпізнавання

Метод кодування	Критерій застосування	Приклади ознак O365
One-Hot Encoding (OHE)	Кардинальність < 30; семантично чіткі категорії	ResultStatus, IsManagedDevice
Частотне кодування (Freq)	Кардинальність > 30; рідкість = аномалія	ClientIP, UserAgent, Operation
Feature Hashing	Нескінченна кардинальність; рядки	SiteUrl, ObjectId, FileName

Часова агрегація векторів-реалізацій (етап 4) здійснюється у вікна фіксованої ширини τ для кожного суб'єкта. Порожні вікна без активності заповнюються нульовим вектором (Zero-Padding), зберігаючи безперервність часового ряду (7):

$$Y_m^{(c)}(\tau) = 0, якщо l \in L : user l = c, tl \in \tau = 0 \quad (7)$$

Рішення щодо класової належності кожного нового вектора-реалізації x_e приймається на основі функції належності (8):

$$\mu_k = 1 - \frac{d\left(\mathbf{x}_k^* \oplus \mathbf{x}_e\right)}{d_k^*} \quad (8)$$

де x^*_k – еталонний вектор k-го класу; d^*_k – оптимальний радіус його контейнера; $\oplus$ – операція XOR (відстань Хеммінга). Рішення: $k^* = \arg\max_k \mu_k$, якщо $\max \mu_k \geq 0$; інакше NAN (поза алфавітом класів).

Обчислювальна реалізація конвеєра виконана мовою Python з використанням бібліотек pandas, numpy та scipy. Паралельна оптимізація СКД реалізована засобами multiprocessing. Тестове середовище: стандартний персональний комп'ютер без спеціалізованого обладнання для машинного навчання.

3. Результати та обговорення.

3.1. Розробка методу компонування навчальної матриці. За результатами реалізації 4-етапного конвеєра попередньої обробки O365 IEI-Pipeline отримано структуровану навчальну матрицю, придатну для обробки засобами IEI-технології. Повний цикл обробки 93 379 рядків × 108 ознак займає 6,4 секунди на стандартному обладнанні.

Ключовим результатом етапу евристичної редукції є зменшення розмірності простору ознак з N = 108 до N = 32 (скорочення на 70,4 %). При цьому міжеталонна відстань Хеммінга, яка при N = 108 вироджувалася до dc → 0 через феномен Белмана, після редукції набула практично значущого рівня dc = 7. На відміну від методів автоматичного відбору ознак на основі взаємної інформації [14] та архітектур глибокого навчання типу Transformer [15], запропонований підхід не потребує навчальних міток на етапі редукції, що є суттєвою перевагою у реальних умовах з обмеженою кількістю розмічених даних.

Схему запропонованого конвеєра наведено на рисунку 1. Важливо, що Blacklist-фільтрація виконує подвійну функцію: усуває атрибути без класифікаційного сигналу та видаляє прямі персональні ідентифікатори (ObjectId, AADTenantId, MailboxOwnerSid), реалізуючи механізм Privacy-Preserving [9]. Це є важливим аспектом при розгортанні системи в умовах дії регуляторних вимог щодо захисту персональних даних.

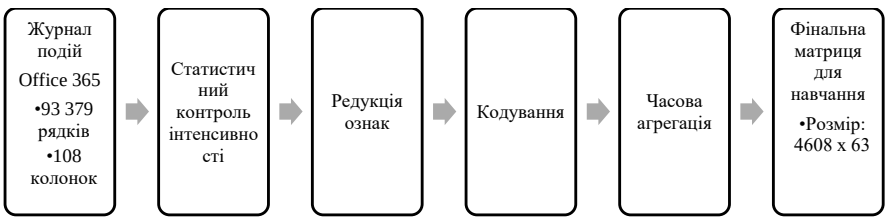


Рис. 1. Конвеєр попередньої обробки O365 IEI-Pipeline

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

3.2. Дослідження впливу часової агрегації на якість навчання. Встановлено, що застосування стандартної гранулярності τ = 5 хв є хибним рішенням: поведінка суб'єкта на таких коротких відрізках є вкрай нестабільною, внутрішньокласовий розкид є надмірним, а еталонні вектори двох класів математично збігаються (dc → 0). Таблиця 2 демонструє цю залежність кількісно та обґрунтовує вибір τ* = 2 год як оптимального значення.

