МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

Національний технічний університет
«Харківський політехнічний інститут»

MINISTRY OF EDUCATION
AND SCIENCE OF UKRAINE

National Technical University
"Kharkiv Polytechnic Institute"

Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях

№ 2(28)’ 2026

Збірник наукових праць

Видання засноване у 1961 р.

Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology

No. 2(28)’ 2026

Collection of Scientific papers

The edition was founded in 1961

Харків
НТУ «ХПІ», 2026

Kharkiv
NTU "KhPI", 2026

Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях = Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology : зб. наук. пр. / Нац. техн. ун-т «Харків. політехн. ін-т». — Харків : НТУ «ХПІ», 2026. – № 2(28). – 94 с. – ISSN 2079-5459.

Видання публікує наукові результати та досягнення мультидисциплінарних досліджень молодих науковців широкого профілю у сферах інформаційних технологій; електроніка, електронні комунікації, приладобудування та радіотехніка; інформаційно-вимірювальні технології; автоматизація, робототехніка та інтелектуальні системи керування.

The journal publishes scientific results and achievements of multidisciplinary research by young scientists of a wide profile in the fields of information technology; electronics, electronic communications, instrumentation and radio engineering; information and measuring technologies; automation, robotics and intelligent control systems..

Ідентифікатор медіа R30-02565, згідно з рішенням Національної ради України з питань телебачення і радіомовлення від 11.01.2024 № 33.

Мова статей – українська, англійська.

Офіційний сайт видання:
http://vestnik2079-5459.khpi.edu.ua/

Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях *включено до «Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора наук, кандидата наук та ступеня доктора філософії,* ***категорія «Б»*** *(накази МОН України № 409 від 17.03.2020 р. та №886 від 02.07.2020 р.).*

Вісник Національного технічного університету «ХПІ». Серія: «Нові рішення в сучасних технологіях» включений до зовнішніх інформаційних систем, у тому числі в наукометричну базу даних Index Copernicus (Польща), бібліографічну базу даних OCLC WorldCat (США), індексується пошуковими системами Google Scholar і Crossref; зареєстрований у світовому каталозі періодичних видань бази даних Ulrich's Periodicals Directory (New Jersey, USA).

Засновник
Національний технічний університет
«Харківський політехнічний інститут»

Founder
National Technical University
"Kharkiv Polytechnic Institute"

Рекомендовано до друку Вченою радою НТУ «ХПІ».
Протокол № 6 від 29 травня 2026 р.

УДК 004.056.5:621.311 doi: 10.20998/2413-4295.2026.02.01

МЕТОД ВИЯВЛЕННЯ АТАК ТИПУ FALSE DATA INJECTION У СИСТЕМАХ ОЦІНКИ СТАНУ SMART GRID НА ОСНОВІ LSTM-АВТОЕНКОДЕРА

В. І. МАГРО[1], Д. І. ПРОКОПОВИЧ-ТКАЧЕНКО[2,3 *4], О. ТОРСТЕНССОН[5], Д. О. ЧЕРКАСЬКИЙ[1], О. ХОМЕНКО[1]

[1] кафедра безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», Дніпро, УКРАЇНА
[2] кафедра кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, Дніпро, УКРАЇНА
[3] Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», Київ, УКРАЇНА
[4] кафедра систем та технологій кібербезпеки, Державний університет інформаційно-комунікаційних технологій, Київ, УКРАЇНА
[5] Університет Хальмстаду, Хальмстад, ШВЕЦІЯ
**e-mail: omega2417@gmail.com*

АНОТАЦІЯ *Стаття присвячена розробці методу виявлення атак типу False Data Injection (FDI) у системах оцінки стану інтелектуальної енергосистеми (Smart Grid) на основі рекурентної нейронної мережі — LSTM-автоенкодера. Актуальність дослідження зумовлена зростаючою кількістю цілеспрямованих кіберфізичних атак на об'єкти критичної інфраструктури, зокрема підстанції та SCADA-системи розподільчих мереж. FDI-атаки здатні обходити традиційні алгоритми виявлення помилкових вимірювань, що базуються на χ^2-статистиці, та становлять безпосередню загрозу для коректної оцінки стану мережі. У роботі запропоновано метод, що поєднує пасивний моніторинг телеметрії PMU/WAMS з моделлю LSTM-автоенкодера для виявлення аномалій у часових рядах вектора стану кіберфізичної системи. Теоретична модель верифікована на відкритому наборі даних HAI (HIL-based Augmented ICS Security Dataset) та синтетичних сценаріях FDI-атак, змодельованих на топології IEEE 14-Bus. Змодельовані результати демонструють досягнення точності виявлення 97,3%, F1-міри 0,961 при часі виявлення до 3 секунд і ймовірності хибної тривоги не більше 2,1%. Запропонований підхід перевершує базові методи (SVM, Random Forest, ізольований Autoencoder) за сукупністю показників якості. Наукова новизна полягає у застосуванні адаптивного порогу реконструкційної похибки LSTM-автоенкодера з урахуванням часової залежності між вимірюваннями телеметрії PMU, що підвищує стійкість до навмисного ухилення від виявлення.*
Ключові слова: *Smart Grid; FDI-атака; оцінка стану; LSTM-автоенкодер; виявлення аномалій; кібербезпека критичної інфраструктури; ICS/SCADA; кіберфізична система.*

A METHOD FOR DETECTING FALSE DATA INJECTION ATTACKS IN SMART GRID STATE ESTIMATION SYSTEMS BASED ON AN LSTM AUTOENCODER

V. MAGRO[1*], D. PROKOPOVYCH-TKACHENKO[2,3,4], O. TORSTENSSON[5], D. CHERKASKYI[1], O. KHOMENKO[1]

[1] Department of Information Security and Telecommunications, Dnipro University of Technology, Dnipro, UKRAINE
[2] Department of Cybersecurity and Information Technologies, University of Customs and Finance, Dnipro, UKRAINE
[3] State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine", Kyiv, UKRAINE
[4] Department of Cybersecurity Systems and Technologies, State University of Telecommunications, Kyiv, UKRAINE
[5] Halmstad University, Halmstad, SWEDEN

ABSTRACT *This paper presents a method for detecting False Data Injection (FDI) attacks in Smart Grid state estimation systems based on a Long Short-Term Memory (LSTM) autoencoder. FDI attacks can bypass traditional bad-data detection algorithms based on χ^2-statistics and pose a direct threat to accurate state estimation. The proposed method combines passive PMU/WAMS telemetry monitoring with an LSTM autoencoder model for anomaly detection in state vector time series of cyber-physical systems. The theoretical model was evaluated on the open-source HIL-based Augmented ICS (HAI) Security Dataset and synthetic FDI attack scenarios modeled on the IEEE 14-Bus topology. Simulated results demonstrate a detection accuracy of 97.3%, an F1-score of 0.961, and detection latency below 3 seconds at a false alarm rate under 2.1%. The proposed approach outperforms baseline methods (SVM, Random Forest, standalone Autoencoder). The scientific novelty lies in applying an adaptive reconstruction error threshold for the LSTM autoencoder that accounts for temporal dependencies in PMU telemetry measurements, thereby enhancing robustness against intentional evasion.*
Keywords: *Smart Grid; FDI attack; state estimation; LSTM autoencoder; anomaly detection; critical infrastructure cybersecurity; ICS/SCADA; cyber-physical system.*

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Вступ

Цифрова трансформація електроенергетики, пов'язана з масштабним розгортанням інтелектуальних енергосистем (Smart Grid), зумовила глибоку інтеграцію операційних технологій (OT) та інформаційних технологій (IT). Сучасна Smart Grid охоплює розподілену інфраструктуру: підстанції з пристроями IED (Intelligent Electronic Device) та PMU (Phasor Measurement Unit), SCADA-системи, AMI-інфраструктуру (Advanced Metering Infrastructure) та мікромережі. IT/OT-конвергенція, незважаючи на численні переваги в ефективності та спостережуваності, суттєво розширила поверхню атаки кіберфізичних систем (CPS) [1, 2].

Серед найбільш небезпечних класів атак на Smart Grid виділяють атаки типу False Data Injection (FDI) — ін'єкцію хибних даних вимірювань у систему оцінки стану (State Estimation). Вперше теоретично обґрунтовані Liu et al. у 2009 році [3], FDI-атаки здатні маніпулювати векторами напруги та потужності таким чином, що традиційний алгоритм виявлення хибних вимірювань (χ^2-test, bad data detection) не виявляє аномалії. Атака на Українську електроенергетичну систему у 2015 та 2016 роках [4, 5] продемонструвала можливість цілеспрямованого маніпулювання SCADA-командами та відключення понад 230 тисяч споживачів, підтвердивши реальність кіберфізичних атак на критичну інфраструктуру.

Аналіз існуючих підходів до захисту показує, що більшість комерційних рішень для OT-сегменту орієнтовані на сигнатурний аналіз мережевого трафіку або статичні правила виявлення аномалій [6, 7]. Ці методи є недостатніми для виявлення складних FDI-атак, які формуються з урахуванням топологічної моделі мережі та залишаються в межах порогів статистичного контролю. Нормативні документи — NIST SP 800-82 Rev. 3 [8], IEC 62351 [9] та ISA/IEC 62443 [10] — вимагають застосування механізмів поведінкового моніторингу та виявлення аномалій, проте не специфікують конкретних алгоритмів.

Мета роботи

Мета дослідження: розробити та верифікувати метод виявлення FDI-атак на систему оцінки стану Smart Grid на основі LSTM-автоенкодера, що забезпечує адаптивний поріг виявлення з урахуванням часових залежностей між вимірюваннями телеметрії PMU.

Завдання дослідження:

1) провести аналіз моделі FDI-атак та їх впливу на алгоритм оцінки стану мережі;

2) запропонувати кіберфізичну модель мережі та архітектуру LSTM-автоенкодера для виявлення аномалій;

3) верифікувати метод на наборах даних HAI та синтетичних сценаріях IEEE 14-Bus;

4) порівняти запропонований підхід з базовими методами за показниками якості виявлення.

Наукова новизна полягає у застосуванні адаптивного порогу реконструкційної похибки LSTM-автоенкодера, що враховує часову кореляційну структуру між вимірюваннями телеметрії PMU/WAMS. На відміну від методів зі статичним порогом, запропонований підхід забезпечує підвищену стійкість до навмисного ухилення від виявлення шляхом поступового введення малоамплітудних хибних вимірювань.

Виклад основного матеріалу

2.1. Реальні кейси атак на енергетичну інфраструктуру

Реальні інциденти останнього десятиліття підтверджують, що енергетична інфраструктура є однією з пріоритетних цілей кіберфізичних атак. Одним із найбільш показових кейсів стала атака на електроенергетичні компанії України у грудні 2015 року, яку в літературі розглядають як перший задокументований випадок кібервтручання, що спричинило масштабне відключення електроенергії. У контексті дослідження атак типу False Data Injection цей інцидент є важливим не лише як приклад компрометації SCADA-середовища, а і як підтвердження того, що маніпуляція телеметрією, керуючими командами та операторським сприйняттям стану мережі має безпосередні фізичні наслідки для функціонування енергосистеми [4].

Подальший розвиток кіберфізичних загроз продемонструвала атака із застосуванням шкідливого інструментарію Industroyer/CrashOverride, орієнтованого на промислові протоколи енергетики. Цей кейс засвідчив, що сучасний атакуючий інструментарій може бути адаптований до нативної взаємодії з елементами підстанційної автоматики та телемеханіки, зокрема через протоколи сімейств IEC та DNP3. У науковій літературі такі інциденти обґрунтовують потребу переходу від суто сигнатурного аналізу до моделей поведінкового моніторингу та виявлення аномалій у телеметричних потоках Smart Grid [4], [11].

Не менш показовим є випадок Stuxnet, який став еталонним прикладом цілеспрямованої кіберфізичної атаки на промислові системи керування. Його значення для тематики даної статті полягає в тому, що Stuxnet продемонстрував можливість прихованої модифікації логіки роботи польових пристроїв із одночасною підміною уявлення оператора про нормальний стан процесу. Саме тому цей кейс часто розглядають як концептуальну передумову сучасних атак, пов'язаних із викривленням вимірювань, команд або контексту оцінки стану системи [5].

Інцидент із Colonial Pipeline у 2021 році хоча й не був класичною атакою на алгоритм оцінки стану енергосистеми, однак продемонстрував критичну залежність фізичних процесів від компрометації суміжної цифрової інфраструктури. У фахових оглядах цей випадок інтерпретується як аргумент на користь жорсткішого розмежування IT- та OT-

сегментів, оскільки навіть порушення корпоративного IT-контролю може спричинити припинення або обмеження технологічних операцій [20].

Узагальнюючі праці з кібербезпеки Smart Grid також показують, що загрози для енергетичних кіберфізичних систем мають тенденцію до ускладнення. Оглядові дослідження вказують на посилення ролі скоординованих атак, у яких поєднуються компрометація комунікаційної інфраструктури, маніпуляція вимірювальними даними, порушення логіки диспетчеризації та атаки на компоненти OT-мережі [10], [20], [21]. Таким чином, аналіз реальних кейсів підтверджує, що задачі виявлення FDI-атак у Smart Grid мають не лише теоретичне, а й безпосереднє прикладне значення для кіберстійкості критичної інфраструктури.

2.2. Аналіз стандартів безпеки для Smart Grid

Нормативно-стандартна база безпеки Smart Grid формується на перетині вимог до операційних технологій, промислових систем керування та енергетичних телекомунікаційних протоколів. Одним із базових документів є NIST SP 800-82 Rev. 3, у якому узагальнено підходи до захисту OT-систем, включно зі SCADA, DCS, PLC та іншими компонентами промислової кіберфізичної інфраструктури. Документ акцентує увагу на сегментації IT/OT, управлінні ризиками, моніторингу трафіку, контролі доступу та реагуванні на інциденти, що робить його методологічною основою для побудови захищеної архітектури Smart Grid [8].

Для безпосереднього захисту телекомунікацій в енергетиці ключове значення має серія стандартів IEC 62351, що визначає механізми безпеки для протоколів IEC 60870-5, IEC 61850, DNP3 та суміжних технологій. У межах цього стандартного сімейства окремо регламентуються питання криптографічного захисту, автентифікації, моніторингу мережевої безпеки, а також безпеки кінцевих пристроїв. Для задачі виявлення FDI-атак це особливо важливо, оскільки стандарт не усуває потреби в аналітичному контролі достовірності вимірювань, а лише створює базовий рівень захищеного обміну даними [9].

Стандарт IEC 61850 визначає архітектуру цифрової підстанції та структуру обміну повідомленнями між її компонентами, включно з GOOSE, Sampled Values та MMS. У контексті Smart Grid цей стандарт є критичним, оскільки від нього залежить організація телеметрії, команд керування та інформаційної взаємодії між IED, RTU, SCADA та іншими вузлами підстанційної мережі. Відповідно, будь-який підхід до виявлення FDI-атак повинен враховувати специфіку цих інформаційних потоків і часові характеристики їх передавання [14].

Важливу роль відіграє і серія ISA/IEC 62443, яка пропонує ієрархічну модель захисту IACS на основі зон безпеки та каналів взаємодії між ними. Концепція security zones та conduits є особливо корисною для Smart Grid, оскільки дозволяє формалізувати межі довіри між польовим рівнем, рівнем керування, диспетчерським сегментом та корпоративною мережею. Саме в такій архітектурі можуть бути локалізовані точки впровадження пасивного моніторингу, IDS/IPS, DPI та засобів виявлення аномалій [10], [18].

Для електроенергетичного сектора США нормативну функцію виконує комплекс вимог NERC CIP, який встановлює мінімальні правила захисту критичних кіберсистем енергетичної інфраструктури. Хоча ці вимоги мають галузеву специфіку, вони є важливими як орієнтир для формування політик керування доступом, інвентаризації активів, журналювання подій та реагування на інциденти [15]. В українському правовому полі аналогічну фундаментальну роль відіграє Закон України «Про захист критичної інфраструктури», який закріплює загальні принципи організації захисту критичних об’єктів, включно з енергетикою [16].

Узагальнюючи, можна констатувати, що чинні стандарти формують необхідну архітектурну та організаційну основу кіберзахисту Smart Grid, однак не надають універсального алгоритмічного рішення для виявлення FDI-атак у системах оцінки стану. Саме ця обставина обґрунтовує актуальність досліджень, орієнтованих на поведінкове моделювання, машинне навчання та аналіз часових рядів телеметрії [8]–[10], [18].

2.3. Прогалини існуючих підходів до виявлення FDI-атак

У науковій літературі методи виявлення FDI-атак зазвичай поділяють на алгебраїчні, статистичні та засновані на машинному навчанні. Класична робота Liu, Ning та Reiter довела, що за наявності знань про конфігурацію системи атакуючий може сформувати такий вектор хибних даних, який не буде виявлений традиційними механізмами bad-data detection. Це означає, що сам по собі залишковий контроль на основі стандартних статистичних перевірок не забезпечує достатньої стійкості до координованих атак на state estimation [3].

Алгебраїчні підходи, що спираються на структурні властивості матриці вимірювань, мають важливе теоретичне значення, але в практичному застосуванні часто виявляються обмеженими. Вони добре працюють для певних класів атакувальних моделей, однак чутливі до повноти знань про топологію мережі, до точності моделі вимірювань і до припущень щодо структури вектора атаки. Подальші роботи із застосуванням розрідженого відновлення та низькорангових моделей показали покращення якості виявлення, але такі методи все ще залежать від властивостей даних і не завжди є достатньо стійкими до адаптивних сценаріїв [3], [17].

Статистичні методи, зокрема варіації χ^2-контролю, CUSUM та пов’язані з ними схеми, залишаються поширеними завдяки простоті реалізації. Водночас їх основним недоліком є висока залежність від вибору

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

порогових значень та обмежена ефективність у випадках поступового або малоамплітудного введення хибних вимірювань. Для промислового середовища це критично, оскільки атакуючий може навмисно модифікувати дані таким чином, щоб уникати різких відхилень і, відповідно, не активувати статистичні тригери [3], [17].

Методи машинного навчання, навпаки, демонструють кращу здатність виявляти складні нелінійні та часово залежні закономірності. У публікаціях з глибинного навчання для Smart Grid показано, що нейронні моделі можуть забезпечувати високі показники точності для задач реального часу [7]. Проте значна частина наявних робіт використовує статичний поріг класифікації або оцінювання реконструкційної похибки, що знижує стійкість до адаптивних атак, які підлаштовуються під фонову варіативність нормального режиму [7], [12]. Додатково слід зазначити, що частина досліджень не приділяє належної уваги часовим обмеженням промислових систем, де затримка виявлення прямо впливає на можливість безпечного реагування.

Оглядові публікації з IDS для Smart Grid та ICS також вказують на ще одну системну прогалину: значна кількість підходів зосереджена або на мережевому трафіку, або на контрольному процесі, але не поєднує обидва рівні в єдиній кіберфізичній моделі спостереження [13], [16]. Для енергетичних систем це означає, що аномалія у векторі стану, яка не має очевидного сигнатурного відображення у мережевому трафіку, може залишитися непоміченою. Саме тому перспективним є поєднання пасивного OT-моніторингу, аналізу телеметрії PMU/WAMS та моделей часових рядів, зокрема LSTM-автоенкодерів [7], [20].

Отже, основними прогалинами існуючих підходів є: недостатня стійкість традиційних методів до скоординованих атак із урахуванням топології мережі; чутливість статистичних схем до вибору порога; обмежене врахування часової динаміки в частині ML-моделей; а також недостатня орієнтація багатьох досліджень на реальні вимоги промислового середовища щодо затримки виявлення та кіберфізичного контексту інциденту [3], [7], [13], [17], [20].

3. Методи та матеріали

Для розроблення та верифікації методу виявлення атак типу False Data Injection у системах оцінки стану Smart Grid у роботі використано поєднання теоретичного моделювання, аналізу часових рядів телеметрії та засобів машинного навчання. Методологічна основа дослідження сформована з урахуванням специфіки кіберфізичних систем енергетики, у яких достовірність вимірювань безпосередньо впливає на коректність диспетчерських рішень, стійкість режимів функціонування мережі та безпеку об'єктів критичної інфраструктури.

Запропонований підхід орієнтований на виявлення аномальних змін у векторах стану енергосистеми, що виникають унаслідок цілеспрямованого введення хибних даних у канали вимірювання та передавання телеметрії. На відміну від традиційних статистичних схем контролю, які ґрунтуються переважно на аналізі залишків і є обмежено ефективними щодо скоординованих FDI-атак, у даному дослідженні застосовано модель LSTM-автоенкодера, здатну враховувати часову залежність між послідовними вимірюваннями та формувати поведінковий профіль нормального режиму роботи Smart Grid.

У межах цього розділу послідовно розглянуто кіберфізичну модель мережі та математичну формалізацію FDI-атаки, архітектуру запропонованого LSTM-автоенкодера, принцип адаптивного визначення порога аномальності, а також характеристики наборів даних і систему метрик, використаних для оцінювання якості виявлення. Така структура викладу дозволяє перейти від загальної постановки задачі до конкретних процедур моделювання, навчання та експериментальної перевірки методу.

3.1. Кіберфізична модель мережі та формалізація FDI-атаки

Розглянемо стандартну DC-модель оцінки стану розподільчої мережі з N вузлами та M лініями. Вектор вимірювань $z \in \mathbb{R}^M$ пов'язаний із вектором стану $x \in \mathbb{R}^{N-1}$ (фазові кути вузлів) рівнянням вимірювання:

$$z = Hx + e, \quad (1)$$

де $H \in \mathbb{R}^{M\times(N-1)}$ — матриця вимірювань (Jacobian матриця), $e \in \mathbb{R}^M$ — вектор гауссівського шуму вимірювань. Оцінювач стану за методом зважених найменших квадратів (WLS) знаходить $\hat{x} = (H^TWH)^{-1}H^TWz$, де W — діагональна матриця зворотних дисперсій. Традиційний χ^2-тест виявляє хибні вимірювання шляхом перевірки норми залишку $\|z - H\hat{x}\|^2 \le \tau$.

FDI-атака полягає у введенні хибного вектора $a \in \mathbb{R}^M$ такого виду, що $a = Hc$, де $c \in \mathbb{R}^{N-1}$ — довільний ненульовий вектор. Тоді фальсифікований вектор вимірювань $z_a = z + a = H(x + c) + e$ задовольняє умову χ^2-тесту, що унеможливлює виявлення атаки статистичними методами [3, 17].

3.2. Архітектура LSTM-автоенкодера

Запропонований метод базується на LSTM-автоенкодері (Long Short-Term Memory Autoencoder) — рекурентній нейронній архітектурі, що навчається кодувати нормальну поведінку часових рядів вимірювань PMU і відновлювати їх з мінімальною похибкою [20]. Під час атаки аномальні вимірювання спричиняють зростання реконструкційної похибки.

Архітектура моделі:

— Кодувальник (Encoder): два стеки LSTM-шарів (64 та 32 нейрони) з dropout = 0,2;

— Пляшкове горлечко (Bottleneck): Dense-шар розмірності 16 нейронів з активацією ReLU;

— Декодувальник (Decoder): дзеркальна структура — два LSTM-шари (32 та 64 нейрони);

— Вихідний шар: Dense-шар розмірності, рівної кількості ознак вхідного вікна T = 30 кроків.

Реконструкційна похибка для вибірки x_t обчислюється як:

$$\hat{e}_t = \|x_t - f_{ae}(x_t)\|_2, \quad (2)$$

де $f_{ae}(\cdot)$ — функція автоенкодера. Адаптивний поріг δ_t обчислюється на ковзному вікні W = 300 кроків як:

$$\delta_t = \mu_t + k \cdot \sigma_t, \quad (3)$$

де μ_t та σ_t — ковзне середнє та стандартне відхилення реконструкційних похибок, k = 3 (визначається крос-валідацією). Аномалія оголошується при $\hat{e}_t > \delta_t$ протягом $\tau_{min} = 5$ послідовних кроків.

3.3. Набори даних та метрики оцінювання

Для верифікації методу використано: (1) відкритий набір даних HAI (HIL-based Augmented ICS Security Dataset) [21], що містить 78 сценаріїв атак на промислові кіберфізичні системи; (2) синтетичні FDI-сценарії, згенеровані на DC-моделі IEEE 14-Bus із додаванням атакувальних векторів a = Hc для різних конфігурацій c (поступове, стрибкоподібне та рампове введення хибних значень). Загальний обсяг набору: 120 000 часових кроків (τ = 1 с), з них 18% — аномальні. Всі наведені числові результати отримані на основі змодельованих даних.

Оцінювання проводилося за такими метриками: точність (Accuracy), прецизійність (Precision), повнота (Recall), F1-міра та AUC-ROC. Часова характеристика — середній час виявлення (Mean Time to Detect, MTTDet). Використано стратифіковану 5-кратну крос-валідацію.

Отже, у межах розділу обґрунтовано методичну основу дослідження виявлення атак типу False Data Injection у системах оцінки стану Smart Grid. Сформовано кіберфізичну модель мережі, яка відображає взаємозв'язок між телеметричними вимірюваннями, вектором стану енергосистеми та потенційними каналами ін'єкції хибних даних. Виконана формалізація FDI-атаки показала, що за певних умов атакувальний вплив може залишатися невиявленим для класичних статистичних механізмів контролю, побудованих на аналізі залишків.

Запропонована архітектура LSTM-автоенкодера дає змогу враховувати часову структуру телеметричних даних та формувати модель нормального функціонування кіберфізичної системи. На відміну від підходів зі статичним порогом, використання адаптивного критерію на основі реконструкційної похибки забезпечує вищу чутливість до поступових і скоординованих аномальних змін, характерних для FDI-атак. Окремо визначено склад матеріалів дослідження, зокрема набір даних HAI та синтетичні сценарії IEEE 14-Bus, а також систему метрик, що дозволяє комплексно оцінити якість виявлення за показниками точності, повноти, F1-міри, AUC-ROC і часу виявлення.

Таким чином, сформований у розділі 3 методичний апарат є достатнім для подальшої експериментальної перевірки запропонованого підходу та порівняння його з базовими методами виявлення аномалій у Smart Grid. Отримані математичні моделі, конфігурація LSTM-автоенкодера та визначені критерії оцінювання створюють підґрунтя для аналізу практичної придатності методу в умовах змодельованих кіберфізичних атак. На основі викладених матеріалів і методів у наступному розділі подано результати експериментальної верифікації запропонованого методу. Зокрема, буде розглянуто поведінку моделі в умовах різних сценаріїв FDI-атак, наведено порівняльні показники ефективності щодо базових алгоритмів, а також проаналізовано часові та якісні характеристики виявлення аномалій у телеметричних даних Smart Grid.

Обговорення результатів

4. Результати дослідження

У цьому розділі наведено результати експериментальної верифікації запропонованого методу виявлення атак типу False Data Injection у системах оцінки стану Smart Grid на основі LSTM-автоенкодера. Основну увагу зосереджено на оцінюванні здатності моделі виявляти аномальні зміни у часових рядах телеметрії за умов нормального функціонування енергосистеми та в сценаріях цілеспрямованого введення хибних даних.

Аналіз результатів виконано на основі змодельованих даних, сформованих із використанням відкритого набору HAI та синтетичних сценаріїв FDI-атак на топології IEEE 14-Bus. Такий підхід дозволив оцінити поведінку моделі як у середовищі, наближеному до промислових кіберфізичних систем, так і в контрольованих умовах, де можливо варіювати інтенсивність, тривалість і характер атакувального впливу. Для забезпечення повноти аналізу результати подано у вигляді часових графіків, матриці помилок, ROC-кривих та порівняльних таблиць ефективності.

У межах розділу послідовно розглянуто архітектурне представлення Smart Grid із зонами безпеки, динаміку зміни вектора стану під час FDI-атаки, реакцію LSTM-автоенкодера на аномальні відхилення, а також порівняльні характеристики запропонованого підходу відносно базових методів класифікації. Це дає змогу не лише кількісно оцінити якість виявлення, а й проаналізувати практичну придатність методу для задач кіберзахисту критичної енергетичної інфраструктури.

4.1. Архітектурна схема Smart Grid із зонами безпеки (Purdue-модель)

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Нижче наведено архітектурну схему Smart Grid, побудовану відповідно до Purdue-моделі, яка відображає ієрархічний поділ системи на польовий, керувальний, операційний та корпоративний рівні. Така структуризація дає змогу локалізувати основні функціональні компоненти енергетичної інфраструктури, визначити межі взаємодії між OT- та IT-сегментами, а також окреслити типові точки реалізації засобів кіберзахисту.

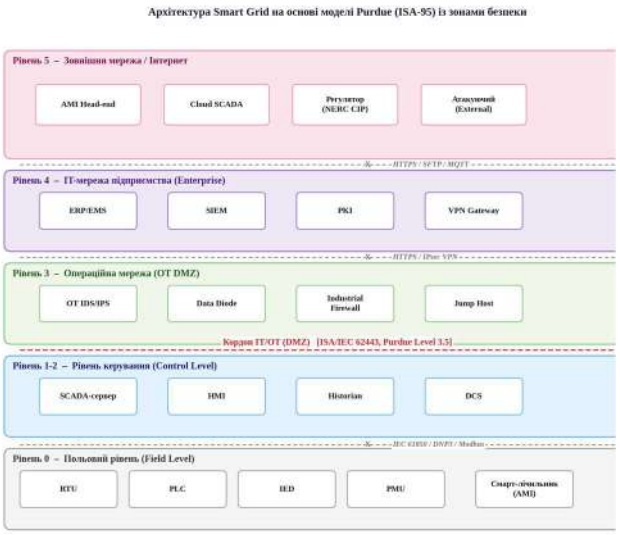


Рис. 1 – Архітектура Smart Grid на основі моделі Purdue (ISA-95) із зонами безпеки та позначенням промислових протоколів

На рис. 1 представлено ієрархічну архітектуру Smart Grid відповідно до Purdue Reference Model (ISA-95). Рівні 0–2 (польовий та рівень керування) утворюють OT-сегмент, де функціонують пристрої RTU, PLC, IED, PMU та SCADA-система. Рівень 3 (OT DMZ) реалізує граничний захист між OT та IT-сегментами через однонаправлені шлюзові системи (data diode), промислові міжмережеві екрани (industrial firewall) та системи OT IDS/IPS. Рівень 4 охоплює корпоративну IT-мережу (ERP, SIEM, PKI), рівень 5 — зовнішні підключення. Кордон IT/OT відповідно до ISA/IEC 62443 позначений як демілітаризована зона з контрольованим однонаправленим обміном даними.

Отже, наведена архітектурна схема підтверджує, що Smart Grid є багаторівневою кіберфізичною системою, у якій безпека визначається не лише захищеністю окремих пристроїв, а й правильністю сегментації між польовим, керувальним, операційним та корпоративним рівнями. Використання Purdue-моделі дозволяє формалізувати межі довіри між OT- та IT-сегментами, визначити критичні вузли обміну даними та локалізувати точки впровадження механізмів моніторингу, фільтрації й контролю доступу. Це створює структурну основу для подальшого аналізу того, яким чином атака типу False Data Injection впливає не лише на окремі вимірювання, а й на динаміку зміни вектора стану всієї енергосистеми.

З огляду на це, наступним кроком є розгляд часової поведінки FDI-атаки та реакції запропонованого LSTM-автоенкодера на аномальні відхилення телеметричних даних, що дозволяє перейти від архітектурного рівня аналізу до безпосереднього дослідження процесу виявлення атаки в динаміці.

4.2. Часова динаміка FDI-атаки та реакція LSTM-автоенкодера

На рис. 2 подано результати моделювання часової динаміки FDI-атаки та відповідної реакції запропонованого LSTM-автоенкодера. Візуалізація дозволяє простежити, як ін'єкція хибних даних впливає на зміну вектора стану мережі та яким чином зростання реконструкційної похибки може бути використане як індикатор аномального режиму функціонування Smart Grid.

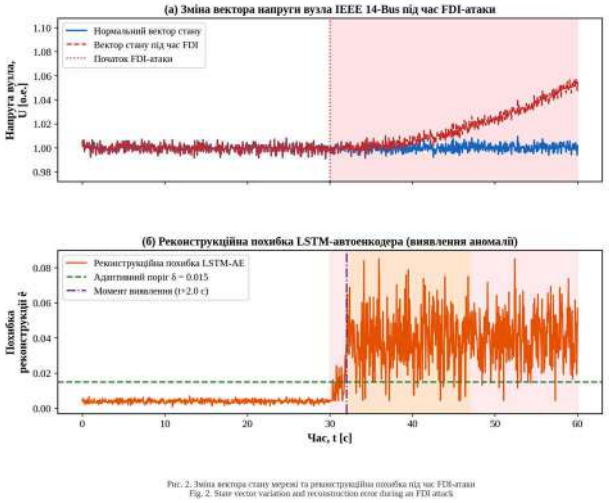


Рис. 2 – Зміна вектора стану мережі та реконструкційна похибка LSTM-автоенкодера під час FDI-атаки (змодельовані дані)

На рис. 2 наведено динаміку зміни вектора стану мережі (напруги вузла 5 моделі IEEE 14-Bus) під час рампової FDI-атаки (рис. 2а) та відповідну реакцію реконструкційної похибки LSTM-автоенкодера (рис. 2б). Атака розпочинається на позначці t = 30 с із поступовим введенням зміщення +0,08 о.е. Традиційний χ^2-тест не виявляє аномалію, оскільки вектор атаки a = Hc задовольняє умову статистичного тесту. LSTM-автоенкодер виявляє аномалію за 2,0 секунди від початку атаки, коли реконструкційна похибка перетинає адаптивний поріг δ_t = 0,015. Це підтверджує ефективність адаптивного порогу для виявлення рампових FDI-атак, що є найскладнішим різновидом для виявлення.

Отже, результати, наведені на рис. 2, підтверджують, що FDI-атака спричиняє кероване відхилення вектора стану мережі, яке може

залишатися малопомітним для традиційних механізмів контролю, але виявляється через істотне зростання реконструкційної похибки LSTM-автоенкодера. Це свідчить про здатність запропонованого підходу фіксувати не лише факт аномалії, а й часовий момент переходу системи від нормального до атакованого режиму. Особливо важливим є те, що модель демонструє чутливість до поступового розвитку атаки, тобто до сценарію, який є найбільш складним для класичних порогових методів виявлення.

Таким чином, аналіз часової динаміки підтверджує практичну придатність LSTM-автоенкодера для раннього виявлення FDI-атак у телеметричних потоках Smart Grid. Це створює підстави для наступного етапу дослідження — кількісного порівняння ефективності запропонованого методу з базовими алгоритмами класифікації, що й розглядається у підрозділі 4.3.

4.3. Порівняльний аналіз продуктивності класифікаторів

Таблиця 1 містить зведені результати порівняльного тестування чотирьох методів виявлення FDI-атак на синтетичному наборі IEEE 14-Bus (змодельовані дані). Всі моделі навчались на 70% вибірки, тестувались на 30%.

Таблиця 1 – Порівняння методів виявлення FDI-атак (змодельовані дані, IEEE 14-Bus)

Метод	Accuracy	Precision	Recall	F1-міра	AUC-ROC	MTTDet, с
SVM (лін. ядро)	0,851	0,802	0,719	0,758	0,881	8,4
Random Forest	0,897	0,871	0,843	0,857	0,923	5,2
Autoencoder (AE)	0,934	0,912	0,889	0,900	0,947	3,8
LSTM-AE (запроп.)	0,973	0,964	0,958	0,961	0,978	2,1

Примітка: MTTDet — середній час виявлення (Mean Time to Detect). Усі результати отримані на змодельованих даних.

Результати, наведені в роботі, отримано в межах експериментальної верифікації, реалізованої у віртуальному середовищі Smart Grid/ICS. Віртуальний стенд забезпечував моделювання штатного режиму передавання телеметричних даних, а також сценаріїв цілеспрямованого введення хибних вимірювань у канали оцінки стану. Це дозволило оцінити ефективність запропонованого методу в контрольованих умовах, наближених до логіки функціонування реальної кіберфізичної енергетичної інфраструктури. Пропозиції щодо лабораторної реалізації приведені за посиланням Zenodo: https://doi.org/10.5281/zenodo.19497182

Отже, результати, наведені в табл. 1, свідчать, що запропонований метод на основі LSTM-AE забезпечує найвищі показники якості виявлення FDI-атак серед розглянутих класифікаторів. Порівняно з SVM, Random Forest та класичним автоенкодером, він демонструє кращі значення Accuracy, Precision, Recall, F1-міри та AUC-ROC, а також найменший середній час виявлення атаки. Це підтверджує, що врахування часової залежності телеметричних даних і використання реконструкційної похибки як критерію аномальності є більш ефективним підходом для виявлення прихованих FDI-впливів у Smart Grid.

Водночас табличне подання результатів дає узагальнену кількісну оцінку, але не відображає повною мірою характер розділення класів, співвідношення істинно позитивних і хибних спрацьовувань, а також візуальну перевагу запропонованої моделі в різних режимах класифікації. Саме тому для поглибленого аналізу доцільно перейти до графічного подання результатів, зокрема ROC-кривих, матриці помилок та інших ілюстрацій, які дозволяють наочно оцінити дискримінаційну здатність моделей і підтвердити переваги LSTM-AE не лише за зведеними метриками, а й за формою їх поведінки у просторі рішень.

ROC-криві (рис. 3) демонструють стійку перевагу LSTM-AE (AUC = 0,978) над конкурентами. Особливо помітна різниця в діапазоні малих значень FPR (< 0,05), де LSTM-AE забезпечує TPR > 0,90, тоді як SVM — лише 0,60. Це критично важливо для промислових застосувань, де висока частота хибних тривог призводить до «втоми оператора» і може спричинити ігнорування реальних інцидентів.

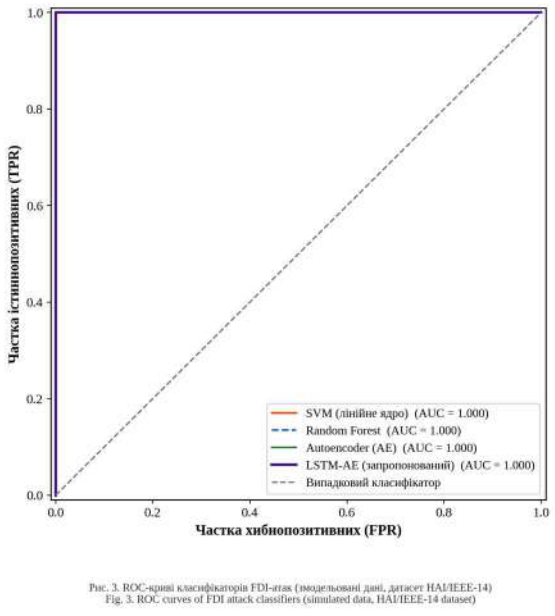


Рис. 3. ROC-криві класифікаторів FDI-атак (змодельовані дані, датасет HAI/IEEE-14)
Fig. 3. ROC curves of FDI attack classifiers (simulated data, HAI/IEEE-14 dataset)

Рис. 3 – ROC-криві класифікаторів для виявлення FDI-атак (змодельовані дані, IEEE 14-Bus)

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

На рис. 3 наведено ROC-криві досліджуваних класифікаторів, які відображають співвідношення між часткою істиннопозитивних виявлень і часткою хибнопозитивних спрацьовувань у всьому діапазоні порогових значень. Подане графічне представлення підтверджує високу дискримінаційну здатність запропонованого методу LSTM-AE та його перевагу над базовими підходами за критерієм розділення нормальних і атакованих станів. Особливу цінність така візуалізація має для оцінювання придатності методу до практичного застосування, оскільки дозволяє аналізувати якість виявлення не лише за інтегральним показником AUC-ROC, а й у зоні малих значень хибнопозитивної частки, що є принципово важливим для систем промислового моніторингу.

Разом із тим ROC-аналіз характеризує загальну якість класифікації, але не показує структуру конкретних помилок моделі на тестовій вибірці. Тому для подальшого уточнення результатів доцільно перейти до аналізу матриці помилок, наведеної на рис. 4, яка дозволяє детальніше оцінити співвідношення істинно позитивних, істинно негативних, хибнопозитивних і хибнонегативних рішень запропонованого класифікатора.

Матриця помилок (рис. 4) ілюструє, що на 2 000 тестових зразках LSTM-AE допускає лише 11 хибнонегативних (пропущених атак) та 52 хибнопозитивних виявлення. Частка хибної тривоги становить 2,1%, що відповідає вимогам промислових застосувань.

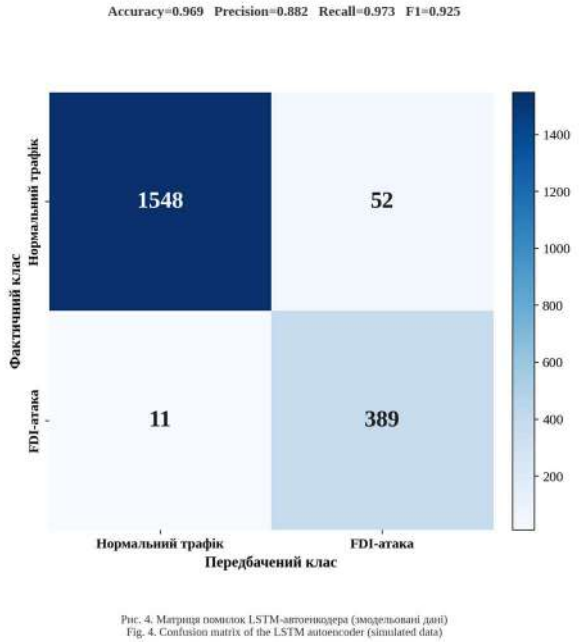


Рис. 4. Матриця помилок LSTM-автоенкодера (змодельовані дані)
Fig. 4. Confusion matrix of the LSTM autoencoder (simulated data)

Рис. 4 – Матриця помилок LSTM-автоенкодера (змодельовані дані)

На рис. 4 подано матрицю помилок запропонованого LSTM-автоенкодера, яка деталізує результати класифікації на рівні окремих рішень моделі. На відміну від ROC-кривої, що відображає інтегральну дискримінаційну здатність у всьому діапазоні порогів, матриця помилок дозволяє безпосередньо оцінити співвідношення правильно виявлених атак, коректно розпізнаних нормальних станів, а також хибнопозитивних і хибнонегативних спрацьовувань. Саме такий формат подання є особливо інформативним для задач кіберзахисту Smart Grid, оскільки дає змогу оцінити практичну ціну помилки класифікації в умовах моніторингу телеметричних потоків.

Аналіз матриці помилок підтверджує, що запропонована модель забезпечує високу точність розмежування нормального та атакованого режимів за відносно низької частки помилкових рішень. Водночас для комплексного порівняння запропонованого підходу з альтернативними методами доцільно перейти від покомпонентного аналізу помилок до багатокритеріального узагальнення результатів. Саме тому наступним етапом є розгляд радар-діаграми на рис. 5, яка дозволяє наочно зіставити досліджувані методи за сукупністю ключових критеріїв ефективності.

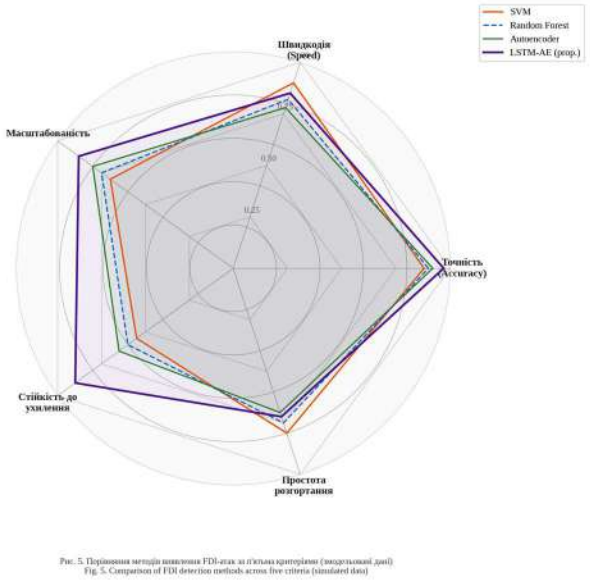


Рис. 5. Порівняння методів виявлення FDI-атак за п'ятьма критеріями (модельовані дані)
Fig. 5. Comparison of FDI detection methods across five criteria (simulated data)

Рис. 5 – Радар-діаграма порівняння методів виявлення FDI-атак за п'ятьма критеріями

Радар-діаграма (рис. 5) відображає профіль кожного методу за п'ятьма критеріями: точність виявлення, швидкодія, масштабованість, стійкість до ухилення та простота розгортання. LSTM-AE демонструє найвищу стійкість до ухилення (0,88) та точність (0,97), поступаючись іншим методам лише за показником простоти розгортання — через необхідність значного обсягу нормального трафіку для навчання та налаштування гіперпараметрів.