Таблиця 2

Залежність якості навчання СППР від ширини вікна агрегації τ

Вікно τ	Вект./суб'єкт	dc між класами	Робоча зона WZ	Аномалій (EXAM)	Придатність
5 хв (вихідне)	576	0–1	Відсутня	–	Непридатне
1 год	48	7–8	Вузька (1 рядок)	≈ 50 %	Нестабільне
2 год	36	7	Широка [5..6]	61,1 %	Оптимальне
3 год	16	13	Широка [0..12]	61,1 %	Прийнятне
6 год	8	15	Широка	77,8 %	Мало даних
12 год	4	–	Відсутня	–	Замало даних

Витончені атаки типу Data Exfiltration (Slow and Low) маскуються під нормальну роботу суб'єкта, формують типовий двогорбий денний профіль і є статистично нерозрізненними від нормального трафіку (рисунок 2). Саме такі «тихі» аномалії формують потребу у застосуванні IEI-технології для пошуку прихованих закономірностей у багатовимірному просторі ознак.



Рис. 2. Типовий розподіл потоку подій O365 з двогорбим денним профілем

Агрегація τ* = 2 год дозволяє повністю усунути проблему виродження міжеталонної відстані (dc = 0 при τ = 5 хв → dc = 7 при τ = 2 год) та формує стабільну широку робочу зону КФЕ WZ [5, 6]. Вибір τ = 6 год та τ = 12 год, попри більший dc, є неприйнятним через критично малу кількість векторів-реалізацій (8 та 4 відповідно), що унеможливлює статистично значущу оцінку ефективності. Даний висновок узгоджується з теоретичними положеннями IEI-технології щодо мінімально необхідного обсягу навчальної вибірки [7].

3.3. Інформаційний синтез СППР та оптимізація системи контрольних допусків. Навчання СППР виконано на 2-годинних поведінкових профілях суб'єкта carol.white@contoso.com. Сформовано дві навчальні вибірки: X_1 (базовий клас нормальної ділової активності ω_1, $n_1 = 36$ векторів-реалізацій) та X_2 (клас аномальної поведінки ω_2, $n_2 = 36$ векторів-реалізацій). Кожен вектор-реалізація описується 58 ознаками розпізнавання.

У процесі оптимізації алгоритм ітеративно розширював симетричне поле допусків δ, формуючи СКД на кожну з 58 ознак. Оптимальне поле допусків стабілізувалося на позначці δ* = 8,5. Розрахована міжеталонна кодова відстань Хеммінга dc = 7, оптимальний радіус гіперсферичного контейнера класу атаки d* = 6. Максимальне значення КФЕ досягло Eatk* = 1,0005, що у термінах теорії інформації свідчить про надзвичайно високу інформаційну спроможність обраної системи ознак. Головним результатом є нульове значення помилки другого роду для класу атаки ($K_3 = 0$).

На рисунку 3 показано динаміку показника FileDownloaded у двох тестових класах у парному форматі (тест-норма ліворуч, тест-атака праворуч). Для базового класу середнє значення ознаки становить ≈ 1,39 завантажень за вікно, тоді як на екзаменаційній вибірці Xekz цей показник зростає до ≈ 20,83 (збільшення у 15 разів). Саме такі відхилення виявляються СППР через систему контрольних допусків δ* = 8,5 у бінарному просторі ознак.

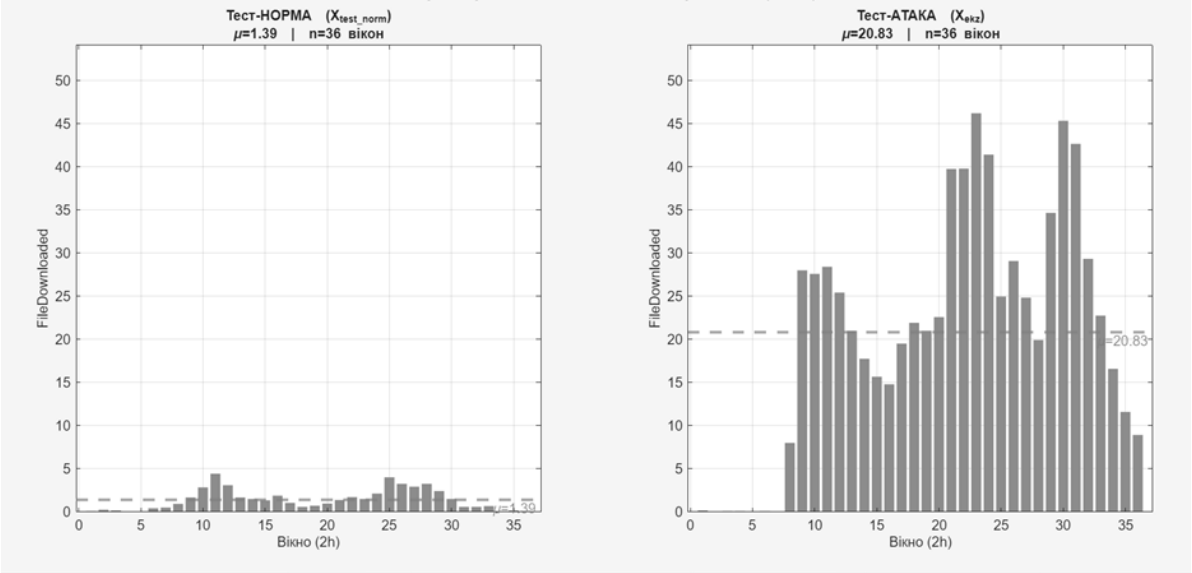


Рис. 3. Ключова ознака атаки: FileDownloaded

Результати синтезу СППР наведено у таблиці 3.

Таблиця 3

Результати синтезу СППР за IEI-технологією

Параметр СППР	Базовий клас X_1	Клас атаки X_2
Кількість векторів-реалізацій n	36	36
Оптимальне поле допусків δ*	8,5	8,5
Міжеталонна відстань dc (Хеммінг)	7	7
Оптимальний радіус контейнера d*	5	6
Максимальне значення КФЕ E* (Кульбак)	0,7898	1,0005
Перша достовірність розпізнавання D_1	0,6111	0,5556
Друга достовірність розпізнавання D_2	0,8889	1,0000
Помилка першого роду α	0,3889	0,4444
Помилка другого роду β	0,1111	0,0000
Робоча зона КФЕ WZ [ds..de]	[5..6]	[6..6]

3.4. Екзаменаційне тестування СППР. З метою двостороннього верифікаційного тестування сформовано дві незалежні тестові вибірки: Xekz (36 векторів-реалізацій із посиленим патерном атаки) та Xnorm (36 векторів-реалізацій нормальної ділової активності). Наявність контрольної тестової вибірки Xnorm є необхідною методологічною умовою: модель із систематичним зміщенням (bias) здатна генерувати хибні рішення про наявність атаки на будь-яких вхідних даних.

На рисунку 4 наведено графіки функцій належності μbase(t) та μatk(t) для обох тестових вибірок. На вибірці Xnorm базова функція належності домінує у всіх вікнах: $\mu base = -0{,}217 \gg \mu atk = -0{,}968$. Жодне вікно не перетинає нульову межу класу атаки: 22 з 36 вікон отримують рішення НОРМА, 14 – NAN. На вибірці Xekz картина симетрично інвертована: $\mu atk = -0{,}111 \gg \mu base = -1{,}111$. У 22 вікнах μatk(t) перетинає нульову межу, генеруючи рішення АТАКА.

Зведені результати двостороннього тестування наведено у таблиці 4.