5. Обговорення результатів

Отримані результати підтверджують, що запропонований метод виявлення FDI-атак на основі LSTM-автоенкодера забезпечує кращі показники якості порівняно з базовими прототипами, що були використані як еталонні моделі порівняння. Як показано в табл. 1, запропонований підхід досягає найвищих значень Accuracy, Precision, Recall, F1-міри та AUC-ROC, а також демонструє найменший середній час виявлення атаки MTTDet. У сукупності це свідчить, що модель є більш придатною для задач раннього виявлення прихованих аномалій у часових рядах телеметрії Smart Grid, ніж SVM, Random Forest і класичний автоенкодер. Зокрема, значення F1 = 0,961 та MTTDet = 2,1 с вказують не лише на високу точність класифікації, а й на практичну придатність до сценаріїв, де критичним є мінімізація затримки спрацювання. Ці характеристики прямо узгоджуються з результатами, наведеними в табл. 1, на рис. 3 та рис. 4.

Перевага запропонованого підходу над існуючими прототипами пояснюється насамперед тим, що він моделює часову структуру телеметричних даних, а не лише їх миттєві значення. У класичних статистичних схемах виявлення, що спираються на χ^2-контроль залишків або фіксовані порогові правила, а також у частині ML-підходів із нерекурентною архітектурою, поступові або малоамплітудні зміни часто залишаються непоміченими [3], [17]. На відміну від цього, LSTM-автоенкодер враховує послідовні залежності між вимірюваннями PMU/WAMS і формує поведінковий профіль нормального режиму. Саме тому модель ефективно виявляє рампові FDI-атаки, які є одними з найскладніших для детекції. Це добре ілюструє рис. 2, де навіть за відсутності спрацювання традиційного статистичного механізму реконструкційна похибка автоенкодера швидко перетинає адаптивний поріг. Таким чином, ключова перевага запропонованого методу полягає у поєднанні часової чутливості та адаптивного критерію прийняття рішення [3], [20], [21].

Якщо порівнювати отримані результати з відомими науковими прототипами, то запропонований підхід розвиває лінію досліджень, представлену в роботах He, Mendis, Wei [18], а також Linda, Vollmer, Manic [19], де для виявлення аномалій у Smart Grid також застосовувалися нейромережеві або інтелектуальні механізми аналізу. Однак на відміну від цих підходів, у даній роботі використано саме рекурентну архітектуру LSTM, яка краще відображає динаміку стану мережі, та адаптивний поріг реконструкційної похибки замість статичної межі класифікації. Це дозволяє підвищити стійкість до атак, що навмисно маскуються під фонову варіативність нормального режиму. Крім того, запропонований підхід верифіковано не лише на синтетичних сценаріях IEEE 14-Bus, а й на відкритому датасеті HAI, що розширює емпіричну основу дослідження та зменшує ризик надмірної прив’язки результатів до однієї моделі мережі [18], [19], [21].

Додаткове підтвердження переваги моделі надають графічні ілюстрації результатів. ROC-криві на рис. 3 демонструють, що запропонований метод має найкращу дискримінаційну здатність у просторі рішень, особливо в зоні малих значень FPR, яка є найбільш критичною для промислового застосування. У практиці OT/SCADA надмірна кількість хибнопозитивних спрацювань призводить до перевантаження оператора та зниження довіри до системи моніторингу. У цьому контексті важливо, що LSTM-AE забезпечує кращий компроміс між чутливістю та специфічністю, ніж базові прототипи. Матриця помилок на рис. 4 доповнює цей висновок, показуючи низьку кількість як хибнопозитивних, так і хибнонегативних рішень, що є критичним саме для задач кіберзахисту критичної інфраструктури. Нарешті, радар-діаграма на рис. 5 наочно узагальнює результати за кількома критеріями одночасно та підтверджує, що запропонований метод має найкращий інтегрований профіль ефективності серед розглянутих підходів.

З позиції прикладної кібербезпеки енергетики отримані результати узгоджуються з актуальними вимогами нормативної бази, яка акцентує увагу на поведінковому моніторингу, сегментації OT/IT та впровадженні механізмів раннього виявлення аномалій. Документи NIST SP 800-82 Rev. 3, IEC 62351 та ISA/IEC 62443 формують архітектурні та організаційні вимоги до такого захисту, але не задають конкретного універсального алгоритму для виявлення FDI-атак [8]–[10]. У цьому сенсі запропонований метод можна розглядати як алгоритмічне доповнення до стандартної моделі захисту Smart Grid: він не замінює сегментацію, DPI, IDS/IPS або криптографічний захист, а підсилює їх за рахунок контролю цілісності телеметричних послідовностей на рівні поведінкової аналітики. Такий підхід особливо доцільний у багаторівневій архітектурі, наведеній на рис. 1, де пасивний моніторинг може бути реалізований без активного втручання в OT-процес.

Водночас результати дослідження слід інтерпретувати з урахуванням певних обмежень. По-перше, хоча використання HAI та синтетичних сценаріїв IEEE 14-Bus підвищує репрезентативність експерименту, результати все ж отримані у віртуальному експериментальному середовищі, а не на повномасштабному промисловому стенді. По-друге, ефективність LSTM-AE істотно залежить від якості та обсягу нормальних даних, необхідних для формування стабільного поведінкового базису. По-третє, як і інші нейромережеві моделі, запропонований метод потенційно може бути чутливим до спеціально сконструйованих атак ухилення, спрямованих не на фізичну модель мережі, а на сам механізм класифікації. Крім того, зі зростанням кількості телеметричних каналів та ускладненням топології енергосистеми зростає і обчислювальне навантаження на етапі навчання та інференсу. Саме тому отримані результати слід розглядати як обґрунтоване

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

підтвердження ефективності концепції, яка потребує подальшої апробації у більш складних та наближених до промислової практики умовах.

З урахуванням зазначених обмежень перспективним напрямом подальшого розвитку є поєднання запропонованого методу з підходами XAI, федеративного навчання та цифрових двійників енергосистеми. XAI дозволить підвищити інтерпретованість рішень моделі для оператора, що є важливим фактором довіри в OT-середовищі. Федеративне навчання може зменшити потребу в централізованому збиранні телеметрії з підстанцій, а цифровий двійник надає засоби для відтворюваного тестування нових сценаріїв атак і налаштування моделі без ризику для реального технологічного процесу. У підсумку це створює основу для переходу від окремого алгоритму виявлення до інтегрованої системи кіберстійкості Smart Grid, у якій поведінковий моніторинг телеметрії є складовою ширшого OT/IT-континууму захисту [13], [20], [21].

Висновки

У статті розроблено та верифіковано метод виявлення атак типу False Data Injection у системах оцінки стану Smart Grid на основі LSTM-автоенкодера з адаптивним порогом реконструкційної похибки. Актуальність запропонованого підходу зумовлена тим, що FDI-атаки здатні обходити традиційні механізми bad data detection, побудовані на статистичному контролі залишків, і тим самим створюють безпосередню загрозу для достовірності оцінки стану енергосистеми та безпечного функціонування кіберфізичної інфраструктури. Запропонований метод орієнтований на виявлення аномальних змін у часових рядах телеметрії PMU/WAMS та враховує часову залежність між послідовними вимірюваннями, що є принциповою перевагою порівняно зі статичними схемами порогового контролю.

У ході дослідження сформовано кіберфізичну модель Smart Grid, формалізовано механізм реалізації FDI-атаки в системі оцінки стану та запропоновано архітектуру LSTM-автоенкодера для аналізу часових рядів телеметричних даних. Показано, що застосування адаптивного порогу реконструкційної похибки дозволяє підвищити чутливість системи до поступових і навмисно замаскованих аномалій, які є найскладнішими для виявлення класичними методами. Експериментальну верифікацію виконано у віртуальному середовищі Smart Grid/ICS із використанням відкритого набору даних HAI та синтетичних сценаріїв FDI-атак на топології IEEE 14-Bus. Це забезпечило контрольовані умови для аналізу поведінки моделі в нормальному та атакованому режимах.

Отримані результати підтвердили ефективність запропонованого підходу. Зокрема, метод забезпечив точність виявлення FDI-атак 97,3% та F1-міру 0,961, що перевищує показники базових методів порівняння, зокрема SVM, Random Forest і класичного автоенкодера. Середній час виявлення рампової FDI-атаки становив 2,1 с за частки хибної тривоги 2,1%, що свідчить про придатність методу до задач раннього виявлення прихованих аномалій у телеметричних потоках. Важливо, що метод продемонстрував стійкість до кількох типів атакувального впливу, а саме до стрибкоподібного, поступового та рампового введення хибних значень. Результати табл. 1, а також візуальний аналіз, представлений на рис. 2–5, підтверджують перевагу LSTM-AE як за інтегральними метриками якості, так і за здатністю зменшувати кількість хибнопозитивних і хибнонегативних рішень.

Окреме значення має те, що запропонований метод не суперечить сучасним вимогам до кіберзахисту Smart Grid, сформульованим у NIST SP 800-82 Rev. 3, IEC 62351 та ISA/IEC 62443, а може розглядатися як їх алгоритмічне доповнення на рівні поведінкового моніторингу телеметрії. На відміну від сигнатурних або суто мережевих підходів, розроблений метод орієнтований на контроль цілісності саме вектора стану енергосистеми, що розширює можливості захисту в умовах IT/OT-конвергенції та ускладнення кіберфізичних загроз.

Разом із тим результати дослідження мають і певні обмеження. Експериментальна перевірка виконувалася у віртуальному середовищі, а не на повномасштабному фізичному промисловому стенді, тому подальша практична апробація в умовах реальної підстанційної або лабораторної інфраструктури залишається необхідною. Крім того, ефективність моделі залежить від наявності достатнього обсягу якісних нормальних даних для навчання, а також від стійкості самої архітектури до потенційних атак ухилення, спеціально орієнтованих на нейромережевий класифікатор.

Перспективами подальших досліджень є розширення експериментальної бази за рахунок апробації методу на реальних промислових стендах із використанням протоколів IEC 61850 та DNP3, інтеграція механізмів федеративного навчання для роботи з розподіленою телеметрією без централізованого збирання даних, а також застосування підходів XAI, зокрема SHAP і LIME, для підвищення інтерпретованості рішень моделі та довіри до неї з боку оператора. У цілому отримані результати дають підстави стверджувати, що запропонований метод є перспективним напрямом підвищення кіберстійкості Smart Grid і може бути використаний як основа для подальшого розвитку інтелектуальних засобів виявлення атак у критичній енергетичній інфраструктурі.

Список літератури (References)

1. Stouffer K., Pease M., Tang C. Y., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security. Gaithersburg, MD : National Institute of Standards and

Technology, 2023. 316 p. DOI: https://doi.org/10.6028/NIST.SP.800-82r3.
2. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 32 p. DOI: https://doi.org/10.6028/NIST.CSWP.29.
3. Stouffer K., Falco J., Scarfone K. Guide to Industrial Control Systems (ICS) Security. Gaithersburg, MD : National Institute of Standards and Technology, 2011. DOI: https://doi.org/10.6028/NIST.SP.800-82r1.
4. Pillitteri V. Y., Brewer T. L., Doxey T. W., Lichtblau A. R., Neumann M. J., Oman P. W., Whitehead D. E. Guidelines for Smart Grid Cybersecurity. Gaithersburg, MD : National Institute of Standards and Technology, 2014. 3 vols.
5. Liu Y., Ning P., Reiter M. K. False data injection attacks against state estimation in electric power grids // Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, Illinois, USA, 2009. P. 21-32. DOI: https://doi.org/10.1145/1653662.1653666.
6. Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon // IEEE Security & Privacy. 2011. Vol. 9, No. 3. P. 49-51. DOI: https://doi.org/10.1109/MSP.2011.67.
7. Liang G., Weller S. R., Zhao J., Luo F., Dong Z. Y. The 2015 Ukraine blackout: Implications for false data injection attacks // IEEE Transactions on Power Systems. 2017. Vol. 32, No. 4. P. 3317-3318. DOI: https://doi.org/10.1109/TPWRS.2016.2631891.
8. He Y., Mendis G. J., Wei J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism // IEEE Transactions on Smart Grid. 2017. Vol. 8, No. 5. P. 2505-2516. DOI: https://doi.org/10.1109/TSG.2017.2703842.
9. Liu L., Esmalifalak M., Ding Q., Emesih V. A., Han Z. Detecting false data injection attacks on power grid by sparse optimization // IEEE Transactions on Smart Grid. 2014. Vol. 5, No. 2. P. 612-621. DOI: https://doi.org/10.1109/TSG.2013.2284438.
10. Zonouz S., Rogers K. M., Berthier R., Bobba R. B., Sanders W. H., Overbye T. J. SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures // IEEE Transactions on Smart Grid. 2012. Vol. 3, No. 4. P. 1790-1799. DOI: https://doi.org/10.1109/TSG.2012.2217762.
11. He H., Yan J. Cyber-physical attacks and defences in the smart grid: a survey // IET Cyber-Physical Systems: Theory & Applications. 2016. Vol. 1, No. 1. P. 13-27. DOI: https://doi.org/10.1049/iet-cps.2016.0019.
12. Linda O., Vollmer T., Manic M. Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge // 2012 5th International Symposium on Resilient Control Systems. Salt Lake City, UT, 2012. P. 124-131. DOI: https://doi.org/10.1109/ISRCS.2012.6309292.
13. Hu Y., Yang A., Li H., Sun Y., Sun L. A survey of intrusion detection on industrial control systems // International Journal of Distributed Sensor Networks. 2018. Vol. 14, No. 8. Article 1550147718794615. DOI: https://doi.org/10.1177/1550147718794615.
14. Shin H.-K., Lee W., Yun J.-H., Min B. G. Two ICS Security Datasets and Anomaly Detection Contest on the HIL-based Augmented ICS Testbed // Proceedings of the 14th USENIX Workshop on Cyber Security Experimentation and Test. 2021. DOI: https://doi.org/10.1145/3474718.3474719.
15. Bekara C. Security issues and challenges for the IoT-based smart grid // Procedia Computer Science. 2014. Vol. 34. P. 532-537. DOI: https://doi.org/10.1016/j.procs.2014.07.064.
16. Jow J., Xiao Y., Han W. A survey of intrusion detection systems in smart grid // International Journal of Sensor Networks. 2017. Vol. 23, No. 3. P. 170-186. DOI: https://doi.org/10.1504/IJSNET.2017.083410.
17. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems // Computers & Security. 2016. Vol. 56. P. 1-27. DOI: https://doi.org/10.1016/j.cose.2015.09.009.
18. Leszczyna R. Standards on cyber security assessment of smart grid // International Journal of Critical Infrastructure Protection. 2018. Vol. 22. P. 70-89. DOI: https://doi.org/10.1016/j.ijcip.2018.05.006.
19. Qassim Q. S., Jamil N., Daud M., Patel A., Ja'affar N. A review of security assessment methodologies in industrial control systems // Information and Computer Security. 2019. Vol. 27, No. 1. P. 47-61. DOI: https://doi.org/10.1108/ICS-04-2018-0048.
20. Boeding M., Boswell K., Hempel M., Sharif H., Lopez J., Perumalla K. Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid // Energies. 2022. Vol. 15, No. 22. Article 8692. DOI: https://doi.org/10.3390/en15228692.
21. Mashima D., Chen Y., Roomi M. M., Lakshminarayana S., Chen D. Cybersecurity for Modern Smart Grid Against Emerging Threats // Foundations and Trends in Privacy and Security. 2023. Vol. 5, No. 4. P. 70-246. DOI: https://doi.org/10.1561/3300000035.

Відомості про авторів (About authors)

Магро Валерій Іванович *– кандидат технічних наук, доцент, професор кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна; ORCID: https://orcid.org/0000-0003-4238-6733; e-mail: magro.v.i@nmu.one.*

Valerii Magro *– PhD, Associate Professor, Professor, Department of Information Security and Telecommunications, Dnipro University of Technology, Dnipro, Ukraine; ORCID: https://orcid.org/0000-0003-4238-6733; e-mail: magro.v.i@nmu.one.*

Прокопович-Ткаченко Дмитро Ігорович *– кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів; старший науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»; докторант кафедри систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій; м. Дніпро / м. Київ, Україна; ORCID: https://orcid.org/0000-0002-6590-3898; e-mail: omega2417@gmail.com.*

Dmytro Prokopovych-Tkachenko *– PhD in Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies, University of Customs and Finance; Senior Research Fellow, State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"; Doctor of Science Candidate at the Department of Cybersecurity Systems and Technologies, State University of Telecommunications; Dnipro / Kyiv, Ukraine; ORCID: https://orcid.org/0000-0002-6590-3898; e-mail: omega2417@gmail.com.*

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Ольга Торстенссон *– викладач, Університет Хальмстаду, Хальмстад, Швеція; ORCID: 0009-0007-2169-6851; e-mail: olga.torstensson@hh.se.*

Olga Torstensson *– Lecturer, Halmstad University, Halmstad, Sweden; ORCID: 0009-0007-2169-6851; e-mail: olga.torstensson@hh.se.*

Черкаський Давид Олександрович *– аспірант кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна; ORCID: https://orcid.org/0009-0003-8516-6252; e-mail: Cherkaskyi.Dav.O@nmu.one.*

Davyd Cherkaskyi *– Postgraduate student, Department of Information Security and Telecommunications, Dnipro University of Technology, Dnipro, Ukraine; ORCID: https://orcid.org/0009-0003-8516-6252; e-mail: Cherkaskyi.Dav.O@nmu.one.*

Хоменко Олексій *– аспірант кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна; ORCID: 0009-0003-7675-380X; e-mail: a.khomenko2020@gmail.com.*

Oleksii Khomenko *– Postgraduate student, Department of Information Security and Telecommunications, Dnipro University of Technology, Dnipro, Ukraine; ORCID: 0009-0003-7675-380X; e-mail: a.khomenko2020@gmail.com.*

Будь ласка, посилайтесь на цю статтю наступним чином:

Магро В. І., Прокопович-Ткаченко Д. І., Торстенссон О., Черкаський Д. О., Хоменко О. Метод виявлення атак типу False Data Injection у системах оцінки стану Smart Grid на основі LSTM-автоенкодера. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 3-14. doi: 10.20998/2413-4295.2026.02.01

Please cite this article as:

Magro V., Prokopovych-Tkachenko D., Torstensson O., Cherkaskyi D., Khomenko O. A method for detecting False Data Injection attacks in Smart Grid state estimation systems based on an LSTM autoencoder. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 3–14, doi: 10.20998/2413-4295.2026.02.01.

Надійшла (received) 11.04.2026
Прийнята (accepted) 24.04.2026
Опублікована (published) 05.06.2026

УДК 004.056.5 doi: 10.20998/2413-4295.2026.02.02

АНАЛІЗ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ У АТОМНІЙ ЕНЕРГЕТИЦІ НА ОСНОВІ ОДНОКЛАСОВОГО НАВЧАННЯ

С.С. ЛИС [1*], О.М. ЛИС[1], І.О. ДЗЮБА[2]

[1]*Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», Львів, УКРАЇНА*
[2]*Інституту енергетики та систем керування, Національний університет «Львівська політехніка», Львів, УКРАЇНА*
[*]*e-mail: Lysss@ukr.net*

АНОТАЦІЯ *У роботі представлено концептуальний зсув у підходах до забезпечення кібербезпеки та технічної надійності атомних електричних станцій (АЕС). Замість традиційної реактивної класифікації відомих атак запропоновано проактивне моделювання «нормального стану» об'єкта (Normal State Recognition), яке дозволяє виявляти будь-які відхилення від фізично обґрунтованої поведінки системи. Це є актуальним з огляду на критичний дефіцит емпіричних даних про кіберінциденти в атомній енергетиці та обмеженість сигнатурних методів у протидії атакам «нульового дня». Обґрунтовано застосування методів однокласового навчання (One-Class Classification, OCC), які навчають алгоритми розпізнавати адекватну поведінку системи без потреби у великих масивах аварійних даних. Для формалізації нормального стану використано чотирьох елементну схему аналізу «режим-стан-об'єкт-взаємозв'язок», що забезпечує структуроване представлення багатовимірного простору даних. Досліджено внутрішні принципи функціонування сучасних архітектур – автоенкодерів (AE/TSAE) та Isolation Forest (iForest), здатних ідентифікувати приховані закономірності та мікроаномалії на ранніх етапах, до виникнення критичних станів.*
Ключові слова*: кіберінцидент, однокласове навчання, виявлення аномалій, пояснюваний штучний інтелект, атомна енергетика, нормальний стан роботи об'єкта, критична інфраструктура.*

ANALYSIS OF INTELLIGENT METHODS FOR DETECTING CYBER INCIDENTS IN NUCLEAR POWER ENGINEERING BASED ON ONE-CLASS LEARNING

S. LYS[1], O. LYS[1], I. DZYUBA[2]

[1]*Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv, Ukraine*
[2]*Institute of Power Engineering and Control Systems, Lviv Polytechnic National University, Lviv, Ukraine*

ABSTRACT *The paper presents a conceptual shift in approaches to ensuring cybersecurity and technical reliability of nuclear power plants (NPPs). Instead of the traditional reactive classification of known attacks, a proactive modeling of the "normal state" of an object (Normal State Recognition) is proposed, which makes it possible to detect any deviations from the physically justified behavior of the system. This is particularly relevant given the critical lack of empirical data on cyber incidents in nuclear power engineering and the limitations of signature-based methods in countering zero-day attacks. The application of one-class classification (OCC) methods is substantiated, as they train algorithms to recognize the proper system behavior without the need for large datasets of аварійних (incident/failure) data. To formalize the normal state, a four-element analysis scheme "mode–state–object–relationship" is used, providing a structured representation of a multidimensional data space. The internal principles of operation of modern architectures – autoencoders (AE/TSAE) and Isolation Forest (iForest) – are studied, as they are capable of identifying hidden patterns and micro-anomalies at early stages, before critical conditions arise.*
Keywords: *cyber incident, one-class learning, anomaly detection, explainable artificial intelligence, nuclear power engineering, normal operating state of an object, critical infrastructure.*

Вступ

Сучасна атомна енергетика перебуває на етапі інтенсивної цифрової трансформації, що супроводжується переходом від аналогових до повністю цифрових систем контролю та управління (I&C). Поєднання операційних технологій (OT) та інформаційних систем (IT) створює нові вектори загроз, включаючи ін'єкції хибних даних (FDI) та атаки типу «відмова в обслуговуванні» (DoS), які здатні маскуватися під фізичні несправності [1-7]. Традиційні системи виявлення вторгнень, засновані на сигнатурах, демонструють обмеженість у протидії атакам «нульового дня», що вимагає розробки методів, здатних ідентифікувати аномалії без попередніх знань про їхній тип. Структурна складність сучасних АЕС та ієрархія інформаційних потоків між різними рівнями управління (рис. 1) обумовлюють необхідність впровадження інтелектуальних засобів моніторингу на кожному етапі обробки даних [1-7].

У цьому контексті особливої актуальності набувають підходи, орієнтовані не на виявлення відомих шаблонів атак, а на формування цілісного уявлення про нормальне функціонування технологічного об'єкта. Така парадигма передбачає

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

побудову моделей, здатних відображати фізично узгоджену поведінку системи в умовах штатної експлуатації, що дозволяє фіксувати навіть незначні відхилення, які можуть бути індикаторами як кібернетичних впливів, так і прихованих технічних несправностей.

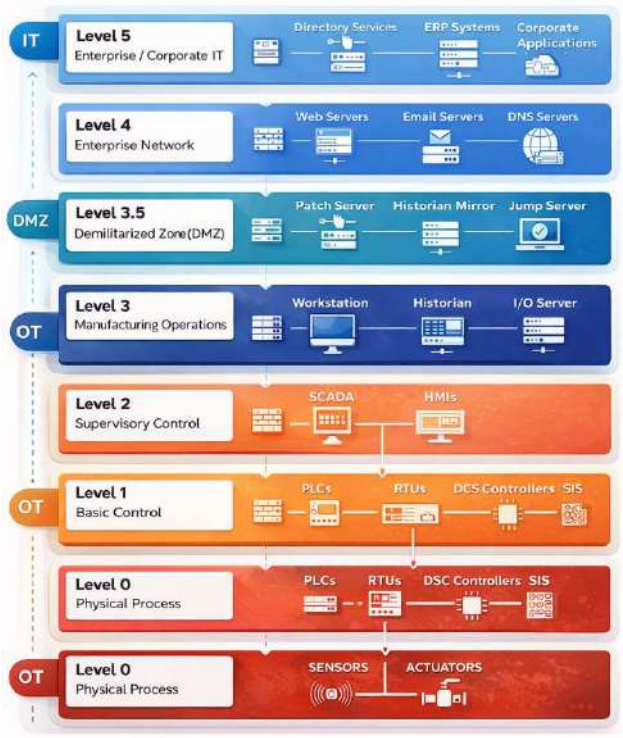


Рис. 1 – Архітектура кіберфізичної системи за моделлю Пердью.

Важливою особливістю кіберфізичних систем атомної енергетики є тісний взаємозв'язок між інформаційними сигналами та фізичними процесами. Це означає, що будь-яке втручання в інформаційний контур потенційно відображається на параметрах технологічного процесу, однак ці зміни можуть бути латентними або компенсованими системами автоматичного регулювання. У зв'язку з цим виникає потреба у методах, здатних виявляти не лише явні аномалії, але й приховані, слабовиражені відхилення у багатовимірному просторі параметрів.

Крім того, зростає значення пояснюваності прийнятих рішень, оскільки в умовах критичної інфраструктури будь-яке автоматизоване втручання має бути обґрунтованим та зрозумілим для оперативного персоналу. Це обумовлює інтеграцію підходів пояснюваного штучного інтелекту, які дозволяють інтерпретувати результати роботи моделей та встановлювати причинно-наслідкові зв'язки між виявленими аномаліями та станом системи.

Таким чином, виникає науково-практична задача розробки інтелектуальних методів виявлення кіберінцидентів, що базуються на аналізі нормального стану об'єкта, враховують багаторівневу структуру АЕС та забезпечують ранню діагностику відхилень у режимі реального часу.

Аналіз літературних джерел та постановка проблеми дослідження

Аналіз сучасних досліджень у галузі кібербезпеки на об'єктах атомної енергетики демонструє зростаючу увагу до методів машинного навчання, орієнтованих на виявлення аномалій в умовах дефіциту позначених даних.

Liu et al. [8] запропонували метод захисту ICS від адверсарних атак на основі LSTM-ED, який ефективно генерує протокольно-валідні зразки та використовує захисний механізм LSTM-FWED без попереднього знання про тип атаки, однак залишається у парадигмі реконструкційних помилок і не використовує переваг однокласового навчання, що обмежує застосовність в умовах критичного дисбалансу класів (30:1), характерного для ядерних енергетичних установок (ЯЕУ). Soomro et al. [9] надали вичерпний огляд застосування supervised learning (CNN, SVM, ANN) для діагностики корозії трубопроводів АЕС, визначивши дефіцит даних як критичну проблему та запропонувавши SMOTE, GAN і transfer learning для її вирішення, проте не розглядали методи OCC, які є природним рішенням саме у випадку відсутності аварійних даних. Dahm et al. [10] розробили XAI-фреймворк на основі RNN та модифікованого SHAP для виявлення FDI-атак у сигналах PUR-1 з точністю понад 93%, застосувавши адаптивне віконування для аналізу залишків, однак використання RNN обмежує масштабованість на надвеликих вибірках, тоді як iForest завдяки лінійній складності ефективно обробляє такі обсяги. Liu et al. [11] запропонували метод на основі DDPM із стратегією "noise-to-noise" для підвищення стійкості моделі до шуму датчиків, продемонструвавши перевагу над AE, VAE та GAN, проте не розглянули питання пояснюваності рішень, що є критичною вимогою NUREG-2261 [3].

Caixeta et al. [12] досягли точності 99,94% у прогнозуванні TRIP на основі LSTM/Transformer із 10-річними даними APS реактора Angra 2, однак їхній supervised підхід вимагає повної розмітки аварійних послідовностей, на противагу цьому OCC-метод навчається виключно на нормі та виявляє раніше невідомі відхилення. Rivas et al. [13] представили інтегровану SDP-систему (LSTM-AE + CNN + LSTM-D) для прогресивних реакторів, що виявляє аномалії за 20 секунд та прогнозує RUL за 720 секунд до порушення меж безпеки, проте модульна архітектура ускладнює масштабування, а відсутність XAI для CNN-класифікатора обмежує довіру операторів. Park et al. [14] розробили RIDA із GRU-AE, LightGBM та SHAP, застосувавши концепцію різноманітності (*diversity*) для підвищення надійності та rule-based систему для оцінки симптомів АОР, однак їхній підхід базується на supervised класифікації 16 попередньо відомих сценаріїв, тоді як iForest є unsupervised і виявляє раніше невідомі типи відхилень. Li et al. [15] підтвердили життєздатність VAE + iForest для виявлення аномалій АЕС у реальному часі (~3 мс), але відсутність XAI-інструментів обмежує можливість

операторів верифікувати фізичну природу аномалій. Натомість сучасна парадигма безпеки обґрунтовує доцільність інтеграції SHAP для кількісної атрибуції внеску сенсорів, забезпечуючи відповідність регуляторним вимогам.

Отже, виникає потреба у комплексному аналізі та систематизації зміни парадигми, замість класифікації конкретних атак система повинна навчаєтися досконало розуміти норму об’єкта, що забезпечує універсальність виявлення. Такий підхід дозволяє знаходити відхилення, спричинені як хакерським втручанням, так і природною деградацією обладнання, забезпечуючи високу надійність критичної інфраструктури.

Формалізація «нормального стану» об’єкта

Формалізація нормального стану є фундаментальним етапом у створенні надійної системи виявлення аномалій для об’єктів атомної енергетики. У роботі використано спеціалізовану чотирьохелементну схему аналізу для структурування багатовимірного простору даних:

- Режим (або mode) визначає глобальний операційний статус реактора, такий як пуск, робота на потужності або зупинка, встановлюючи фізичні межі для очікуваної поведінки сигналів.
- У межах кожного режиму система може проходити через множину валідних станів, які відповідають конкретним сукупностям умов усіх системних змінних у певний момент часу.
- Об’єкти визначаються як окремі фізичні або віртуальні одиниці системи, починаючи від датчиків нейтронного потоку і закінчуючи пакетами даних у мережевих потоках.
- Взаємозв’язок описує логічні або фізичні взаємодії між цими об’єктами, наприклад, протокольний зв’язок між програмованим логічним контролером (ПЛК) та віддаленим терміналом (див. табл. 1). Для моделювання зв'язків між об'єктами використовуються промислові протоколи, зокрема Modbus та Ethernet, які є стандартом для SCADA-систем, що використовуються на об'єктах атомної енергетики [1, 2].

Таблиця 1 – Елементи системного формалізму характеристики станів об'єктів атомної енергетики

Компонент	Фізична реалізація	Роль
Режим	Глобальний статус (пуск, робота, зупинка)	Встановлює контекст для порогів
Стан	Набір умов об'єктів та зв'язків у момент *t*	Визначає точку в просторі ознак
Об'єкт	Датчики, прилади, ПЛК, віртуальні дані	Суб'єкт прямого моніторингу
Взаємозв'язок	Ethernet, Modbus	Індикатор цілісності комунікацій

Аномалії виникають, коли внутрішня або зовнішня подія змушує систему змінити властивості об’єкта або порушити встановлені зв’язки між ними. Шляхом представлення цих компонентів у вигляді високовимірного вектора ознак, нормальний стан формує щільне скупчення даних у математичному просторі. Визначення відхилення базується на тому, чи потрапляє поточний вектор стану в межі цього заздалегідь вивченого кластера «адекватної» роботи. Представлена логіка є особливо ефективною для застосувань на об'єктах атомної енергетики, де фізичні закони, зокрема нейтронна кінетика, суворо обмежують можливі переходи між станами. Таким чином, модель вивчає не просто набір цифр, а динамічні залежності, як-от співвідношення між потужністю реактора та температурою теплоносія. Це забезпечує відповідність нормального стану фізичній реальності об’єкта та мінімізує вплив електронного шуму.

Механізм та сутність навчання алгоритмів

Основна задача дослідження – перехід до концепції навчання на основі одного класу (OCC), який дозволяє моделі ідентифікувати аномалії за принципом «не-норма», що є критично важливим для атомної енергетики, де дані про аварійні режими та кібератаки є надзвичайно дефіцитними або недоступними через міркування безпеки. Використання методів однокласового навчання забезпечує стійкість системи до раніше невідомих типів атак та поступової фізичної деградації компонентів. Механізм навчання спрямований на вилучення глибинних статистичних та фізичних кореляцій, які визначають стабільну поведінку реактора. У результаті система стає експертом у розпізнаванні здорового стану, автоматично маркуючи будь-яку невідповідність як підозрілу подію. Цей процес вимагає суворого математичного визначення меж прийнятної поведінки в багатовимірному просторі сигналів.

Побудова опису меж норми. У межах парадигми OCC навчання алгоритмів фокусується на створенні компактної описової моделі, яка оточує скупчення нормальних даних у багатовимірному просторі. На відміну від стандартних класифікаторів, які намагаються розділити два класи гіперплощиною, OCC будує замкнену межу навколо здорових точок. Процес навчання мінімізує об’єм цієї межі, одночасно гарантуючи, що максимальна кількість прикладів нормальної експлуатації потрапляє всередину. Алгоритм вивчає не лише абсолютні значення параметрів (потік нейтронів, тиск), а й складні часові залежності між ними, що формує «цифровий відбиток» норми. Якщо вектор стану системи S_i виходить за межі цієї оболонки, система констатує відхилення без потреби знати причину його виникнення. Використання ансамблевих методів, зокрема Isolation Forest (iForest) [12, 13], дозволяє цій межі бути адаптивною до різних режимів роботи –

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

аномальний бал (*anomaly score*) визначається глибиною ізоляції точки в дереві розбиттів: нормальні точки ізолюються значно глибше, ніж аномальні. Такий механізм забезпечує нульовий рівень помилкових спрацьовувань (False Positives) при правильному налаштуванні гіперпараметрів на валідаційній вибірці. Важливим аспектом є стійкість цієї межі до природних коливань інтенсивності нейтронів, які не повинні сприйматися як аномалії. Впровадження інструментів стабільності навчання гарантує, що модель не перенавчається на випадкових шумах, зберігаючи здатність до узагальнення.

Математична логіка виявлення відхилень через реконструкцію. Фундаментальним механізмом виявлення в некерованих нейронних архітектурах є аналіз похибки реконструкції (Reconstruction Error). Автоенкодери [11, 15] навчаються стискати вхідний вектор ознак X, що складається з 67 сигналів ОТ та 11 ІТ, у латентне представлення низької розмірності $h = f(X)$, а потім відновлювати його до початкового стану $\hat{X} = g(h)$. Оскільки нейронна мережа в ході навчання засвоїла виключно приклади нормальної експлуатації, вона оптимізується для ідеального відновлення саме цих патернів. У разі появи аномалії – ін'єкції хибних даних або технічної несправності – мережа не здатна ефективно реконструювати вхідний сигнал, що призводить до математичного зростання похибки E_{rec} , що розраховується як квадрат евклідової відстані між оригіналом та відновленим вектором:

$$E_{rec} = ||X - \hat{X}||^2$$

Якщо значення перевищує заздалегідь визначений статистичний поріг τ, система ініціює сигнал тривоги. Він встановлюється на основі валідаційних даних «норми» з урахуванням допустимого рівня помилкових тривог і фактично відображає верхню межу природних коливань сигналів у штатних режимах роботи. На практиці такий поріг часто визначається через статистичні характеристики похибки на нормальних даних, зокрема:

$$\tau = \mu_E + k * \sigma_E,$$

де μ_E позначає математичне сподівання похибки реконструкції, σ_E – її середньоквадратичне відхилення, а коефіцієнт k визначає поріг чутливості детектора. Використання такої статистичної оцінки дозволяє алгоритму гнучко адаптуватися до природної варіативності технологічних процесів, ефективно мінімізуючи ймовірність хибних спрацьовувань.

З програмної точки зору, принцип дії автоенкодера ґрунтується на зниженні розмірності вхідних даних із подальшим їх відновленням, що дозволяє сформувати базовий профіль нормальної роботи системи. Відповідно, похибка реконструкції виконує функцію метрики віддаленості поточного вектора стану від множини нормальних режимів. За умов штатної експлуатації значення цієї похибки прямує до мінімуму. Однак у разі виникнення аномалій порушуються приховані кореляційні зв'язки між сигналами, що спричиняє різке зростання помилки відновлення. Концептуально це можна інтерпретувати як оцінку відхилення від нормальних станів M:

$$E_{rec}(X) \approx dist(X, M)^2$$

Навчена модель неявно фіксує фізично припустимі межі функціонування ЯЕУ, детерміновані законами термодинаміки та нейтронної кінетики. Її головна перевага у здатності ідентифікувати порушення складних багатовимірних взаємозв'язків, не зосереджуючись лише амплітудні відхилення ізольованих параметрів. Що нижчим є значення E_{rec}, то вищою є ймовірність належності стану до номінального експлуатаційного профілю. Фундаментальний принцип методу візуалізовано на рисунку 2. Процес відновлення нормальних сигналів відбувається з високою точністю, тоді як поява аномалій супроводжується різким зростанням похибки, що і слугує їх тригером.

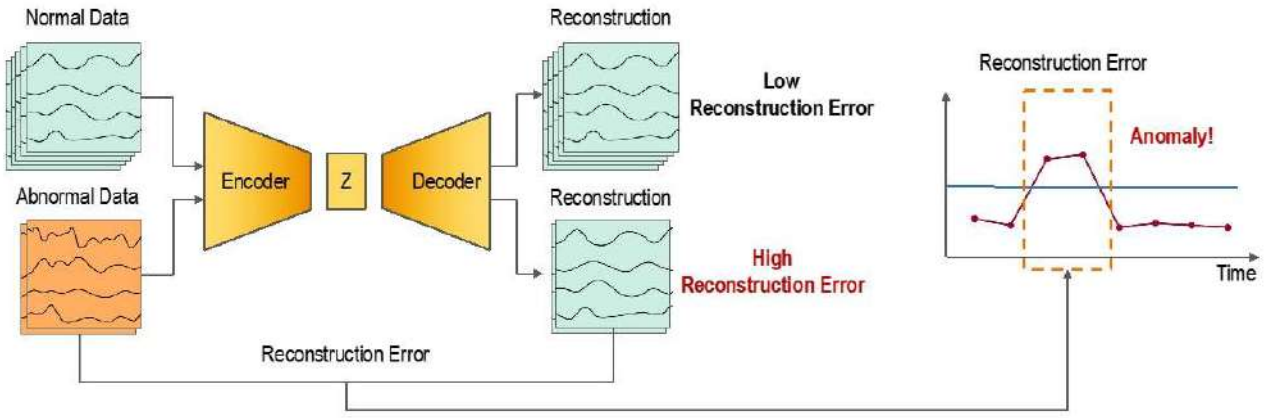


Рис. 2 – Інтерпретація моделі виявлення аномалій на основі автоенкодера.

Використання двоетапних автоенкодерів (TSAE) [7] дозволяє розділити навчання на аналіз динаміки часових рядів та аналіз відхилень, що значно підвищує чутливість до мікро-аномалій. Дана логіка дозволяє виявляти приховані тренди, які ще не досягли критичних порогів спрацювання традиційних систем захисту, забезпечуючи оператору додатковий час для прийняття рішень.

Аналіз методологій досліджень та збору даних

Проведено аналіз дослідження, виконаних на базі цифрового дослідницького реактора PUR-1 (Університет Пердью) [6, 10], які передбачали повний цикл збору даних у реальному часі, їхню попередню обробку та структурування для потреб алгоритмів машинного навчання. Було розроблено сценарій використання, що охоплює 14 різних станів системи, включаючи нормальну роботу та 13 аномальних станів різної природи. Такий підхід дозволив підтвердити здатність ШІ розпізнавати норму в умовах, максимально наближених до реальної експлуатації АЕС. Особлива увага приділялася фізичній достовірності даних та їхній відповідності законам нейтронної кінетики та термодинаміки. Зібрані дані є одними із найбільших у галузі відкритих досліджень кібербезпеки АЕС.

Параметризація та характеристика наборів даних. Для побудови репрезентативного профілю «нормального стану» було зібрано 67 багатовимірних сигналів операційних технологій (ОТ) та 11 сигналів інформаційних технологій (ІТ). ОТ-дані включають критичні фізичні показники, такі як потік нейтронів (*n*-flux), положення регулюючих стрижнів (RR position), температуру теплоносія першого контуру та напругу на магнітах приводів. ІТ-дані відображають мережеву активність між рівнями 3 та 4 архітектури, включаючи кількість пакетів на секунду, використання центрального процесора (CPU load) та мережеву затримку (Latency). Перелік сигналів і приклади даних наведено в табл. 2.

Таблиця 2 – Склад багатовимірних сигналів для навчання моделі ШІ

Параметр	Категорія (ОТ/ІТ)	Походження	Приклад даних
Потік нейтронів	ОТ (Process)	Level 0	Фізичні імпульси $(n/cm^2 \cdot s)$
Положення стрижнів	ОТ (Control)	Level 2	Дискретні кроки приводу
Пакети на секунду	ІТ (Comm)	Level 4	Мережевий трафік TCP/IP
Завантаження CPU	ІТ (Host)	Level 4	Ресурси робочої станції

Загальний обсяг «чистої норми» для навчання склав понад 13,4 мільйона точок даних для ОТ та 638,000 для ІТ, що охоплюють період експлуатації з серпня 2022 по червень 2023 року [9, 11]. Такий масштаб вибірки дозволив алгоритмам ШІ вивчити всі можливі стаціонарні коливання та допустимі перехідні процеси реактора. Дані були розподілені на навчальну, валідаційну та тестову вибірки у пропорції 60/20/20 відповідно, що є академічним стандартом для запобігання перенавчанню. Співвідношення балансу класів (*Balance Ratio*) у тестах підтримувалося на рівні 30:1 (норма до аномалії), що відображає реальний експлуатаційний дисбаланс подій. Вибір саме цих сигналів ґрунтувався на знаннях домену, відсікаючи нерелевантні параметри температуру в приміщенні чи стан системи HVAC.

Попередня обробка та робота з артефактами даних. Реальні дані ЯЕУ містять значну кількість артефактів, які за відсутності належної обробки можуть призвести до високого рівня хибнопозитивних тривог. У ході дослідження було виявлено, що випадкові викиди (*outliers*), спричинені електронним шумом датчиків [9, 11], або фізичними процесами (бульбашки на термопарі), становлять приблизно 0,0482% від загального обсягу. Окремою проблемою стали нульові значення (0,78% даних), які з'являються кластерами в режимі вимкнення через специфіку протоколів Modbus та UDP. Методологія обробки включала етап очищення від NaN-значень та нормалізацію за методом Standard Scaling для приведення всіх сигналів до єдиного масштабу. Для захоплення часових залежностей було застосовано метод «Sliding Window» з оптимальною довжиною 20 секунд та кроком в 1 секунду. Таке вікно дозволяє ШІ зафіксувати розвиток перехідного процесу, відрізняючи його від миттєвого шуму (рис. 3). Крім того, враховувалися «артефакти оператора» – варіації в сигналах, спричинені різними підходами персоналу до управління потужністю, які модель повинні сприймати як частину нормальної поведінки. Використання методів зниження розмірності через кодування в автоенкодерах дозволило зменшити вплив випадкових шумів, фокусуючи увагу алгоритму на ключових фізичних параметрах.

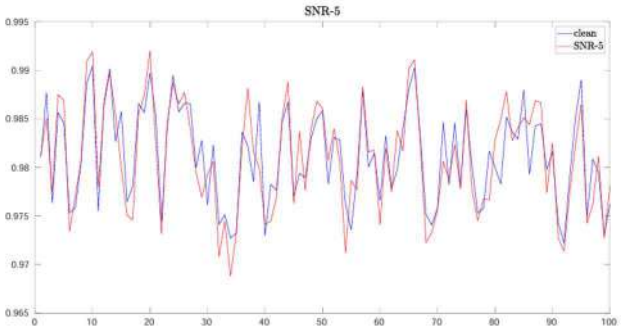


Рис. 3 – Приклади коливань даних та артефактів.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Поданий графік ілюструє приклад сигналу, змодельованого за допомогою S3K, до якого було додано шум із співвідношенням сигнал/шум (SNR-5). Синя крива представляє еталонний сигнал без артефактів, тоді як червона демонструє, як випадкові коливання впливають на форму сигналу, ускладнюючи його аналіз. Такий підхід візуалізації важливий для дослідження систем, що використовуються на об'єктах атомної енергетики, адже навіть незначний рівень шуму може спричинити помилкові спрацьовування алгоритмів виявлення аномалій. Це підкреслює необхідність застосування методів попередньої обробки даних та зниження розмірності, що допомагають виділити фізично значущі характеристики, усуваючи випадкові перешкоди.

Обговорення результатів дослідження

За результатами порівняльного аналізу чотирьох алгоритмів одноклasового навчання, представлених у таблиці 3, модель Isolation Forest продемонструвала найвищу ефективність у розпізнаванні нормального стану з показником F1-score на рівні 0,94-0,97. Ця перевага зумовлена принциповою відповідністю механізму ізоляції парадигмі OCC: алгоритм будує ансамбль бінарних дерев розбиттів виключно на нормальних даних, а аномальний бал (*anomaly score*) визначається глибиною ізоляції точки – без будь-яких міток аварійних станів. На відміну від LOF, iForest ефективно обробляє високорозмірний простір 78 сигналів із мінімальною деградацією продуктивності при варіюванні довжини вікна навчання.

Алгоритм COPOD, попри свою пояснюваність через хвостові ймовірності, демонструє знижену ефективність в умовах сильних фізичних кореляцій між параметрами реактора (нейтронний потік – температура теплоносія), оскільки спирається на припущення про незалежність маргінальних розподілів. SVDD, у свою чергу, стикається з квадратичною обчислювальною складністю при роботі з масивом понад 13,4 мільйона точок та суттєво деградує в умовах дисбалансу класів 30:1, характерного для реальної експлуатації АЕС. Важливою перевагою iForest стала його відносна пояснюваність у поєднанні з інструментами SHAP [7, 10], що дозволяє кількісно визначити внесок конкретних сенсорів у формування аномального балу та верифікувати фізичну природу відхилення. Згідно з вимогами NRC (NUREG-2261) [2] та МАГАТЕ [4, 5], така прозорість є обов'язковою умовою для впровадження ШІ у критичні функції безпеки АЕС.

Таблиця 3 – Порівняльна ефективність алгоритмів у виявленні відхилень

Алгоритм	Показник F1	Рівень XAI	Стійкість до шуму
Isolation Forest (iForest)	0.94 -0.97	Високий	Висока
LOF (Local Outlier Factor)	0.81 -0.88	Низький	Низька
COPOD (Copula-Based OD)	0.84 -0.90	Середній	Середня
SVDD (Support Vector Data Description)	0.79 -0.86	Низький	Середня

Для інтерпретації відхилень у розглянутих дослідженнях інтегровано інструменти SHAP, які кількісно оцінюють внесок кожного сенсора у формування аномального балу, та 1D Grad-CAM [14] для аналізу частотних спектрів у реконструкційних архітектурах. Ці методи забезпечують інженерний контроль над автоматизованою системою, дозволяючи персоналу підтвердити фізичну природу виявленого відхилення. Таким чином, інтегрована архітектура не лише констатує аномалію, а й надає доказову базу для подальшого прийняття рішень.

Висновок

Навчання алгоритмів виключно на нормальних станах об'єкта визначено як найбільш життєздатну стратегію для забезпечення безпеки інфраструктури об'єктів атомної енергетики. Оскільки передбачити всі можливі конфігурації майбутніх кібератак та фізичних відмов неможливо, ШІ має виступати як експерт із розпізнавання «здорової» поведінки системи. Підхід дозволяє ідентифікувати загрози «нульового дня» та складні маніпуляції з даними за фактом їхньої статистичної невідповідності еталонному розподілу. Це нівелює потребу в позначених аварійних даних, які практично відсутні в реальних умовах експлуатації АЕС.

Встановлено, що використання реконструкційних моделей, зокрема архітектури TSAE, забезпечує можливість ранньої ідентифікації аномальних трендів ще до активації традиційних систем захисту. Показано, що модель здатна виявляти ознаки аномалій за 38 хвилин до спрацювання автоматичного аварійного відключення реактора (*scram*). Це вікно часу надає операторам стратегічну перевагу для проведення керованої зупинки, що є критичним для мінімізації економічних втрат та запобігання пошкодженню дороговартісного обладнання.

Доведено, що інтеграція інструментів прозорості, таких як SHAP та 1D Grad-CAM, є обов’язковим фактором для успішного ліцензування систем ШІ, що використовуються на об'єктах атомної енергетики. Відповідно до стратегічного плану NRC США (NUREG-2261), оператор повинен чітко розуміти логіку, за якою система ініціювала сигнал тривоги. Прозорість прийняття рішень забезпечує довіру

персоналу до рекомендацій ШІ та дозволяє швидко локалізувати джерело проблеми. Відсутність XAI залишається основним бар'єром для впровадження «чорних скриньок» глибокого навчання у критичні цикли управління.

Підтверджено спроможність запропонованих алгоритмів функціонувати в умовах насиченого інформаційного фону реактора, що містить електронний шум та систематичні похибки приладів. Застосування методу «Sliding Window» тривалістю 20 секунд у поєднанні з попередньою нормалізацією дозволяє моделі ігнорувати випадкові сплески без втрати чутливості до реальних аномалій, що гарантує високу точність виявлення навіть при втраті частини мережевих пакетів під час DoS-атак.

Список літератури

1. Purdue Model For ICS Security. *Purdue Model enhances ICS security through network segmentation and defense-in-depth to safeguard critical infrastructure*. 2025.
2. Cybersecurity of Digital I&C Systems | Nuclear Regulatory Commission. *Nuclear Regulatory Commission*, January 12, 2026.
3. U.S. Nuclear Regulatory Commission. *Artificial Intelligence Strategic Plan: Fiscal Years 2023-2027* (NUREG-2261). Washington, DC, 2023.
4. International Atomic Energy Agency. Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G, Implementing Guide. Vienna: IAEA, 2021.
5. International Atomic Energy Agency. New Research Project on Computer Security For Nuclear AI. International Atomic Energy Agency | Atoms for Peace and Development. Paulina Rosol-Barrass**,** IAEA Department of Nuclear Safety and Security, 20 October 2025.
6. Purdue University / U.S. NRC. Characterization of Nuclear Cyber Security States Using Artificial Intelligence and Machine Learning. Technical Letter Report TLR-RES/DE-2024-03e. 2024.
7. Jiapeng Yang, Zuhua Jiang, TSAE: A teacher-student transformer autoencoder for restoration of fNIRS signals with channel contribution weights analysis, Advanced Engineering Informatics, Volume 72, 2026, https://doi.org/10.1016/j.aei.2026.104450.
8. Yaru Liu, Lijuan Xu, Shumian Yang, Dawei Zhao, Xin Li, Adversarial sample attacks and defenses based on LSTM-ED in industrial control systems, Computers & Security, Volume 140, 2024, https://doi.org/10.1016/j.cose.2024.103750.
9. Afzal Ahmed Soomro, Osman K. Siddiqui, Afaque Shams, Belal Almomani, Machine learning applications in nuclear power plant piping inspection: A review of methods, data, and future trends, Annals of Nuclear Energy, Volume 225, 2026, https://doi.org/10.1016/j.anucene.2025.111760.
10. Zachery Dahm, Vasileios Theos, Konstantinos Vasili, William Richards, Konstantinos Gkouliaras, Stylianos Chatzidakis, A one-class explainable AI framework for identification of non-stationary concurrent false data injections in nuclear reactor signals, Nuclear Engineering and Design, Volume 444, 2025, https://doi.org/10.1016/j.nucengdes.2025.114359.
11. Shiqiao Liu, Zifei Zhu, Xinwen Zhao, Yangguang Wang, Xiang Sun, Lei Yu, Unsupervised anomaly detection for Nuclear Power Plants based on Denoising Diffusion Probabilistic Models, Progress in Nuclear Energy, Volume 178, 2025, https://doi.org/10.1016/j.pnucene.2024.105521.
12. Bernardo M. Caixeta, Marcelo C. Santos, Alan M.M. de Lima, Victor H.C. Pinheiro, Roberto Schirru, LSTM and transformer-based approach for nuclear reactor event sequence forecasting and TRIP detection, Progress in Nuclear Energy, Volume 196, 2026, https://doi.org/10.1016/j.pnucene.2026.106354.
13. Andy Rivas, Gregory Kyriakos Delipei, Ian Davis, Satyan Bhongale, Jason Hou, A system diagnostic and prognostic framework based on deep learning for advanced reactors, Progress in Nuclear Energy, Volume 170, 2024, https://doi.org/10.1016/j.pnucene.2024.105114.
14. Ji Hun Park, Hye Seon Jo, Sang Hyun Lee, Sang Won Oh, Man Gyun Na, A reliable intelligent diagnostic assistant for nuclear power plants using explainable artificial intelligence of GRU-AE, LightGBM and SHAP, Nuclear Engineering and Technology, Volume 54, Issue 4, 2022, Pages 1271-1287,https://doi.org/10.1016/j.net.2021.10.024.
15. Xiangyu Li, Tao Huang, Kun Cheng, Zhifang Qiu, Tan Sichao, Research on anomaly detection method of nuclear power plant operation state based on unsupervised deep generative model, Annals of Nuclear Energy, Volume 167, 2022, https://doi.org/10.1016/j.anucene.2021.108785.

References

1. Purdue Model For ICS Security. *Purdue Model enhances ICS security through network segmentation and defense-in-depth to safeguard critical infrastructure*. 2025.
2. Cybersecurity of Digital I&C Systems | Nuclear Regulatory Commission. *Nuclear Regulatory Commission*, January 12, 2026.
3. U.S. Nuclear Regulatory Commission. *Artificial Intelligence Strategic Plan: Fiscal Years 2023-2027* (NUREG-2261). Washington, DC, 2023.
4. International Atomic Energy Agency. Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G, Implementing Guide. Vienna: IAEA, 2021.
5. International Atomic Energy Agency. New Research Project on Computer Security For Nuclear AI. International Atomic Energy Agency | Atoms for Peace and Development. Paulina Rosol-Barrass**,** IAEA Department of Nuclear Safety and Security, 20 October 2025.
6. Purdue University / U.S. NRC. Characterization of Nuclear Cyber Security States Using Artificial Intelligence and Machine Learning. Technical Letter Report TLR-RES/DE-2024-03e. 2024.
7. Jiapeng Yang, Zuhua Jiang, TSAE: A teacher-student transformer autoencoder for restoration of fNIRS signals with channel contribution weights analysis, Advanced Engineering Informatics, Volume 72, 2026, https://doi.org/10.1016/j.aei.2026.104450.
8. Yaru Liu, Lijuan Xu, Shumian Yang, Dawei Zhao, Xin Li, Adversarial sample attacks and defenses based on LSTM-ED in industrial control systems, Computers & Security, Volume 140, 2024, https://doi.org/10.1016/j.cose.2024.103750.
9. Afzal Ahmed Soomro, Osman K. Siddiqui, Afaque Shams, Belal Almomani, Machine learning applications in nuclear power plant piping inspection: A review of methods, data, and future trends, Annals of Nuclear Energy, Volume 225, 2026, https://doi.org/10.1016/j.anucene.2025.111760.
10. Zachery Dahm, Vasileios Theos, Konstantinos Vasili, William Richards, Konstantinos Gkouliaras, Stylianos Chatzidakis, A one-class explainable AI framework for identification of non-stationary concurrent false data

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

injections in nuclear reactor signals, Nuclear Engineering and Design, Volume 444, 2025, https://doi.org/10.1016/j.nucengdes.2025.114359.
11. Shiqiao Liu, Zifei Zhu, Xinwen Zhao, Yangguang Wang, Xiang Sun, Lei Yu, Unsupervised anomaly detection for Nuclear Power Plants based on Denoising Diffusion Probabilistic Models, Progress in Nuclear Energy, Volume 178, 2025, https://doi.org/10.1016/j.pnucene.2024.105521.
12. Bernardo M. Caixeta, Marcelo C. Santos, Alan M.M. de Lima, Victor H.C. Pinheiro, Roberto Schirru, LSTM and transformer-based approach for nuclear reactor event sequence forecasting and TRIP detection, Progress in Nuclear Energy, Volume 196, 2026, https://doi.org/10.1016/j.pnucene.2026.106354.
13. Andy Rivas, Gregory Kyriakos Delipei, Ian Davis, Satyan Bhongale, Jason Hou, A system diagnostic and prognostic framework based on deep learning for advanced reactors, Progress in Nuclear Energy, Volume 170, 2024, https://doi.org/10.1016/j.pnucene.2024.105114.
14. Ji Hun Park, Hye Seon Jo, Sang Hyun Lee, Sang Won Oh, Man Gyun Na, A reliable intelligent diagnostic assistant for nuclear power plants using explainable artificial intelligence of GRU-AE, LightGBM and SHAP, Nuclear Engineering and Technology, Volume 54, Issue 4, 2022, Pages 1271-1287,https://doi.org/10.1016/j.net.2021.10.024.
15. Xiangyu Li, Tao Huang, Kun Cheng, Zhifang Qiu, Tan Sichao, Research on anomaly detection method of nuclear power plant operation state based on unsupervised deep generative model, Annals of Nuclear Energy, Volume 167, 2022, https://doi.org/10.1016/j.anucene.2021.108785.

Відомості про авторів / About the Authors

Лис Степан Степанович – кандидат технічних наук, доцент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: lysss@ukr.net, тел.: (032) 258-23-15; ORCID: 0000-0002-7359-1177.

Stepan Lys – Assoc. Prof., Ph.D., Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: lysss@ukr.net; ORCID: 0000-0002-7359-1177.

Лис Ольга Михайлівна – студентка; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: olha.lys.kb.2024@lpnu.ua, тел.: (032) 258-23-15.

Olha Lys – student, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: olha.lys.kb.2024@lpnu.ua.

Дзюба Ігор Орестович – аспірант; Інституту енергетики та систем керування, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: ihor.o.dziuba@lpnu.ua, тел.: (032) 258-26-20.

Ihor Dzyuba – postgraduate student, Institute of Power Engineering and Control Systems, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 26 20; Email: ihor.o.dziuba@lpnu.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Лис С. С., Лис О. М., Дзюба І. О. Аналіз інтелектуальних методів виявлення кіберінцидентів у атомній енергетиці на основі однокласового навчання. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 15-22. doi: 10.20998/2413-4295.2026.02.02

Please cite this article as:

Lys S., Lys O., Dzyuba I. Analysis of intelligent methods for detecting cyber incidents in nuclear power engineering based on one-class learning. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2025, no. 2(28), pp. 15–22, doi: 10.20998/2413-4295.2026.02.02.

Надійшла (received) 23.04.2026
Прийнята (accepted) 07.05.2026
Опублікована (published) 05.06.2026

УДК 004.8-9 doi:10.20998/2413-4295.2026.02.03

ІНФОРМАЦІЙНА СИСТЕМА КЛАСИФІКАЦІЇ ДОСТОВІРНОСТІ НОВИН НА ОСНОВІ ДВОНАПРАВЛЕНИХ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ

***О. В. ЛОЗИНСЬКА*[*1], *В.А. ВИСОЦЬКА*[1], *О.О. МАРКІВ*[1]**

[1] *кафедра інформаційних систем та мереж, Національний університет «Львівська політехніка», м. Львів, Україна*
[*]*e-mail: olha.v.lozynska@lpnu.*

АНОТАЦІЯ *У роботі досліджено проблему автоматизованого виявлення дезінформації в сучасному інформаційному просторі. Запропоновано інформаційну систему аналізу новинного контенту, побудовану на основі методів машинного навчання, опрацювання природної мови та глибоких нейронних мереж. Основою системи є багатовихідна модель із використанням двонаправлених рекурентних нейронних мереж, що забезпечує врахування контексту тексту та підвищення точності класифікації. Особливістю запропонованого підходу є реалізація змагального навчання між генератором і детектором фейкового контенту, що дає змогу адаптувати систему до нових стратегій створення дезінформації. Розроблена система виконує бінарну класифікацію новин за ознакою достовірності, а також прогнозує можливого автора та джерело публікації. Для підготовки даних застосовано процедури очищення тексту, токенізації та паддінгу, а також кодування категоріальних ознак. Для реалізації програмного забезпечення використано бібліотеки TensorFlow/Keras та Gradio. Проведене експериментальне тестування підтвердило ефективність системи у виявленні як фейкових, так і достовірних новин. Результати тестування підтвердили здатність моделі розпізнавати характерні мовні ознаки фейкових і достовірних повідомлень, зокрема сенсаційність, емоційність та формальний стиль викладу. Значення метрики F1 на тестових даних становить 78 %, що свідчить про задовільну точність роботи прототипу, а середній час опрацювання запиту до 250 символів склав 2,7 секунди. Проведені експерименти також підтвердили коректність функціонування модулів попереднього опрацювання тексту, нейромережевої моделі та вебінтерфейсу користувача. Запропоноване рішення може бути використане для автоматизованого моніторингу інформаційного простору та протидії поширенню дезінформації. Подальший розвиток дослідження передбачає збільшення обсягу навчального датасету, інтеграцію системи з платформами фактчекінгу та соціальними мережами, а також вдосконалення методів мультимодального аналізу текстової й візуальної інформації.*

Ключові слова: *фейкові новини; опрацювання природної мови; машинне навчання; двонаправлена довга короткочасна пам'ять; класифікація тексту; детекція дезінформації.*

INFORMATION SYSTEM FOR CLASSIFICATION OF NEWS RELIABILITY BASED ON BIDIRECTIONAL RECURRENT NEURAL NETWORKS

***O. LOZYNSKA*[1*], *V.VYSOTSKA* [1*], *O. MARKIV*[1]**

[1] *Department of Information Systems and Networks, Lviv Polytechnic National University, Lviv, UKRAINE*

ABSTRACT *The paper investigates the problem of automated detection of disinformation in the modern information space. An information system for analyzing news content is proposed, built on machine learning, natural language processing, and deep neural networks. The system is based on a multi-output model using bidirectional recurrent neural networks of the Bidirectional LSTM type, which ensures that the text's context is taken into account and increases classification accuracy. A feature of the proposed approach is the implementation of competitive learning between the generator and the fake content detector, which allows the system to adapt to new strategies for creating disinformation. The developed system performs binary classification of news based on reliability and also predicts the possible author and publication source. Text cleaning, tokenization, and padding procedures, as well as coding of categorical features, were used to prepare the data. The TensorFlow/Keras and Gradio libraries were used to implement the software. Experimental testing confirmed the system's effectiveness in detecting both fake and reliable news. The test results confirmed the model's ability to recognize characteristic linguistic features of fake and authentic messages, in particular sensationalism, emotionality, and formal style of presentation. The F1-score on the test data is 78%, indicating satisfactory accuracy of the prototype, and the average processing time for a query up to 250 characters was 2.7 seconds. The experiments also confirmed the correct functioning of the text preprocessing modules, the neural network model, and the web user interface. The proposed solution can be used for automated monitoring of the information space and countering the spread of disinformation. Further research involves increasing the size of the training dataset, integrating the system with fact-checking platforms and social networks, and improving methods for multimodal analysis of text and visual information.*

Keywords*: fake news; natural language processing; machine learning; bidirectional long short-term memory; text classification; disinformation detection.*

Вступ

Проблема автоматичного виявлення фейкових новин і визначення їх достовірності є однією з ключових у сучасних дослідженнях з опрацювання природної мови та машинного навчання. Дані дослідження охоплюють мультимодальні підходи з використанням глибокого навчання для опрацювання не лише тексту, а й додаткових ознак (зображення,

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

метадані), що стають все актуальнішими напрямками у задачах розпізнавання дезінформації.

Згідно з науковою роботою [1], розроблено низку ефективних підходів для виявлення фейкових новин із використанням методів глибокого навчання та представлень природної мови. Автори даної праці узагальнюють дослідження і зазначають, що трансформерні архітектури демонструють значно вищі показники порівняно з традиційними методами машинного навчання завдяки здатності враховувати контекстну інформацію в тексті.

Одним із оглядових досліджень є стаття [2], яка систематизує підходи до оцінювання фейкових новин із використанням методів машинного та глибокого навчання, включаючи згорткову нейронну мережу (CNN), мережу довгої короткочасної пам'яті (LSTM), а також двонаправлену довготривалу короткочасну пам'ять (Bi-LSTM). Автори зазначають, що моделі на основі рекурентних мереж здатні враховувати довготривалі залежності у тексті, що особливо важливо для коректної класифікації новинних матеріалів у контексті семантики.

Конкретні приклади застосування двонаправленої довготривалої короткочасної пам'яті для класифікації новин представлені у роботах [3-4]. Авторами представлено інтеграцію механізмів уваги разом із Bi-LSTM, що дало змогу підвищити продуктивність для виявлення фейкових новин із показниками точності до 97,7 %.

У сфері гібридних рішень слід відзначити працю [5], яка поєднує текстові ознаки зі статистичними моделями. Авторами розроблено систему класифікації фейкових новин на основі глибокого навчання в поєднанні з методами опрацювання природної мови, яка продемонструвала високу якість класифікації у своїй реалізації.

У науковій праці [6] запропоновано використання гібридних методів, які поєднують традиційні методи представлення ознак (TF-IDF) з сучасними підходами машинного навчання. Наприклад, комбінація TF-IDF із контекстними векторними представленнями дала змогу ефективно визначати джерела та розповсюджувачів дезінформації.

Авторами наукової роботи [7] запропоновано гібридну архітектуру, яка інтегрує метрики опрацювання природної мови з класичними класифікаторами машинного навчання (логістична регресія, метод опорних векторів, наївний класифікатор Байєса) для підвищення точності виявлення фейкових новин. Дана архітектура показала високі результати на відкритих наборах даних.

У дослідженнях [8–9] наголошується, що сучасні трансформерні та мультимодальні архітектури забезпечують високу ефективність у задачах виявлення фейкових новин, однак залишаються проблеми узагальнення моделей та стійкості до контенту, згенерованого ШІ.

У статті [10] описано модель GROVER, яка поєднує генерацію та детекцію фейкових новин на основі трансформерної архітектури. GROVER – це дослідницький проєкт від Allen Institute for AI, який поєднує генерацію та детекцію фейкових новин. Даний проєкт базується на нейронній мережі для аналізу текстів, підтримує генерацію нових загроз, але не має повноцінної адаптивної системи.

Отже, сучасні наукові дослідження зосереджені на використанні глибоких рекурентних і трансформерних моделей, а також їх гібридних комбінацій з традиційними орієнтованими методами. Ці підходи дають змогу досягати високої точності класифікації фейкових новин і стають основою для подальшого розвитку систем автоматичного аналізу новинного контенту.

У науковій праці [11] наведено порівняльний аналіз ефективності детекторів контенту на основі штучного інтелекту, таких як Turnitin та Originality. Продуктивність детекторів оцінювалася за такими метриками, як повнота, F1-оцінка та точність. Згідно з наведеними результатами, обидва детектори погано спрацювали з гібридними текстами.

Дослідження [12] присвячене оцінці ефективності сучасних ШІ-детекторів та їх стійкості до модифікацій тексту.

Авторами даного дослідження розроблено прототип системи, що включає глибокий семантичний аналіз, опрацювання природної мови та моделі машинного навчання, а також елементи навчання з підкріпленням. Це робить його більш універсальним порівняно з відомими аналогами. Важливою перевагою розробленої системи є наявність змагального навчання (генератор-детектор), що дає змогу адаптуватися до нових типів фейків. GROVER частково реалізує подібний підхід. Крім того, система має вбудовані механізми безперервного навчання, та передбачає інтеграцію з динамічними базами знань та API, що є важливим для масштабування і точності. Таким чином, розроблена система має значний потенціал завдяки:

- використанню сучасних ШІ-підходів,
- мультимодальності,
- адаптивності до нових загроз,
- інтеграції з базами знань.

Водночас вона поступається аналогам у реальній масштабованості, оскільки перебуває на етапі розробки.

Мета роботи

Метою дослідження є розроблення методу, який здатен ефективно виявляти складні фейки та адаптуватися до нових стратегій генерації дезінформації. Для вирішення цього завдання потрібно: провести аналіз відомих методів та підходів виявлення дезінформації; застосувати модель на основі двонаправлених рекурентних нейронних мереж типу Bidirectional LSTM; розробити систему,

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

яка буде здійснювати бінарну класифікацію достовірності новини (Fake/Real), передбачення автора та визначення джерела публікації.

Виклад основного матеріалу

Інформаційна система класифікації достовірності новин

Ключовим інноваційним рішенням є розроблення системи, що включає два взаємодіючі компоненти: генератор та детектор. Генератор цілеспрямовано створює складні фейкові матеріали, які імітують характеристики реальної дезінформації та експлуатують відомі слабкості детекторів. Детектор, використовуючи передові методи опрацювання природної мови, машинного навчання, інтеграцію з базами фактчекінгу та спеціалізовані моделі для виявлення ШІ-контенту, навчається ідентифікувати ці складні фейки. Центральним елементом системи є змагальна петля (adversarial loop), де генератор і детектор постійно «змагаються» та навчаються на результатах взаємодії, що призводить до безперервного вдосконалення обох компонентів. Проведені експерименти демонструють функціональність системи у визначенні достовірності новин з високою точністю.

Розроблене програмне забезпечення орієнтоване на аналіз текстового контенту новин із метою визначення їхньої достовірності, а також прогнозування можливого автора та джерела публікації. Основою системи є модель глибокого навчання, реалізована із застосуванням бібліотеки TensorFlow/Keras.

Архітектура системи складається з двох основних компонентів (рис. 1): модуля машинного навчання та інтерактивного вебзастосунку. Модуль машинного навчання реалізує повний цикл опрацювання даних, що включає очищення тексту, токенізацію, нормалізацію довжини послідовностей та кодування категоріальних ознак. Для обмеження розмірності простору авторів і джерел застосовано підхід виділення найбільш частотних категорій із віднесенням інших до узагальнених класів.

Модуль машинного навчання використовує модель, побудовану у вигляді багатовихідної нейронної мережі, яка містить шар векторного представлення слів, двонаправлені шари довгої короткочасної пам'яті для врахування контексту, а також повнозв’язні шари для кожного із завдань класифікації (вихід для мітки, вихід для автора, вихід для джерела). Для запобігання перенавчанню було застосовано регуляризацію за допомогою шару проріджування (Dropout).

Навчання моделі здійснюється із використанням оптимізатора Adam та відповідних функцій втрат для кожного типу задачі. Вагові коефіцієнти дають змогу регулювати важливість окремих підзадач у процесі оптимізації.

Інтерактивний веб-додаток забезпечує взаємодію користувача із системою. Він реалізує завантаження навченої моделі та допоміжних компонентів, опрацювання введеного тексту, формування передбачень і відображення результатів. Інтерфейс створено з використанням бібліотеки Gradio, що забезпечує простоту використання та швидкий доступ до функціоналу системи.

.

Рис. 1 – Архітектура системи визначення достовірності новини

Під час запуску веб-додатка здійснюється завантаження збереженої моделі машинного навчання та допоміжних об’єктів попереднього опрацювання даних. Це забезпечує готовність системи до виконання аналізу текстових даних без необхідності повторного навчання моделі.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Попереднє опрацювання вхідного тексту реалізовано спеціальною функцією, яка виконує очищення текстових даних відповідно до процедури, застосованої на етапі навчання моделі. Зокрема, текст переводиться до нижнього регістру, після чого видаляються символи, що не належать до літер латинського або кириличного алфавіту, цифр чи пробілів.

Після очищення тексту виконується токенізація тексту та доповнення послідовностей до однакової довжини, після чого підготовлені дані передаються до навченої нейромережевої моделі. Отримані результати аналізуються окремо для кожного завдання класифікації. Для визначення достовірності новини здійснюється бінарна класифікація за мітками «Fake» або «Real» залежно від значення ймовірності клас ("Real" якщо ймовірність > 0.5, інакше "Fake"). Додатково обчислюється рівень впевненості моделі у прийнятому рішенні. Для прогнозування автора та джерела публікації використовується вибір класу з максимальною ймовірністю за допомогою спеціальної функції та відповідних енкодерів категорій, після чого також визначається рівень впевненості передбачення.

Проведене тестування на контрольних прикладах показало, що система здатна ефективно розрізняти фейкові та достовірні новини. Зокрема, тексти з ознаками сенсаційності та неправдоподібності класифікуються як фейкові з високим рівнем впевненості, тоді як формалізовані повідомлення офіційного характеру визначаються як достовірні. Передбачення автора та джерела залежать від представленості відповідних категорій у навчальній вибірці, що зумовлює появу узагальнених класів у випадках невизначеності.

Таким чином, розроблена система демонструє здатність до комплексного аналізу новинного контенту, забезпечуючи не лише визначення достовірності інформації, а й додаткову аналітику щодо її походження, що є важливим для протидії поширенню дезінформації в сучасному інформаційному просторі.

Обговорення результатів

Для перевірки працездатності розробленого програмного забезпечення було проведено серію експериментів із використанням контрольних прикладів текстів новин різного типу. Отримані результати підтвердили здатність системи ефективно виконувати класифікацію новин за критерієм достовірності, а також здійснювати прогнозування ймовірного автора та джерела публікації.

У першому контрольному прикладі система аналізувала новину із вираженими ознаками дезінформації: «Сенсація! Вчені виявили, що коти таємно правлять світом через інтернет-меми». За результатами аналізу новину було класифіковано як фейкову з рівнем впевненості 90,24 %. Водночас модель визначила автора та джерело як Other_Author і Other_Source із відносно низькими показниками впевненості – 35,60 % та 40,22 % відповідно. Такий результат є очікуваним, оскільки подібні сенсаційні повідомлення зазвичай не мають чітко ідентифікованого автора або офіційного джерела. Висока точність класифікації свідчить про здатність моделі розпізнавати характерні мовні патерни фейкових новин, зокрема сенсаційність, емоційність та абсурдність тверджень. Відносно, низька впевненість для автора та джерела (напр., 30–40%) також підтверджує, що модель не знайшла явних ознак відомого їй автора/джерела.

Другий приклад містив текст офіційного характеру: «Міністерство фінансів оголосило про нові податкові пільги для малого бізнесу, що почнуть діяти з наступного кварталу». Система класифікувала новину як достовірну з рівнем впевненості 88,70 %. Передбачення автора та джерела також були віднесені до категорій Other_Author та Other_Source, однак із дещо вищими рівнями впевненості — 55,10 % та 65,40 % відповідно. Отримані результати демонструють, що модель успішно розпізнає ознаки офіційного стилю викладу, характерного для реальних інформаційних повідомлень, зокрема формальну лексику, нейтральний тон та наявність конкретної державної установи.

Проведені експерименти підтвердили коректність функціонування всіх основних компонентів системи: модуля попереднього опрацювання тексту, механізму токенізації, нейромережевої моделі класифікації та веб-інтерфейсу користувача. Застосування багатовихідної архітектури дало змогу не лише визначати достовірність новини, а й додатково оцінювати потенційного автора та джерело публікації, що підвищує інформативність результатів аналізу.

Для визначення оцінки точності детектора проведено розрахунок метрики F1, який на тестових даних становить 78%, що відповідає задовільному рівню для прототипу. Середній час відповіді демонстраційного інтерфейсу (продуктивність) на запит довжиною до 250 символів становить 2,7 секунди, що є відмінним показником для прототипу. Також оцінено зручність використання інтерфейсу та базові аспекти безпеки на рівні файлів моделі прототипу.

Водночас результати дослідження засвідчили, що точність прогнозування автора та джерела значною мірою залежить від наповнення навчальної вибірки та кількості представлених у ній категорій. Використання узагальнених категорій Other_Author та Other_Source свідчить про необхідність розширення датасету та збільшення кількості прикладів для рідкісних джерел і авторів. Попри це, система продемонструвала достатній рівень ефективності у виконанні основного завдання – автоматизованого виявлення фейкових новин.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Висновки

У результаті проведеного дослідження розроблено та протестовано інформаційну систему аналізу новинного контенту, призначену для автоматизованого виявлення фейкових новин, а також прогнозування ймовірного автора та джерела публікації. Запропонований підхід базується на використанні сучасних методів опрацювання природної мови та нейромережевих моделей глибокого навчання, що забезпечують ефективну класифікацію текстових даних.

У межах роботи було реалізовано багатовихідну архітектуру нейронної мережі із застосуванням шарів векторного представлення, двонаправленої довготривалої короткочасної пам'яті та шарів проріджування, що дало змогу одночасно виконувати кілька задач аналізу тексту. Для забезпечення роботи системи було створено інтерактивний веб-додаток на основі бібліотеки Gradio, який надає користувачу можливість здійснювати аналіз новин у зручному форматі.

Результати експериментального тестування підтвердили працездатність розробленого програмного забезпечення. Система успішно класифікувала контрольні приклади новин із високими показниками впевненості, коректно розрізняючи достовірний та фейковий контент. Найкращі результати були отримані для новин із вираженими ознаками дезінформації та клікбейтного стилю, що свідчить про здатність моделі виявляти характерні мовні патерни фейкових повідомлень.

Додатковою перевагою запропонованого підходу є використання оцінки впевненості моделі, що підвищує інтерпретованість результатів та дає змогу користувачеві оцінити надійність отриманих прогнозів. Водночас дослідження показало, що точність визначення автора та джерела значною мірою залежить від обсягу та репрезентативності навчальної вибірки.

До основних обмежень роботи системи належать невеликий розмір датасету, обмежена кількість категорій авторів і джерел, а також відсутність спеціалізованого донавчання моделі. Перспективами подальших досліджень є розширення навчальної вибірки, інтеграція системи із зовнішніми платформами фактчекінгу та соціальними мережами, а також удосконалення механізмів мультимодального аналізу текстового та візуального контенту.

Отже, отримані результати підтверджують доцільність використання методів машинного навчання та технологій опрацювання природної мови для автоматизованого виявлення дезінформації й створюють основу для подальшого розвитку інтелектуальних систем протидії фейковим новинам.

Список літератури

1. Alnabhan M. Q., Branco P. Fake News Detection Using Deep Learning: Systematic Literature Review. *IEEE Access*. 2024. Vol. 12. P. 114435-114459. doi: 10.1109/ACCESS.2024.3435497.
2. Padalko H., Chomko V., Chumachenko D. A novel approach to fake news classification using LSTM-based deep learning models. *Frontiers in Big Data*. 2024. Vol. 6. P. 1320800. doi:10.3389/fdata.2023.1320800.
3. Alghamdi J., Luo S., Lin Y. A comprehensive survey on machine learning approaches for fake news detection. *Multimedia Tools and Applications.* 2023. Vol. 8. P.1-59. doi:10.1007/s11042-023-17470-8.
4. Ahmad I., Yousaf M., Yousaf S., Ahmad M. Fake news detection using machine learning ensemble methods. *Complexity.* 2020. Vol. 5. P. 1–11. doi:10.1155/2020/8885861.
5. Nadeem M., Abbas P., Zhang W., Rafique S., Iqbal S. (). Enhancing Fake News Detection with a Hybrid NLP-Machine Learning Framework. *IECE Transactions on Intelligent Systematics*. 2024. Vol. 1. P. 203-214. doi:10.62762/TIS.2024.461943.
6. Lozynska O., Vysotska V., Markiv O. Identifying Sources and Participants of Propaganda in TikTok Using Machine Learning. *Central Ukrainian Scientific Bulletin Technical Sciences.* 2025. Vol. 12(43). P. 90-98. doi:10.32515/2664-262X.2025.12(43).1.90-98.
7. Vysotska V., Nazarkevych M., Vladov S., Lozynska O., Markiv O., Romanchuk R., Danylyk V. Devising a method for detecting information threats in the Ukrainian cyber space based on machine learning. *Східно-Європейський журнал передових технологій*. 2024. № 6/2(132). P. 36–48.
8. Sabarmathi K.R., Gowthami K., Sanjay S. Fake news detection using machine learning and Natural Language Inference (NLI). *IOP Conference Series: Materials Science and Engineering.* 2021. 1084. 012018. Doi: 10.1088/1757-899X/1084/1/012018.
9. Dongre A. K., Kalaiarasi G. A Survey on Fake News Detection Using Multivariate Feature Selection and Hybrid Deep Learning Approach. *1st International Conference on AIML-Applications for Engineering & Technology (ICAET)*, Pune, India. 2025. P. 1-9. doi: 10.1109/ICAET63349.2025.10932142.
10. Zellers R., Holtzman A., Rashkin H., et al. Defending Against Neural Fake News. arXiv. 2019. doi:0.48550/arXiv.1905.126.
11. Hadra M., Cambridge K., Mesbah M. Evaluating the Accuracy and Reliability of AI Content Detectors in Academic Contexts. *Int J Educ Integr*. 2026. Vol. 22, 4. doi:10.21203/rs.3.rs-7359956/v1.
12. Makhmutova A., Sharimbayev B., Amirzhanov A., Shalkarbay-uly A. Testing the Limits: Evaluating AI Detectors' Accuracy and the Impact of Obfuscation Techniques on AI-Generated Text. *Journal of Advances in Information Technology*. 2026. Vol. 17. P. 438-449. doi:10.12720/jait.17.3.438-449.

References (transliterated)

1. Alnabhan M. Q., Branco P. Fake News Detection Using Deep Learning: Systematic Literature Review. *IEEE Access*, 2024, Vol. 12, pp. 114435-114459, doi: 10.1109/ACCESS.2024.3435497.
2. Padalko H., Chomko V., Chumachenko D. A novel approach to fake news classification using LSTM-based deep learning models. *Frontiers in Big Data*, 2024, Vol. 6, pp. 1320800, doi:10.3389/fdata.2023.1320800.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

3. Alghamdi J., Luo S., Lin Y. A comprehensive survey on machine learning approaches for fake news detection. *Multimedia Tools and Applications*, 2023, Vol. 8, pp.1-59, doi:10.1007/s11042-023-17470-8.
4. Ahmad I., Yousaf M., Yousaf S., Ahmad M. Fake news detection using machine learning ensemble methods. *Complexity,* 2020, Vol. 5, pp. 1–11, DOI:10.1155/2020/8885861.
5. Nadeem M., Abbas P., Zhang W., Rafique S., Iqbal S. (). Enhancing Fake News Detection with a Hybrid NLP-Machine Learning Framework. *IECE Transactions on Intelligent Systematics*, 2024, Vol. 1, pp. 203-214, doi:10.62762/TIS.2024.461943.
6. Lozynska O., Vysotska V., Markiv O. Identifying Sources and Participants of Propaganda in TikTok Using Machine Learning. *Central Ukrainian Scientific Bulletin Technical Sciences*, 2025, Vol. 12(43), pp. 90-98, doi:10.32515/2664-262X.2025.12(43).1.90-98.
7. Vysotska V., Nazarkevych M., Vladov S., Lozynska O., Markiv O., Romanchuk R., Danylyk V. Devising a method for detecting information threats in the Ukrainian cyber space based on machine learning. *Eastern-European Journal of Enterprise Technologies*, 2024, Vol. 6/2(132), pp. 36–48.
8. Sabarmathi K.R, Gowthami K., Sanjay S. Fake news detection using machine learning and Natural Language Inference (NLI). *IOP Conference Series: Materials Science and Engineering,* 2021, 1084, 012018, doi: 10.1088/1757-899X/1084/1/012018.
9. Dongre A. K., Kalaiarasi G. A Survey on Fake News Detection Using Multivariate Feature Selection and Hybrid Deep Learning Approach. 1st International Conference on AIML-Applications for Engineering & Technology (ICAET), Pune, India, 2025, pp. 1-9, doi: 10.1109/ICAET63349.2025.10932142.
10. Zellers R., Holtzman A., Rashkin H., et al. Defending Against Neural Fake News. arXiv, 2019, doi:0.48550/arXiv.1905.126.
11. Hadra M., Cambridge K., Mesbah M. Evaluating the Accuracy and Reliability of AI Content Detectors in Academic Contexts. Int J Educ Integr, 2026, Vol. 22, 4, doi:10.21203/rs.3.rs-7359956/v1.
12. Makhmutova A., Sharimbayev B., Amirzhanov A., Shalkarbay-uly A. Testing the Limits: Evaluating AI Detectors' Accuracy and the Impact of Obfuscation Techniques on AI-Generated Text. Journal of Advances in Information Technology, 2026, Vol. 17, pp. 438-449, doi:10.12720/jait.17.3.438-449.

Відомості про авторів (About authors)

Лозинська Ольга Володимирівна – кандидат технічних наук, доцент, доцент кафедри інформаційних систем та мереж, Національний університет "Львівська політехніка"; Львів, Україна; ORCID: 0000-0002-5079-0544; e-mail: olha.v.lozynska@lpnu.ua.

Lozynska Olga – Candidate of Technical Sciences (Ph. D.), Docent, Docent of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine; ORCID: 0000-0002-5079-0544; e-mail: olha.v.lozynska@lpnu.ua.

Висоцька Вікторія Анатоліївна – доктор технічних наук, доцент, професор кафедри інформаційних систем та мереж, Національний університет "Львівська політехніка"; Львів, Україна; ORCID: 0000-0001-6417-3689; e-mail: victoria.a.vysotska@lpnu.ua.

Vysotska Victoria – Doctor of Technical Sciences, Docent, Professor of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine; ORCID: 0000-0001-6417-3689; e-mail: victoria.a.vysotska@lpnu.ua.

Марків Оксана Олександрівна – кандидат технічних наук, доцент, доцент кафедри інформаційних систем та мереж, Національний університет "Львівська політехніка"; Львів, Україна; ORCID: 0000-0002-1691-1357; e-mail: oksana.o.markiv@lpnu.ua.

Markiv Oksana – Candidate of Technical Sciences (Ph. D.), Docent, Docent of Information Systems and Networks Department, Lviv Polytechnic National University, Lviv, Ukraine; ORCID: 0000-0002-1691-1357; e-mail: oksana.o.markiv@lpnu.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Лозинська О.В., Висоцька В. А., Марків О.О. Інформаційна система класифікації достовірності новин на основі двонаправлених рекурентних нейронних мереж. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 23-28. doi:10.20998/2413-4295.2026.02.03.

Please cite this article as:

Lozynska O., Vysotska V., Markiv O. Information system for classification of news reliability based on bidirectional recurrent neural networks. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 23–28, doi:10.20998/2413-4295.2026.02.03.

Надійшла (received) 26.05.2026
Прийнята (accepted) 28.05.2026
Опублікована (published) 05.06.2026

UDC 004.6: 005.3 doi:10.20998/2413-4295.2026.02.04

ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ДАНИХ ДЛЯ ЗРОСТАННЯ IT-БІЗНЕСУ

І. К. ДЕРЕТЮК*[1], М. М. КОЗУЛЯ[2]

[1] кафедра кафедри програмної інженерії та інтелектуальних технологій управління, НТУ «ХПІ» м. Харків, Україна
[2] кафедра кафедри програмної інженерії та інтелектуальних технологій управління, НТУ «ХПІ» м. Харків, Україна
**e-mail: Illia.Deretiuk@cs.khpi.edu.ua*

АНОТАЦІЯ *Сьогодні рішення, що ґрунтуються на даних, стають дедалі необхіднішими, якщо не суттєвими, у сучасному бізнес-світі. У цій статті багатогранне поняття прийняття рішень на основі даних (DDDM) в IT розглядається з точки зору теоретичних основ, прикладної спрямованості та потенційних переваг. Розглянуто необхыдны для дослыдження основи методів, керованих даними, описано, як використовувати технологічні інструменти для розробки та підтримки додатків, керованих даними, включаючи сховища даних, інтеграцію даних та аналіз даних. Особливий акцент робиться на організаційних змінах, необхідних для безперешкодного впровадження культури, керованої даними: зміна поведінки лідерства, підвищення кваліфікації співробітників та реінжиніринг бізнес-процесів. У статті також розглянуто різні проблеми впровадження DDDM, включаючи проблеми якості даних, проблеми інтеграції технологій та опір культурі змін. Аналіз демонструє, як компанії будь-якого розміру та сфер діяльності можуть використовувати аналітику даних для оптимізації бізнес-процесів, кращого управління клієнтами та стимулювання зростання продажів. В заключному розділі статті пыдсумовано ключові висновки дослідження, а також рекомендації для організацій, які прагнуть покращити свої аналітичні можливості в надії вижити в умовах дедалі більш цифрового конкурентного середовища.*
Ключові слова: *прийняття рішень на основі даних; бізнес-аналітика; аналітика даних; організаційна трансформація; управління IT*

DATA-DRIVEN DECISION MAKING FOR IT BUSINESS GROWTH

I. DERETIUK [1*], M. KOZULIA[2]

[1] Department of Software Engineering and Management Intelligent Technologies, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2] Department of Software Engineering and Management Intelligent Technologies, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

ABSTRACT *Today the decisions that are underpinned by data are becoming more necessary, if not essential, in today's business world. In this article the multi-faceted notion of data-driven decision-making (DDDM) in IT is discussed in terms of theoretical foundations, an application focus, and potential benefits. The foundation of data-driven methods required for research is discussed, and how to use technology tools to develop and support data-driven applications, including data warehouses, data integration, and data analytics, is described. Special emphasis is placed on organizational change necessary for the seamless adoption of a data-driven culture: leadership behavior change, employee skillbuilding and business process re-engineering. The article also discusses the various DDDM implementation challenges, including data quality issues, technology integration issues, and change cultural resistance. The analysis demonstrates how companies of all sizes and domains can utilize data analytics to streamline business processes, manage customers better, and stimulate sales growth. We summarize the study's key findings in the final section of the paper, as well as recommendations for organizations in their quest to improve their analytics capacity in hopes of surviving in an increasingly digital competitive environment.*
Keywords*: data-driven decision making; business intelligence; data analytics; organizational transformation; IT management*

Introduction

The globally transforming industries pressurized by digital technologies significantly altered the nature of organization and competition. In this era, data has evolved to be one of the most important strategic assets for contemporary businesses, particularly the IT enterprises. Data-Driven Decision Making (DDDM) is a buzzword that describes a philosophical change that is occurring in the business world from old-fashioned, gut-based, decision making techniques to more quantitative, empirical, evidence-based, data-driven approaches. This change is an indication that there is an increasing awareness that in a climate of rising market turbulence and technological disruption, organizations can no longer afford to depend on historical precedent or the experience of senior executives to make critical business calls.