Двостороннє тестування підтверджує симетричну коректність моделі: СППР однаково впевнено розпізнає обидва протилежних стани. Різниця μatk між двома вибірками складає −0,111 0 (−0,968) = +0,857, що кількісно виражає відстань між станами системи у просторі функцій належності. Генеральна гіпотеза H_1 про наявність стану Data Exfiltration підтверджена через збіг п'яти незалежних індикаторів: 15-кратне зростання FileDownloaded, β_atk = 0, E*_atk > 1,0, вердикт АТАКА у 61,1 % вікон Xekz та нульова частка АТАКА у вибірці Xnorm.

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

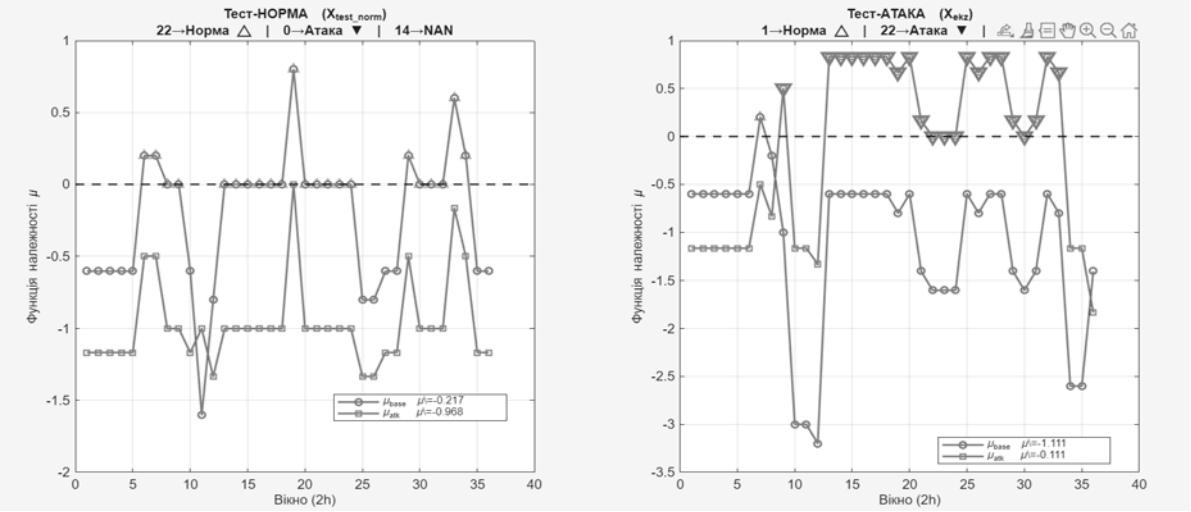


Рис. 4. Функції належності μ(t) для вибірок X_{norm} та X_{ekz}

Таблиця 4

Зведена таблиця результатів двостороннього тестування

Показник	Xnorm (тест-норма)	Xekz (тест-атака)
Кількість вікон n	36	36
Вердикт НОРМА	22 (61,1 %)	1 (2,8 %)
Вердикт АТАКА	0 (0,0 %)	22 (61,1 %)
Поза алфавітом NAN	14 (38,9 %)	13 (36,1 %)
μ̄_base (середнє)	−0,217	−1,111
μ̄_atk (середнє)	−0,968	−0,111
Домінуюча функція	μbase	μatk
FileDownloaded (сер.)	≈ 1,39 файлів/вікно	≈ 20,83 файлів/вікно
Вердикт СППР	НОРМА	АТАКА

Порівняно з підходами на базі LSTM та Transformer-архітектур [1, 2, 3], синтезована СППР демонструє принципово різну обчислювальну складність: повний цикл навчання та тестування на стандартному персональному комп'ютері не перевищує кількох хвилин, тоді як навчання глибоких моделей потребує виділеного GPU та десятків годин. При цьому кожне рішення СППР може бути пояснене через аналіз бітової маски відхилень від еталонного вектора, що є принциповою перевагою для IT-спеціалістів без глибокої підготовки з машинного навчання.