Several concurrent business and technological trends further underscore the value of DDDM. First, organizations are experiencing exponential increases in available data (commonly known as "big data"), which represents both opportunity and challenge for organizations. New industry projections estimate the global data sphere will expand to 186 zettabytes by 2025, with a compound annual growth rate of nearly 27% over 2020. This explosion of data, when tapped into effectively, can offer unparalleled visibility into customer

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

behavior, operational effectiveness, and market factors [1].

Second, analytic tools have come a long way to enable organizations to analyze and interpret intricate sets of data. These days many business intelligence platforms, machine learning libraries, and data visualization tools have opened up access to advanced analytics capabilities that were once only within reach of large enterprises with substantial IT budgets. These technological advances have reduced the barriers to adoption of data-enabled methods and raised the competitive bar for data usage in all sectors of the economy.

The third is that the COVID-19 pandemic has served as a forcing function for digital acceleration, with companies being forced to scramble to adjust to such shocks as remote delivery of services, evolving consumer demand and impaired supply chains. This time of rapid transformation has underscored the importance of real-time data analytics and agile decision-making processes, and many organizations have reported that their abilities to react and predict with data were crucial in enabling them to effectively weather the storm.

Within the IT sector specifically, the adoption of DDDM practices has become particularly crucial due to several industry-specific factors. The rapid pace of technological innovation creates constant pressure to identify and capitalize on emerging opportunities while avoiding obsolete technologies. The project-based nature of much IT work requires precise estimation of timelines, resources, and costs. Additionally, the knowledge-intensive character of IT services means that human capital decisions - from hiring to professional development - can significantly impact organizational performance.

Despite these compelling reasons for adoption, many IT companies continue to struggle with implementing effective DDDM strategies. Common barriers include data silos within organizations, lack of analytical skills among employees, cultural resistance to data-centric approaches, and difficulties in integrating new analytical tools with legacy systems. Moreover, the sheer volume and variety of available data can lead to "analysis paralysis," where decision-makers become overwhelmed by information rather than empowered by it. All the problems for integrating DDDM are mentioned on Fig.1.

Theoretical Foundations of Data-Driven Decision Making

The notion of organizations embracing evidence-based decision making has roots in multiple academic disciplines and theoretical traditions. Its insight adds useful background in relation to current DDDM practices and it can also be used to explain why DDDM has becoming popular recently [2].

One of the early antecedents to the current form of DDDM is found in the scientific management school developed by Frederick Taylor in the early 1900s. Taylor's theory of systematic observation, measurement, and analysis of work performance created the concept of making management decisions based on reality, factors that can be quantified, rather than gut feelings and selective memory. Although Taylor's approach was first used in manufacturing, the broader case for cutting an empirical path has colored subsequent management theories in a variety of contexts. Quantitative techniques in business.

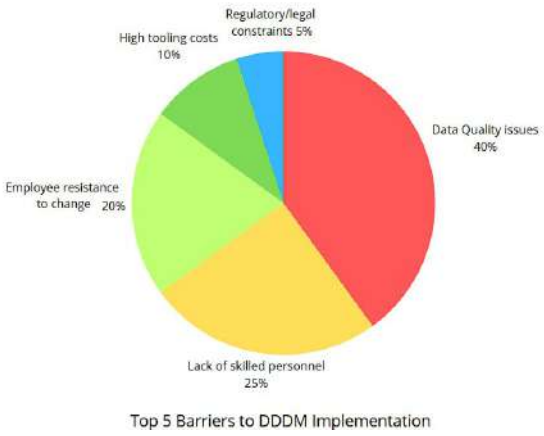


Fig. 1. – Top 5 obstacles for DDDM integration

During mid-20th century or development of operations research and management science and its application of quantitative approach to problems of decisions making in organization. These fields brought in advanced mathematical modeling techniques around optimization, forecasting, and resource allocation - many of which are still among the core of modern analytics practice. Herbert Simon's early studies of bounded rationality and satisficing behavior informed this work and emphasized the way decision processes can be enhanced through improved information and analysis. The concept of the quality management system began to emerge in the 1950s and the 1960s, notably with the work done by Feigenbaum. Feigenbaum's 1951 book, Quality Control: Principles, Practice, and Administration, emphasized the importance of quality control in the business world: The Quality Control Program, which calls for continuous measurement and action, was developed in 1949 by W. Edwards Deming. The Plan-Do-Check-Act cycle espoused by Deming has cemented the practice using performance data to guide iterative improvement in quality and productivity. The ideas were eventually refactored, re-tested, & further proven by Six Sigma methodology which brought about more heavy-weight statistical methods for process monitoring and improvement [3].

The business intelligence revolution that crystallized as its own industry sector in the 1990s was an important part of the evolution toward DDDM. Early provisions of BI systems have been centered around backward-looking reporting and descriptive analytics offerings managers the ability to have a historical snap

shot view of how an organization was performing. Though limited by today's standards, these systems were an important early step toward greater discipline in the use of data in decision-making. Thus, the theoretical landscape of DDDM has expanded further in the 21st century, shaped by a number of interrelated developments.

The revolution in big data has challenged traditional ideas of how data should be managed and analyzed – new methods are needed to cope with the scale, pace, and diversity of sources now available. "In parallel, machine learning and AI have made possible new categories of advanced predictive and prescriptive analytics, beyond the simple descriptive reporting that was once the standard, to actually prescribing the most optimal actions," Hayes said.

From the cognitive point of view, behavioral economics research has clarified how evidence-based methods can be used to counter decision biases. Daniel Kahneman and other work has shown that human judgement is easily swayed by systematic biases and heuristics that statistical thinking can mitigate. This study offers good theoretical support for DDDM as a promising solution to becoming better informed with decision results.

At an organizational level, theory, such as resource-based view (RBV), has put forward that the capacity of a firm to capture, analyze and act on data might be a valuable, rare, inimitable resource serving to support a competitive advantage. This theoretical approach contributes to explaining why some organizations are more successful in exploiting their data assets than others and emphasizes the need to build organizational capabilities in data analysis and data interpretation [4].

Adoption of DDDM practices in organizations can also be explained through the diffusion of innovations theory. This theory explains why some organizations adopt data-driven approaches earlier than others and provides insight into the key factors driving the decision to adopt, factors such as perceived benefits, compatibility and organizational readiness. With specific reference to IT firms, several other theoretical viewpoints are particularly applicable.

DDDM for IT business development demonstrates a shift from intuitive approaches to evidence-based strategic management and deep analytics [5]. In the modern era of digital transformation, DDDM is seen not just as a competitive advantage, but as a critical condition for business survival [5–7].

The technology acceptance model (TAM) sheds light on why IT professionals perceive and offer support for analytical tools, and sociotechnical systems theory offers guidelines for integrating technical systems with organizational structure and processes. This is where the dynamic capabilities framework can be useful as an aid for understanding how IT firms may apply data-based methods for sensing and responding to fast-paced changes in their markets. These combined theories will help to provide a strong conceptual framework for understanding the DDDM principles and practices in IT organizations. They show that evidence-based models aren't so much a set of technical tools as a holistic management mindset grounded in a tromp through some of the most influential literature in a variety of fields of inquiry. This dose of theoretical depth is why DDDM has been able to provide so much value across a wide variety of organizational contexts and why it is expected to become more important as technologies evolve.

The fundamental basis of DDDM is the transformation of raw data into knowledge through a hierarchy of levels of abstraction [5]. Researchers identify four key types of analytics that form the intellectual basis for decision-making:

1 Descriptive: analyzing historical data to understand past events [7].

2 Diagnostic: identifying cause-and-effect relationships and patterns [7].

3 Predictive: using statistical models and machine learning to predict future outcomes [7].

4 Prescriptive: suggesting specific actions based on predictive insights to optimize outcomes [7].

For effective implementation of DDDM, a powerful data storage and processing base is required. Current research emphasizes the role of modern database systems, such as RDBMS for structured data, NoSQL for the flexibility and scale of "big data", as well as NewSQL, which combine the best of both worlds [8].

Management accounting in IT companies is evolving towards creating an information field for monitoring costs and efficiency of business processes in real time [9]. The use of Process Mining methods allows for automated analysis of bottlenecks in the development (SDLC), marketing and technical support processes [9].

Research confirms the direct impact of analytics on the excellence of IT project management, in particular through the following indicators [9-10]:

- Return on investment (ROI): maximizing financial returns.
- Budget compliance: controlling cost overruns through predictive risk analytics.
- Resource utilization: optimizing the allocation of human and technical capacities.

Discussion of results

Enabling data-driven decision making in IT organizations, however, demands a strong technological backbone to serve different analytical needs. This infrastructure enables the collection, storage, processing, and visualization of data in ways that stimulate decisions making at all levels of an organization. The complexity and number of these structures may differ greatly between organizations and depending on the type of decision supported in particular [11].

At the simplest level, a DDDM system will need data acquisition and ingestion facilities. In the case of IT companies, data sources are often wide-ranging in nature

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

and can involve such internal systems for us as project management tools, CRM (customer relationship management) platforms, version control systems, and help desk solutions. External sources could include market research reports, competitor studies, social media feeds, economic indicators and so on. Contemporary data ingestion pipelines need support for both structured data (e.g., records of databases) and unstructured data (e.g., text documents, images or log files), oftentimes in real time or near real time.

Data storage and handling is also another key element in the technological resources. Legacy relational database management systems (RDBMS) are still relevant for structured data workloads, but new data lakes and NoSQL systems have appeared for managing semi-structured datasets and unstructured data at scale. The decision of storage option is based on the volume, velocity, variety (3Vs of big data), and the kind of analysis that is needed. A lot of these organizations go with a hybrid approach, where you have different storage technologies based on use case, but still have mechanisms for data integration and consistency across the platforms.

Data processing and analytics functionalities are the backbone of the DDDM ecosystem. This level consists of ETL, or cleaning, transforming and integrating the data and exploratory, diagnostic, predictive, and prescriptive analytics engines. However, batch computation frameworks continue to be relevant for a large number of analytical workloads – the emergence of stream processing frameworks for gaining real-time insights has not nullified the importance of batch processing frameworks. The increasing deployment of “machine learning” and “artificial intelligence” methods has also massively extended the scope of what can be analyzed, supporting increasingly-complex pattern-recognition, anomaly detection and automated decision making.

On the user interface side of the DDDM infrastructure, we have business intelligence (BI) and data visualization tools. They do this by simplifying complex analytical work while also translating results into easier-to-understand dashboards, data stories, reports, and other visually oriented insight. Today, many BI tools are self-serve and more and more end users can do the exploration of data and even build their own visualization with little reliance or support from their IT departments. The story behind the data Beautiful charts and visualizations help you uncover insights that would go unnoticed in traditional tabular reports.

The technical implementation of these disparate pieces is problematic. Data integration middleware, APIs, and ETL pipelines play a wide role in the (smooth) flow of data between systems and the quality and consistency of the data throughout the analytical process. Data governance software helps administer metadata, enforce quality standards and maintain compliance with regulations such GDPR or CCPA.

In recent years, the infrastructure of DDDM has been significantly altered by cloud computing. Cloud-based analytics environments have several advantages over traditional on-premises capabilities, including improved scalability, lower initial costs and the ability to use state-of-the-art analytics functionalities without major skills investments to in-house teams. The big cloud providers have now complete analytics suites that connect storage, processing, and visualization together, with pre-built connectors and pre-configured machine learning models on top of all the common data sources.

Another significant trend in DDDM infrastructure is edge computing. As a result, we can perform data processing close to the source of the data generation (e.g., on IoT devices or local servers), saving the latency, bandwidth, and real-time decision-making in distributed environment. This is particularly true for IT companies creating or consuming edge applications and services.

Security and privacy guarantees should be part of the DDDM design of any infrastructure. Sensitive data are protected through encryption, access control and audit logging including anomaly detection. Privacy-preserving analytics methods, like differential privacy or homomorphic encryption, allow data to be analyzed for insights without revealing personal or sensitive details [12].

The technical deployment of DDDM is not fixed, but need be in a state of flux to meet business requirements and technology progress. DevOps practices have become popular with many organizations looking to automate the development, deployment, and support of their analytical systems. These approaches prioritize using automation, continuous integration/continuous delivery (CI/CD), and ensuring that data engineers, analysts, and business users work closely together.

In context of IT companies in particular, the DDDM infrastructure oftentimes should serve specialized use cases, such as software development analytics, IT operations monitoring or cybersecurity threat detection. These might be integrations with development tools, bespoke analysis algorithms, or an original approach to visualizing data the only way that makes sense to technical audiences. Let's not forget the human dimension of our DDDM infrastructure (Fig. 2). No matter how good the technological machinery it is doomed to fail without the correct training, documentation and support. Without user adoption strategies, the organization, the human capital, is handicapped, unable to effectively use the capabilities of the available technology.

When evaluating these infrastructure investments, IT organizations face the delicate task of balancing multiple but competing priorities, such as flexibility versus standardization, innovation versus stability, self-service versus governance. The ideal structure will be different for each individual company, depending on size, sector, or strategic goals. But there are some principles that tend to remain the same regardless of the organization: the infrastructure must be elastic enough to support growth, flexible enough to incorporate the latest technologies, and aligned with the company’s broader data strategy and business goals.

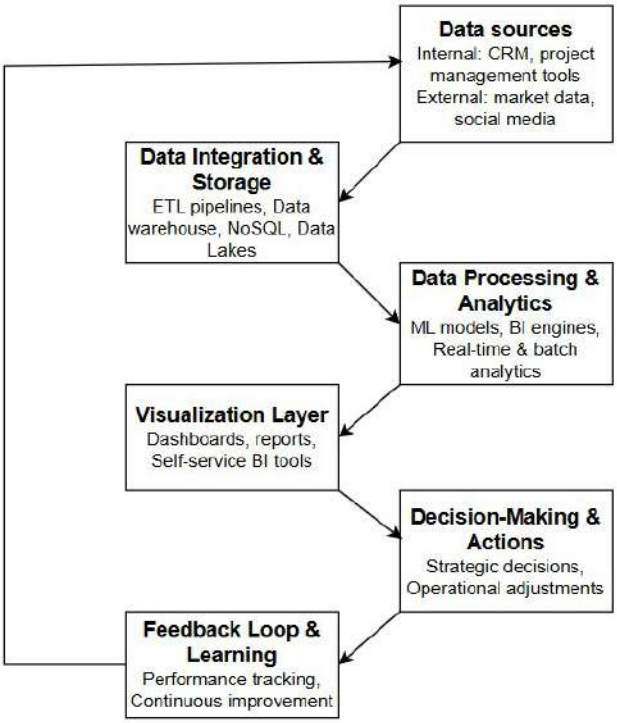


Fig. 2. – Infrastructure of DDDM

Conclusions

A comprehensive analysis of data-driven decision making (DDDM) in the IT sector provides critical insights that will enable us to connect theory, technology, and practical implementation. The synthesis of key findings can be summarized into practical recommendations for enterprises seeking to harness the power of data. The main statements include:

1) The shift from experience-based decisions to data-backed strategies is no longer optional for IT companies. (Fig. 2).

2) Companies adopting DDDM demonstrate 20-40% improvements in operational efficiency, risk mitigation, and customer satisfaction (based on case studies from Microsoft, Google, and mid-sized SaaS firms) (Fig. 1).

3) Documented results from DDDM adopters include:

• 30% faster project delivery (via predictive resource allocation).

• 25% higher customer retention (through personalized engagement).

• 15% cost reduction (by optimizing cloud spend and DevOps workflows).

Список літератури

1. Selvarajan, Guru Prasad. Augmenting Business Intelligence with AI: A Comprehensive Approach to Data-Driven Strategy and Predictive Analytics. International Journal of All Research Education and Scientific Methods, 2023, 11.10: 2121-2132.
2. Provost, F. and Fawcett, T. (2021). Business Data Science: Combining Machine Learning and Economics to Solve Real Problems. O'Reilly Media Inc. 383p.
3. McKinsey Global Institute. The Data-Driven Enterprise: Why Organizations Must Accelerate Their Digital Transformation. [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025
4. Shmueli, G., Bruce, P. C., Gedeck, P., & Patel, N. R. Data Mining for Business Analytics: Concepts, Techniques, and Applications in Python. WILEY. 608p.
5. Chantal Emmanuel Sylvestre. The Role of Data-Driven Decision Making in Business Strategy. Research Output Journal of Education, 2024 3(3):80-84.
6. Скабара І.М. Трансформація процесу формування стратегії розвитку іт-підприємств на засадах концепції agile. Економіка та суспільство, В. №85 / 2026. DOI: https://doi.org/10.32782/2524-0072/2026-85-40
7. Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. (2022). Optimizing business decision-making with advanced data analytics techniques. Iconic Research and Engineering Journals, 6(5), 184-203.
8. Hosen, M. S., Islam, R., Naeem, Z., Folorunso, E. O., Chu, T. S., Al Mamun, M. A., & Orunbon, N. O. (2024). Data-driven decision making: Advanced database systems for business intelligence. Nanotechnology Perceptions, 20(3), 687-704. DOI : https://doi.org/10.62441/nano-ntp.v20iS3.768
9. Папінко А. Створення інформації про бізнес-процеси IT-компанії в управлінському обліку. Вісник економіки. 2023. Вип. 4. С. 150–170. DOI: https://doi.org/10.35774/visnyk2023.04.150
10. Pantović, V., Vidojević, D., Vujičić, S., Sofijanić, S., & Jovanović-Milenković, M. (2024). Data-driven decision making for sustainable IT project management excellence. Sustainability, 16(7), 3014. DOI: https://doi.org/10.3390/su16073014
11. Building a Data-Driven Culture: How to Empower Teams With Insights [Online]. Available: https://www.confluent.io/blog/data-driven-culture/
12. Böttcher, S., Vieluf, S., Bruno, E. et al. Data quality evaluation in wearable monitoring. Sci Rep 12, 21412 (2022). https://doi.org/10.1038/s41598-022-25949-x

References (transliterated)

1. Selvarajan, Guru Prasad. Augmenting Business Intelligence with AI: A Comprehensive Approach to Data-Driven Strategy and Predictive Analytics. International Journal of All Research Education and Scientific Methods, 2023, 11.10: 2121-2132.
2. Provost, F. and Fawcett, T. (2021). Business Data Science: Combining Machine Learning and Economics to Solve Real Problems. O'Reilly Media Inc. 383p.
3. McKinsey Global Institute. The Data-Driven Enterprise: Why Organizations Must Accelerate Their Digital Transformation. [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025
4. Shmueli, G., Bruce, P. C., Gedeck, P., & Patel, N. R. Data Mining for Business Analytics: Concepts, Techniques, and Applications in Python. WILEY. 608p.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

5. Chantal Emmanuel Sylvestre. The Role of Data-Driven Decision Making in Business Strategy. Research Output Journal of Education, 2024 3(3):80-84.
6. Skabara I.M. Transformatsiia protsesu formuvannia stratehii rozvytku it-pidpryiemstv na zasadakh kontseptsii agile. Ekonomika ta suspilstvo, V. №85 / 2026. DOI: https://doi.org/10.32782/2524-0072/2026-85-40
7. Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. (2022). Optimizing business decision-making with advanced data analytics techniques. Iconic Research and Engineering Journals, 6(5), 184-203.
8. Hosen, M. S., Islam, R., Naeem, Z., Folorunso, E. O., Chu, T. S., Al Mamun, M. A., & Orunbon, N. O. (2024). Data-driven decision making: Advanced database systems for business intelligence. Nanotechnology Perceptions, 20(3), 687-704. DOI : https://doi.org/10.62441/nano-ntp.v20iS3.768
9. Papinko A. Stvorennia informatsii pro biznes-protsesy IT-kompanii v upravlinskomu obliku. Visnyk ekonomiky. 2023. Vyp. 4. S. 150–170. DOI: https://doi.org/10.35774/visnyk2023.04.150
10. Pantović, V., Vidojević, D., Vujičić, S., Sofijanić, S., & Jovanović-Milenković, M. (2024). Data-driven decision making for sustainable IT project management excellence. Sustainability, 16(7), 3014. DOI: https://doi.org/10.3390/su16073014
11. Building a Data-Driven Culture: How to Empower Teams With Insights [Online]. Available: https://www.confluent.io/blog/data-driven-culture/
12. Böttcher, S., Vieluf, S., Bruno, E. et al. Data quality evaluation in wearable monitoring. Sci Rep 12, 21412 (2022). https://doi.org/10.1038/s41598-022-25949-x

Відомості про авторів (About authors)

Деретюк Ілля Костянтинович – аспірант, Національний технічний університет «Харківський політехнічний інститут», аспірант кафедри програмної інженерії та інтелектуальних технологій управління; м. Харків, Україна; ORCID: https://orcid.org/0009-0009-6472-3850; e-mail: Illia.Deretiuk@cs.khpi.edu.ua

Deretiuk Illia – postgraduate student, Department of Software Engineering and Management Intelligent Technologies, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; ORCID: https://orcid.org/0009-0009-6472-3850; e-mail: Illia.Deretiuk@cs.khpi.edu.ua.

Козуля Марія Михайлівна – кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри програмної інженерії та інтелектуальних технологій управління; ORCID: https://orcid.org/0000-0002-4090-8481; e-mail: mariia.kozulia@khpi.edu.ua.

Kozulia Mariia – candidate of technical science (Ph. D.), Docent, Position, Department of Software Engineering and Management Intelligent Technologies, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine; https://orcid.org/0000-0002-4090-8481; e-mail: mariia.kozulia@khpi.edu.ua.

Please cite this article as:

Deretiuk I., Kozulia M. Data-driven decision making for IT business growth. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 29–34, doi:10.20998/2413-4295.2026.02.04.

Будь ласка, посилайтесь на цю статтю наступним чином:

Деретюк І.К., Козуля М.М. Прийняття рішень на основі даних для зростання ІТ-бізнесу. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 29-34. doi:10.20998/2413-4295.2026.02.04.

Надійшла (received) 16.05.2026
Прийнята (accepted) 26.05.2026
Опублікована (published) 05.06.2026

УДК 004.056.5 doi: 10.20998/2413-4295.2026.02.05

ОРГАНІЗАЦІЯ ФІЗИЧНОГО ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ ТА РЕКОМЕНДАЦІЙ МАГАТЕ

С.С. ЛИС*, А.Я. ІСОПЕНКО, В.В. ЗАГАРОВСЬКИЙ

Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», Львів, УКРАЇНА
**e-mail: Lysss@ukr.net*

АНОТАЦІЯ *Розглянуто теоретичні та практичні аспекти фізичного захисту комп'ютерних систем як невід'ємного елементу комплексної інформаційної безпеки підприємств критичної інфраструктури. Проаналізовано сучасні підходи до організації фізичного захисту відповідно до міжнародних стандартів і рекомендацій МАГАТЕ, зокрема принципи багаторівневого захисту та зональної архітектури безпеки. Визначено основні категорії заходів безпеки (технічні, адміністративні та фізичні) та обґрунтовано їх взаємодоповнюючий характер. Особливу увагу приділено ідентифікації чутливих цифрових активів, класифікації загроз фізичній безпеці комп'ютерних систем, включаючи внутрішні загрози, атаки на ланцюг постачання та ризики відмови фізичних систем захисту. Розглянуто сучасні засоби контролю фізичного доступу, захисту обладнання на рівні пристроїв, а також механізми управління конфігураціями та безпеки знімних носіїв. Запропоновано модель зональної архітектури фізичного захисту комп'ютерних систем для об'єктів критичної інфраструктури. Наведено приклад її практичного впровадження на умовному підприємстві водопостачання, що демонструє ефективність застосування запропонованого підходу. Отримані результати підтверджують, що інтеграція фізичного захисту в загальну програму комп'ютерної безпеки суттєво підвищує рівень захищеності інформаційних систем.*
Ключові слова: *фізичний захист, комп'ютерні системи, інформаційна безпека, критична інфраструктура, зональна модель, багаторівневий захист, контроль доступу.*

ORGANIZATION OF PHYSICAL PROTECTION OF COMPUTER SYSTEMS OF CRITICAL INFRASTRUCTURE BASED ON IAEA STANDARDS AND RECOMMENDATIONS

S. LYS*, A. ISOPENKO, V. ZAHAROVSKYI

Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv, Ukraine

ABSTRACT *The paper examines theoretical and practical aspects of physical protection of computer systems as an integral component of comprehensive information security for critical infrastructure enterprises. Modern approaches to organizing physical protection in accordance with international standards and IAEA recommendations are analyzed, in particular the principles of layered (defense-in-depth) protection and zonal security architecture. The main categories of security measures (technical, administrative, and physical) are identified, and their complementary nature is substantiated. Special attention is paid to the identification of sensitive digital assets, classification of threats to the physical security of computer systems, including insider threats, supply chain attacks, and risks associated with failures of physical protection systems. Modern means of physical access control, device-level equipment protection, as well as configuration management mechanisms and removable media security are considered. A model of zonal architecture for physical protection of computer systems for critical infrastructure facilities is proposed. An example of its practical implementation at a hypothetical water supply enterprise is provided, demonstrating the effectiveness of the proposed approach. The obtained results confirm that the integration of physical protection into the overall computer security program significantly enhances the level of protection of information systems.*
Keywords: *physical protection, computer systems, information security, critical infrastructure, zonal model, layered protection, access control.*

Вступ

Сучасні комп'ютерні системи є основою функціонування критичної інфраструктури від атомних електростанцій і підприємств оборонно-промислового комплексу до банківського сектору та органів державної влади. Динамічне зростання кількості кіберзагроз і постійне вдосконалення методів атак змусили фахівців з інформаційної безпеки переосмислити традиційні підходи до захисту. Сьогодні стало очевидним, що суто програмні або мережеві засоби захисту є недостатніми без відповідного фізичного рівня безпеки, тобто рівня, який нерідко залишається поза увагою при проєктуванні систем захисту.

Фізичний захист комп'ютерних систем охоплює сукупність заходів, спрямованих на запобігання несанкціонованому фізичному доступу до обладнання, його пошкодженню, знищенню або несанкціонованій модифікації. Такі заходи утворюють

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

перший і найбільш матеріальний рівень захисту в моделях інформаційної безпеки, оскільки будь-яка цифрова система фізично існує у вигляді апаратного забезпечення, що може бути знищене, вкрадене або модифіковане.

Міжнародне агентство з атомної енергії (МАГАТЕ) у своїй публікації «Методи комп'ютерної безпеки для ядерних об'єктів» [1], одному з найбільш деталізованих міжнародних стандартів у сфері захисту комп'ютеризованих систем, окремо виділяє фізичний контроль як самостійний та рівноправний рівень заходів безпеки. Хоча ця публікація розроблена для потреб ядерної галузі, закладені в ній методологічні підходи мають універсальний характер і можуть застосовуватися в будь-яких організаціях, що управляють критично важливими інформаційними системами.

Традиційно основна увага у сфері інформаційної безпеки приділяється програмним і мережевим засобам захисту. Проте практика останніх років демонструє, що ігнорування фізичного рівня безпеки призводить до виникнення критичних вразливостей. Отримавши фізичний доступ до обладнання, зловмисник може обійти більшість логічних механізмів захисту, що робить фізичний захист невід'ємною складовою комплексної системи безпеки.

Особливої актуальності ця проблема набуває в умовах зростання кількості комбінованих атак, які поєднують кібернетичні та фізичні вектори впливу, а також загроз, пов'язаних із внутрішніми порушниками та компрометацією ланцюгів постачання обладнання. У таких умовах виникає необхідність формування інтегрованого підходу до захисту комп'ютерних систем, що враховує взаємозалежність фізичних і логічних механізмів безпеки.

Аналіз літературних джерел та постановка проблеми дослідження

Методологічною основою цього дослідження слугує публікація Міжнародного агентства з атомної енергії "Методи комп'ютерної безпеки для ядерних об'єктів" (Серія МАГАТЕ з ядерної захищеності, Технічні настанови № 17-Т, 2021) [1], як один із найбільш систематизованих міжнародних документів у галузі захисту комп'ютеризованих систем критичної інфраструктури. Документ формалізує концепції чутливих цифрових активів, зонального підходу та трирівневої моделі заходів безпеки (технічні, адміністративні, фізичні). Суміжну проблематику організаційного впровадження програм комп'ютерної безпеки розглядає Керівництво з впровадження МАГАТЕ № 42-G "Комп'ютерна безпека для ядерної захищеності" [2], а захист ядерної інформації як складову фізичного захисту носіїв і каналів передачі даних – публікація NSS 23-G [3]. Разом ці три документи утворюють ієрархічну систему вимог МАГАТЕ, що охоплює стратегічний, операційний і технічний рівні захисту та є точкою відліку для порівняльного аналізу будь-яких галузевих підходів.

Серед фундаментальних праць у галузі інженерії безпеки ключове місце посідає монографія Р. Андерсона "Інженерія безпеки" [4], яка системно розкриває принципи проектування надійних розподілених систем, зокрема питання фізичного захисту та моделювання загроз. Андерсон обґрунтовує необхідність розгляду фізичного рівня як інтегральної складової загальної архітектури безпеки, а не як ізольованого технічного завдання.

Нормативну базу досліджень формують два провідних стандарти. Міжнародний стандарт ISO/IEC 27001:2022 [5] встановлює вимоги до систем управління інформаційною безпекою, включаючи заходи фізичного та екологічного захисту, і задає системний підхід до управління ризиками на основі ідентифікації активів, оцінки загроз і вибору пропорційних засобів контролю. Американський стандарт NIST SP 800-53 Rev. 5 [6] деталізує конкретні заходи фізичного захисту для федеральних інформаційних систем і широко застосовується операторами критичної інфраструктури як практичний орієнтир незалежно від галузевої приналежності.

Значний внесок у розуміння практичних наслідків ігнорування фізичного рівня захисту зробили дослідження резонансних кіберінцидентів. Аналіз кібератаки на українську електромережу 2015 року [7] документально підтвердив, що комбіновані атаки, які поєднують цифрові та фізичні вектори, є найбільш руйнівними за своїми наслідками. Р. Лангнер у своєму аналізі Stuxnet [8] показав, що цей шкідливий код поширювався виключно через фізичні носії (USB-накопичувачі), долаючи мережі з "повітряним проміжком", тобто прецедент, що документально підтвердив критичну роль фізичного контролю над пристроями введення/виведення.

Практичні аспекти управління паролями та автентифікацією як складової фізичного доступу висвітлено у настанові K. Scarfone та M. Souppaya (NIST SP 800-118) [9]. Вітчизняна наукова школа представлена навчальним посібником Г. М. Гулака та П. М. Складанного "Основи інформаційної безпеки" [10], який систематизує теоретичні засади захисту інформації стосовно українських реалій правового регулювання.

IAEA-NSS-46-T [11] окреслює значення оцінювання ефективності систем фізичного захисту (PPS) і має практичну спрямованість як технічне керівництво. Водночас вона носить переважно описовий характер і не містить елементів наукової новизни чи методологічної деталізації. Відсутність конкретних підходів, метрик або результатів знижує її аналітичну цінність у науковому контексті.

Праця [12] висвітлює актуальну проблему кіберзахисту ядерних об'єктів і пропонує структурований підхід до оцінювання реагування на інциденти, що є її сильною стороною. Водночас методологія та результати описані узагальнено, без конкретних метрик ефективності чи порівняння з існуючими підходами. Стаття [13] демонструє чітко окреслену технічну новизну – ризик-орієнтовану модель із використанням транспортного графа для оцінки безпеки перевезення радіоактивних матеріалів.

Робота [14] охоплює актуальну проблему інтегрованого управління безпекою (IMSS) у ядерній галузі та спирається на різноманітні джерела, що підсилює її практичну значущість. Водночас методологія подана узагальнено, без чіткої конкретизації обсягу даних і критеріїв аналізу, а результати частково мають описовий характер без достатньої аналітичної глибини. В статті [15] висвітлено актуальну проблему підготовки з кібербезпеки, методологія систематичного огляду описана занадто загально, а результати мають декларативний характер без кількісного підтвердження чи конкретних KPI.

Разом із тим аналіз наявних джерел виявляє певну фрагментованість, тобто питання фізичного захисту комп'ютерних систем нерідко розглядаються відокремлено від логічних засобів, без належного акценту на їхній взаємозалежності.

Мета роботи

Метою роботи є аналіз концептуальних засад фізичного захисту комп'ютерних систем, дослідження сучасних методів і засобів забезпечення фізичної безпеки, а також розробка практичної моделі зональної архітектури захисту для об'єктів критичної інфраструктури.

Концептуальні основи фізичного захисту комп'ютерних систем

Трирівнева модель заходів безпеки. Сучасна теорія інформаційної безпеки розглядає захист комп'ютерних систем як багатовимірне завдання, що вимагає одночасного застосування заходів трьох категорій (рис. 1). Згідно з підходом МАГАТЕ [1], до цих категорій належать технічні, адміністративні та фізичні заходи контролю. Кожна категорія виконує власну функцію і компенсує природні обмеження інших.

Технічні заходи включають апаратне та програмне забезпечення, що використовується для запобігання, виявлення та пом'якшення наслідків несанкціонованих дій: міжмережеві екрани, системи виявлення вторгнень, засоби шифрування, механізми автентифікації [4]. Адміністративні заходи охоплюють організаційні процедури, нормативні документи, програми навчання персоналу та перевірку благонадійності співробітників.

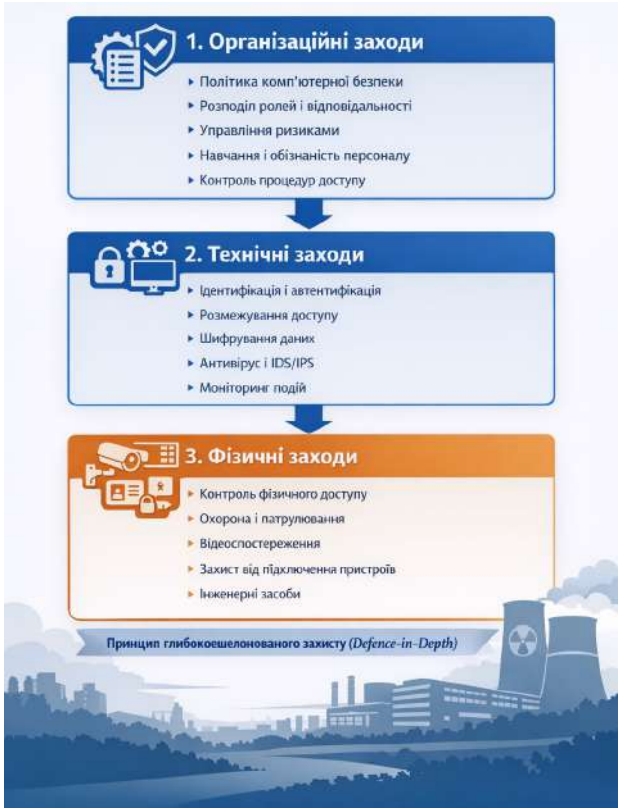


Рис. 1 – Трирівнева модель заходів комп'ютерної безпеки за класифікацією МАГАТЕ.

Фізичні заходи контролю утворюють базовий рівень, без якого ефективність двох інших категорій є суттєво обмеженою. Публікація МАГАТЕ дає таке визначення: «Заходи фізичного контролю – це фізичні бар'єри, що захищають прилади, комп'ютеризовані системи та допоміжні активи від фізичного пошкодження та запобігають несанкціонованому фізичному доступу» [1]. Це визначення підкреслює подвійну функцію фізичного захисту: превентивну – недопущення несанкціонованого доступу, та захисну – запобігання фізичному пошкодженню обладнання .

Заходи трьох категорій (рис. 1) не є взаємозамінними, а лише взаємодоповнюючими. Наприклад, навіть найдосконаліший міжмережевий екран не захистить систему від зловмисника, який отримав фізичний доступ до сервера і підключив до нього знімний носій із шкідливим програмним забезпеченням.

Чутливі цифрові активив. Ключовим об'єктом фізичного захисту є чутливі цифрові активи (ЧЦА) - будь-яке обладнання або компоненти, що використовуються для зберігання, обробки, контролю або передачі чутливої інформації: системи управління, мережі, інформаційні системи [1]. До ЧЦА відносяться комп'ютерні робочі станції, сервери баз даних, мережеве комутаційне обладнання,

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

програмовані логічні контролери (ПЛК), портативні пристрої та знімні носії інформації.

Чутлива інформація в контексті ЧЦА охоплює не лише дані як такі, а й програмне забезпечення виконання, вбудоване мікропрограмне забезпечення (firmware), інструменти розроблення, засоби технічного обслуговування та операційні системи [1]. Таке розширене розуміння є принципово важливим для побудови системи фізичного захисту, оскільки фізичний доступ до апаратного забезпечення потенційно надає зловмиснику можливість модифікації будь-якого з цих компонентів без залишення очевидних цифрових слідів.

Ідентифікація та інвентаризація всіх ЧЦА є першим практичним кроком у побудові системи фізичного захисту. Без чіткого розуміння того, яке саме обладнання потребує захисту, де воно розташоване і яку роль відіграє в загальній інфраструктурі, неможливо ефективно спланувати та впровадити заходи безпеки [1, 5, 6].

Зони комп'ютерної безпеки. Зональна модель є основоположним архітектурним рішенням для структурованого захисту комп'ютерних систем. Згідно з МАГАТЕ, «зона комп'ютерної безпеки – це група систем, що мають спільні фізичні та/або логічні межі і яким призначено однаковий рівень безпеки» [1]. Рівень комп'ютерної безпеки зони визначається найвищим ступенем захисту, необхідним будь-якій функції, що виконується системами в межах цієї зони.

Фізична зона і логічна зона безпеки можуть збігатися або відрізнятися. У зоні найвищого рівня (зона 1А) як фізичні, так і логічні межі визначаються строго, тобто потрібні і фізичні бар'єри, і логічне розмежування. На нижчих рівнях фізичні вимоги можуть бути менш жорсткими, однак повністю не знімаються [1]. Зональна модель дозволяє застосовувати диференційований підхід до захисту: найбільш критичні активи зосереджуються у найбільш захищених зонах з мінімальним числом уповноважених осіб.

Зональна модель та принцип багаторівневого захисту

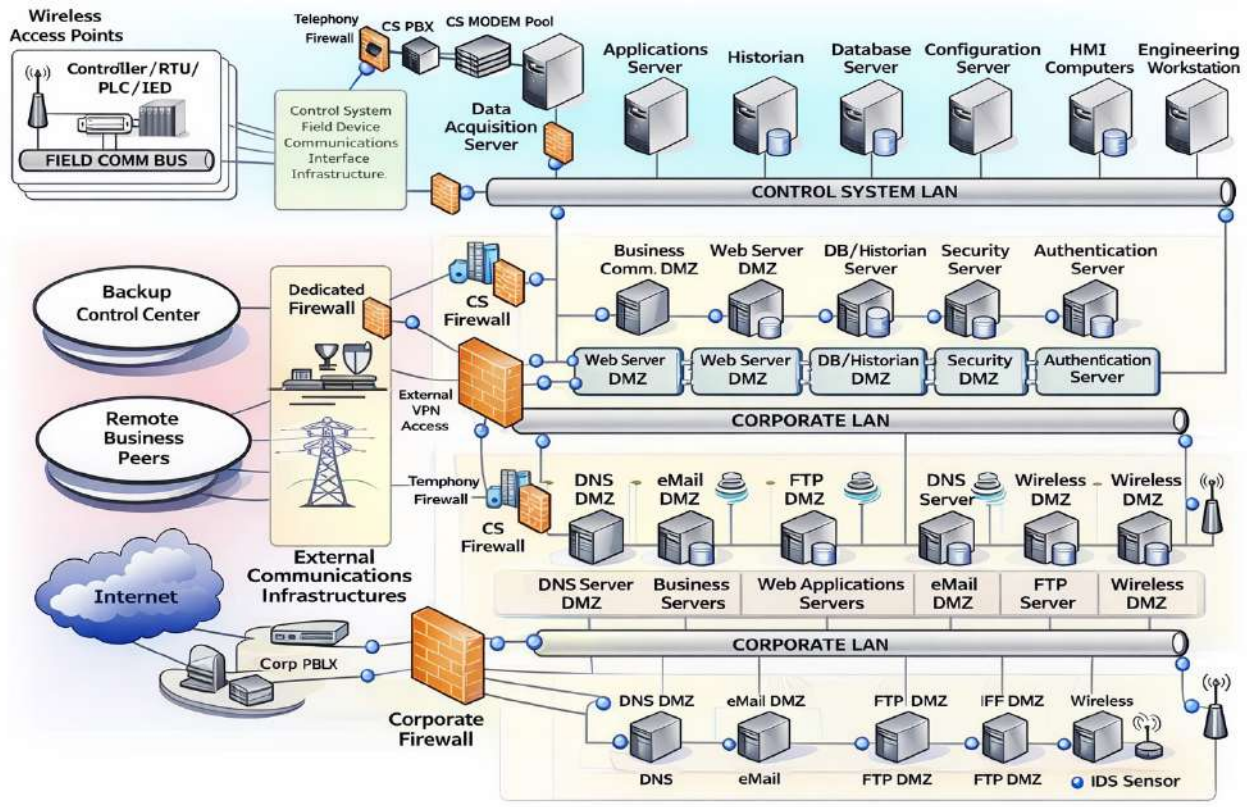


Рис. 2 – Архітектура концентричних зон безпеки за принципом багаторівневого захисту.

Межі зон (рис. 2) зазвичай обладнуються засобами фізичного контролю доступу - замкненими шафами, бар'єрами, блокаторами портів - та механізмами роз'єднання потоків даних - фільтрами пакетів, міжмережевими екранами, діодами даних [1]. Поєднання фізичних та логічних бар'єрів унеможливлює несанкціонований доступ навіть у разі часткового подолання одного з рівнів захисту.

Принцип багаторівневого захисту. Концепція багаторівневого захисту (від англ. defence in depth) передбачає, що жоден окремий засіб захисту не є абсолютно надійним, тому необхідно застосовувати кілька незалежних і гетерогенних шарів безпеки [4]. Відповідно до МАГАТЕ, будь-який зловмисник має подолати або обійти кілька шарів заходів комп'ютерної безпеки, перш ніж отримає можливість скомпрометувати критичну систему [1].

У контексті фізичного захисту це означає послідовне застосування: зовнішнього периметрового огородження; систем контролю доступу до будівлі; відеоспостереження та охорони; контролю доступу до серверних приміщень та апаратних залів; захищених серверних стійок із замками; блокаторів портів на окремих пристроях. Кожний шар компенсує можливі слабкості попереднього. Якщо зловмисник подолав зовнішній периметр, внутрішні бар'єри все одно перешкоджають йому дістатися до критичного обладнання.

Важливою вимогою до ефективного багаторівневого захисту є гетерогенність шарів - використання різних технологій і підходів знижує ймовірність того, що один вектор атаки дозволить подолати всі рівні одночасно [1, 10]. Наприклад, поєднання електронних замків, механічних бар'єрів та відеоспостереження робить обхід системи значно складнішим, ніж використання лише одного типу засобів.