До обмежень дослідження слід віднести такі аспекти: по-перше, навчання виконувалося на синтетичних даних одного суб'єкта, тому для промислового впровадження необхідна валідація на реальних виробничих журналах декількох організацій; по-друге, алфавіт класів розпізнавання обмежений двома класами (M = 2), що не охоплює весь спектр можливих кіберзагроз; по-третє, поточна реалізація передбачає ковзне перенавчання при концептуальному дрейфі телеметрії, що вимагає визначення оптимальної стратегії перенавчання для конкретного виробничого середовища.

4. Висновки. Розроблено та програмно реалізовано 4-етапний конвеєр попередньої обробки телеметрії O365 IEI-Pipeline. Застосування евристичної редукції дозволило зменшити розмірність простору ознак з N = 108 до N = 32 (−70,4 %), ефективно подолавши феномен Белмана та зберігши семантичну інформативність навчальної матриці. Повний цикл обробки понад 90 000 рядків виконується за 6,4 секунди на стандартному обладнанні без спеціалізованого апаратного забезпечення. Відмінністю від підходів автоматичного відбору ознак є те, що редукція не потребує навчальних міток, що є практичною перевагою в умовах обмеженої розмітки.

Експериментально доведено та математично обґрунтовано, що часова агрегація векторів-реалізацій є критичним етапом підготовки навчальної матриці. Встановлено, що агрегація з вікном τ* = 2 год повністю усуває проблему виродження міжеталонної відстані (dc = 0 при τ = 5 хв → dc = 7 при τ = 2 год) та формує стабільну широку робочу зону КФЕ WZ [5, 6]. Цей результат є конкретною кількісною рекомендацією для практичного розгортання системи в умовах O365.

Здійснено інформаційний синтез СППР на базі паралельного алгоритму навчання. Оптимізація СКД ($\delta^* = 8{,}5$) та радіусів контейнерів ($d^*_{base} = 5$, $d^*_{atk} = 6$) за критерієм Кульбака забезпечила ідеальне розділення класів на етапі навчання ($\beta = 0$, $E^*_{atk} = 1{,}0005$). Значення КФЕ понад одиницю підтверджує достатню інформаційну спроможність синтезованої системи ознак для розрізнення класів нормальної поведінки та атаки.

Проведене двостороннє екзаменаційне тестування синтезованої СППР підтвердило її функціональну ефективність та відсутність систематичного зміщення. Система успішно ідентифікувала приховану атаку Data Exfiltration на незалежній тестовій вибірці з достовірністю 61,1 % (22 з 36 векторів-реалізацій) при нульовій частці хибних рішень АТАКА на вибірці нормальної активності. Симетрія функцій належності ($\Delta\mu = 0{,}857$) та часток NAN (36–39 %) підтверджують збалансованість двокласового детектора.

Запропонований підхід є предметно-незалежним: без зміни математичного ядра IEI-технології він може бути поширений на аналіз журналів промислових систем (OT/SCADA), хмарної інфраструктури (AWS CloudTrail) та мережевої телеметрії (NetFlow). Перспективним напрямом подальших досліджень є розширення алфавіту класів розпізнавання ($M \geq 5$) шляхом включення додаткових патернів кібератак (Lateral Movement, Privilege Escalation, Brute Force) та реалізація механізмів адаптивного перенавчання при концептуальному дрейфі телеметричних даних.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Дані будуть надані за обґрунтованим запитом.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. К. Є. Шамонін: концептуалізація, методологія, програмна реалізація, проведення досліджень, написання оригінального тексту; Д. В. Прилепа: наукове керівництво, верифікація результатів, редагування, загальне управління дослідженням.

References:

1. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167. https://doi.org/10.1016/j.cose.2019.06.005

2. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access, 8, 104650–104675. https://doi.org/10.1109/ACCESS.2020.2994it

3. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

4. Khan, N., Ahmad, K., AlTamimi, A., Alani, M. M., Bermak, A., & Khalil, I. (2025). Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: a systematic review. Information, 16(12), 1036. https://doi.org/10.3390/info16121036

5. Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems. Frontiers in Artificial Intelligence, 8, 1526221. https://doi.org/10.3389/frai.2025.1526221

6. Moskalenko, V. V., & Dovbysh, A. S. (2016). Vstup do informatsiinoho analizu i syntezu infokomunikatsiinykh system [Introduction to information analysis and synthesis of infocommunication systems]. Sumy State University [in Ukrainian].