Засоби та методи фізичного захисту

Контроль фізичного доступу до приміщень. Контроль фізичного доступу до приміщень, де розташоване комп'ютерне обладнання, є першочерговим завданням фізичного захисту. МАГАТЕ виділяє такі основні засоби: приміщення із контрольованим доступом, захищені двері з електронними або механічними замками, системи ідентифікації на основі ключ-карток або біометричних даних, датчики руху, системи відеоспостереження, а також індикатори несанкціонованого втручання [1, 6]. При використанні PIN-кодів та парольної автентифікації як складової систем контролю фізичного доступу (рис. 3) слід дотримуватися вимог щодо складності та регулярної зміни облікових даних, визначених у відповідних настановах [9].

Застосування цих засобів є диференційованим залежно від рівня безпеки зони. Серверні приміщення та апаратні зали, в яких розміщене найбільш критичне обладнання, потребують найвищого рівня контролю: доступ до них повинен надаватися лише мінімально необхідному числу осіб, кожен факт входу та виходу фіксується, а всі дії в приміщенні документуються [5, 6]. Це суттєво обмежує можливості як зовнішніх зловмисників, так і внутрішніх порушників.

Рис. 3 – Електронний замок із PIN-клавіатурою як засіб двофакторного контролю фізичного доступу до захищеного приміщення.

Окрему увагу слід приділяти так званим «сірим зонам» – місцям, де кабелі та обладнання виходять за межі захищених приміщень, наприклад: кабельні траси, технічні шахти, підвальні приміщення. МАГАТЕ вказує на необхідність захисту польових пристроїв, розташованих поза периметром фізичного захисту [1, 6], оскільки вони нерідко стають точкою проникнення в інфраструктуру.

Захист обладнання на рівні пристроїв. Поряд із захистом приміщень необхідно застосовувати засоби захисту на рівні окремих пристроїв. До таких засобів належать: замкнені серверні стійки та шафи, що запобігають фізичному доступу до серверів навіть у разі проникнення в серверне приміщення; блокатори USB-портів та інших інтерфейсів введення/виведення, що унеможливлюють підключення несанкціонованих зовнішніх пристроїв; замки Кенсінгтона та аналогічні кріпильні рішення для стаціонарного обладнання [1, 6].

Особливу роль відіграють індикатори втручання (tamper indicators) - пломби, спеціальні наклейки або механічні елементи, що фіксують сам факт несанкціонованого відкриття корпусу пристрою. МАГАТЕ наголошує, що обладнання повинно бути перевірено на відсутність слідів втручання при прийманні і надалі [1] (рис. 4).

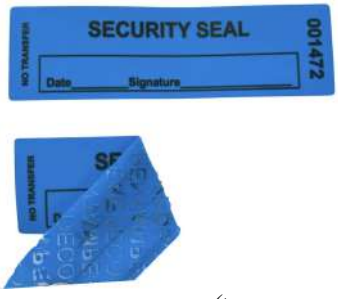


Рис. 4 – Індикатор втручання (tamper seal) на корпусі обладнання (засіб виявлення несанкціонованого фізичного доступу).

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Такі індикатори є простим, але ефективним засобом раннього виявлення спроб фізичної атаки на апаратне забезпечення.

Управління конфігураціями як елемент фізичного захисту. Управління конфігураціями є важливим адміністративно-технічним інструментом, безпосередньо пов'язаним із фізичним захистом. Згідно з МАГАТЕ, воно передбачає ведення детальних актуальних записів про всі встановлені апаратні та програмні компоненти, їх розташування, з'єднання та параметри налаштування [1, 5]. Регулярна верифікація відповідності реального стану обладнання задокументованій конфігурації дозволяє своєчасно виявити будь-які несанкціоновані зміни.

Перед виконанням будь-яких процедур, що можуть обійти або знизити ефективність чинних заходів безпеки - наприклад, технічного обслуговування, яке вимагає тимчасового вимкнення засобів захисту, - необхідно проводити і документувати відповідні перевірки [1, 5]. У таких ситуаціях мають застосовуватися компенсуючі заходи, що забезпечують еквівалентний рівень захисту на час відключення основних засобів безпеки.

Фізична безпека знімних носіїв та мобільних пристроїв. Знімні носії інформації (USB-накопичувачі, компакт-диски, зовнішні жорсткі диски) та мобільні пристрої становлять особливий вектор фізичних загроз. МАГАТЕ наголошує, що персонал повинен забезпечити використання в межах об'єкту виключно дозволених знімних носіїв та мобільних пристроїв [1]. Для цього необхідний жорсткий реєстраційний контроль: будь-який носій, що вноситься в захищену зону або виноситься з неї, повинен бути задокументований.

Особливу небезпеку становить те, що навіть повністю ізольовані від мережі системи («повітряний проміжок», air gap) залишаються вразливими через переривчасте використання знімних носіїв для оновлень або передачі даних [1]. Саме через цей вектор було реалізовано кібератаку Stuxnet, що вразила промислові центрифуги для збагачення урану - і це є показовим прикладом того, як ігнорування фізичного контролю над носіями може мати катастрофічні наслідки [7, 8].

Загрози фізичній безпеці комп'ютерних систем

Внутрішні загрози. Внутрішні загрози є одними з найнебезпечніших у контексті фізичного захисту, оскільки внутрішній порушник - на відміну від зовнішнього зловмисника - вже має законний фізичний доступ до об'єкту і обладнання. МАГАТЕ класифікує внутрішніх порушників за рівнем авторизації та ступенем зловмисності намірів [1, 3]. До цієї категорії належать як навмисні порушники, що діють в інтересах третіх сторін або з особистих мотивів, так і ненавмисні - співробітники, що припускаються помилок через недбалість або незнання вимог безпеки. Порівняльний рівень усіх ідентифікованих загроз наведено на рис. 5.

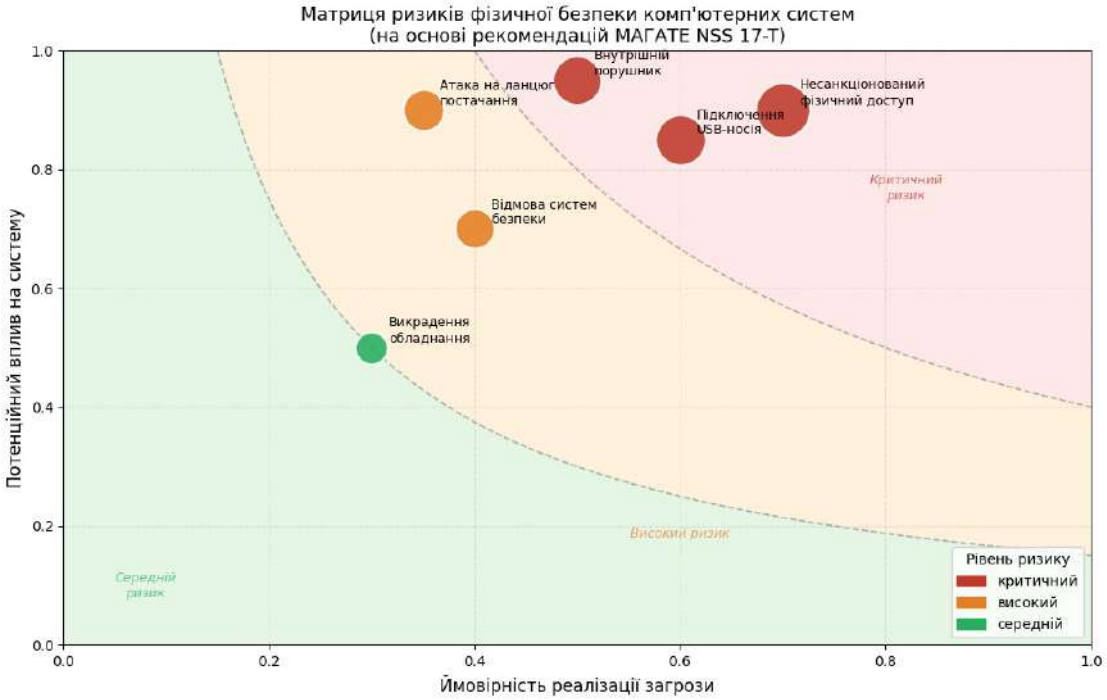


Рис. 5 – Матриця ризиків фізичної безпеки комп'ютерних систем.

Для протидії внутрішнім загрозам застосовується комплекс взаємодоповнюючих заходів. Принцип мінімальних привілеїв передбачає обмеження фізичного доступу персоналу лише тими зонами та пристроями, які безпосередньо необхідні для виконання їхніх службових функцій. Принцип двох осіб (two-person rule) вимагає присутності двох незалежних уповноважених осіб для виконання

певних критичних операцій з обладнанням, що унеможливлює одноосібні несанкціоновані дії. Розподіл службових обов'язків між різними особами та підрозділами не дає одній людині отримати повний контроль над критичними активами.

МАГАТЕ також указує, що процедури, які містять інструкції щодо вимкнення або обходу заходів безпеки, повинні гарантувати фіксацію таких дій у журналах [1]. Обов'язкове протоколювання всіх привілейованих дій з обладнанням є водночас стримуючим фактором для потенційних порушників і засобом ретроспективного розслідування інцидентів.

Модель зональної архітектури фізичного захисту

Для практичної ілюстрації концептуальних засад, викладених у попередніх розділах, розроблено модель зональної архітектури фізичного захисту комп'ютерних систем організації, що управляє критично важливою інформаційною інфраструктурою (таб. 1). Модель базується на градуйованому підході МАГАТЕ [1] і відображає триярусну ієрархію зон безпеки із відповідними засобами фізичного та логічного контролю на кожному рівні.

Таблиця 1 – Модель зональної архітектури фізичного захисту комп'ютерних систем

Зона / Рівень	Об'єкти захисту (ЧЦА)	Засоби фізичного контролю	Засоби логічного контролю на межі
ЗОНА А (Найвищий рівень)	Сервери БД, системи резервного копіювання, мережеве ядро, ПЛК, криптографічні модулі	Біометрика + смарт-картка + PIN; замкнені стійки; блокатори портів; CCTV 24/7; правило двох осіб; індикатори втручання	Діод даних; міжмережевий екран класу L4; суворе білісписання; ізоляція мережного сегмента
ЗОНА Б (Середній рівень)	Робочі станції персоналу, адміністративні термінали, мережеве комутаційне обладнання, знімні носії	Смарт-картка + PIN; електронні замки; CCTV; блокатори USB; реєстр відвідувань; принцип мінімальних привілеїв	Фільтр пакетів; VLAN-ізоляція; IDS/IPS; контроль цілісності конфігурацій
ЗОНА В (Базовий рівень)	Загальнодоступні термінали, мережева інфраструктура загального використання, польові пристрої на периметрі	Механічні замки; CCTV; індикатори втручання на обладнанні; контроль доступу до приміщень	Зовнішній периметровий ME; DMZ; базова автентифікація; загальний моніторинг мережі
Зовнішній периметр: огородження об'єкту, охорона, системи виявлення вторгнення на периметрі			

Запропонована модель реалізує принцип концентричних зон захисту, де кожна внутрішня зона є більш захищеною, ніж зовнішня. Межі між зонами є точками застосування засобів одночасно фізичного та логічного контролю, що унеможливлює несанкціонований доступ навіть у разі часткового подолання одного рівня. Важливою особливістю моделі є її масштабованість. Вона може бути адаптована до будь-якого типу організації, від невеликого підприємства (де зони А та Б можуть бути суміщені в одному приміщенні) до розгалуженої критичної інфраструктури з множинними майданчиками. Розподіл обов'язків та принцип мінімальних привілеїв застосовуються як на рівні фізичного доступу до кожної зони, так і на рівні логічних прав у відповідних мережних сегментах, що відповідає рекомендаціям МАГАТЕ щодо інтеграції фізичного та логічного захисту в єдину програму комп'ютерної безпеки [1].

Таблиця 2 – Матриця відповідності загроз фізичної безпеки та контрзаходів

Загроза	Рівень ризику	Превентивні контрзаходи	Детективні / реактивні заходи
Несанкціонований фізичний доступ до приміщення	Критичний	Багатофакторна автентифікація; зонування доступу; правило двох осіб; замки з fail-secure	CCTV; журнали доступу; сигналізація; негайне сповіщення адміністратора безпеки
Підключення несанкціонованого знімного носія (USB)	Критичний	Фізичні блокатори портів; реєстр дозволених носіїв; заборона особистих пристроїв у зонах А, Б	Endpoint DLP; аудит підключень; сканування носіїв перед використанням
Внутрішній порушник (навмисний)	Критичний	Принцип мінімальних привілеїв; розподіл обов'язків; перевірка благонадійності персоналу	Аудит дій персоналу; протоколювання привілейованих операцій; UEBA-системи
Атака на ланцюг постачання (апаратні закладки)	Високий	Вимоги безпеки у специфікаціях закупівель; перевірені постачальники; контроль цілісності при прийманні	Перевірка індикаторів втручання; верифікація прошивки; апаратний аудит після встановлення
Відмова фізичних систем безпеки внаслідок кібератаки	Високий	Резервне живлення (ДБЖ); механічне резервування замків; ізоляція мереж управління СКУД	Моніторинг стану систем СКУД; автоматичне сповіщення при відмові; регулярне тестування
Фізичне знищення або викрадення обладнання	Середній	Замки Кенсінгтона; стійки з замками; шифрування дисків; геолокаційний моніторинг активів	CCTV із записом; інвентаризаційний облік; процедура дистанційного знищення даних

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Наведена матриця відображає комплексний підхід до управління фізичними ризиками, де для кожної загрози передбачено як превентивні (що знижують імовірність реалізації загрози), так і детективні та реактивні заходи (що забезпечують виявлення та реагування у разі її реалізації) таблиця 2. Такий підхід узгоджується з принципом багаторівневого захисту, оскільки відмова превентивного шару не означає повного успіху атаки, детективний шар забезпечує своєчасне виявлення та мінімізацію наслідків [1].

Таблиця 3 демонструє, що розглянуті заходи фізичного захисту мають чітку нормативну основу в усіх трьох провідних стандартах, що підтверджує їхню обґрунтованість і міжнародне визнання.

Таблиця 3 – Відповідність заходів фізичного захисту вимогам стандартів МАГАТЕ, ISO/IEC 27001 та NIST SP 800-53

Захід фізичного захисту	МАГАТЕ NSS 17-T [1]	ISO/IEC 27001:2022 [5]	NIST SP 800-53 Rev.5 [6]
Контроль фізичного доступу до приміщень	Розділ 5 (Фізичні заходи контролю), Зони КБ	Annex A 7.2 — Фізичний вхід; A 7.3 — Захист офісів	PE-2 Авторизація фіз. доступу; PE-3 Контроль доступу
Зональна модель (defence in depth)	Розділ 4 (Зони КБ); Градуйований підхід	A 5.29 — ІБ при перебоях; A 8.22 — Сегрегація мереж	SC-7 Захист меж; PE-19 Витік інформації
Захист знімних носіїв та блокування портів	Розділ 5.7 (Знімні носії та мобільні пристрої)	A 7.10 — Носії інформації; A 8.11 — Маскування даних	MP-7 Використання носіїв; SC-41 Відключення портів
Управління конфігураціями та індикатори втручання	Розділ 5.8 (Управління конфігураціями)	A 8.9 — Управління конфігурацією; A 7.4 — Моніторинг фіз. безпеки	CM-2 Базова конфігурація; PE-6 Моніторинг фіз. доступу
Принцип мінімальних привілеїв та розподіл обов'язків	Розділ 6.3 (Внутрішні загрози); Правило двох осіб	A 5.3 — Розподіл обов'язків; A 5.15 — Контроль доступу	AC-5 Розподіл обов'язків; AC-6 Найменші привілеї
Відеоспостереження та моніторинг	Розділ 5.2 (Виявлення та реагування); Моніторинг ефективності	A 7.4 — Моніторинг фізичної безпеки	PE-6 Моніторинг фіз. доступу; IR-5 Відстеження інцидентів

Наявність відповідних вимог одночасно у рекомендаціях МАГАТЕ [1], ISO/IEC 27001:2022 [5] та NIST SP 800-53 [6] свідчить про консенсус міжнародної спільноти фахівців з безпеки щодо необхідності та пріоритетності цих заходів. Для організацій, що прагнуть досягти відповідності кільком стандартам одночасно, реалізація заходів, представлених у таблиці, забезпечить виконання вимог усіх трьох нормативних документів у частині фізичного захисту.

Практичний сценарій впровадження зональної моделі на регіональному підприємстві водопостачання

Для ілюстрації практичного застосування розглянутих концепцій розглянемо умовний сценарій на основі типового регіонального підприємства водопостачання, що управляє автоматизованими системами диспетчерського управління (SCADA) та відповідає за постачання питної води населенню чисельністю близько 300 тисяч осіб. Вибір саме такого об'єкта зумовлений тим, що підприємства водопостачання є типовими операторами критичної інфраструктури, які поєднують промислові системи управління (ПЛК, SCADA) із загальноофісними інформаційними системами, а отже, демонструють типову для таких об'єктів неоднорідність вимог до фізичного захисту [1, 5].

Стан до впровадження заходів. До проведення аудиту безпеки підприємство мало такий стан фізичного захисту: серверна кімната, в якій розміщено SCADA-сервер та бази даних технологічних параметрів, закривалася на один механічний замок без журналювання доступу; всі USB-порти на робочих станціях диспетчерів були відкриті; персонал мав звичку підключати особисті флеш-накопичувачі для перенесення документів; ПЛК на насосних станціях, розташованих за периметром будівлі, фізично не були захищені від стороннього доступу; відеоспостереження було відсутнє в серверному приміщенні і вкрай обмеженим на виробничому майданчику. Водночас підприємство мало непогано налаштований мережевий периметр (міжмережевий екран, антивірус), що створювало хибне відчуття захищеності [4, 10].

Інвентаризація чутливих цифрових активів. Першим кроком стала повна інвентаризація всіх ЧЦА відповідно до методології МАГАТЕ [1]. Було ідентифіковано: SCADA-сервер та інженерну робочу станцію в серверній кімнаті головного офісу; три ПЛК Siemens S7-300 на насосних станціях № 1, 2, 3 за периметром будівлі; чотири диспетчерські робочі станції в операційному залі; мережеве комутаційне обладнання (два керованих комутатори та маршрутизатор); архівний сервер з базою даних технологічних параметрів за останні 5 років. Для кожного активу було визначено його місцезнаходження, рівень критичності та перелік осіб, що мають доступ до нього.

Визначення зон безпеки та їх меж. На основі інвентаризації було визначено три зони відповідно до градуйованого підходу МАГАТЕ [1]: Зона А (найвищий рівень) – серверна кімната з SCADA-сервером та архівним сервером, доступ лише для системного адміністратора та начальника відділу АСУ (2 особи); Зона Б (середній рівень) – операційний зал з диспетчерськими станціями, доступ для 12 диспетчерів і 3 інженерів у межах робочих змін; Зона В (базовий рівень) – решта

офісних та виробничих приміщень, включно з насосними станціями, де встановлено ПЛК. Польові пристрої (ПЛК) були виокремлені як окремий підтип Зони В з підвищеними вимогами через їх розташування поза будівлею [1, 6].

Впровадження засобів фізичного контролю по зонах. Для Зони А: механічний замок замінено на електронний замок зі зчитувачем смарт-карток та PIN-кодом (двофакторна автентифікація); встановлено IP-камеру всередині приміщення з безперервним записом; на серверних стійках встановлено окремі замки; усі USB-порти на серверах фізично заблоковано; введено правило двох осіб для будь-яких технічних робіт усередині Зони А. Для Зони Б: встановлено електронні замки зі зчитувачами карток на дверях операційного залу; USB-порти на диспетчерських станціях заблоковано фізичними блокаторами та заборонено на рівні групових політик; запроваджено реєстр дозволених знімних носіїв. Для ПЛК на насосних станціях: шафи з ПЛК закрито на замки та обладнано індикаторами втручання (tamper seals); встановлено датчики відкриття дверей шафи з сигналом до диспетчерського центру [1, 5, 6] (рис. 6).

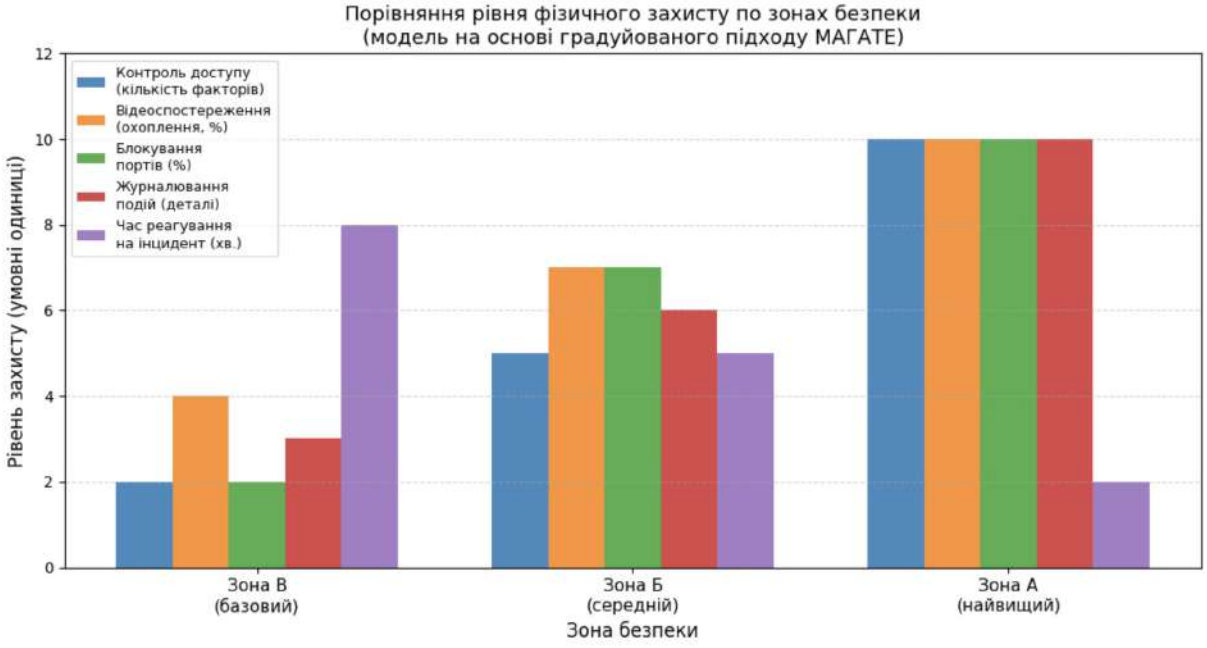


Рис. 6 – Порівняння рівня фізичного захисту по зонах безпеки умовного підприємства водопостачання після впровадження зональної моделі.

Крок 4. Організаційні заходи та управління конфігурацією. Паралельно з технічними заходами було впроваджено організаційні процедури: затверджено перелік уповноважених осіб для кожної зони з принципом мінімальних привілеїв; розроблено інструкцію щодо поводження зі знімними носіями; введено обов'язкове документування всіх технічних робіт у серверній кімнаті; складено та затверджено базову конфігурацію для кожного ЧЦА з регулярною верифікацією відповідності реального стану. Крім того, електронний замок Зони А налаштовано в режимі fail-secure (у разі відключення живлення двері залишаються замкненими), а для живлення замку передбачено резервний акумулятор [1, 5].

Результати впровадження. Через три місяці після впровадження під час планової перевірки один із підрядників, що мав доступ до Зони В для технічного обслуговування насосного обладнання, спробував підійти до шафи ПЛК насосної станції № 2 без відповідного дозволу. Датчик відкриття дверей зафіксував спробу і автоматично надіслав сповіщення диспетчеру, а інцидент було задокументовано та розслідувано. До впровадження такий підхід залишився б непоміченим. Аудит журналів доступу до Зони А також виявив кілька спроб входу за межами дозволених годин, що дозволило своєчасно переглянути рівні доступу персоналу. Жодного інциденту, пов'язаного з підключенням несанкціонованих USB-носіїв, зафіксовано не було, тоді як до блокування такі факти відбувалися, за оцінками, до двох разів на місяць [1, 7].

Наведений сценарій підтверджує, що навіть відносно нескладне і бюджетно доступне впровадження зональної моделі та базових засобів фізичного контролю дає вимірюваний практичний ефект: інциденти, які раніше залишалися непоміченими, стають видимими та відстежуваними. Ключовим є не вартість технічних засобів, а системність підходу – дотримання принципів МАГАТЕ щодо інвентаризації ЧЦА, визначення зон, застосування багаторівневого захисту та безперервного моніторингу [1, 2, 5].

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Висновок

У роботі розглянуто принципи багаторівневого захисту, зонування безпеки, класифікацію загроз та підходи до їх нейтралізації відповідно до міжнародних стандартів і рекомендацій МАГАТЕ.

Показано, що фізичний захист комп'ютерних систем є самостійним і рівноправним рівнем інформаційної безпеки, що не може бути замінений технічними або адміністративними заходами. Ігнорування фізичного рівня безпеки створює критичні вразливості навіть у системах, що добре захищені з програмної точки зору. Зловмисник, що отримав фізичний доступ до обладнання, здатен обійти будь-які логічні засоби захисту.

Встановлено, що зональна модель та принцип багаторівневого захисту є найбільш ефективними архітектурними підходами до організації фізичного захисту. Вони дозволяють диференційовано застосовувати заходи залежно від критичності активів і забезпечують стійкість системи до атак завдяки відсутності єдиної точки відмови: подолання одного шару захисту не дає змоги скомпрометувати всю систему.

Доведено, що внутрішні загрози та атаки на ланцюг постачання є специфічними векторами, для протидії яким стандартних периметрових засобів захисту недостатньо. Необхідне системне застосування принципів мінімальних привілеїв, розподілу обов'язків, двох осіб, а також суворий контроль процесів закупівель і приймання обладнання.

Як бачимо, повноцінна ефективність фізичного захисту досягається лише за умови його інтеграції в загальну програму комп'ютерної безпеки організації, узгодженості з планом фізичного захисту об'єкту та безперервного моніторингу. Методологічний підхід МАГАТЕ, розроблений для захисту ядерних установок, є зразковим і може бути адаптований до будь-яких організацій, що управляють критично важливими інформаційними системами, тобто від промислових підприємств до установ державного управління.

Список літератури

1. International Atomic Energy Agency. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T. Vienna: IAEA, 2021. 242 p.
2. International Atomic Energy Agency. Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G, Implementing Guide. Vienna: IAEA, 2021.
3. International Atomic Energy Agency. Security of Nuclear Information. IAEA Nuclear Security Series No. 23-G, Implementing Guide. Vienna: IAEA, 2015.
4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken, NJ: John Wiley & Sons, 2020. 1232 p.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
6. NIST Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
7. Lee, R. M., Assante, M. J., Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC: SANS Industrial Control Systems, 2016. 28 p.
8. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011. Vol. 9, No. 3. P. 49–51.
9. Scarfone K., Souppaya M. Guide to Enterprise Password Management. NIST Special Publication 800-118 (Draft). Gaithersburg: NIST, 2009.
10. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки : навчальний посібник. Київ : Київський університет імені Бориса Грінченка, 2019. 320 с.
11. IAEA-NSS-46-T, Evaluation of Physical Protection Systems at Nuclear Facilities, Technical Guidance, International Atomic Energy Agency (IAEA), 2025. https://doi.org/10.61092/iaea.pckz-it39
12. Aneka Choi, Cheonho Park, JuHyeon Lee, Seungho Jeon, Jung Taek Seo. Framework for evaluating cyber incident response capabilities of nuclear facility operators through operation-based exercises. Nuclear Engineering and Technology, Volume 57, Issue 11, 2025. https://doi.org/10.1016/j.net.2025.103772
13. Amal Touarsi, Amina Kharchaf, Chakir El Mahjoub. A novel methodology assessment to study the performance of the physical protection system for enhancing the security of nuclear and other radioactive materials during transport. Annals of Nuclear Energy, Volume 219, 2025. https://doi.org/10.1016/j.anucene.2025.111408
14. Marja Ylönen, Kim Björkman. Integrated management of safety and security (IMSS) in the nuclear industry — Organizational culture perspective. Safety Science, Volume 166, 2023. https://doi.org/10.1016/j.ssci.2023.106236
15. Nabin Chowdhury, Vasileios Gkioulos. Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, Volume 40, 2021. https://doi.org/10.1016/j.cosrev.2021.100361

References

1. International Atomic Energy Agency. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T. Vienna: IAEA, 2021. 242 p.
2. International Atomic Energy Agency. Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G, Implementing Guide. Vienna: IAEA, 2021.
3. International Atomic Energy Agency. Security of Nuclear Information. IAEA Nuclear Security Series No. 23-G, Implementing Guide. Vienna: IAEA, 2015.
4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken, NJ: John Wiley & Sons, 2020. 1232 p.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
6. NIST Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
7. Lee, R. M., Assante, M. J., Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC: SANS Industrial Control Systems, 2016. 28 p.
8. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011. Vol. 9, No. 3. P. 49–51.
9. Scarfone K., Souppaya M. Guide to Enterprise Password Management. NIST Special Publication 800-118 (Draft). Gaithersburg: NIST, 2009.

10. Buryachok V. L., Kyrychok R. V., Skladanyy P. M. Osnovy informatsiynoyi ta kibernetychnoyi bezpeky : navchal′nyy posibnyk. Kyyiv : Kyyivs′kyy universytet imeni Borysa Hrinchenka, 2019. 320 s.
11. IAEA-NSS-46-T, Evaluation of Physical Protection Systems at Nuclear Facilities, Technical Guidance, International Atomic Energy Agency (IAEA), 2025. https://doi.org/10.61092/iaea.pckz-it39
12. Aneka Choi, Cheonho Park, JuHyeon Lee, Seungho Jeon, Jung Taek Seo. Framework for evaluating cyber incident response capabilities of nuclear facility operators through operation-based exercises. Nuclear Engineering and Technology, Volume 57, Issue 11, 2025. https://doi.org/10.1016/j.net.2025.103772
13. Amal Touarsi, Amina Kharchaf, Chakir El Mahjoub. A novel methodology assessment to study the performance of the physical protection system for enhancing the security of nuclear and other radioactive materials during transport. Annals of Nuclear Energy, Volume 219, 2025. https://doi.org/10.1016/j.anucene.2025.111408
14. Marja Ylönen, Kim Björkman. Integrated management of safety and security (IMSS) in the nuclear industry — Organizational culture perspective. Safety Science, Volume 166, 2023. https://doi.org/10.1016/j.ssci.2023.106236
15. Nabin Chowdhury, Vasileios Gkioulos. Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, Volume 40, 2021. https://doi.org/10.1016/j.cosrev.2021.100361

Відомості про авторів / About the Authors

Лис Степан Степанович – кандидат технічних наук, доцент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: lysss@ukr.net, тел.: (032) 258-23-15; ORCID: 0000-0002-7359-1177.

Stepan Lys – Assoc. Prof., Ph.D., Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: lysss@ukr.net; ORCID: 0000-0002-7359-1177.

Ісопенко Андрій Ярославович – студент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: andrii.isopenko.kb.2024@lpnu.ua, тел.: (032) 258-23-15.

Andrii Isopenko – student, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: andrii.isopenko.kb.2024@lpnu.ua.

Загаровський Віталій Васильович – студент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: vitalii.zaharovskyi.kb.2024@lpnu.ua, тел.: (032) 258-23-15.

Vitalii Zaharovskyi – student, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: vitalii.zaharovskyi.kb.2024@lpnu.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Лис С. С., Ісопенко А. Я., Загаровський В.В. Організація фізичного захисту комп’ютерних систем критичної інфраструктури на основі стандартів та рекомендацій МАГАТЕ. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 35-45. doi:10.20998/2413-4295.2026.02.05.

Please cite this article as:

Lys S., Isopenko A., Zaharovskyi V. Organization of physical protection of computer systems of critical infrastructure based on IAEA standards and recommendations. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 35–45, doi:10.20998/2413-4295.2026.02.05.

Надійшла (received) 07.04.2026
Прийнята (accepted) 28.04.2026
Опублікована (published) 05.06.2026

УДК 537.876.4 doi: 10.20998/2413-4295.2026.02.06

ДИНАМІЧНЕ КЕРУВАННЯ СПЕКТАЛЬНИМИ ХАРАКТЕРИСТИКАМИ ОДНОВИМІРНИХ ФОТОННИХ КРИСТАЛІВ

Г. С. ХРИПУНОВ[1], А. В. МЕРІУЦ[1], Т. М. ШЕЛЕСТ[2], А. О. ТРУБІЛІН[1], С. С. КРИВОНІС[2]

[1]кафедра мікро- та наноелектроніки, Національний технічний університет «ХПІ», Харків, УКРАЇНА
[2]кафедра фізики, Національний технічний університет «ХПІ», Харків, УКРАЇНА
[*]e-mail: Tetiana.Shelest@khpi.edu.ua

АНОТАЦІЯ *Методом передатної матриці проведено теоретичне дослідження впливу локальних дефектів на спектральні характеристики одновимірних фотонних кристалів, сформованих із періодично повторюваних діелектричних шарів. Проаналізовано спектри пропускання, відбиття та поглинання електромагнітних хвиль у фотонних кристалах за наявності дефектів заміщення, вставлення, двійників та поверхневих дефектів та наявності загасання в шарах. Для конструювання фотонних кристалів з заданими властивостями запропоновано підхід, заснований на використанні графіків, які ілюструють динаміку зміни положень границь зон і дефектних мод при зміні параметрів дефектного шару. Ці графіки дозволяють зручно і швидко обирати параметри дефектного шару за бажаним значенням частоти дефектної моди. Продемонстровано можливість динамічного керування положенням дефектних мод шляхом використання комбінованих дефектів за участі шару повітря, ширину якого можна змінювати в реальному часі. Наявність шару повітря також дозволяє отримати одразу дві рухомі дефектні моди в забороненій зоні. Отримані результати можуть бути корисними для проєктування приладових структур фотоніки та радіоелектроніки надвисокочастотного діапазону.*

Ключові слова: *одновимірний фотонний кристал, дефектні моди, діелектрична проникність, заборонена зона, дефект, спектри пропускання та відбиття*

DYNAMIC CONTROL OF SPECTRAL CHARACTERISTICS IN ONE-DIMENSIONAL PHOTONIC CRYSTALS

G. S. KHRYPUNOV[1], A. V. MERIUTS[1], T. M. SHELEST[2], A. O. TRUBILIN[1], S. S. KRYVONIS[2]

[1] Department of Micro- and Nanoelectronics, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, UKRAINE
[2] Department of Physics, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, UKRAINE

ABSTRACT *Theoretical study of the influence of local defects on the spectral characteristics of one-dimensional photonic crystals formed by periodically repeated dielectric layers has been carried out using the transfer matrix method. The transmission, reflection, and absorption spectra of electromagnetic waves in photonic crystals have been analyzed in the presence of substitutional, interstitial, twin, and surface defects, as well as accounting for losses in the layers. For the design photonic crystals with specified properties, an approach based on the use of plots illustrating the evolution of the band-edge positions and defect modes as a function of defect layer parameters has been proposed. These plots enable convenient and rapid selection of defect layer parameters corresponding to a desired defect mode frequency. The possibility of dynamic control of defect mode positions by employing combined defects involving an air layer with tunable thickness has been demonstrated. The presence of the air layer also allows for the emergence of two simultaneously tunable defect modes within the bandgap. The obtained results can be useful for the design of device structures in photonics and microwave terahertz electronics.*

Keywords: *one-dimensional photonic crystal, defect modes, dielectric permittivity, photonic bandgap, defect, transmission and reflection spectra*

Вступ

Унікальні фізичні властивості одновимірних фотонних кристалів (1D ФК) дозволяють застосовувати їх для керування розповсюдженням електромагнітних хвиль в високочастотній і надвисокочастотній електроніці [1]. Останні наукові публікації показують, що такі штучні періодичні структури також мають великі перспективи для застосування в приладових структурах наноелектроніки [2], спінтроніки [3, 4], оптоелектроніки та фотоніки [5 - 8], зокрема, для створення вузькосмугових фільтрів, сенсорів та багатофункціональних фотонних пристроїв із високою чутливістю [9 – 11].

Фотонні кристали є штучними періодичними структурами з наперед заданими властивостями. Основними особливостями таких періодичних структур, незалежно від сфери їхнього застосування, є: по-перше, створення ними дозволених і заборонених зон для розповсюдження електромагнітних хвиль або інших частинок і квазічастинок в твердому тілі [12], та, по-друге, можливість отримання штучних середовищ з ефективною від'ємною діелектричною або магнітною проникністю [13]. Дозволені й заборонені зони для

розповсюдження електромагнітних хвиль з'являються за рахунок періодичної модуляції діелектричної (або магнітної) проникності з періодом, порівнянним з довжиною електромагнітної хвилі, падаючої на ФК. У такому середовищі, подібно до електронів в звичайному кристалі, відбувається квантування властивостей фотонів, яке призводить до формування фотонних заборонених зон.

Аналогічно тому, як у звичайних кристалах введення дефектів призводить до модифікації енергетичного спектру електронів, у фотонних кристалах порушення періодичності зумовлює появу локалізованих дефектних мод у фотонній забороненій зоні, що проявляється у вигляді вузьких резонансних максимумів у спектрах пропускання та відбиття [14]. Сучасні дослідження 1D ФК спрямовані на пошук ефективного керування положенням, кількістю і добротністю таких мод, як за рахунок параметрів структури, зокрема товщиною та фізичними властивостями матеріалів, так і за рахунок зовнішніх впливів. Так, наприклад, у ФК з використанням шару надпровідника в матриці спостерігається висока керованість дефектних мод під дією температури, тиску та кута падіння хвилі, що забезпечує створення високочутливих оптичних сенсорів нового покоління [15 – 17].

Таким чином, дослідження впливу різних типів дефектів у 1D ФК на його спектральні характеристики і пошук можливостей динамічного керування цими характеристиками є актуальним для подальшої розробки фізичних засад конструктивно-технологічних рішень інноваційних приладових структур на основі ФК.

Мета роботи

Проведення теоретичного дослідження впливу дефектів на спектральні характеристики 1D ФК, сформованих із шарів діелектриків, а також пошук можливостей динамічного керування цими характеристиками для розробки фізичних основ створення приладових структур на основі 1D ФК для НВЧ радіоелектроніки.

Методика досліджень

Дослідження розповсюдження електромагнітних хвиль в одновимірних періодичних структурах було виконано методом передатної матриці, який описаний, наприклад, у [14, 18]. В цьому методі рівняння Максвела доповнені граничними умовами, які полягають в неперервності тангенціальних компонент поля на границях розділу середовищ з різними властивостями. Підставивши компоненти поля в граничні умови, наприклад, для першого шару періодичної структури, можна отримати передатну матрицю, яка встановлює зв'язок полів на початку і в кінці шару (для першого шару це точки $z = 0$ та $z = d_1$). Наприклад, для ТЕ хвилі маємо:

$$\begin{pmatrix} E_y(0) \\ H_x(0) \end{pmatrix} = m(d_1)\begin{pmatrix} E_y(d_1) \\ H_x(d_1) \end{pmatrix},$$

$$m(d_1) = \begin{pmatrix} \cosh(ik_{z1}d_1) & -\dfrac{\omega}{ck_{z1}}\sinh(ik_{z1}d_1) \\ -\dfrac{ck_{z1}}{\omega}\sinh(ik_{z1}d_1) & \cosh(ik_{z1}d_1) \end{pmatrix}, \quad (1)$$

де $k_z = \sqrt{\varepsilon\omega^2/c^2 - k_x^2}$, $k_x = (\varepsilon\omega/c)\sin\theta$, θ – кут падіння хвилі на границю структури, ε – діелектрична проникність.

Матриця $m(d_1)$ є передатною матрицею шару. Аналогічно, можна отримати передатну матрицю для другого шару $m(d_2)$, яка буде відрізнятися від $m(d_1)$ тільки заміною індексу $1 \rightarrow 2$. Для того, щоб пов'язати поля на початку і в кінці одного періоду структури (в точках $z = 0$ і $z = d = d_1 + d_2$), потрібно знайти добуток цих матриць, тобто передатну матрицю для одного періоду $m = m(d_1)m(d_2)$.

Оскільки структура є періодичною, а поля на границях періоду можуть відрізнятися тільки на фазовий множник, то:

$$E(0) = E(d)\exp(i\bar{k}d). \quad (2)$$

У періодичній структурі залежність від поперечної координати визначається не хвильовими числами шарів k_{z1}, k_{z2}, а усередненим за весь період блохівським хвильовим числом, яке пов'язане з власними числами передатної матриці рівнянням $q^2 + (m_{11} + m_{22})q + 1 = 0$, $q = \exp(i\,\bar{k}d)$.

Для встановлення зв'язку між точками періодичної структури, які знаходяться на відстані цілої кількості періодів N, необхідно знайти добуток матриць одного періоду, або звести матрицю m у відповідний ступінь за допомогою теореми Абеле [14]. За допомогою передатної матриці $M = m^N$ для всієї періодичної структури загальною довжиною L, яка розташована між двома однорідними середовищами a і b, можна отримати вирази для амплітудних коефіцієнтів пропускання τ і відбиття r для періодичної структури:

$$t = \frac{2\exp(ik_{zb}L)}{\left(M_{11} - \dfrac{ck_{zb}}{\omega}M_{12}\right) + \left(\dfrac{k_{zb}}{k_{za}}M_{22} - \dfrac{\omega}{ck_{za}}M_{21}\right)},$$

$$r = \frac{\left(M_{11} - \dfrac{ck_{zb}}{\omega}M_{12}\right) - \left(\dfrac{k_{zb}}{k_{za}}M_{22} - \dfrac{\omega}{ck_{za}}M_{21}\right)}{\left(M_{11} - \dfrac{ck_{zb}}{\omega}M_{12}\right) + \left(\dfrac{k_{zb}}{k_{za}}M_{22} - \dfrac{\omega}{ck_{za}}M_{21}\right)}. \quad (3)$$

Енергетичні відносні коефіцієнти пропускання й відбиття визначаються як модулі відповідних амплітудних коефіцієнтів:

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

$$T = |t|^2, \ R = |r|^2. \quad (4)$$

За наявності втрат при розповсюдженні хвилі в деякому середовищі їх можна врахувати введенням комплексної діелектричної проникності $\varepsilon = \varepsilon' - i\varepsilon''$, а енергію ($A$), яка була поглинена середовищем, можна розрахувати, користуючись законом збереження енергії: $T + R + A = 1$.

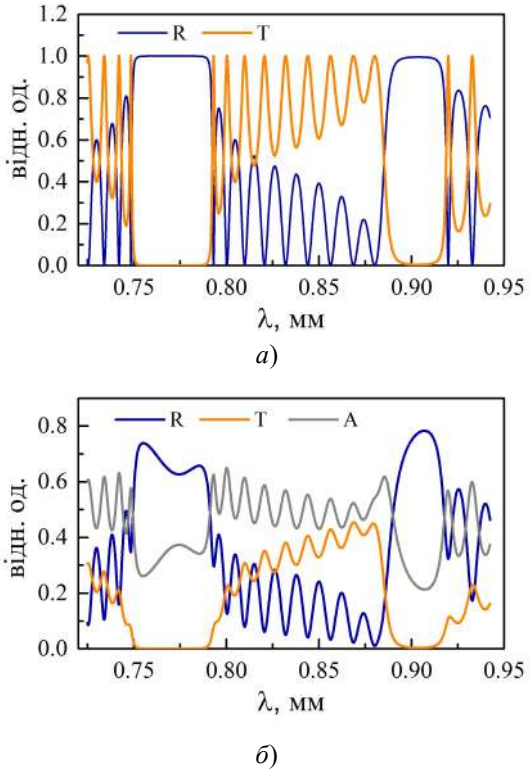
На основі викладених теоретичних уявлень була розроблена комп'ютерна програма для розрахунку спектральних характеристик коефіцієнтів відбиття, пропускання і поглинання одновимірного фотонного кристалу з різними типами дефектів.

Обговорення результатів

1. Одновимірний фотонний кристал без дефектів, вплив загасання

Для наявності в спектрі пропускання і відбиття ФК дозволених і заборонених смуг мають виконуватися дві умови. По-перше, товщини шарів повинні бути порядку довжини хвилі $d_{1,2} \sim \lambda$, оскільки для $\lambda <\sim 0.1 d_{1,2}$ заборонені зони стають настільки вузькими, що їх складно виділити. А для хвиль $\lambda >\sim 6 d_{1,2}$ структура ФК буде сприйматися як однорідне середовище з деякою ефективною діелектричною проникністю. Надалі ми будемо розглядати частоти 300 – 400 ГГц, що потрапляють в частотний діапазон 6G. В якості матеріалів для ФК слід обирати такі, які мають якомога більшу різницю діелектричної проникності, що дозволить створити суттєвий контраст при розповсюдженні електромагнітної хвилі. В якості модельної структури ми розглядаємо далі ФК, сформований з шару кварцу (SiO_2) з відносною діелектричною проникністю $\varepsilon_{SiO_2} = 3.8$, і товщиною $d_1 = 0.5$ мм, і шару кремнію (Si) з відносною діелектричною проникністю $\varepsilon_{Si} = 11.85$, і товщиною $d_2 = 0.5$ мм. Технологія отримання цих матеріалів необхідної якості добре відпрацьована сучасною електронною промисловістю. Розглядаємо ФК $N\{SiO_2/Si\}$, який має 10 періодів ($N = 10$). Як видно з розрахованих спектрів пропускання і відбиття при нормальному падінні електромагнітних хвиль ($\theta = 0°$) в обраному частотному діапазоні спостерігається дві заборонені зони для довжин хвиль 0.75 – 0.793 мм та 0.89 – 0.918 мм (рис. 1, а). При зміні кута падіння до 15° – 20° картину зон можна вважати практично сталою, вона лише трохи зміщується в бік коротших хвиль. Суттєве спотворення цієї картини спостерігається починаючи з кутів падіння хвилі 30° – 40°, а для кута падіння 60° заборонені зони в обраному частотному діапазоні зникають.

Другою умовою спостереження чіткої картини зон є низький рівень втрат в обраному частотному діапазоні в матеріалах, з яких складено ФК. Моделювання свідчить, що величина діелектричних втрат суттєво впливає на вигляд спектральних характеристик ФК. Якщо тангенс кута діелектричних втрат, ($\varepsilon''/\varepsilon' = \mathrm{tg}(\delta)$) досягає 1 %, то спектри суттєво спотворюються, хоча наявність зонної структури спектру ще можна спостерігати (рис. 1 б)), але більша частина енергії хвиль поглинається в матеріалах, з яких складено фотонний кристал.



а)

б)

Рис. 1 – Спектри пропускання, відбиття і поглинання ФК 10{SiO_2-Si} без дефектів: а) без втрат, б) з втратами tg(δ) = 0.0038

Для якісного кварцу тангенс кута діелектричних втрат має порядок $\mathrm{tg}(\delta) \approx 10^{-4}$, а для чистого кремнію в темноті ця величина буде ще меншою $\leq 5 \cdot 10^{-5}$. Такі малі втрати трохи зменшують пропускання в дозволених зонах і на 1 – 2 % зменшують відбиття в заборонених зонах та дещо згладжують границі заборонених зон. При цьому спектр пропускання залишається практично незмінним. В подальших розрахунках прийнято, що втрати в шарах є малими, як вказано вище, але не дивлячись на це слід зауважити, що в разі наявності в складі ФК шару навіть з мінімальним загасанням виникає можливість суттєвого поглинання на дефектній моді (див. рис. 2), навіть якщо шар дефекту сам по собі зовсім не має втрат. Збільшення кількості періодів ФК призводить до того, що енергія на дефектній моді може практично повністю поглинатися замість того, щоб проходити через кристал, як це відбувається за повної відсутності втрат. При цьому поглинання на всіх інших частотах не зазнає суттєвих змін.

2. Вплив дефектів та динамічне керування спектрами

Для одновимірного ФК розглянемо наступні типи дефектів: I тип – двійник, коли дефект змінює порядок чергування шарів; II тип – дефект заміщення, коли шар з матеріалу, відмінного від тих, які складають періодичну структуру, вбудований на місце одного з матричних шарів; III тип – дефект вставлення, коли додатковий шар іншого матеріалу, вставлений між регулярно повторюваними періодами матриці ФК; IV тип – поверхневий дефект, граничний випадок дефекту III-го типу; Дефект I-го типу насправді може бути зведеним до дефекту III-го типу. Для будь-якого з локальних дефектів загальний вид передатної матриці був представлений як добуток матриці регулярної частини кристалу, яка знаходиться перед дефектом, на матрицю дефекту і на матрицю регулярної частини кристалу, яка знаходиться після дефекту:

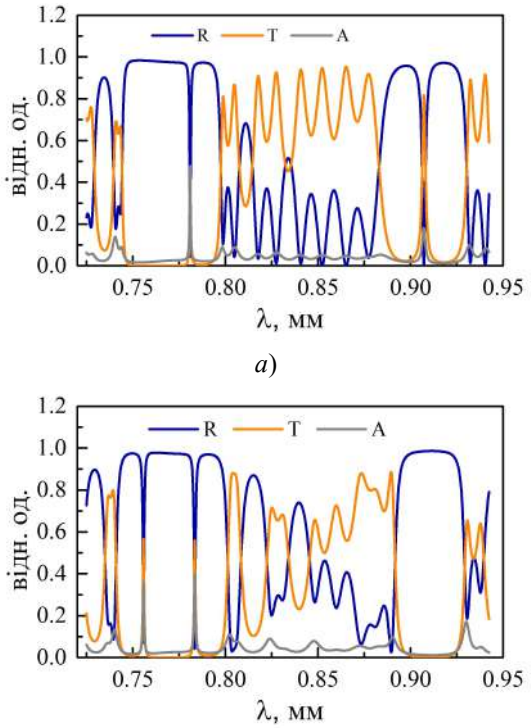
$$M = m^{N1} m_v m^{N2}, \quad (5)$$

де $N_{1,2}$ – кількість періодів ФК до та після дефекту, m_v – матриця дефектного шару, яка визначатися виразом, аналогічним до (1) з заміною індексу 1 на індекс v.

Для дефекту можна обирати як матеріали, які мають діелектричну проникність відмінну від такої для матеріалів шарів ФК, а можна використати ті самі матеріали, які складають ФК, але з іншою товщиною, не порушуючи регулярний порядок шарів. Можна запропонувати різні варіанти комбінацій заміщення чи вставлення дефектних шарів з точки зору співвідношення величини діелектричної проникності дефектного шару і шарів, з яких складено ФК. Наявність дефекту призводить до появи так званої дефектної моди в заборонених зонах, тобто частоти, на якій стає можливим пропускання. Для прикладу на рис. 2 приведено спектри для обраного вище ФК у випадку дефекту заміщення.

Модельні розрахунки показують, що принципової відмінності впливу виду дефекту на вигляд спектру немає. Зазвичай зміною товщини шару можна отримати якісно ідентичні картини спектральних характеристик для всіх зазначених вище локальних дефектів. Також загальним результатом для будь якого типу дефекту є те, що зміщення дефектного шару від центру до краю кристалу призводить до зменшення пропускання на дефектній моді. Коли дефект опиняється на початку, або в кінці ФК, тобто фактично стає поверхневим дефектом (типу IV), то дефектна мода зникає. При цьому різниця в спектрах пропускання і відбиття для положення дефекту на початку або в кінці структури спостерігається в дозволених зонах, тоді як заборонені зони залишаються майже однаковими з незначним зміщенням положення їхніх країв. Таким чином, можна сказати, що поверхневий дефект не впливає на спектр пропускання і відбиття в заборонених зонах, якщо його діелектрична проникність є постійною величиною і не містить уявної частини (тобто, втрат).

Як видно з графіків на рис. 2, в залежності від співвідношення параметрів дефектного шару та параметрів матричних шарів ФК дефектна мода може існувати не в усіх зонах. Також з результатів моделювання випливає, що найбільші зміни в спектрі спостерігаються тоді, коли діелектрична проникність дефектного шару максимально відрізняється від такої для шарів, які складають період ФК.



а)

б)

Рис. 2 – Спектри пропускання, відбиття і поглинання ФК з повітрям в якості дефектного шару заміщення: а) 5{SiO₂/Si}/Air/Si/4{SiO₂/Si} – заміщений шар SiO₂, б) 5{SiO₂/Si}/SiO₂/Air/4{SiO₂/Si}– заміщений шар Si

Для отримання загальної уяви про вплив дефекту на вигляд спектральних характеристик і передбачення положення дефектної моди, а також кількості таких мод в забороненій зоні в залежності від параметрів дефекту, ми пропонуємо підхід, заснований на використанні графіків, які ілюструють динаміку зміни положень границь зон і дефектних мод при зміні параметрів дефектного шару (рис. 3). На цих графіках показано положення заборонених зон які знаходяться між суцільними лініями, і положення дефектної моди, яке позначено точками, як функцію ширини дефектного шару d_v. Схожий вигляд мають залежності і від ε_v, але залежності від d_v є більш реальними, оскільки забезпечити неперервну зміну ε_v в широких межах набагато складніше ніж зміну d_v.

Як видно з модельних графіків (рис. 3), і, як випливає з виразів для матричних елементів (1), ці

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

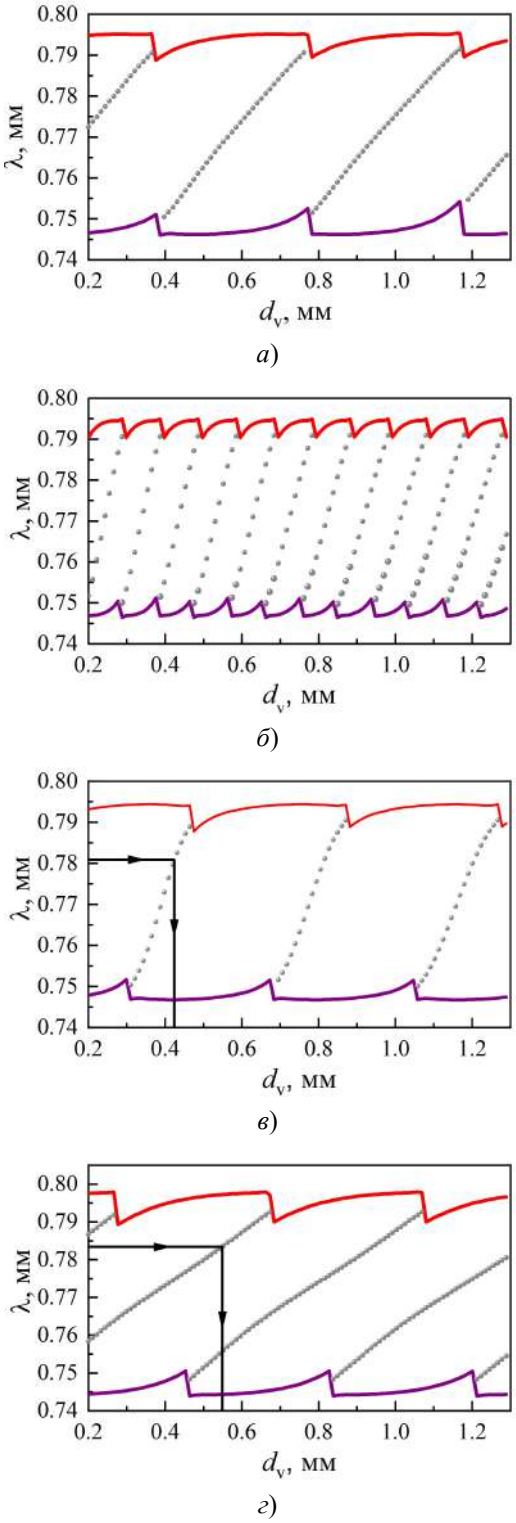


Рис. 3 – Положення заборонених зон (лінії) і дефектної моди (точки), як функція ширини дефектного шару d_v для ФК з дефектом:
а) 5{SiO₂/Si}/Air(ε_v = 1)/5{SiO₂/Si};
б) 5{SiO₂/Si}/Ge(ε_v = 16)/5{SiO₂/Si};
в) 5{SiO₂/Si}/Air/Si/4{SiO₂/Si};
г) 5{SiO₂/Si}/SiO₂/Air/4{SiO₂/Si}

графіки є періодичними функціями d_v і ε_v. Вони дозволяють показати всі зміни в спектрі, що стосуються заборонених зон і зумовлені внесенням дефекту до ФК, а також залежність цих змін від ширини дефектного шару. Як видно з цих графіків, наявність або відсутність дефектної моди залежить від товщини дефектного шару. Поява дефектної моди в забороненій зоні призводить до розширення зон по відношенню до їхньої ширини в бездефектному кристалі. Максимальна ширина забороненої зони спостерігається коли ширина дефектного шару така, що дефектна мода знаходиться посередині забороненої зони, а мінімальна, коли дефектна мода виходить з зони, що викликає достатньо різке звуження зони до її значення в бездефектному кристалі. За наявності двох дефектних мод в одній зоні зміна її ширини подвоюється. Графіки зображені на рис. 3 дозволяють обрати параметри дефектного шару для отримання потрібного положення дефектної моди. Провівши горизонтальну лінію, яка відповідає бажаній робочій частоті, до перетину з лінією, яка визначає положення дефектної моди в забороненій зоні, можна визначити необхідну товщину дефектного шару. Як приклад, лінії, проведені на рис. 3 в) та г) відповідають спектру з дефектними модами, зображеними на рис. 2 а) та б), відповідно. Як бачимо, на рис. 3 г) вертикальна лінія перетнула дві лінії дефектних мод, що відповідає двом модам в забороненій зоні на рис. 2 б).

Якщо дефектний шар являє собою шар твердого матеріалу, то неперервна зміна товщини цього шару в готовому приладі є неможливою, тому динамічне керування положенням дефектної моди потребує впливу на його діелектричну проникність. В разі ж, якщо дефект являє собою шар повітря, керування положенням дефектної моди в динамічному режимі стає можливим. В такому разі за допомогою крокових двигунів і мікрогвинтів стає можливим налаштування положення дефектної моди в забороненій зоні і керування кількістю таких мод (одна або дві, рис. 3 г). Біше ступенів свободи в налаштуванні положення дефектної моди можна отримати, якщо використовувати комбінований дефект, розмітивши додотковий діелектричний шар в шарі повітря. Загальну формулу структури ФК з таким комбінованим дефктом можна записати у вигляді: N{D1/D2}/(A1/Dv/A2)/N{D1/D2}, тут D1, D2, Dv – символи діелектричних шарів матриці ФК, і додаткового твердого делектричного шару, A1, A2 – символи шару повітря.

В якості прикладу на рис. 4 приведено декілька результатів моделювання положення заборонених зон і дефектних мод для такої структури (з параметрами ФК прийнятими вище), як функції ширини шару повітря ($0 < d_{a1} < 1$ мм, $d_{a2} = 1 - d_{a1}$), d_v = 0.5 мм.

Як видно з графіків, обраний діапазон варіювання d_{a1} є надлишковим, але він демонструє періодичність і дозволяє обрати максимальне доцільне значення d_{a1}. Для даного ФК достатньо було

б варіювати d_{a1} в діапазоні від 0 до 0.4 мм, щоб отримати всі можливі варіанти положення дефектних мод. Також з результатів моделювання видно, що на

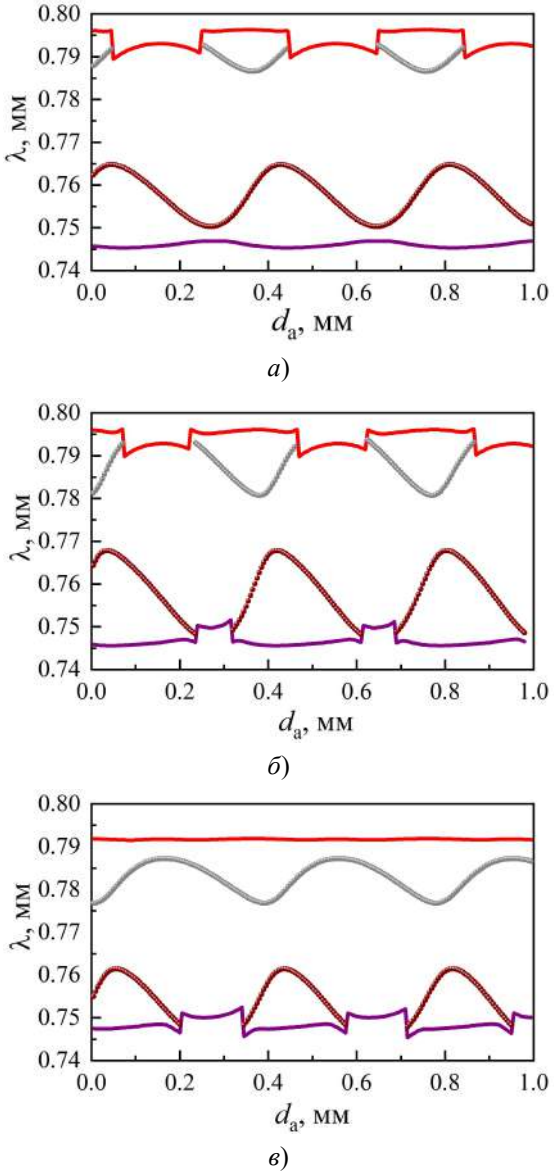


Рис. 4 – Положення заборонених зон (лінії) і дефектної моди (точки), як функція ширини шару повітря ($0 < d_{a1} < 1$, $d_{a2} = 1 - d_{a1}$) для ФК з комбінованим дефектом:
а) 5{SiO₂/Si}/(Air/SiO₂/Air)/5{SiO₂/Si};
б) 5{SiO₂/Si}/(Air/Si/Air)/5{SiO₂/Si};
в) 5{SiO₂/Si}/(Air/Ge/Air)/5{SiO₂/Si};

відміну від простого дефекту, коли дефектна мода проходить через всю зону при зміні його параметрів, для комбінованого дефекту завжди залишається область заборонених частот в яку дефектні моди не потрапляють. Разом з тим виникає можливість комбінувати частоту однієї дефектної моди з двома різними частотами іншої дефектної моди, змінюючи положення шару Dv між шарами повітря A1, A2. Можна також отримати майже стале положення однієї з дефектних мод, яке практично не буде залежати від позиції шару Dv між шарами повітря. Так, наприклад, для фотонного кристалу $5\{SiO_2/Si\}/(Air/GaSb(\varepsilon_v = 15)/Air)/5\{SiO_2/Si\}$, незалежно від значення $0 < d_{a1} < 1$ мм, дефектна мода буде знаходитися в діапазоні $0.77498 < \lambda < 0.77522$ мм, тобто амплітуда зміщення в залежності від позиції шару GaSb буде ~ 0.24 мкм.

Висновки

Показана можливість динамічного керування положенням дефектної моди у ФК при використанні в якості дефекту вставлення або дефекту заміщення шару повітря або комбінованого дефекту, в якому до шару повітря додано рухомий делектричний шар. Такий комбінований дефект дає більше можливих варіантів для обрання пари робочих дефектних мод. Керування шириною шару повітря може бути технічно легко реалізовано для довжин хвиль від сантиметрового до суб мілімітрового діпазонів. Для практичного конструювання ФК з заданими властивостями запропоновано підхід, заснований на використанні графіків, які ілюструють динаміку зміни положень границь зон і дефектних мод при зміні параметрів дефектного шару.

Показано, що в реальних ФК, в яких шари мають втрати, виникає необхідність обмеження кількості періодів для збереження достатнього рівня пропускання на дефектній моді.

Можливість динамічного керування положенням дефектної моди розширює перспективи застосування досліджених структур ФК в системах зв'язку.

Список літератури

1. Mohamed A. G., Elsayed H. A., Mehaney A., Aly A. H., Sabra W. Transmittance properties of one-dimensional metamaterial nanocomposite photonic crystal in GHz range. *Scientific Reports*. 2022. Vol. 12. P. 18331. doi: 10.1038/s41598-022-21455-2.
2. Ramanujam N. R., Wilson K. S. Joseph, Revathy V., Lenin M. Maria, Jothy V. Bena Properties of one Dimensional Photonic Crystals with Defects Thickness and Temperature Dependence. *Materials Today: Proceedings*. 2015. Vol. 2, Issue 3. P. 959-964. doi: 10.1016/j.matpr.2015.06.016.
3. Lubert-Perquel D., Acharya S., Johnson J. C. Optically Addressing Exciton Spin and Pseudospin in Nanomaterials for Spintronics Applications. *ACS Appl. Opt. Mater.* 2023. Vol. 1. P. 1742–1760. doi: 10.1021/acsaom.3c00299.
4. Koopmans B., Li P., Pezeshki H., Demirer E., Simons G., Jiao Y., van der Tol J., and Lavrijsen R. Towards on-Chip Spintronic-Photonic Integration. *In 2024 IEEE International Magnetic Conference - Short Papers, INTERMAG Short Papers.* 2024. Article No. 10576952. doi: 10.1109/INTERMAGShortPapers61879.2024.10576952.
5 Si Y., Ju Z., Ma H., Xia K., Lin S., Tang R., Sun B., Sun C., Li L. Realization and simulation of silicon-on-sapphire mid-infrared one-dimensional photonic crystal cavities. *Appl. Phys. Lett.* 2025. Vol. 126. P. 021101. doi: 10.1063/5.0241260.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

6. Sadoun B., Mouetsi S., Hocini A. and Hocini A. Optical properties of one-dimensional photonic crystal and light absorption enhancement in planar a-Si:H solar cell. *IOP Conference Series: Materials Science and Engineering*. 2021. Vol. 1046. Article No. 012014. doi: 10.1088/1757-899X/1046/1/012014.
7. Gangwar R. K., Pathak A. K., and Kumar S. Recent Progress in Photonic Crystal Devices and Their Applications: A Review. *Photonics*. 2023. Vol. 10, Issue 11. Article No. 1199. doi: 10.3390/photonics10111199.
8. Kou D., Zhang S., and Ma W. Recent Advances in 1D Photonic Crystals: Diverse Morphologies and Distinctive Structural Colors for Multifaceted Applications. *Adv. Opt. Mater*. 2024. Vol. 12, Issue 19. Article No. 2400192. doi: 10.1002/adom.202400192.
9. Hao K., Li Z., Wang X., Yang S., Zhang J. and Gao Y. Transmission characteristics of one-dimensional photonic crystal with dielectric defect layer in near-infrared band. *Proc. of SPIE*. 2020. Vol. 11564. Article No. 1156403 doi: 10.1117/12.257955.
10. Wu M.-R., Wu C.-J., Chang S.-J. Investigation of defect modes in a defective photonic crystal with a semiconductor metamaterial defect. *Physica E: Low-dimensional Systems and Nanostructures*. 2014. Vol. 64. P. 146-151. doi: 10.1016/j.physe.2014.07.023.
11 Gryga M., Ciprian D., Gembalova L., Hlubina P. One-Dimensional Photonic Crystal with a Defect Layer Utilized as an Optical Filter in Narrow Linewidth LED-Based Sources. *Crystals*. 2023. Vol. 13, No 1. Article No. 93. doi:10.3390/cryst13010093.
12. Aly A. H., Abdel Ghany S. E. S., Fadlallah M. M., Salman F. E., Kamal B. M. Transmission and temperature sensing characteristics of a binary and ternary photonic band gap. *Journal of Nanoelectronics and Optoelectronics*. 2015. Vol. 10, No. 1. P. 1-6. doi: 10.1166/jno.2015.1697.
13. Fu L., Lin M., Liang Z., Wang Q., Zheng Y. and Ouyang Z. The Transmission Properties of One-Dimensional Photonic Crystals with Gradient Materials. *Materials*. 2022. Vol. 15. Issue 22. Article No. 8049. doi: 10.3390/ma15228049.
14. Bass F. G. and Bulgakov A. A. Kinetic and Electrodynamic Phenomena in Classical and Quantum Semiconductor Superlattices. New York: Nova Science. 1997.
15. Thabet R., Barkat O. Transmission Spectra in One-dimensional Defective Photonic Crystal Integrating Metamaterial and Superconductor. *Journal of Superconductivity and Novel Magnetism*. 2022. Vol. 35. P. 1473 – 1482. doi: 10.1007/s10948-022-06195-8.
16. Lyubchanskii I. L., Dadoenkova N. N., Zabolotin A. E., Lee Y. P. and Rasing Th. A one-dimensional photonic crystal with a superconducting defect layer. *J. Opt. A: Pure Appl. Opt*. 2009. Vol. 11. Article 114014. doi: 10.1088/1464-4258/11/11/114014.
17. Liu A., Gao H., Xiao Y., Zheng J., Zhang Q. Tunable narrow-and-sharp defect modes and transmission peak degeneracy in periodic superconducting photonic crystals. *PLOS One*. 2026. Vol.21, No. 1. Article No. e0341241. doi: 10.1371/journal.pone.0341241.
18. Yariv A., Yeh P. Optical waves in crystals. New York: Jon Wiley & Suns, 1984.

References (transliterated)

1. Mohamed A. G., Elsayed H. A., Mehaney A., Aly A. H., Sabra W. Transmittance properties of one-dimensional metamaterial nanocomposite photonic crystal in GHz range. Scientific Reports. 2022. Vol. 12. P. 18331. doi: 10.1038/s41598-022-21455-2.
2. Ramanujam N. R., Wilson K. S. Joseph, Revathy V., Lenin M. Maria, Jothy V. Bena Properties of one Dimensional Photonic Crystals with Defects Thickness and Temperature Dependence. Materials Today: Proceedings. 2015. Vol. 2, Issue 3. P. 959-964. doi: 10.1016/j.matpr.2015.06.016.
3. Lubert-Perquel D., Acharya S., Johnson J. C. Optically Addressing Exciton Spin and Pseudospin in Nanomaterials for Spintronics Applications. ACS Appl. Opt. Mater. 2023. Vol. 1. P. 1742–1760. doi: 10.1021/acsaom.3c00299.
4. Koopmans B., Li P., Pezeshki H., Demirer E., Simons G., Jiao Y., van der Tol J., and Lavrijsen R. Towards on-Chip Spintronic-Photonic Integration. In 2024 IEEE International Magnetic Conference - Short Papers, INTERMAG Short Papers. 2024. Article No. 10576952. doi: 10.1109/INTERMAGShortPapers61879.2024.10576952.
5 Si Y., Ju Z., Ma H., Xia K., Lin S., Tang R., Sun B., Sun C., Li L. Realization and simulation of silicon-on-sapphire mid-infrared one-dimensional photonic crystal cavities. Appl. Phys. Lett. 2025. Vol. 126. P. 021101. doi: 10.1063/5.0241260.
6. Sadoun B., Mouetsi S., Hocini A. and Hocini A. Optical properties of one-dimensional photonic crystal and light absorption enhancement in planar a-Si:H solar cell. IOP Conference Series: Materials Science and Engineering. 2021. Vol. 1046. Article No. 012014. doi: 10.1088/1757-899X/1046/1/012014.
7. Gangwar R. K., Pathak A. K., and Kumar S. Recent Progress in Photonic Crystal Devices and Their Applications: A Review. Photonics. 2023. Vol. 10, Issue 11. Article No. 1199. doi: 10.3390/photonics10111199.
8. Kou D., Zhang S., and Ma W. Recent Advances in 1D Photonic Crystals: Diverse Morphologies and Distinctive Structural Colors for Multifaceted Applications. Adv. Opt. Mater. 2024. Vol. 12, Issue 19. Article No. 2400192. doi: 10.1002/adom.202400192.
9. Hao K., Li Z., Wang X., Yang S., Zhang J. and Gao Y. Transmission characteristics of one-dimensional photonic crystal with dielectric defect layer in near-infrared band. Proc. of SPIE. 2020. Vol. 11564. Article No. 1156403 doi: 10.1117/12.257955.
10. Wu M.-R., Wu C.-J., Chang S.-J. Investigation of defect modes in a defective photonic crystal with a semiconductor metamaterial defect. Physica E: Low-dimensional Systems and Nanostructures. 2014. Vol. 64. P. 146-151. doi: 10.1016/j.physe.2014.07.023.
11 Gryga M., Ciprian D., Gembalova L., Hlubina P. One-Dimensional Photonic Crystal with a Defect Layer Utilized as an Optical Filter in Narrow Linewidth LED-Based Sources. Crystals. 2023. Vol. 13, No 1. Article No. 93. doi:10.3390/cryst13010093.
12. Aly A. H., Abdel Ghany S. E. S., Fadlallah M. M., Salman F. E., Kamal B. M. Transmission and temperature sensing characteristics of a binary and ternary photonic band gap. Journal of Nanoelectronics and Optoelectronics. 2015. Vol. 10, No. 1. P. 1-6. doi: 10.1166/jno.2015.1697.
13. Fu L., Lin M., Liang Z., Wang Q., Zheng Y. and Ouyang Z. The Transmission Properties of One-Dimensional Photonic Crystals with Gradient Materials. Materials. 2022. Vol. 15. Issue 22. Article No. 8049. doi: 10.3390/ma15228049.
14. Bass F. G. and Bulgakov A. A. Kinetic and Electrodynamic Phenomena in Classical and Quantum Semiconductor Superlattices. New York: Nova Science. 1997.
15. Thabet R., Barkat O. Transmission Spectra in One-dimensional Defective Photonic Crystal Integrating

Metamaterial and Superconductor. Journal of Superconductivity and Novel Magnetism. 2022. Vol. 35. P. 1473 – 1482. doi: 10.1007/s10948-022-06195-8.
16. Lyubchanskii I. L., Dadoenkova N. N., Zabolotin A. E., Lee Y. P. and Rasing Th. A one-dimensional photonic crystal with a superconducting defect layer. J. Opt. A: Pure Appl. Opt. 2009. Vol. 11. Article 114014. doi: 10.1088/1464-4258/11/11/114014.
17. Liu A., Gao H., Xiao Y., Zheng J., Zhang Q. Tunable narrow-and-sharp defect modes and transmission peak degeneracy in periodic superconducting photonic crystals. PLOS One. 2026. Vol.21, No. 1. Article No. e0341241. doi: 10.1371/journal.pone.0341241.
18. Yariv A., Yeh P. Optical waves in crystals. New York: Jon Wiley & Suns, 1984.

Відомості про авторів (About authors)

Хрипунов Геннадій Семенович – доктор технічних наук, професор, проректор Національного технічного університету «Харківський політехнічний інститут»; м. Харків, Україна; ORCID: https://orcid.org/0000-0002-6448-5938; e-mail: Gennadiy.Khrypunov@khpi.edu.ua

Khrypunov Gennadiy – Doctor of Technical Sciences, Professor, Vice-Rector of National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-6448-5938; e-mail: Gennadiy.Khrypunov@khpi.edu.ua

Меріуц Андрій Володимирович – кандидат фізико-математичних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри мікро- та наноелектроніки; м. Харків, Україна; ORCID: https://orcid.org/0000-0003-4176-2530; e-mail: Andrii.Meriuts@khpi.edu.ua.

Meriuts Andrii – Candidate of Physical and Mathematical Sciences (Ph. D.), Docent, Associate Professor, Department of
Micro- and NanoElectronics, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0003-4176-2530; e-mail: Andrii.Meriuts@khpi.edu.ua.

Шелест Тетяна Миколаївна – кандидат фізико-математичних наук, доцент, Національний технічний університет
«Харківський політехнічний інститут», доцент кафедри фізики; м. Харків, Україна; ORCID: https://orcid.org/0000-0002-8116-6189; e-mail: Tetiana.Shelest@khpi.edu.ua.

Shelest Tetiana – Candidate of Physical and Mathematical Sciences (Ph. D.), Docent, Associate Professor, Department of Physics, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-8116-6189; e-mail: Tetiana.Shelest@khpi.edu.ua.

Трубілін Антон Олексійович – Національний технічний університет «Харківський політехнічний інститут», магістр кафедри мікро- та наноелектроніки; м. Харків, Україна; e-mail: 8367775@ukr.net

Trubilin Anton – Master, Department of Micro- and NanoElectronics, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine; e-mail: 8367775@ukr.net

Кривоніс Світлана Станіславівна – доцент кафедри фізики Національного технічного університету «Харківський політехнічний інститут»; м. Харків, Україна; ORCID: https://orcid.org/0000-0002-1938-293X; e-mail: Svitlana.Kryvonis@khpi.edu.ua.

Kryvonis Svitlana – Associate Professor, Department of Physics, National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-1938-293X; e-mail: Svitlana.Kryvonis@khpi.edu.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Хрипунов Г. С., Меріуц А. В., Шелест Т. М., Трубілін А. О., Кривоніс С. С. Динамічне керування спектральними характеристиками одновимірних фотонних кристалів. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 46-53. doi: 10.20998/2413-4295.2026.02.06

Please cite this article as:

Khrypunov G., Meriuts A., Shelest T., Trubilin A., Kryvonis S. Dynamic control of spectral characteristics in one-dimensional photonic crystals. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 46–53, doi: 10.20998/2413-4295.2026.02.06.

Надійшла (received) 15.05.2026
Прийнята (accepted) 28.05.2026
Опублікована (published) 05.06.2026

УДК 658.562: 620.179.16: 620.179.17 **doi:10.20998/2413-4295.2026.02.07**

ДІАГРАМА СПРЯМОВАНОСТІ ПРЯМОГО СУМІЩЕНОГО ЕЛЕКТРОМАГНІТНО-АКУСТИЧНОГО ПЕРЕТВОРЮВАЧА В ІМПУЛЬСНОМУ РЕЖИМІ

О.М. БОРОДЕНКО[1], Г.М. СУЧКОВ[2], П.А. ЯКОВЛЄВ[3]

[1] кафедра інформаційно – вимірювальних технологій, аспірант, НТУ «ХПІ», Харків, Україна, Україна
[2] кафедра інформаційно – вимірювальних технологій, професор кафедри, НТУ «ХПІ», Харків, Україна
[3] кафедра інформаційно – вимірювальних технологій, магістр, НТУ «ХПІ», Харків, Україна
[*]e-mail: hpi.suchkov@gmail.com

АНОТАЦІЯ. *В Україні виробляються і експлуатуються великі об'єми металопродукції різного призначення, в тому числі критичних для функціювання промисловості і господарства. Якість такої продукції в значній мірі забезпечується використанням ультразвукових методів контролю. Робота ультразвукових дефектоскопів і товщиномірів може забезпечувати надійність контролю у випадку відповідності отриманих результатів дійсності. Одним із факторів, що суттєво впливає на результат контролю є діаграма спрямованості ультразвукового перетворювача, який формує ультразвукове поле в об'ємі металовиробу. Ультразвукове поле повинно бути вузьким, мати мінімальні бокові пелюстки по відношенню до центрального робочого променя тощо. Такі вимого характерні як для традиційних контактних сенсорів, так і для електромагнітно-акустичних перетворювачів. Діаграми спрямованості для прямих суміщених електромагнітно-акустичних перетворювачів на цей час вивчені недостатньо. Тому в виконаних дослідженнях в спрощеному вигляді розроблена фізико – математична модель перетворення імпульсів квазімагнітного та пакетного електромагнітного полів в ультразвукові імпульси в поверхневому шарі феромагнітного об'єкта контролю. Визначена формула для розрахунків ультразвукового поля в металевому напівпросторі. Встановлено, що для збудження вузької діаграми спрямованості ультразвукового поля значної інтенсивності центрального променя і з незначними бічними пелюстками необхідно високочастотну котушку індуктивності електромагнітно-акустичного перетворювача виконувати в вигляді періодичної структури. Моделюванням показано, що в порівнянні з традиційними підходами отриманий результат практично не має бокових пелюсток у створеному в металі ультразвуковому полі. Результати моделювання було перевірено експериментально на феромагнітних зразках в вигляді напівциліндрів радіусами 90, 70, 50 і 30 мм, для чого було створено дослідний стенд. Встановлено, що в експериментальних результатах, в порівнянні з отриманими при моделюванні, при всіх досліджених зразках діаграма спрямованості має більш гострий характер. При цьому бічних пелюсток ультразвукового поля в рамках чутливості приладів ультразвукового стенду не встановлено. Це говорить про перспективність використання імпульсних електромагнітно-кустичних перетворювачів для контролю феромагнітних металовиробів в різних областях промисловості.*

Ключові слова: *металовиріб; ультразвуковий; контроль; електромагнітно-акустичний; діаграма спрямованості.*

DIRECTION DIAGRAM OF A DIRECT COMBINED ELECTROMAGNETIC-ACOUSTIC TRANSDUCER IN PULSE MODE

O.M. BORODENKO[1], H.M. SUCHKOV[2], P.A. YAKOVLIEV[3]

[1] information-measurement technologies department, post-graduate student, NTU "KhPI", Kharkiv, Ukraine
[2] information-measurement technologies department, professor, NTU "KhPI", Kharkiv, Ukraine
[3] information-measurement technologies department, master student, NTU "KhPI", Kharkiv, Ukraine

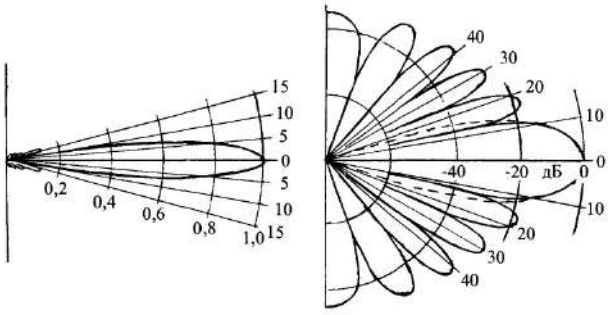
ABSTRACT. *In Ukraine, large volumes of metal products for various purposes are produced and operated, including those critical for the functioning of industry and economy. The quality of such products is largely ensured by the use of ultrasonic inspection methods. The operation of ultrasonic flaw detectors and thickness gauges can ensure the reliability of testing if the results obtained correspond to reality. One of the factors that significantly affects the testing result is the beam pattern of the ultrasonic transducer, which forms an ultrasonic field in the volume of the metal product. The ultrasonic field must be narrow, have minimal side lobes in relation to the central working beam, etc. Such requirements are characteristic of both traditional contact sensors and electromagnetic-acoustic transducers. The beam patterns for direct combined electromagnetic-acoustic transducers have not been studied sufficiently at this time. Therefore, in the conducted studies, a simplified physical and mathematical model of the conversion of quasimagnetic and packet electromagnetic field pulses into ultrasonic pulses in the surface layer of a ferromagnetic testing object was developed. A formula for calculating the ultrasonic field in a metal half-space was determined. It was established that to excite a narrow ultrasonic field with a directional diagram with a significant intensity of the central beam and with insignificant side lobes, it is necessary to perform the high-frequency inductance coil of the electromagnetic-acoustic converter in the form of a periodic structure. The simulation showed that, in comparison with traditional approaches, the obtained result has practically no side lobes in the ultrasonic field created in the metal. The simulation results were experimentally verified on ferromagnetic samples in the form of semi-cylinders with radii of 90, 70, 50 and 30 mm, for which a test stand was created. It was found that in the experimental results, in comparison with those obtained during modeling, the directivity diagram for all the studied samples has a sharper character. At the same time, the side lobes of the ultrasonic field within the sensitivity of the ultrasonic stand devices are not established. This*

indicates the prospects of using pulsed electromagnetic-acoustic transducers for controlling ferromagnetic metal products in various areas of industry.
Key Words: *metal product; ultrasonic; control; electromagnetic-acoustic; radiation pattern.*

Вступ

Надзвичайно важливою характеристикою ультразвукових перетворювачів є діаграма спрямованості (ДС) звукового поля в об'єкті контролю (ОК) [1]. В значній мірі вона визначає чутливість контролю, точність вимірювання товщини, швидкості розповсюдження ультразвукових імпульсів, координати дефектів, крок сканування об'єкту контролю, роздільну здатність, вимірювання розмірів дефектів, що має значення при встановленні якості ОК [2].

Вказані характеристики ультразвукових перетворювачів відносяться як до п'єзоелектричних [3] так і до електромагнітно-акустичних (ЕМА) [4] перетворювачів (ЕМАП). Причому в відомих теоретичних роботах [5], як правило, досліджено вплив на ДС безперервного випромінення ультразвукових хвиль [2, 3], що приводить до появи бічних пелюсток значної величини, рис. 1. В результаті дані контролю можуть не вірно визначатися. Якість контролю буде недостатньою.



а б

Рис.1 – Типове представлення ДС: а – у відносних одиницях; б – в дБ. Основна пелюстка – 0

З рис. 1 випливає, що бічні пелюстки ДС можуть суттєво спотворювати результати ультразвукового контролю (УЗК), оскільки вони можуть формувати відбиття від дефектів і результат контролю не буде відповідати реальності. Слід враховувати, що в основній (центральній) пелюстці зосереджено близько 80% енергії, яка випромінюється.

Відомо багато праць [4–12], в яких фахівці з багатьох сторін розглядають питання формування ДС з заданими характеристиками, які, відповідно, визначаються в основному конструкцією ЕМАП та параметрами імпульсів струму їх живлення [4, 7, 12, 13]. Очевидно, що живлення ЕМАП пакетними імпульсами струму (з кількома періодами частоти заповнення) [14, 15], тобто проміжними характеристиками між короткими імпульсами і безперервним випроміненням ультразвукових імпульсів буде мати значення при ультразвуковому контролі [16, 17] і потребує відповідних досліджень.

Раніше було визначено, що вплинути на ДС з метою зменшення бокових пелюсток можливо шляхом використання плоских високочастотних котушок з періодичним розташуванням провідників [9, 13].

В напрямку розробки нових ЕМАП працюють як вітчизняні фірми, наприклад НПФ «Ультракон-Сервис» [17], УкрНДІНК [18], Укрінтех [19], ХІМЛАБОРРЕАКТИВ [20] та інші, так і закордонні: Olympus [21], SONATEST [22], Hitachi [23] та інші, що говорить про важливість досліджень ДС таких перетворювачів.

Мета роботи

Метою роботи є обґрунтування раціональних конструкцій ЕМАП за показником діаграми спрямованості ультразвукових полів в металевих об'єктах.

Виклад основного матеріалу

Теоретичні положення з формування діаграми спрямованості ЕМА перетворювача при імпульсному збудженні поляризуючого магнітного поля.

На сьогодні імпульсними магнітами вдалося створити постійну величину магнітного поля в поверхневому шарі ОК в вигляді напівпростору на протязі заданого часового інтервалу [14]. Тому будемо вважати, що на ОК діє квазіпостійне магнітне поле. Тоді ДС буде визначатися конструкцією високочастотної котушки індуктивності ЕМАП.

В якості фізичної моделі розглянемо конструкцію високочастотної котушки індуктивності, що наведена на рис. 2. Нехай над поверхнею металічного об'єкту 1 розташована високочастотна котушка індуктивності у вигляді ділянок 2.1, 2.2, 2.3 безкінечно тонкої стрічки шириною a. Відстань між ділянками плоскої стрічки дорівнює b. При розрахунках $в = a$. Кут θ спостереження ультразвукового поля в точці A об'єму ОК на відстані r і називається кутом розкриття діаграми спрямованості.

На ОК 1 діє квазіпостійне нормальне магнітне поле $\boldsymbol{B}_t$ або тангенціальне $\boldsymbol{B}_l$. Під провідниками 2.1, 2.2 і 2.3 (для прикладу беремо 3 провідника) в поверхневому шарі ОК в ділянках 3.1, 3.2, 3.3 будуть збуджуватися електромагнітні поля за рахунок пакетного високочастотного синусоїдального струму в провідниках високочастотної котушки ЕМАП. В результаті в об'ємі металу будуть формуватися ультразвукові промені з кутом розкриття θ, який визначається за відомим виразом

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

$$\sin\theta = n\lambda / r \qquad (1)$$

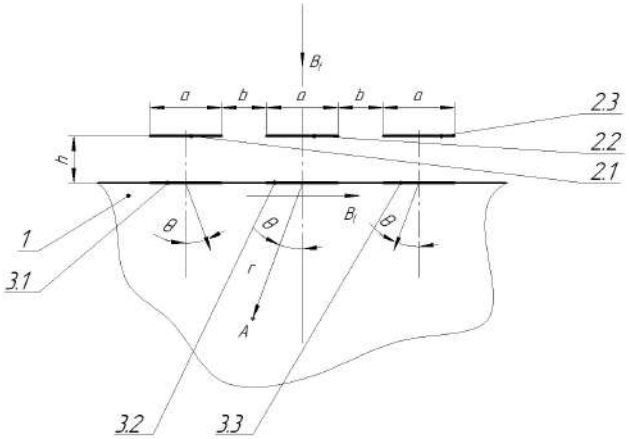


Рис.2 – Модель для розрахунків ДС ЕМАП в металічному ОК

де *n* числовий коефіцієнт, що визначається рівнем амплітуди головної пелюстки ДС (*n* = 0,61 для рівня 0 дБ, тобто центрального ультразвукового променя).

Для одиничної ділянки стрічки (наприклад 2.2) високочастотної котушки індуктивності можна записати вираз для амплітуди:

- для поздовжньої хвилі при тангенціальному квазістаціонарному намагнічуванні

$$A_{2.2l} = \frac{jB_l S}{8\pi\mu r} e^{-k_l h \sin\theta} \qquad (2)$$

Відповідно для поперечної хвилі при нормальному намагнічуванні

$$A_{2.2t} = \frac{jB_t S}{8\pi\mu r} e^{-k_l h \sin\theta} \qquad (3)$$

де k_l – хвильове число для поздовжніх хвиль; k_t – хвильове число для поперечних хвиль; μ – постійна Ламе для матеріалу ОК; j – сила струму в стрічці високочастотної котушки індуктивності ЕМАП; B_l і B_t – максимальні значення величин індукції тангенціального та нормального квазістаціонарного магнітного поля відповідно; h – зазор між ділянками стрічок котушки індуктивності і поверхнею ОК; r – відстань від поверхні ОК до точки спостереження, для якої розраховується амплітуда ультразвукової хвилі.