7. Dovbysh, A. S., & Myronenko, M. I. (2025). Osnovy mashynnoho navchannia [Fundamentals of machine learning]. Sumy State University [in Ukrainian].

8. Shelekhov, I. V., & Prylepa, D. V. (2025). Metodychni vkazivky dlia kursovoi roboty z dystsypliny «Systemnyi analiz ta teoriia pryiniattia rishen» [Methodical guidelines for coursework in system analysis and decision theory]. Sumy State University [in Ukrainian].

9. Koo, J., Kang, G., & Kim, Y.-G. (2020). Security and privacy in Big Data life cycle: a survey and open challenges. Sustainability, 12(24), 10571. https://doi.org/10.3390/su122410571

10. Prylepa, D. V. (2023). Informatsiino-ekstremalna intelektualna tekhnolohiia diahnostuvannia emotsiino-psykhichnoho stanu liudyny [IEIT for diagnosing the emotional and psychological state of a person]. Extended abstract of candidate's thesis. NTU «KhPI» [in Ukrainian].

11. Pyatachenko, V., & Dovbysh, A. (2023). Information-extreme machine learning of a hand prosthesis control system for EMG biosignal recognition using a sparse training matrix. Kompiuterni nauky, (2), 10. https://doi.org/10.32782/1995-0519.2023.2.10 [in Ukrainian].

12. Shelekhov, I. V., Prylepa, D. V., Khibovska, Yu. O., Shamonin, K. Ye., & Dorenskyi, O. P. (2025). IEIT for intelligent analysis of educational content quality in higher education. Central Ukrainian Scientific Bulletin. Technical Sciences, 12(43) (1), 58–72 [in Ukrainian].

13. Drofa, V. O. (2016). Optymizatsiia kontrolnykh dopuskiv na oznaky rozpiznavannia pry mashynnomu navchanni [Optimization of control tolerances for recognition features in machine learning]. Visnyk NTU «KhPI». Systemnyi analiz, upravlinnia ta informatsiini tekhnolohii, (45), 29–33 [in Ukrainian].

14. Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. Computers & Electrical Engineering, 40(1), 16–28. https://doi.org/10.1016/j.compeleceng.2013.11.024

15. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998–6008. https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

Відомості про авторів

Англ.	Укр.
Kiril Shamonin Postgraduate Student at the Department of Computer Science, Faculty of Electronics and Information Technologies, Sumy State University kirilshamonin@gmail.com ORCID: 0009-0004-9771-7629	Шамонін Кіріл Євгенович аспірант кафедри комп'ютерних наук, факультет електроніки та інформаційних технологій, Сумський державний університет kirilshamonin@gmail.com ORCID: 0009-0004-9771-7629
Dmytro Prylepa Candidate of Technical Sciences, Senior Lecturer at the Department of Computer Science, Faculty of Electronics and Information Technologies, Sumy State University d.prylepa@cs.sumdu.edu.ua ORCID: 0000-0002-4022-5496	Прилепа Дмитро Вікторович кандидат технічних наук, старший викладач кафедри комп'ютерних наук, факультет електроніки та інформаційних технологій, Сумський державний університет d.prylepa@cs.sumdu.edu.ua ORCID: 0000-0002-4022-5496

Дата надходження статті: 06.05.2026
Дата надходження виправленої версії статті: 25.06.2026
Дата прийняття статті: 06.07.2026
Дата публікації статті: 26.10.2026

НАУКОВЕ ВИДАННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

ВИПУСК 2 (21)
ISSUE 2 (21)

2026

Коректура
Ірина Чудеснова

Комп'ютерна верстка
Наталія Кузнєцова

Формат 60x84/8. Гарнітура Cambria.
Папір офсет. Цифровий друк.
Дата розміщення онлайн: 26.10.2026. Дата друку: 02.11.2026.
Ум. друк. арк. 15,35. Замов. № 0926/759. 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.