Складаючи ультразвукові промені від усіх ділянок провідників високочастотної котушки індуктивності ЕМАП отримаємо результуючу ДС

$$DC = \frac{2C}{a\omega tg\alpha}\left[\sin\left(\frac{a\omega\sin\alpha}{2C}\right)\right] \exp\left(-\frac{h\omega\sin\alpha}{C}\right) \frac{\sin\left[\frac{N}{2}\left(\frac{2\pi}{\lambda}d\sin\alpha-\varphi\right)\right]}{\sin\left[\frac{1}{2\left(\frac{2\pi}{\lambda}d\sin\alpha-\varphi\right)}\right]}, \qquad (4)$$

де h – зазор між високочастотною котушкою і ОК; a – ширина стрічки ділянки високочастотної котушки; C – швидкість розповсюдження ультразвукової хвилі в матеріалі ОК; α - кут поширення ультразвукового променя; ω – кутова частота ультразвукових імпульсів; N – кількість ділянок високочастотної котушки індуктивності; λ - довжина ультразвукової хвилі в матеріалі ОК; φ – дорівнює 0, коли ділянки високочастотної котушки включені з одною фазою, і дорівнює π, коли ділянки високочастотної котушки включені протифазно; d – розмір високочастотної котушки.

Для перевірки розробленої фізико-математичної моделі були виконані розрахунки ультразвукового поля у металевому напівпросторі, для прикладу варіант результату яких наведено на рис.3.

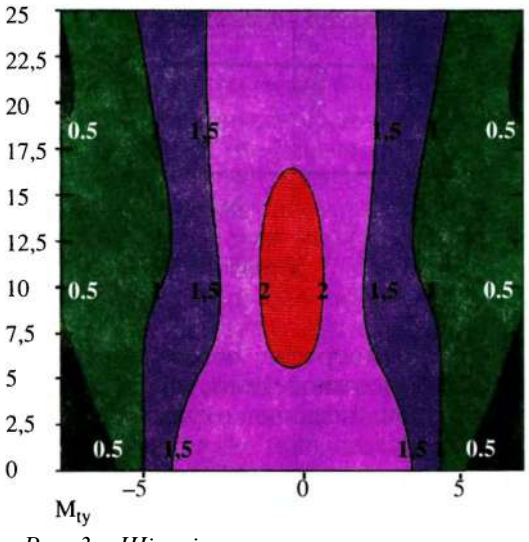


Рис. 3 – Щільність ультразвукового поля в металевому ОК в результаті оптимізації конструкції високочастотної котушки індуктивності ЕМАП

Експериментальні дослідження.

Для перевірки теоретичних досліджень було виготовлено зразки з стальних матеріалів у вигляді

напівциліндрів. Схема проведення експериментальних досліджень наведена на рис. 4.

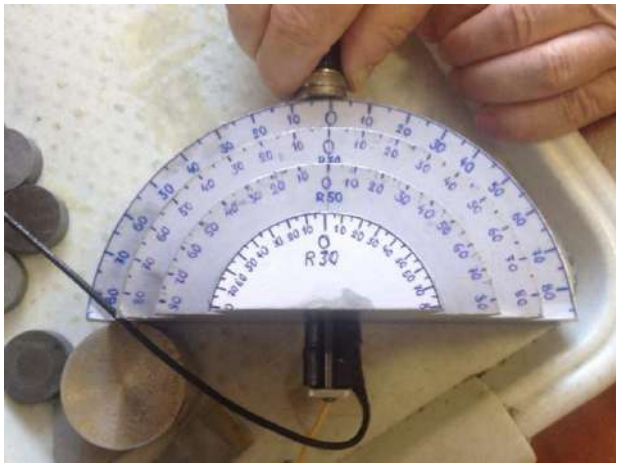


Рис. 4 – Схема вимірювання діаграми спрямованості ЕМАП на сталевому феромагнітному зразку в режимі прийому та в режимі випромінення

Згідно з схемою ЕМАП випромінює ультразвукові промені, які фіксуються приймаючим перетворювачем. Після цього перетворювач переміщується по криволінійній поверхні зразка, а ЕМАП приймає ультразвукові імпульси. Таким чином визначається ДС в режимі прийому і в режимі випромінення ультразвукових імпульсів.

Результати побудови ДС в режимі випромінення при різних радіусах зразків наведено на рис. 5.

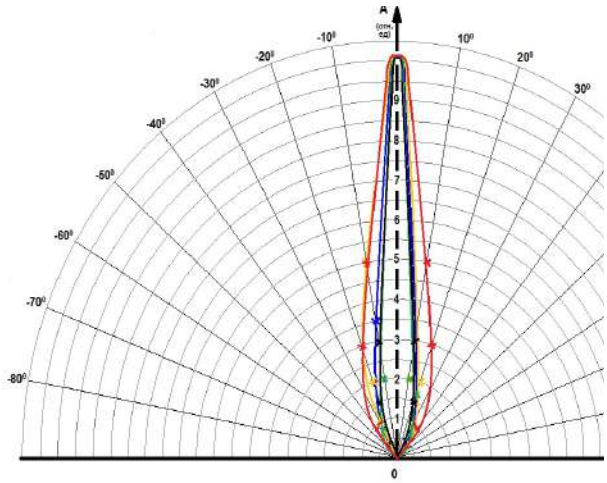


Рис. 5 – ДС в режимі випромінення ЕМАП при напівциліндрах радіусами 90, 70, 50 і 30 мм

Оскільки збуджене ультразвукове поле симетричне, то зображення на рис.5 наведено частково.

ДС ЕМАП в режимі прийому наведено на рис. 6

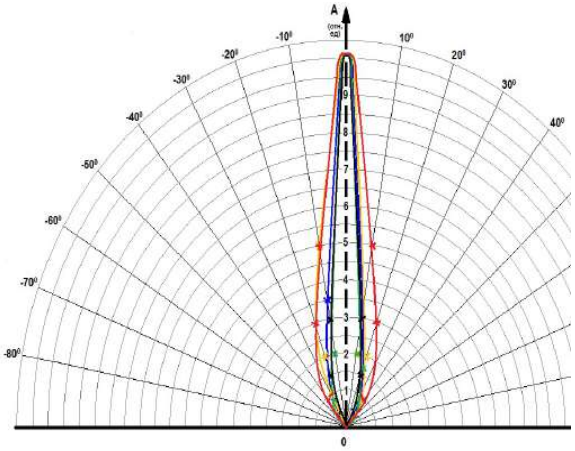


Рис. 6 – ДС ЕМАП в режимі прийому для різних сталевих зразків (напівциліндри з радіусом 90, 70, 50 і 30 мм)

Обговорення результатів

Дані, що наведені на рис.3 показують, що комплексний підхід до побудови конструкції ЕМАП дають можливість підвищити концентрацію ультразвукового поля в ОК вздовж напрямку центрального променя та практично виключити появу бічних пелюсток ДС. В такому варіанті точність визначення координат дефектів в ОК буде підвищуватися.

Аналіз результатів експериментальних досліджень підтвердив результати модельних досліджень. Причому на рівні чутливості використаних приладів контролю бічних пелюсток ДС не виявлено на різних товщинах ОК.

Висновки

Показана можливість виконувати моделювання збудження і прийому ультразвукових імпульсів в металевих об’єктах в випадку намагнічування ОК імпульсним магнітним полем з заданою тривалістю, достатньою для виконання контролю. Тобто квазіпостійним магнітним полем.

Визначена можливість побудови діаграми спрямованості ультразвукового поля в ОК за рахунок побудови високочастотної котушки індуктивності ЕМАП в вигляді періодичної структури.

Надано формули для розрахунків ДС та наведені приклади моделювання ультразвукового поля в металевому напівпросторі.

Результати експериментальних досліджень ДС підтвердили висновки модельних досліджень.

Список літератури

1. Цапенко В. К., Куц Ю. В. Основи ультразвукового неруйнівного контролю: підручник. Київ, 2010. 448 с.
2. Карпаш М.О., Рибіцький І.В., Котурбаш Т.Т., Бондаренко О.Г., Карпаш О.М. Акустичний контроль

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

конструкцій та устаткування у нафтогазовій галузі. Монографія. – Видавництво: ІФНТУНГ, 2012. – 420 с.
3. Лютак З.П., Лютак І.З. Технологія акустичного контролю нафтогазового обладнання. Видавництво: ІФНТУНГ, 2015. 417 с.
4. Десятніченко О. В. Електромагнітно-акустичний товщиномір для контролю металовиробів з діелектричними покриттями: дис. канд. техн. наук: 05.11.13. Харків, 2015. 172 с.
5. Liang, C.–H. Inequality condition for grating lobes of planar phased array / C.–H. Liang, L. Li, X.–J. Dang // Progress In Electromagnetics Research B. – 2008. – Vol. 4. – P. 101–113.
6. Ванджура, А. Р., Лисенко Ю. Ю. Автоматизований ультразвуковий контроль рейок. XVIII Науково-практична конференція студентів, аспірантів та молодих вчених “Ефективність та автоматизація інженерних рішень у приладобудуванні”, 06-07 грудня 2022 р, м. Київ, Україна: збірник праць конференції. – Київ : КПІ ім. Ігоря Сікорського, 2022. – С. 202-205.
7. Плєснецов С.Ю. Розвиток методів та засобів для електромагнітно-акустичного контролю стрижневих, трубчастих та листових металовиробів: автореф. дис. д-ра техн. наук. Харків, 2021. 40 с.
8. Мигущенко Р.П., Сучков Г.М., Петрищев О.М., Болюх В.Ф., Плєснецов С.Ю., Кочерга А.І. Інформаційно-вимірювальні електромеханічні перетворювачі для оцінки якості поверхні феромагнітних металовиробів ультразвуковими хвилями Релея // Технічна електродинаміка. – 2017. – № 2. – С. 70–76.
9. Jianpeng He, Steve Dixon, Samuel Hill, Ke Xu. A New Electromagnetic Acoustic Transducer Design for Generating and Receiving S0 Lamb Waves in Ferromagnetic Steel Plate. *Sensors*, 2017, vol. 17(5), pp. 10−23. https://doi.org/10.3390/s17051023
10. Suchkov G.M., TaranenkoYu.K., Khomyak Yu.V. A Non-Contact Multifunctional Ultrasonic Transducer for Measurements and Non-Destructive Testing // Measurement Techniques, 2016, №12, Volume 59, Issue 9, pp 990–993. DOI:10.1007/s11018-016-1081-3
11. Boughedda H., Hacib T., Chelabi M., Acikgoz H., Le Bihan Y. Electromagnetic Acoustic Transducer for cracks detection in conductive material. 2015. 4th International Conference on Electrical Engineering (ICEE). Pages: 1–4. DOI:10.1109/INTEE.2015.7416717.
12. Сучков Г.М., Ноздрачова К.Л., Хащина С.В., Глоба С.М. Спосіб ультразвукового контролю виробів широкосмуговим електромагнітним перетворювачем. Патент на корисну модель № 71700, G01N29/04. Зявл. 28.12.2011 №u2011 15525, опубл. Бюл №14. 25.07.2012.
13. Сучков Г.М. Розвиток теорії і практики створення приладів для електромагнітно-акустичного контролю металовиробів: автореф. дис. докт. техн. наук. Харків: НТУ “ХПІ”. 2005. 521 с.
14. Сучков Г.М., Донченко А.В. Удосконалення електромагнітно-акустичних перетворювачів для ультразвукового контролю якості феромагнітних металовиробів. Тези доповіді Міжнародної наукової інтернет- конференції «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 74). 6–7 лютого 2023 р., м. Тернопіль – м. Переворськ (Польща).
15. G. M. Suchkov, V.F. Bolyukh, A.I. Kocherga, R.P. Mygushchenko, O. Yu. Kropachek, Increasing the efficiency of the surface-mounted ultrasonic electromagnetic-acoustic transducer due to the magnetic field source. Технічна електродинаміка. № 2, 2023, с. 3–8. DOI:https:// doi.org/10.15407/techned2023.02.003
16. Salam Bussi, Suchkov G., Mygushchenko R., Kropachek O., Plesnetsov S. Electromagnetic-acoustic transducers for ultrasonic measurements, testing and diagnostics of ferromagnetic metal products // Ukrainian Metrological Journal, 2019, No.4, pp. 41−49. https://doi.org/10.24027/2306-7039.4.2019.195956
17. www.ultracon-service.com.ua
18. https://cpdk.com.ua/service/ultrazvukovyj-kontrol
19. Укрінтех https://ukrintech.com.ua/ultrazvukovij-kontrol
20. ТОВ «ХІМЛАБОРРЕАКТИВ https://industry.hlr.ua/nodestructtest/ultrasonic-flaw-detection/ultrasonic-phased-array-method/
21. 21. Olympus Ukraine https://www.olympus.ua
22. https://sonatest.com/
23. https://www.hitachienergy.com/about-us/company-profile/country-and-regional-information/ukraine

References (transliterated)

1. Tsapenko V. K., Kuts Yu. V. Osnovy ultrazvukovoho neruinivnoho kontroliu: pidruchnyk. Kyiv, 2010. 448 p.
2. Karpash M.O., Rybitskyi I.V., Koturbash T.T., Bondarenko O.H., Karpash O.M. Akustychnyi kontrol konstruktsii ta ustatkuvannia u naftohazovii haluzi. Monohrafiia. – Vydavnytstvo: IFNTUNH, 2012. – 420 p.
3. Liutak Z.P., Liutak I.Z. Tekhnolohiia akustychnoho kontroliu naftohazovoho obladnannia. Vydavnytstvo: IFNTUNH, 2015. 417 p.
4. Desiatnichenko O. V. Elektromahnitno-akustychnyi tovshchynomir dlia kontroliu metalovyrobiv z dielektrychnymy pokryttiamy: dys. kand. tekhn. nauk: 05.11.13. Kharkiv, 2015. 172 p.
5. Liang, C.–H. Inequality condition for grating lobes of planar phased array / C.–H. Liang, L. Li, X.–J. Dang // Progress In Electromagnetics Research B. – 2008. – Vol. 4. – P. 101–113.
6. Vandzhura, A. R., Lysenko Yu. Yu. Avtomatyzovanyi ultrazvukovyi kontrol reiok. XVIII Naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh “Efektyvnist ta avtomatyzatsiia inzhenernykh rishen u pryladobuduvanni”, 06-07 hrudnia 2022 r, m. Kyiv, Ukraina: zbirnyk prats konferentsii. – Kyiv : KPI im. Ihoria Sikorskoho, 2022. – P. 202-205.
7. Pliesnetsov S.Iu. Rozvytok metodiv ta zasobiv dlia elektromahnitno-akustychnoho kontroliu stryzhnevykh, trubchastykh ta lystovykh metalovyrobiv: avtoref. dys. d-ra tekhn. nauk. Kharkiv, 2021. 40 p.
8. Myhushchenko R.P., Suchkov H.M., Petryshchev O.M., Boliukh V.F., Pliesnetsov S.Iu., Kocherha A.I. Informatsiino-vymiriuvalni elektromekhanichni peretvoriuvachi dlia otsinky yakosti poverkhni feromahnitnykh metalovyrobiv ultrazvukovymy khvyliamy Releia // Tekhnichna elektrodynamika. – 2017. – № 2. – P. 70–76.
9. Jianpeng He, Steve Dixon, Samuel Hill, Ke Xu. A New Electromagnetic Acoustic Transducer Design for Generating and Receiving S0 Lamb Waves in Ferromagnetic Steel Plate. Sensors, 2017, vol. 17(5), pp. 10−23. https://doi.org/10.3390/s17051023
10. Suchkov G.M., TaranenkoYu.K., Khomyak Yu.V. A Non-Contact Multifunctional Ultrasonic Transducer for Measurements and Non-Destructive Testing // Measurement Techniques, 2016, №12, Volume 59, Issue 9, pp 990–993. DOI:10.1007/s11018-016-1081-3
11. Boughedda H., Hacib T., Chelabi M., Acikgoz H., Le Bihan

Y. Electromagnetic Acoustic Transducer for cracks detection in conductive material. 2015. 4th International Conference on Electrical Engineering (ICEE). Pages: 1–4. DOI:10.1109/INTEE.2015.7416717.
12. Suchkov H.M., Nozdrachova K.L., Khashchyna S.V., Hloba S.M. Sposib ultrazvukovoho kontroliu vyrobiv shyrokosmuhovym elektromahnitnym peretvoriuvachem. Patent na korysnu model № 71700, G01N29/04. Ziavl. 28.12.2011 №u2011 15525, opubl. Biul №14. 25.07.2012.
13. Suchkov H.M. Rozvytok teorii i praktyky stvorennia pryladiv dlia elektromahnitno-akustychnoho kontroliu metalovyrobiv: avtoref. dys. dokt. tekhn. nauk. Kharkiv: NTU “KhPI”. 2005. 521 p.
14. Suchkov H.M., Donchenko A.V. Udoskonalennia elektromahnitno-akustychnykh peretvoriuvachiv dlia ultrazvukovoho kontroliu yakosti feromahnitnykh metalovyrobiv. Tezy dopovidi Mizhnarodnoi naukovoi internet- konferentsii «Informatsiine suspilstvo: tekhnolohichni, ekonomichni ta tekhnichni aspekty stanovlennia (vypusk 74). 6–7 liutoho 2023 r., m. Ternopil – m. Perevorsk (Polshcha).
15. G. M. Suchkov, V.F. Bolyukh, A.I. Kocherga, R. P. Mygushchenko, O. Yu. Kropachek, Increasing the efficiency of the surface-mounted ultrasonic electromagnetic-acoustic transducer due to the magnetic field source. Tekhnichna elektrodynamika. № 2, 2023, s. 3–8. DOI:https:// doi.org/10.15407/techned2023.02.003
16. Salam Bussi, Suchkov G., Mygushchenko R., Kropachek O., Plesnetsov S. Electromagnetic-acoustic transducers for ultrasonic measurements, testing and diagnostics of ferromagnetic metal products // Ukrainian Metrological Journal, 2019, No.4, pp. 41−49. https://doi.org/10.24027/2306-7039.4.2019.195956
17. www.ultracon-service.com.ua
18. https://cpdk.com.ua/service/ultrazvukovyj-kontrol
19. Ukrintekh https://ukrintech.com.ua/ultrazvukovij-kontrol
20. TOV «KhIMLABORREAKTYV https://industry.hlr.ua/nodestructtest/ultrasonic-flaw-detection/ultrasonic-phased-array-method/
21. Olympus Ukraine https://www.olympus.ua
22. https://sonatest.com/
23. https://www.hitachienergy.com/about-us/company-profile/country-and-regional-information/ukraine

Відомості про авторів (About authors)

Бороденко Олексій Миколайович, аспірант, кафедра інформаційно-вимірювальних технологій, Національний технічний університет «Харківський політехнічний інститут», аспірант, м. Харків, Україна; ORCID 0009-0007-4264-1534; e-mail: borodenkoa23@gmail.com.

Borodenko Oleksii, post-graduate, Department of Information and Measurement Technologies, National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine, ORCID 0009-0007-4264-1534; e-mail: borodenkoa23@gmail.com.

Сучков Григорій Михайлович, доктор технічних наук, професор, кафедра інформаційно-вимірювальних технологій, Національний технічний університет «Харківський політехнічний інститут», м. Харків, Україна; ORCID 0000-0002-1805-0466; e-mail: hpi.suchkov@gmail.com.

Suchkov Hryhorii, Doctor of Science, Professor, Professor of the Department of Information and Measurement Technologies, National Technical University «Kharkiv Polytechnic Institute», Kharliv, Ukraine, ORCID 0000-0002-1805-0466; e-mail: hpi.suchkov@gmail.com

Яковлєв Павло Андрійович, кафедра інформаційно-вимірювальних технологій, магістр, Національний технічний університет «Харківський політехнічний інститут», м. Харків, Україна.

Yakovlev Pavlo, Department of Information and Digital Technologies, Master, National Technical University “Kharkiv Polytechnic Institute”, Kharkov, Ukraine.

Будь ласка, посилайтесь на цю статтю наступним чином:

Бороденко О.М., Сучков Г.М., Яковлєв П.А. Діаграма спрямованості прямого суміщеного електромагнітно-акустичного перетворювача в імпульсному режимі. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 54-59. doi:10.20998/2413-4295.2026.02.07.

Please cite this article as:

Borodenko O., Suchkov H., Yakovliev P. Direction diagram of a direct combined electromagnetic-acoustic transducer in pulse mode. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 54–59, doi:10.20998/2413-4295.2026.02.07.

Надійшла (received) 24.02.2026
Прийнята (accepted) 24.04.2026
Опублікована (published) 05.06.2026

УДК 699.86:536.2:620.193.95 doi:10.20998/2413-4295.2026.02.08

ДЕГРАДАЦІЯ ПОКАЗНИКІВ ЯКОСТІ ТЕПЛОІЗОЛЯЦІЙНИХ МАТЕРІАЛІВ ПРИ ТЕПЛОВИХ НАВАНТАЖЕННЯХ

Г. І. КАНЮК [1*]***, О. М. ЕПІК*** [1]

[1] кафедра автоматизації, метрології та енергоефективних технологій, Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, УКРАЇНА
[*] e-mail: mezzer@ukr.net

АНОТАЦІЯ *У роботі розглянуто деградацію показників якості теплоізоляційних матеріалів при тривалій дії теплових навантажень. Предметом аналізу є зміна теплопровідності, термічного опору, водопоглинання, міцності при стиску, стабільності геометричних розмірів та експлуатаційної придатності матеріалів у режимах підвищеної температури й тривалої експлуатації. Показано, що сам по собі тепловий вплив рідко діє ізольовано: у реальній огороджувальній конструкції він поєднується з дифузією вологи, циклічними коливаннями температури, старінням зв'язувальних компонентів, релаксацією пористої структури та локальними теплопровідними включеннями. Через це деградація має не лише матеріалознавчий, а й конструктивно-експлуатаційний характер. Для пінополімерних матеріалів одним із визначальних механізмів є зміна газового складу в порах і термоокиснювальне старіння полімерної матриці; для мінераловатних виробів – ущільнення волокнистої структури, втрата частини гідрофобних властивостей, зволоження та зміна ефективної теплопровідності; для фасадних систем із штукатурним шаром – накопичення пошкоджень у контакті шарів і зростання чутливості до вологісно-теплових циклів. Доведено, що оцінювати деградацію лише за початковим значенням коефіцієнта теплопровідності недостатньо. Для довготривалої оцінки потрібні або натурні спостереження, або прискорені випробування, які відтворюють теплове старіння, зволоження, кліматичну циклічність і зміну структури матеріалу. Розглянуто такі методи, як застосування теплового старіння, метод зрізування для піноматеріалів, прискорені погодні випробування та кінетичні моделі типу Арреніуса. Встановлено, що на практиці більшу увагу приділено динаміці теплопровідності в огороджувальних конструкціях, впливу вологості, експлуатаційній придатності фасадних систем і оцінюванню довговічності теплоізоляційних шарів. Запропоновано систему показників деградації для властивостей, що знижуються в часі, та окремо для коефіцієнта теплопровідності, який при старінні, як правило, зростає. Для інженерного прогнозування використано узагальнену температурно-часову модель деградації, у якій швидкість процесу залежить від температури за експоненціальним законом. На цій основі побудовано схематичні графіки залежності показника деградації від температури використання та тривалості експлуатації. Проведено порівняння методів зниження деградації: оптимізації сировинного складу, гідрофобізації, захисних покриттів, двошарових рішень, обмеження теплопровідних включень, керування вологісним режимом і моніторингу стану. Найперспективнішим визначено метод комплексного обмеження зволоження матеріалу та вузла в цілому, оскільки саме волога найчастіше переводить теплове старіння з повільного режиму в прискорений.*
Ключові слова: *теплоізоляційні матеріали; показники якості; теплопровідність; теплове старіння; деградація; довговічність*

DEGRADATION OF QUALITY INDICATORS OF THERMAL INSULATION MATERIALS UNDER THERMAL LOADS

G. KANJUK [1*]***, O. YEPIK*** [1]

[1] Department of Automation, Metrology, and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, UKRAINE.
[*] e-mail: mezzer@ukr.net

ABSTRACT *The article examines the degradation of quality indicators of thermal insulation materials under prolonged thermal loads. The analysis focuses on changes in thermal conductivity, thermal resistance, water absorption, compressive strength, dimensional stability, and serviceability of materials operating under elevated temperatures and long-term use. It is shown that thermal exposure by itself rarely acts in isolation: in a real building envelope, it is combined with moisture diffusion, cyclic temperature fluctuations, aging of binder components, relaxation of the porous structure, and local thermal bridges. For this reason, degradation has not only a materials-science dimension but also a structural and operational one. For foamed polymer materials, one of the governing mechanisms is the change in gas composition within the pores and the thermo-oxidative aging of the polymer matrix; for mineral wool products, it is the densification of the fibrous structure, partial loss of hydrophobic properties, moisture accumulation, and changes in effective thermal conductivity; for facade systems with a plaster layer, it is the accumulation of damage at layer interfaces and increased sensitivity to hygrothermal cycles. It is demonstrated that assessing degradation solely on the basis of the initial value of the thermal conductivity coefficient is insufficient. Long-term evaluation requires either field observations or accelerated tests that reproduce thermal aging, moisture exposure, climatic cyclic loading, and changes in material structure. The following methods are considered: thermal aging, the slicing method for foam materials, accelerated weathering tests, and Arrhenius-type kinetic models. It has been established that, in practice, greater attention is paid to the dynamics of thermal conductivity in building envelope structures, the influence of moisture, the serviceability of facade systems, and the assessment of the*

durability of thermal insulation layers. A system of degradation indicators is proposed for properties that decrease over time, as well as a separate indicator for the thermal conductivity coefficient, which generally increases during aging. For engineering prediction, a generalized temperature-time degradation model is used, in which the process rate depends on temperature according to an exponential law. On this basis, schematic graphs were constructed to show the dependence of the degradation indicator on service temperature and duration of operation. A comparison was made between methods for reducing degradation, including optimization of raw material composition, hydrophobization, protective coatings, two-layer solutions, limitation of thermal bridges, moisture regime control, and condition monitoring. The most promising approach was identified as the integrated limitation of moisture accumulation in both the material and the assembly as a whole, since moisture is the factor that most often shifts thermal aging from a slow mode to an accelerated one.
Keywords: *thermal insulation materials; quality indicators; thermal conductivity; thermal aging; degradation; durability*

Вступ

Для теплоізоляційного матеріалу початково низька теплопровідність ще не означає стабільного результату при експлуатації. У процесі експлуатації змінюються температура матеріалу, його вологісний стан, мікроструктура пор, контакт шарів і стан поверхневого захисту. Усе це впливає на фактичний термічний опір огородження. Якщо деградація не врахована на етапі проєктування або вибору матеріалу, розрахункові теплотехнічні показники виявляються завищеними, а енергоспоживання, ризик конденсації та локальних пошкоджень – недооціненими. Для фасадних систем проблема ускладнюється дією температурних циклів, зволоженням, штукатурним шаром і вузлами кріплення; для пінополімерів – старінням газонаповненої пористої структури; для волокнистих утеплювачів – зміною ефективної структури при нагріванні та зволоженні [1, 4, 6, 9, 10].

Практичне значення задачі визначається тим, що нормативні вимоги до теплоізоляції будівель спираються на показники, які мають зберігатися не лише в момент введення конструкції в експлуатацію, а й впродовж розрахункового строку служби. Тому наукове завдання полягає не в разовому вимірюванні властивостей, а в побудові придатної моделі деградації, яка поєднує температуру, час та експлуатаційні чинники.

У наукових публікаціях простежується перехід від опису окремих теплотехнічних параметрів до аналізу їх зміни в часі. У роботі А. Данішевського наведено експоненційну інтерпретацію деградації теплопровідності фасадних теплоізоляційних матеріалів та показано, що для ряду поширених утеплювачів приріст λ у тривалому періоді може бути істотним [1]. Близький за логікою підхід подано в дослідженні динаміки теплопровідності пінополіуретанової ізоляції в складі огороджувальної конструкції, де зміна теплотехнічних характеристик розглянута не ізольовано, а через загальний опір теплопередачі системи [2]. В наукових працях також приділено велику увагу до ролі вологості: А. Лялюк досліджує вплив вологовмісту на теплопровідність теплоізоляційного матеріалу методами багатофакторного планування [3], а в роботі А. Постоленка та А. Величка експлуатаційна придатність фасадної системи пов'язується з вологісно-тепловими впливами та рішенням межі між шарами [4].

Окремий напрям формують праці, присвячені довговічності фасадних теплоізоляційних систем. Так стійкість систем із штукатурним шаром визначається не тільки властивостями самого утеплювача, а й сукупною дією кліматичних циклів, станом покриття, адгезією та локальними включеннями [5–8]. Це зміщує акцент від матеріалу як такого до вузла і системи в цілому. Нормативну рамку для такого підходу задають ДБН В.2.6-31:2021 та ДСТУ 9191:2022, у яких фіксуються теплотехнічні та експлуатаційні показники, що мають враховуватися під час вибору теплоізоляційного матеріалу, зокрема гранична температура застосування, вологість, водопоглинання, морозостійкість і паропроникність [9, 10].

В існуючих дослідженнях цього питання переважає експериментально-модельний підхід. Для пінних утеплювачів придатність прискореного старіння визначається шляхом теплового впливу і зрізування як засобу оцінки довготривалої теплотехнічної поведінки [11]. Досліджено порівняння лабораторних підходів ISO 11561 та EN 13166 та встановлено, що оцінка довготривалої зміни теплопровідності суттєво залежить від методу випробування [14]. Існують експериментальні підтвердження зростання теплопровідності поширених утеплювачів зі збільшенням температури та вологості [12], та підкреслюється, що паспортне значення термічного опору R за стандартної температури часто не відтворює поведінку в реальних умовах [13]. У роботі [15] зміна довготривалої теплопровідності та біоколоноїзація теплоізоляційних штукатурок досліджені з використанням прискорених схем старіння, де застосовано моделі Арреніуса, Пека і Коффіна-Менсона. Сукупно ці праці показують, що адекватна оцінка деградації вимагає поєднання матеріалознавчого експерименту, тепловологісного аналізу та моделювання швидкості старіння [11–15].

Мета роботи

Метою роботи є узагальнення сучасних підходів до оцінювання деградації показників якості теплоізоляційних матеріалів при теплових навантаженнях і формування придатної для інженерного використання системи відповідних показників та залежностей.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Виклад основного матеріалу

1. Основні показники якості теплоізоляційних матеріалів

Для теплоізоляційних матеріалів базовим показником є коефіцієнт теплопровідності:

$$\lambda = \frac{q\,\delta}{\Delta T},\ \text{Вт/(м·К)}, \tag{1}$$

де q – щільність теплового потоку, Вт/м²; δ – товщина шару матеріалу, м; ΔT – перепад температур на шарі, К.

Термічний опір однорідного шару, м²·К/Вт:

$$R = \frac{\delta}{\lambda}. \tag{2}$$

Для багатошарової конструкції загальний опір теплопередачі доцільно записати так:

$$R_{\Sigma} = \frac{1}{\alpha_{\text{в}}} + \sum\nolimits_{i=1}^{n} \frac{\delta_i}{\lambda_i} + \frac{1}{\alpha_{\text{з}}}, \tag{3}$$

де $\alpha_{\text{в}}$ і $\alpha_{\text{з}}$ – коефіцієнти тепловіддачі відповідно з внутрішнього та зовнішнього боку, Вт/(м²·К); $\delta_{\text{і}}$ – товщина i-го шару, м; $\lambda_{\text{і}}$ – коефіцієнт теплопровідності i-го шару, Вт/(м·К); n – кількість шарів [2].

Коефіцієнт теплопередачі:

$$U = \frac{1}{R_{\Sigma}},\ \text{Вт/(м²·К)}. \tag{4}$$

Щільність матеріалу:

$$\rho = \frac{m}{V}, \tag{5}$$

де m – маса зразка, кг; V – об'єм, м³.

Водопоглинання за масою:

$$W_m = \frac{m_{\text{вл}} - m_{\text{сух}}}{m_{\text{сух}}} \cdot 100\%, \tag{6}$$

де $m_{\text{вл}}$ – маса зволоженого зразка, кг; $m_{\text{сух}}$ – маса сухого зразка, кг.

Міцність при стиску:

$$\sigma_{\text{ст}} = \frac{F_{\max}}{A},\ \text{Па}, \tag{7}$$

де $F_{\max}$ – максимальне навантаження, Н; A – площа навантаження, м².

Для практичної оцінки якості саме теплозахисної функції матеріалу визначальними є λ, R, U, W_m, стабільність геометрії та збереження механічної цілісності. Такий набір узгоджується з нормативним вибором матеріалу, де поряд із теплопровідністю враховуються вологість, водопоглинання, морозостійкість, паропроникність і гранична температура застосування [9, 10].

2. Показник деградації

Оскільки різні властивості змінюються в протилежних напрямах, універсальний показник доцільно задавати в нормованій формі.

Для показників, що зменшуються внаслідок старіння, наприклад міцності чи термічного опору:

$$D_P(T,t) = 1 - \frac{P(T,t)}{P_0}, \tag{8}$$

де D_P – безрозмірний показник деградації; $P(T, t)$ – поточне значення показника при температурі використання T і часі експлуатації t; P_0 – початкове значення показника.

Для теплопровідності, де погіршення пов'язане зі зростанням λ:

$$D_\lambda(T,t) = \frac{\lambda(T,t) - \lambda_0}{\lambda_0}, \tag{9}$$

де λ_0 – початкове значення коефіцієнта теплопровідності.

Для інженерного прогнозування зручно застосувати узагальнену температурно-часову модель:

$$D(T,t) = 1 - \exp\left[-k(T)\,t\right], \tag{10}$$

де

$$k(T) = B\exp\left(-\frac{E_a}{R_g T}\right). \tag{11}$$

Тут B – множник; E_a – енергія активації процесу старіння, Дж/моль; R_g – універсальна газова стала. За малих значень деградації ця залежність переходить у наближення $D(T, t)=k(T)t$. Така форма не є універсальним стандартом для всіх матеріалів, але добре узгоджується з двома групами підходів, підтверджених у сучасній літературі: експоненційним описом погіршення теплопровідності та кінетичними моделями прискореного старіння на основі температурного прискорення [1, 11, 14, 15].

3. Механізми деградації при теплових навантаженнях та методи визначення показника деградації

При підвищенні температури змінюється не лише миттєве значення λ, а й сама структура матеріалу. Для газонаповнених пінополімерів значення мають дифузія газів крізь комірки,

релаксація полімерної матриці та старіння зв'язків у матеріалі. Для мінераловатних утеплювачів тепловий вплив зазвичай виявляється через зміну вологоутримання, ущільнення структури та втрату частини функціональних добавок, а для штукатурних теплоізоляційних систем – через взаємодію утеплювача, клейового шару, армування і покриття. У реальній огороджувальній конструкції саме комбінація температури та вологи найчастіше прискорює деградацію сильніше, ніж температура окремо [3–8, 12, 13, 15].

Перша група визначення деградації – натурні довготривалі спостереження. Їхня перевага полягає в тому, що вони відтворюють реальний режим роботи конструкції. Недолік очевидний: для отримання достовірної динаміки потрібні роки спостережень. Саме тому такі дані цінні, але дорогі та повільні [1, 2].

Друга група – прискорені лабораторні випробування. Для піноматеріалів застосовують теплове старіння і метод зрізування; для систем із зовнішнім шаром – циклічні температурно-вологісні режими; для фасадних штукатурних систем – погодні та кліматичні цикли. Перевага цих методів у швидкому отриманні еквівалентної довготривалої відповіді, однак результат чутливий до вибраної схеми випробувань [6, 8, 11, 14, 15].

Третя група – експериментально-розрахункові моделі, де результати вимірювань λ, W_m, R, $\sigma_{ст}$ обробляють регресійно або через кінетичні залежності. Для суто теплового старіння доречні моделі типу Арреніуса; для поєднання температури й вологості – моделі, споріднені з підходом Пека; для циклічних впливів – моделі, аналогічні Коффіну-Менсону [3, 15].

Четверта група – оцінка деградації через конструктивну поведінку системи. У цьому випадку відстежують не лише зміну властивостей матеріалу, а й наслідок для всієї огороджувальної конструкції: зменшення R_Σ, появу зон ризику конденсації, локальних теплопровідних включень та дефектів примикань [2, 4, 7, 9].

4. Методи зниження показника деградації

Найбільш розповсюджені підходи до зниження деградації такі (рис. 1):

- зменшення зволоження матеріалу за рахунок гідрофобізації, керування дифузією пари, герметизації примикань;
- використання термостабільних матриць, волокон і добавок;
- двошарові теплоізоляційні рішення зі зміщенням швів;
- зменшення точкових теплопровідних включень і дефектів кріплення;
- застосування захисних паропроникних покриттів і штукатурних систем зі стабільною адгезією;
- контроль експлуатаційного стану та своєчасний ремонт локальних ушкоджень [3, 10, 12, 15].

Найперспективнішим підходом слід вважати комплексне обмеження зволоження теплоізоляційного матеріалу та вузла, тобто поєднання гідрофобізації, паропроникного зовнішнього шару, правильного розташування шарів за пародифузійним опором і усунення водопровідних дефектів. Підвищення температури саме по собі часто збільшує λ помірно, тоді як сумісна дія температури та вологості дає значно сильніший ефект. Це підтверджують і теоретичні дослідження впливу вологовмісту, і експерименти, де вологість різко підсилює ріст теплопровідності [3, 4, 12, 15].

При t=const, зі зростанням температури швидкість деградації збільшується, як це показано на рис. 2. До певного діапазону температур зміна може бути відносно повільною, але після переходу через межу, чутливу для конкретної структури матеріалу або його зв'язувального, деградація прискорюється. Для різних класів утеплювачів ця межа неоднакова, тому графік відображає тенденцію, а не значення для конкретного виробу [10–15].

Рис. 1 – Структура методів зниження показника деградації

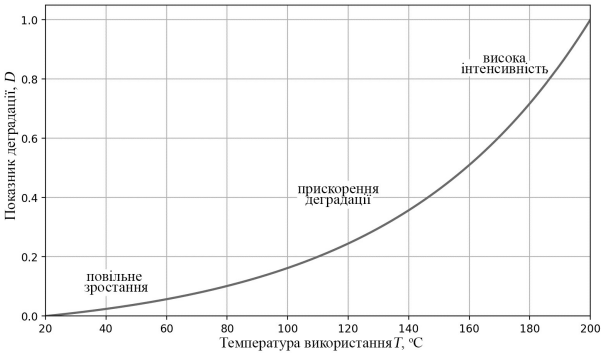


Рис. 2 – Залежність показника деградації від часу експлуатації

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Для випадку T=const та моделі $D(T,t)=1-\exp\left[-k(T)t\right]$, залежність деградації буде мати вигляд, як показано на рис. 3.

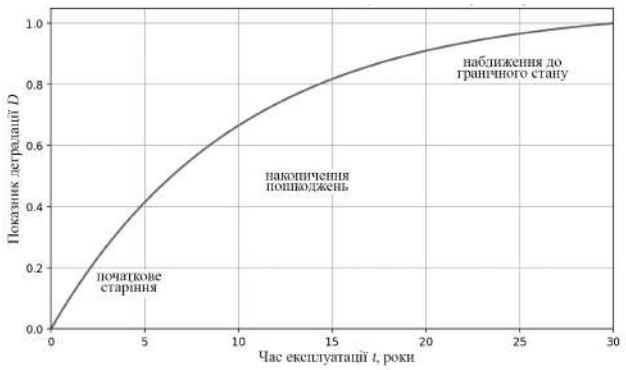


Рис. 3 – Залежність показника деградації від часу експлуатації

На початковому етапі зміна може бути помірною, далі проявляється накопичення пошкоджень, а при наближенні до граничного стану темп приросту деградації зменшується через нормування показника. Така форма відповідає експоненційній залежності накопичення змін та узгоджується з довготривалими й прискореними моделями старіння [1, 11, 14, 15].

Порівняльний графік деградації без захисту і з методом обмеження зволоження, наведено на рис. 4. На схемі крива із захистом відповідає комплексному керуванню вологісним режимом. Її нахил менший, бо зменшується інтенсивність зволоження, а разом із нею – приріст ефективної теплопровідності та ризик структурних пошкоджень. Це не універсальна модель для всіх матеріалів, а якісне відображення, яке демонструє те, що саме волога часто виступає множником деградації [3, 4, 12, 15].

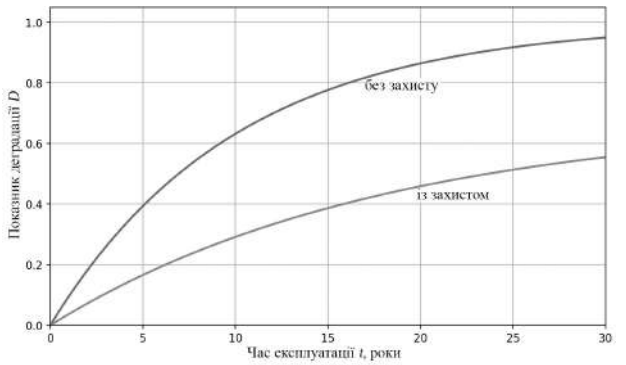


Рис. 4 – Залежність показника деградації від температури використання

Обговорення результатів

Аналіз показав, що поняття деградації для теплоізоляційних матеріалів не можна зводити лише до старіння матеріалу в лабораторному сенсі. Для частини утеплювачів вирішальною є внутрішня еволюція структури, але для фасадних і багатошарових систем не менше значення мають межі шарів, кріплення, зволоження та погодні цикли. Тому один і той самий матеріал може демонструвати різну швидкість деградації в залежності від системи, де він працює. Це пояснює, чому лабораторні методи прискореного старіння корисні, але не дають повної картини без конструктивної інтерпретації [2, 4, 6, 14, 15].

З методичної точки зору найбільш надійною виглядає комбінація трьох рівнів оцінки: пряме вимірювання властивостей, прискорене відтворення старіння і подальше моделювання деградації через температуру та час. Саме така зв'язка дає можливість переносити дані з лабораторії в експлуатаційний прогноз. Водночас для коректного прогнозу потрібно уникати формального перенесення однієї кінетичної моделі на всі матеріали. Для пінополімерів і волокнистих теплоізоляторів визначальні механізми різні, а тому параметри моделі мають встановлюватися окремо.

Для інженерного опису деградації доцільно використовувати нормовані показники $D_P(T,t)$ та $D_\lambda(T,t)$, а для прогнозування – узагальнену температурно-часову залежність $D(T,t)=1-\exp\left[-k(T)t\right]$. Найбільш інформативними методами визначення деградації є поєднання натурних спостережень, прискорених лабораторних випробувань і експериментально-розрахункових моделей. Окреме застосування будь-якого одного методу дає обмежений результат.

Висновки

Деградація показників якості теплоізоляційних матеріалів при теплових навантаженнях проявляється насамперед через зростання коефіцієнта теплопровідності, зменшення термічного опору, зміну вологісного стану, втрату міцності та стабільності структури.

Оцінювання стану теплоізоляційного матеріалу лише за початковим значенням теплопровідності є недостатнім. Для довготривалої оцінки слід враховувати температуру використання, час експлуатації, зволоження та конструктивні умови роботи матеріалу.

Найперспективнішим способом зменшення деградації є комплексне керування вологісним режимом матеріалу та вузла: гідрофобізація, паропроникний захисний шар, контроль примикань і зменшення надходження вологи. Саме цей підхід найпослідовніше знижує інтенсивність погіршення теплотехнічних характеристик при тривалій дії теплових навантажень.

Список літератури

1. Данішевський А. Інтенсивність деградації теплопровідності теплоізоляційних матеріалів фасадів будівель. Енергетика: економіка, технології, екологія. 2026. № 1. С. 96–102. DOI: 10.20535/1813-5420.1.2026.355379.
2. Данішевський А. С., Басок Б. І. Динаміка теплопровідності пінополіуретанової ізоляції огороджувальної конструкції будівлі. Енергетика: економіка, технології, екологія. 2025. № 2. С. 30–34. DOI: 10.20535/1813-5420.2.2025.327137.
3. Лялюк А. О. Планування багатофакторного експерименту при дослідженні впливу вологовмісту теплоізоляційного матеріалу на його теплопровідність. Сучасні технології, матеріали і конструкції в будівництві. 2025. № 2. С. 149–155. DOI: 10.31649/2311-1429-2025-2-149-155.
4. Постоленко А. М., Величко А. М. Експлуатаційна придатність конструкцій зовнішніх стін із фасадною теплоізоляцією та опорядженням штукатурками при застосуванні двошарової теплоізоляції. Наука та будівництво. 2024. № 3(41). С. 25–34. DOI: 10.33644/2313-6679-3-2024-4.
5. Сердюк В. Р., Рудик А. В., Гоголь Т. В. Аналіз сучасного ринку теплоізоляційних матеріалів для енергоефективних будівель. Сучасні технології, матеріали і конструкції в будівництві. 2024. № 1. С. 41–51. DOI: 10.31649/2311-1429-2024-1-41-51.
6. Олексієнко О. Б. Наукові основи забезпечення стійкості фасадних систем з штукатурним шаром до кліматичних впливів. Наука та будівництво. 2022. № 1(31). С. 42–50. DOI: 10.33644/2313-6679-16-2022-5.
7. Олексієнко О. Б. 3D-моделювання точкових теплопровідних включень у фасадних теплоізоляційних системах. Наука та будівництво. 2023. № 2(36). С. 74–82. DOI: 10.33644/2313-6679-2-2023-8.
8. Фаренюк Г. Г., Олексієнко О. Б. Аналіз критеріїв оцінки фасадних конструктивних систем зі штукатурним шаром // Наука та будівництво. 2020. № 4(26). С. 3–14. DOI: 10.33644/scienceandconstruction.v26i4.1.
9. ДБН В.2.6-31:2021. Теплова ізоляція та енергоефективність будівель. Київ, 2021. Чинний від 01.09.2022.
10. ДСТУ 9191:2022. Теплоізоляція будівель. Метод вибору теплоізоляційного матеріалу для утеплення будівель. Київ, 2022.
11. Bae M., Ahn H., Kang J., Choi G., Choi H. Determination of the Long-Term Thermal Performance of Foam Insulation Materials through Heat and Slicing Acceleration. Polymers. 2022. Vol. 14, No. 22. Art. 4926. DOI: 10.3390/polym14224926.
12. Wang Y., Zhang S., Wang D., Liu Y. Experimental Study on the Influence of Temperature and Humidity on the Thermal Conductivity of Building Insulation Materials. Energy and Built Environment. 2023. Vol. 4, No. 4. P. 386–398. DOI: 10.1016/j.enbenv.2022.02.008.
13. Tariku F., Shang Y., Molleti S. Thermal Performance of Flat Roof Insulation Materials: A Review of Temperature, Moisture and Aging Effects. Journal of Building Engineering. 2023. Vol. 76. Art. 107142. DOI: 10.1016/j.jobe.2023.107142.
14. Kim J.-H., Kim S.-M., Kim J.-T. Comparison of Thermal Conductivity and Long-Term Change of Building Insulation Materials According to Accelerated Laboratory Test Methods of ISO 11561 and EN 13166 Standard. Energies. 2024. Vol. 17. Art. 6105. DOI: 10.3390/en17236105.
15. Pinchard L., Parracha J. L., Veiga R., Matias L., Santos Silva A., Duarte S., Nunes L. Weather Ageing Effects on the Long-Term Thermal Conductivity and Biological Colonisation of Thermal Insulating Mortars with EPS, Cork and Aerogel. Energy and Buildings. 2024. Vol. 315. Art. 114403. DOI: 10.1016/j.enbuild.2024.114403.

References (transliterated)

1. Danishevskij A. Intensivnist degradaciyi teploprovidnosti teploizolyacijnih materialiv fasadiv budivel. Energetika: ekonomika, tehnologiyi, ekologiya. 2026. № 1. S. 96–102. DOI: 10.20535/1813-5420.1.2026.355379.
2. Danishevskij A. S., Basok B. I. Dinamika teploprovidnosti pinopoliuretanovoyi izolyaciyi ogorodzhuvalnoyi konstrukciyi budivli. Energetika: ekonomika, tehnologiyi, ekologiya. 2025. № 2. S. 30–34. DOI: 10.20535/1813-5420.2.2025.327137.
3. Lyalyuk A. O. Planuvannya bagatofaktornogo eksperimentu pri doslidzhenni vplivu vologovmistu teploizolyacijnogo materialu na jogo teploprovidnist. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2025. № 2. S. 149–155. DOI: 10.31649/2311-1429-2025-2-149-155.
4. Postolenko A. M., Velichko A. M. Ekspluatacijna pridatnist konstrukcij zovnishnih stin iz fasadnoyu teploizolyaciyeyu ta oporyadzhennyam shtukaturkami pri zastosuvanni dvosharovoyi teploizolyaciyi. Nauka ta budivnictvo. 2024. № 3(41). S. 25–34. DOI: 10.33644/2313-6679-3-2024-4.
5. Serdyuk V. R., Rudik A. V., Gogol T. V. Analiz suchasnogo rinku teploizolyacijnih materialiv dlya energoefektivnih budivel. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2024. № 1. S. 41–51. DOI: 10.31649/2311-1429-2024-1-41-51.
6. Oleksiyenko O. B. Naukovi osnovi zabezpechennya stijkosti fasadnih sistem z shtukaturnim sharom do klimatichnih vpliviv. Nauka ta budivnictvo. 2022. № 1(31). S. 42–50. DOI: 10.33644/2313-6679-16-2022-5.
7. Oleksiyenko O. B. 3D-modelyuvannya tochkovih teploprovidnih vklyuchen u fasadnih teploizolyacijnih sistemah. Nauka ta budivnictvo. 2023. № 2(36). S. 74–82. DOI: 10.33644/2313-6679-2-2023-8.
8. Farenyuk G. G., Oleksiyenko O. B. Analiz kriteriyiv ocinki fasadnih konstruktivnih sistem zi shtukaturnim sharom // Nauka ta budivnictvo. 2020. № 4(26). S. 3–14. DOI: 10.33644/scienceandconstruction.v26i4.1.
9. DBN V.2.6-31:2021. Teplova izolyaciya ta energoefektivnist budivel. Kiyiv, 2021. Chinnij vid 01.09.2022.
10. DSTU 9191:2022. Teploizolyaciya budivel. Metod viboru teploizolyacijnogo materialu dlya uteplennya budivel. Kiyiv, 2022.
11. Bae M., Ahn H., Kang J., Choi G., Choi H. Determination of the Long-Term Thermal Performance of Foam Insulation Materials through Heat and Slicing Acceleration. Polymers. 2022. Vol. 14, No. 22. Art. 4926. DOI: 10.3390/polym14224926.
12. Wang Y., Zhang S., Wang D., Liu Y. Experimental Study on the Influence of Temperature and Humidity on the Thermal Conductivity of Building Insulation Materials. Energy and Built Environment. 2023. Vol. 4, No. 4. P. 386–398. DOI: 10.1016/j.enbenv.2022.02.008.
13. Tariku F., Shang Y., Molleti S. Thermal Performance of Flat Roof Insulation Materials: A Review of Temperature, Moisture and Aging Effects. Journal of Building Engineering. 2023. Vol. 76. Art. 107142. DOI: 10.1016/j.jobe.2023.107142.
14. Kim J.-H., Kim S.-M., Kim J.-T. Comparison of Thermal Conductivity and Long-Term Change of Building Insulation Materials According to Accelerated Laboratory Test Methods

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

of ISO 11561 and EN 13166 Standard. Energies. 2024. Vol. 17. Art. 6105. DOI: 10.3390/en17236105.
15. Pinchard L., Parracha J. L., Veiga R., Matias L., Santos Silva A., Duarte S., Nunes L. Weather Ageing Effects on the Long-Term Thermal Conductivity and Biological Colonisation of Thermal Insulating Mortars with EPS, Cork and Aerogel. Energy and Buildings. 2024. Vol. 315. Art. 114403. DOI: 10.1016/j.enbuild.2024.114403.

Відомості про авторів (About authors)

Канюк Геннадій Іванович **–** доктор технічних наук, професор, завідувач кафедри автоматизації, метрології та енергоефективних технологій; Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0000-0003-1399-9039; e-mail: mezzer@ukr.net;

Kanjuk Gennadii – Doctor of Technical Sciences, Professor of the Department of Automation, Metrology, and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0000-0003-1399-9039; e-mail: kanjuk77@gmail.com;

Єпік Олександр Михайлович **–** аспірант кафедри автоматизації, метрології та енергоефективних технологій;Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0009-0005-
4909-6431; e-mail: oleksandrepik0@gmail.com;

Yepik Oleksandr – Postgraduate student of the Department of Automation, Metrology, and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0009-0005-4909-6431; e-mail: oleksandrepik0@gmail.com;

Будь ласка, посилайтесь на цю статтю наступним чином:

Канюк Г.І., Єпік О.М. Деградація показників якості теплоізоляційних матеріалів при теплових навантаженнях. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 4 (22). С. 60-66. doi:10.20998/2413-4295.2026.02.08.

Please cite this article as:

Kanjuk G., Yepik O. Degradation of quality indicators of thermal insulation materials under thermal loads. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 4(22), pp. 60–66, doi:10.20998/2413-4295.2026.02.08.

Надійшла (received) 17.04.2026
Прийнята (accepted) 08.05.2026
Опублікована (published) 05.06.2026

УДК 621.643:536.2 doi:10.20998/2413-4295.2026.02.09

ВПЛИВ ВОЛОГОСТІ НА ЯКІСТЬ ТЕПЛОІЗОЛЯЦІЇ ПАРОПРОВОДІВ

А. Ю. МЕЗЕРЯ [1*], ***Н. С. АНТОНЕНКО*** [1], ***В. М. КНЯЗЄВА*** [1], ***О. М. БЛИЗНИЧЕНКО*** [1], ***Т. Ю. ВАСИЛЕЦЬ*** [1]

[1] кафедра автоматизації, метрології та енергоефективних технологій, Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, УКРАЇНА
[*]e-mail: mezzer@ukr.net

АНОТАЦІЯ *У роботі розглянуто вплив вологості на показники якості теплоізоляції паропроводів з урахуванням того, що для ізоляційних систем, які працюють на поверхнях з підвищеною температурою, вологовміст не зводиться лише до локального погіршення теплозахисних властивостей, а змінює теплопровідність, термічний опір, інтенсивність лінійних тепловтрат, механічну міцність і прогнозований строк нормальної експлуатації ізоляційного шару. Вихідною передумовою є те, що в пористій або волокнистій структурі теплоізоляційного матеріалу зростання вологовмісту супроводжується частковим витісненням повітря з порового простору, збільшенням частки теплопереносу через рідку фазу, зміною густини, а за тривалої дії температури паропроводу ще й прискоренням деградаційних процесів, пов'язаних зі старінням структури, циклічним перерозподілом вологи та ослабленням гідрофобних властивостей матеріалу. Показано, що ефективне вирішення цього питання знаходиться в напрямку досліджень теплопровідності теплоізоляційних матеріалів, експериментальному визначенню їхніх властивостей, тепловологісному стану огороджувальних конструкцій та деградації теплофізичних характеристик, а також детальної розробки моделі волого-залежної теплопровідності, зв'язаного тепло- і масопереносу у зволоженій мінеральній ваті, старіння ізоляції труб при високих температурах та оптимізацію теплоізоляції перегрітих паропроводів. Показано, що універсальних числових коефіцієнтів, придатних для всіх типів ізоляції та всіх режимів експлуатації відсутні. З метою теоретичних досліджень використовуються узагальнені інженерні залежності, форма яких відповідає науковій літературі, а конкретні параметри моделей мають визначатися для вибраного матеріалу експериментально. Запропоновано формули для оцінювання впливу вологості на теплопровідність, механічну міцність та час нормальної експлуатації, а також окремо подано залежності температурного впливу та сумісного впливу вологості й температури паропроводу. Побудовано розрахункові графіки нормованих залежностей, які відображають характер зміни основних показників якості ізоляції. Отримані узагальнення доцільно використовувати при виборі теплоізоляційних матеріалів для паропроводів, при оцінюванні ризику зволоження ізоляції, а також при формуванні критеріїв технічного обслуговування, де контроль вологості повинен розглядатися як складова забезпечення енергоефективності та довговічності ізоляційної системи, а не як другорядний експлуатаційний фактор.*
Ключові слова: *теплоізоляційні матеріали; показники якості; теплопровідність; водопоглинання; довговічність; вологостійкість.*

THE EFFECT OF MOISTURE ON THE QUALITY OF STEAM PIPELINE THERMAL INSULATION

A. MEZERYA [1*], ***N. ANTONENKO*** [1], ***V. KNIAZIEVA*** [1], ***O. BLIZNICHENKO*** [1], ***T. VASILETS*** [1]

[1] Department of Automation, Metrology, and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, UKRAINE.
[*]e-mail: mezzer@ukr.net

ABSTRACT *The paper examines the effect of moisture on the quality indicators of steam pipeline thermal insulation, taking into account that, for insulation systems operating on elevated-temperature surfaces, moisture content is not limited to a local deterioration of heat-shielding properties, but also alters thermal conductivity, thermal resistance, the intensity of linear heat losses, mechanical strength, and the predicted period of normal service life of the insulation layer. The underlying premise is that, in the porous or fibrous structure of a thermal insulation material, an increase in moisture content is accompanied by partial displacement of air from the pore space, an increase in the share of heat transfer through the liquid phase, and a change in density, while prolonged exposure to steam pipeline temperature additionally accelerates degradation processes associated with structural ageing, cyclic moisture redistribution, and weakening of the material's hydrophobic properties. It is shown that an effective solution to this problem lies in research on the thermal conductivity of thermal insulation materials, the experimental determination of their properties, the hygrothermal state of enclosing structures, and the degradation of thermophysical characteristics, as well as in the detailed development of a moisture-dependent thermal conductivity model, coupled heat and mass transfer in wet mineral wool, ageing of pipe insulation at high temperatures, and optimization of thermal insulation for superheated steam pipelines. It is shown that universal numerical coefficients suitable for all types of insulation and all operating conditions do not exist. For the purposes of theoretical investigation, generalized engineering relationships are used, the form of which is consistent with the scientific literature, while the specific model parameters must be determined experimentally for the selected material. Formulas are proposed for assessing the effect of moisture on thermal conductivity, mechanical strength, and normal service life, and the relationships describing the effect of steam pipeline temperature alone, as well as the combined effect of moisture and temperature, are presented separately. Calculated plots of normalized relationships have been constructed, reflecting the pattern of variation in the main*

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

insulation quality indicators. The obtained generalizations are advisable for use in the selection of thermal insulation materials for steam pipelines, in assessing the risk of insulation wetting, and in establishing maintenance criteria, where moisture control should be regarded as a component of ensuring the energy efficiency and durability of the insulation system rather than as a secondary operational factor.
Keywords: *thermal insulation materials; quality indicators; thermal conductivity; water absorption; durability; moisture resistance*

Вступ

Для паропроводів теплова ізоляція працює в режимі, де одночасно діють підвищена температура стінки, змінні теплові потоки, атмосферне зволоження, проникнення пари, локальні дефекти зовнішньої оболонки та цикли нагрівання й охолодження, тому навіть помірне накопичення вологи не лише збільшує тепловтрати, а й змінює умови старіння самого матеріалу. Саме тому питання вологості в таких системах пов'язане не тільки з паливною економічністю, а й з довговічністю ізоляції, стабільністю температурного режиму, безпечністю експлуатації та точністю енергетичних розрахунків. Окремі роботи показують, що зростання вологовмісту підвищує теплопровідність теплоізоляційного матеріалу, а для трубопровідних систем істотним чинником тепловтрат залишається також вологість середовища навколо труби. Нові дослідження для волокнистих ізоляцій труб і високотемпературних трубопровідних систем також підтверджують, що волога та температура повинні розглядатися як взаємопов'язані фактори, а не як дві незалежні поправки. Це безпосередньо пов'язано з практичними завданнями енергоефективної експлуатації паропроводів, вибору матеріалів, визначення допустимого строку служби ізоляції та обґрунтування міжремонтних інтервалів.

Сучасні наукові дослідження формують достатньо чітке уявлення про базові закономірності, але роботи переважно стосуються огороджувальних конструкцій, фасадних систем і теплових мереж, а не безпосередньо паропроводів. В роботах [1, 2] розроблено та апробовано підходи до експериментального визначення теплопровідності теплоізоляційних матеріалів, зокрема мінераловатних, що дає методичну основу для дослідження волого-залежних властивостей. У статтях [3, 4] систематизовано параметри, які впливають на енергоефективність теплоізоляційних систем, та запропоновано моделі їх комплексного оцінювання, що важливо для переходу від ізольованого аналізу одного показника до багатофакторного опису стану теплоізоляції. Безпосередньо впливу вологовмісту на теплопровідність присвячені праці [5–7], де вологість розглядається як один з визначальних чинників зміни термічного опору і обґрунтовується потреба в натурних експериментах та регресійних моделях. Для трубопровідної тематики важливою є робота [8], у якій показано, що на тепловтрати мереж істотно впливають вологість піску й ґрунту, спосіб прокладання та товщина ізоляції. Тепловологісний стан розглядається в контексті експлуатаційної придатності теплоізоляції [9], а вчені прямо ставлять питання деградації теплофізичних характеристик у часі та показують, що зростання теплопровідності під час експлуатації має накопичувальний характер [10, 11].

Багато наукових робіт істотно деталізують фізику процесу саме для зволожених і високотемпературних ізоляційних систем [12–16]. Так у статті [12] запропоновано модель теплопровідності теплоізоляційних матеріалів з урахуванням вологості, а в роботі [13] досліджено зв'язаний тепло-, масо- та імпульсоперенос у зволоженій мінеральній ваті, що працює на циліндричній поверхні. Доведено, що високотемпературне старіння змінює теплопровідність ізоляцій труб [14]. Проводяться дослідження щодо питання експериментального аналізу поведінки вологої мінераловатної ізоляції труб із різними гідрофобними обробками [15] та оптимізації теплоізоляції перегрітих паропроводів з урахуванням температури, тиску, діаметра та життєвого циклу [16]. Разом з тим, існуючі дослідження не дають універсальних коефіцієнтів, які можна безпосередньо перенести на будь-який теплоізоляційний матеріал паропроводу, оскільки числові параметри істотно залежать від структури волокон, гідрофобізації, щільності, температурного діапазону і режиму зволоження. Саме це і формує дослідницьку прогалину: для інженерного аналізу потрібні не декларативні висновки про зростання теплопровідності, а система узагальнених залежностей, яка одночасно пов'язує вологість, температуру паропроводу, втрату міцності та скорочення строку служби.

Мета роботи

Метою даної роботи є узагальнення закономірностей впливу вологості на якість теплоізоляції паропроводів та побудова системи інженерних залежностей, придатної для подальшого експериментального калібрування під конкретний теплоізоляційний матеріал.

Виклад основного матеріалу

Для циліндричного паропроводу з ізоляцією визначальним енергетичним показником є лінійна щільність тепловтрат, яку доцільно записувати через ефективну теплопровідність зволоженої ізоляції:

$$q_l = \frac{2\pi\left(\theta_{\text{тр}} - \theta_{\text{з}}\right)}{\ln\left(r_2 / r_1\right) / \lambda_{\text{еф}} + 1 / \left(\alpha_{\text{з}} r_2\right)}, \qquad (1)$$

де q_l – лінійні тепловтрати, Вт/м; $\theta_{тр}$ – температура зовнішньої поверхні труби під ізоляцією, °С; $\theta_з$ – температура зовнішнього середовища, °С; r_1 – зовнішній радіус труби, м; r_2 – зовнішній радіус ізоляції, м; $\alpha_з$ – коефіцієнт тепловіддачі від поверхні ізоляції в навколишнє середовище, Вт/(м²·К); $\lambda_{еф}$ – ефективна теплопровідність ізоляції, Вт/(м·К).

Для оцінювання власне теплозахисної здатності ізоляційного шару зручно також використовувати циліндричний термічний опір:

$$R_{ц} = \frac{\ln\left(r_2 / r_1\right)}{2\pi\lambda_{еф}}, \qquad (2)$$

з якого безпосередньо видно, що будь-яке зростання $\lambda_{еф}$ веде до зменшення опору і зростання тепловтрат.

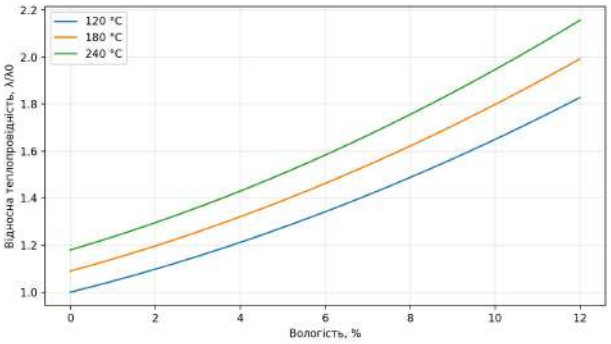


Рис. 1 – Модель впливу вологості на теплопровідність теплоізоляції

Вплив вологості на теплопровідність у робочому інтервалі доцільно описувати квадратичною регресійною залежністю (рис 1.):

$$\lambda\left(w\right) = \lambda_0\left(1 + a_w w + b_w w^2\right), \qquad (3)$$

де λ_0 – теплопровідність сухого матеріалу за еталонної температури θ_0; w – масовий вологовміст, частки одиниці або %; a_w, b_w – експериментально визначені коефіцієнти чутливості до вологи.

Якщо діапазон вологості вузький, достатньою лінеаризації:

$$\lambda\left(w\right) = \lambda_0\left(1 + a_w w\right). \qquad (4)$$

Для термічного опору ізоляційного шару при такому підході маємо:

$$R_{ц}\left(w\right) = \frac{\ln\left(r_2 / r_1\right)}{2\pi\lambda\left(w\right)}. \qquad (5)$$

Фізичний зміст цих залежностей полягає в тому, що зволоження порового простору, яке підтверджено у працях [5–7, 12, 13, 15], призводить до зростання ефективної теплопровідності і відповідного зменшення термічного опору.

Окремий вплив температури паропроводу на теплопровідність доцільно задавати залежністю:

$$\lambda\left(\theta_{тр}\right) = \lambda_0\left[1 + a_T\left(\theta_{тр} - \theta_0\right)\right], \qquad (6)$$

де a_T – коефіцієнт температурної чутливості в обраному інтервалі температур.

Для високотемпературної тривалої дії, коли вже йдеться не про миттєву температурну поправку, а про старіння структури, доцільно застосовувати експоненційну модель деградації:

$$\lambda\left(t\right) = \lambda_0 e^{kt}, \qquad (7)$$

де t – час експлуатації; k – коефіцієнт інтенсивності деградації.

Саме така форма моделі прямо фігурує в новій українській роботі [11], а для трубної ізоляції високотемпературний вплив на теплопровідність і старіння підтверджено також у [14, 16].

Сумісний вплив вологості та температури паропроводу доцільно описувати узагальненим виразом:

$$\begin{aligned}\lambda_{еф}\left(w, \theta_{тр}\right) = \lambda_0\left[1 + a_w w + b_w w^2 + \right. \\ \left. + a_T\left(\theta_{тр} - \theta_0\right) + a_{wT} w\left(\theta_{тр} - \theta_0\right)\right]\end{aligned}, \qquad (8)$$

де a_{wT} – коефіцієнт взаємодії вологості й температури. Саме введення члена взаємодії є принциповим, оскільки для паропроводу температура не просто додає власний внесок у зміну властивості, а змінює характер масопереносу, швидкість висушування, повторного зволоження та старіння волокон або зв'язувальних компонентів. Гідрофобна модифікація в такій постановці не змінює виду рівняння, але зменшує коефіцієнти a_w, b_w і, як правило, a_{wT}.

Для механічної міцності теплоізоляції, якщо її розглядати як нормований показник здатності матеріалу зберігати форму, щільність контакту з трубою та опір руйнуванню під час експлуатації, доцільно використовувати експоненційну форму спаду. Вплив вологості можна записати так (рис. 2):

$$\sigma_{м}\left(w\right) = \sigma_0 e^{-b_{w\sigma} w}, \qquad (9)$$

а вплив температури:

$$\sigma_{м}\left(\theta_{тр}\right) = \sigma_0 e^{-b_{T\sigma}\left(\theta_{тр} - \theta_0\right)}, \qquad (10)$$

де $\sigma_м$ – механічна міцність або її нормоване представлення; σ_0 – міцність у сухому еталонному стані; $b_{w\sigma}$, $b_{T\sigma}$ – коефіцієнти чутливості.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

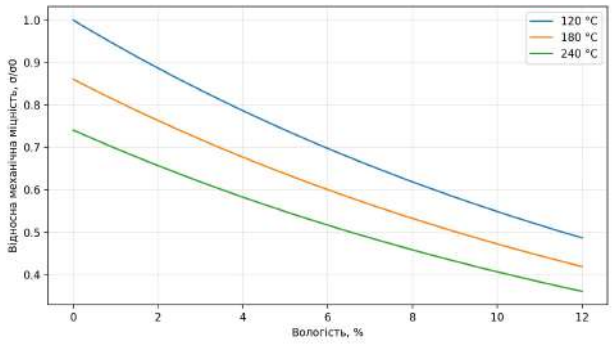


Рис. 2 – Модель впливу вологості на міцність теплоізоляції

Для сумісного впливу природною є залежність (рис. 3):

$$\sigma_{\text{м}}\left(w,\theta_{\text{тр}}\right)=\sigma_0 e^{-\left[b_{w\sigma}w+b_{T\sigma}\left(\theta_{\text{тр}}-\theta_0\right)+b_{wT\sigma}w\left(\theta_{\text{тр}}-\theta_0\right)\right]}, \qquad (11)$$

де $b_{wT\sigma}$ – коефіцієнт взаємодії.

Ці рівняння встановлюють залежність прискореного погіршення властивостей за сумісної дії вологи та температурного старіння.

Час нормальної експлуатації ізоляції доцільно пов'язувати не з календарним віком як таким, а з досягненням граничного стану. Якщо критерієм відмови прийняти досягнення граничної теплопровідності $\lambda_{\text{гр}}$, то для загальної деградаційної моделі можна записати так (рис. 4):

$$\tau_{\text{н}}=\ln\left(\lambda_{\text{тр}}/\lambda_0\right)/k_{\text{д}}\left(w,\theta_{\text{тр}}\right), \qquad (12)$$

де $\tau_{\text{н}}$ – час нормальної експлуатації;

$$k_{\text{д}}\left(w,\theta_{\text{тр}}\right)=k_0+k_w w+k_T\left(\theta_{\text{тр}}-\theta_0\right)+k_{wT}w\left(\theta_{\text{тр}}-\theta_0\right) \qquad (13)$$

– інтегральна інтенсивність деградації; k_0 – базова інтенсивність старіння в сухому еталонному режимі; k_w, k_T, k_{wT} – коефіцієнти впливу вологості, температури та їх взаємодії.

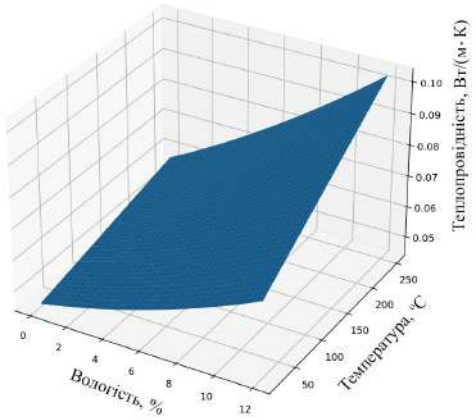


Рис. 3 – Модель впливу вологості та температури на теплопровідність теплоізоляції

Якщо як граничний критерій приймається втрата міцності, замість $\lambda_{\text{гр}}$ вводиться $\sigma_{\text{гр}}$, а сама структура залежності зберігається. Такий підхід безпосередньо спирається на модель деградації теплопровідності, запропоновану в [11], і добре узгоджується з результатами [14], де високотемпературне старіння матеріалів трубної ізоляції дає різний, але помітний приріст теплопровідності.

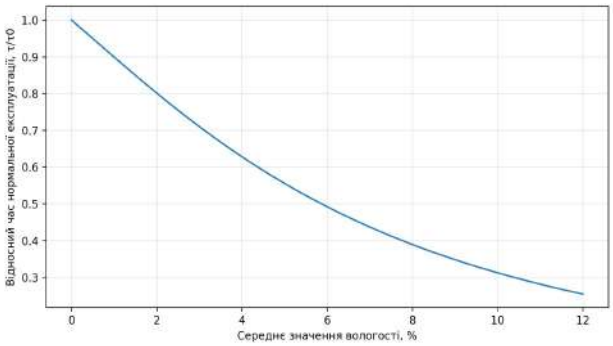


Рис. 4 – Модель впливу вологості на час нормальної експлуатації теплоізоляції

Отримані моделі добре перекликаються з дослідженнями інших авторів, наприклад [11], де досліджено інтенсивність деградації теплопровідності семи традиційних теплоізоляційних матеріалів, що використовуються при оздоблені фасадів огороджувальних конструкцій будівель, та на основі багаторічних польових випробувань (2013–2024 рр.) побудовано експоненційну модель зміни теплопровідності (рис. 5), і визначено коефіцієнти швидкості деградації.

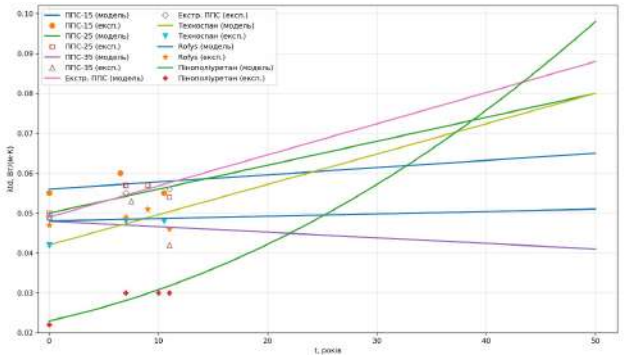


Рис. 5 – Прогноз зміни коефіцієнта теплопровідності λ(t) до 50 років експлуатації на основі експоненційної моделі з нанесенням експериментальних значень

Обговорення результатів

Волога майже завжди погіршує теплозахисну якість ізоляції, але сам механізм цього погіршення для паропроводу не зводиться до простого зростання теплопровідності. Одночасно змінюються локальний температурний профіль, інтенсивність випаровування та конденсації в товщі матеріалу, ступінь збереження

гідрофобності й умови старіння волокнистої структури. Для трубної ізоляції особливо небезпечною є не одноразова подія зволоження, а повторювані цикли «нагрівання – перерозподіл вологи – часткове висушування – повторне зволоження», оскільки саме вони формують накопичуваний деградаційний ефект, який надалі проявляється як зростання теплопровідності, втрата геометричної стабільності та скорочення фактичного строку служби.

З інженерної точки зору це означає, що під час вибору теплоізоляції для паропроводів недостатньо орієнтуватися на паспортне значення теплопровідності в сухому стані; матеріал доцільно оцінювати за чутливістю до зволоження, стабільністю при робочій температурі, здатністю зберігати механічну цілісність і поведінкою системи «матеріал – гідрозахисна оболонка – кріплення – шви». У цьому сенсі контроль вологості слід розглядати як елемент керування якістю ізоляції, а не лише як експлуатаційне спостереження.

Висновки

Вологість є одним із найбільш чутливих чинників погіршення якості теплоізоляції паропроводів, оскільки її зростання підвищує ефективну теплопровідність, зменшує термічний опір і збільшує лінійні тепловтрати. Температура паропроводу не може розглядатися окремо від вологості, тому що вона одночасно впливає на власне теплофізичні характеристики матеріалу, інтенсивність старіння і механізм перерозподілу вологи в ізоляційному шарі; через це сумісний вплив вологості й температури доцільно описувати моделями з членом взаємодії. Для оцінювання строку нормальної експлуатації запропоновано переходити від статичної перевірки сухого паспортного стану до деградаційних моделей граничного стану, в яких базовими аргументами виступають вологість, температура і час дії. Практично це означає, що вибір ізоляції для паропроводу має спиратися на чотири групи показників: суху теплопровідність, вологочутливість, високотемпературну стабільність і збереження механічної цілісності, а експлуатаційний контроль повинен охоплювати не лише температуру поверхні, а й ознаки зволоження та стан зовнішньої оболонки ізоляції.

Список літератури

1. Бікс Ю. С., Ратушняк Г. С., Ратушняк О. Г., Лялюк А. О. Установка для дослідження теплопровідності енергоефективних теплоізоляційних матеріалів рослинного походження. Сучасні технології, матеріали і конструкції в будівництві. 2020. Т. 28. № 1. С. 100–107. DOI: 10.31649/2311-1429-2020-1-100-107.
2. Ратушняк Г. С., Бікс Ю. С., Лялюк А. О. Експериментальні дослідження теплопровідності теплоізоляційних матеріалів із мінеральної вати. Сучасні технології, матеріали і конструкції в будівництві. 2022. Т. 32. № 1. С. 43–48. DOI: 10.31649/2311-1429-2022-1-43-48.
3. Hayrullin A. R., Haibullina A. I., Gusyachkin A. M. Thermal Conductivity of Insulation Material: Effect of Moisture Content and Wet-Drying Cycle. Materials Science Forum. 2023. Vol. 1085. P. 119–124. DOI: 10.4028/p-c1g33d
4. Ратушняк Г. С., Бікс Ю. С., Лялюк А. О., Ратушняк Д. А. Моделювання системи інтелектуальної підтримки прийняття рішень з оцінювання енергоефективності огороджувальних конструкцій будівель з використанням лінгвістичних змінних. Сучасні технології, матеріали і конструкції в будівництві. 2024. Т. 36. № 1. С. 91–95. DOI: 10.31649/2311-1429-2024-1-91-95.
5. Лялюк А. О. Планування багатофакторного експерименту при дослідженні впливу вологовмісту теплоізоляційного матеріалу на його теплопровідність. Сучасні технології, матеріали і конструкції в будівництві. 2025. Т. 39. № 2. С. 149–155. DOI: 10.31649/2311-1429-2025-2-149-155.
6. Lu F., Kaviany M., Williams J., Addison-Smith T. Heat, mass and momentum transport in wet mineral-wool insulation: Experiment and simulation. International Journal of Heat and Mass Transfer. 2024. Vol. 228. Art. 125644. DOI: 10.1016/j.ijheatmasstransfer.2024.125644.
7. Sinyavin A., Hayrullin A., Khusnutdinova M., Dyachuk J., Haibullina A., Ilyin V., Bronskaya V., Bashkirov D. Comparative Experimental Analysis of Wet-State Thermal Performance in Pipe Mineral Wool Insulation with Different Hydrophobic Treatments. Energies. 2025. Vol. 18, no. 22. Art. 6074. DOI: 10.3390/en18226074..
8. Джеджула В. В. Вплив особливостей прокладання та експлуатації трубопроводів на енергоефективність теплових мереж. Сучасні технології, матеріали і конструкції в будівництві. 2024. Т. 37. № 2. С. 193–199. DOI: 10.31649/2311-1429-2024-2-193-199.
9. Постоленко А., Величко А. Експлуатаційна придатність конструкцій зовнішніх стін із фасадною теплоізоляцією та опорядженням штукатурками при застосуванні двошарової теплоізоляції. Наука та будівництво. 2025. Т. 41. № 3. DOI: 10.33644/2313-6679-3-2024-4.
10. Басок Б. І., Гончарук С. М., Данішевський А. С., Гоман Є. І. Динаміка теплофізичних характеристик термоізоляційних матеріалів фасадів будівлі. Енерготехнології та ресурсозбереження. 2025. Т. 84. № 3. С. 119–128. DOI: 10.33070/etars.3.2025.09.
11. Данішевський А. Інтенсивність деградації теплопровідності теплоізоляційних матеріалів фасадів будівель. Енергетика: економіка, технології, екологія. 2026. № 1. DOI: 10.20535/1813-5420.1.2026.355379.
12. Pei W., Ming F., Zhang M., Wan X. A thermal conductivity model for insulation materials considering the effect of moisture in cold regions. Cold Regions Science and Technology. 2023. Vol. 207. Art. 103770. DOI: 10.1016/j.coldregions.2022.103770.
13. Lu F., Kaviany M., Williams J., Addison-Smith T. Heat, mass and momentum transport in wet mineral-wool insulation: Experiment and simulation. International Journal of Heat and Mass Transfer. 2024. Vol. 228. Art. 125644. DOI: 10.1016/j.ijheatmasstransfer.2024.125644.
14. Lakatos Á., Csík A., Lucchi E., La Rosa A. D. Thermal performance and ageing effects to model the life cycle assessment of heat-protective thermal insulation materials in pipe systems. International Communications in Heat and Mass Transfer. 2025. Vol. 164. Part A. Art. 108819. DOI: 10.1016/j.icheatmasstransfer.2025.108819.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

15. Sinyavin A., Hayrullin A., Khusnutdinova M., Dyachuk J., Haibullina A., Ilyin V., Bronskaya V., Bashkirov D. Comparative Experimental Analysis of Wet-State Thermal Performance in Pipe Mineral Wool Insulation with Different Hydrophobic Treatments. Energies. 2025. Vol. 18. No. 22. Art. 6074. DOI: 10.3390/en18226074.
16. Lou C., Zhai C., Li L., Shang Y., Li X., Li D. Thermal insulation design for superheated steam pipeline transport: Balancing technical and economic factors for optimal performance. Applied Thermal Engineering. 2025. Vol. 269, Part B. Art. 126134. DOI: 10.1016/j.applthermaleng.2025.126134.

References (transliterated)

1. Biks Yu. S., Ratushnyak G. S., Ratushnyak O. G., Lyalyuk A. O. Ustanovka dlya doslidzhennya teploprovidnosti energoefektivnih teploizolyacijnih materialiv roslinnogo pohodzhennya. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2020. T. 28. № 1. S. 100–107. DOI: 10.31649/2311-1429-2020-1-100-107.
2. Ratushnyak G. S., Biks Yu. S., Lyalyuk A. O. Eksperimentalni doslidzhennya teploprovidnosti teploizolyacijnih materialiv iz mineralnoyi vati. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2022. T. 32. № 1. S. 43–48. DOI: 10.31649/2311-1429-2022-1-43-48.
3. Hayrullin A. R., Haibullina A. I., Gusyachkin A. M. Thermal Conductivity of Insulation Material: Effect of Moisture Content and Wet-Drying Cycle. Materials Science Forum. 2023. Vol. 1085. P. 119–124. DOI: 10.4028/p-c1g33d
4. Ratushnyak G. S., Biks Yu. S., Lyalyuk A. O., Ratushnyak D. A. Modelyuvannya sistemi intelektualnoyi pidtrimki prijnyattya rishen z ocinyuvannya energoefektivnosti ogorodzhuvalnih konstrukcij budivel z vikoristannyam lingvistichnih zminnih. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2024. T. 36. № 1. S. 91–95. DOI: 10.31649/2311-1429-2024-1-91-95.
5. Lyalyuk A. O. Planuvannya bagatofaktornogo eksperimentu pri doslidzhenni vplivu vologovmistu teploizolyacijnogo materialu na jogo teploprovidnist. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2025. T. 39. № 2. S. 149–155. DOI: 10.31649/2311-1429-2025-2-149-155.
6. Lu F., Kaviany M., Williams J., Addison-Smith T. Heat, mass and momentum transport in wet mineral-wool insulation: Experiment and simulation. International Journal of Heat and Mass Transfer. 2024. Vol. 228. Art. 125644. DOI: 10.1016/j.ijheatmasstransfer.2024.125644.
7. Sinyavin A., Hayrullin A., Khusnutdinova M., Dyachuk J., Haibullina A., Ilyin V., Bronskaya V., Bashkirov D. Comparative Experimental Analysis of Wet-State Thermal Performance in Pipe Mineral Wool Insulation with Different Hydrophobic Treatments. Energies. 2025. Vol. 18, no. 22. Art. 6074. DOI: 10.3390/en18226074..
8. Dzhedzhula V. V. Vpliv osoblivostej prokladannya ta ekspluataciyi truboprovodiv na energoefektivnist teplovih merezh. Suchasni tehnologiyi, materiali i konstrukciyi v budivnictvi. 2024. T. 37. № 2. S. 193–199. DOI: 10.31649/2311-1429-2024-2-193-199.
9. Postolenko A., Velichko A. Ekspluatacijna pridatnist konstrukcij zovnishnih stin iz fasadnoyu teploizolyaciyeyu ta oporyadzhennyam shtukaturkami pri zastosuvanni dvosharovoyi teploizolyaciyi. Nauka ta budivnictvo. 2025. T. 41. № 3. DOI: 10.33644/2313-6679-3-2024-4.
10. Basok B. I., Goncharuk S. M., Danishevskij A. S., Goman Ye. I. Dinamika teplofizichnih harakteristik termoizolyacijnih materialiv fasadiv budivli. Energotehnologiyi ta resursozberezhennya. 2025. T. 84. № 3. S. 119–128. DOI: 10.33070/etars.3.2025.09.
11. Danishevskij A. Intensivnist degradaciyi teploprovidnosti teploizolyacijnih materialiv fasadiv budivel. Energetika: ekonomika, tehnologiyi, ekologiya. 2026. № 1. DOI: 10.20535/1813-5420.1.2026.355379.
12. Pei W., Ming F., Zhang M., Wan X. A thermal conductivity model for insulation materials considering the effect of moisture in cold regions. Cold Regions Science and Technology. 2023. Vol. 207. Art. 103770. DOI: 10.1016/j.coldregions.2022.103770.
13. Lu F., Kaviany M., Williams J., Addison-Smith T. Heat, mass and momentum transport in wet mineral-wool insulation: Experiment and simulation. International Journal of Heat and Mass Transfer. 2024. Vol. 228. Art. 125644. DOI: 10.1016/j.ijheatmasstransfer.2024.125644.
14. Lakatos Á., Csík A., Lucchi E., La Rosa A. D. Thermal performance and ageing effects to model the life cycle assessment of heat-protective thermal insulation materials in pipe systems. International Communications in Heat and Mass Transfer. 2025. Vol. 164. Part A. Art. 108819. DOI: 10.1016/j.icheatmasstransfer.2025.108819.
15. Sinyavin A., Hayrullin A., Khusnutdinova M., Dyachuk J., Haibullina A., Ilyin V., Bronskaya V., Bashkirov D. Comparative Experimental Analysis of Wet-State Thermal Performance in Pipe Mineral Wool Insulation with Different Hydrophobic Treatments. Energies. 2025. Vol. 18. No. 22. Art. 6074. DOI: 10.3390/en18226074.
16. Lou C., Zhai C., Li L., Shang Y., Li X., Li D. Thermal insulation design for superheated steam pipeline transport: Balancing technical and economic factors for optimal performance. Applied Thermal Engineering. 2025. Vol. 269, Part B. Art. 126134. DOI: 10.1016/j.applthermaleng.2025.126134

Відомості про авторів (About authors)

Мезеря Андрій Юрійович **–** кандидат технічних наук, доцент кафедри автоматизації, метрології та енергоефективних технологій; Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0000-0001-8337-2739; e-mail: mezzer@ukr.net;

Mezerya Andrii – Candidate of Technical Sciences Associate Professor of the Department of Automation, Metrology and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0000-0000-0001-8337-2739; e-mail: mezzer@ukr.net;

Антоненко Наталія Сергіївна **–** кандидат технічних наук, доцент кафедри автоматизації, метрології та енергоефективних технологій; Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0009-0000-0879-1642; e-mail: n.s.antonenko@karazin.ua;

Antonenko Natalia – Candidate of Technical Sciences Associate Professor of the Department of Automation, Metrology and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0009-0000-0879-1642; e-mail: n.s.antonenko@karazin.ua;

Князєва Вікторія Миколаївна **–** кандидат технічних наук, доцент кафедри автоматизації, метрології та енергоефективних технологій; Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0000-0002-3106-4897; e-mail: vitok911@ukr.net;

Kniazieva Viktoria – Candidate of Technical Sciences Associate Professor of the Department of Automation, Metrology and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0000-0002-3106-4897; e-mail: vitok911@ukr.net;

Близниченко Олена Миколаївна **–** кандидат технічних наук, доцент кафедри автоматизації, метрології та енергоефективних технологій; Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0009-0000-1654-1598; e-mail: art-studio_diana_@ukr.net;

Bliznichenko Olena – Candidate of Technical Sciences Associate Professor of the Department of Automation, Metrology and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0009-0000-1654-1598; e-mail: art-studio_diana_@ukr.net;

Василець Тетяна Юхимівна **–** кандидат технічних наук, доцент кафедри автоматизації, метрології та енергоефективних технологій; Харківський національний університет ім. В.Н. Каразіна, Майдан Свободи, 4, м. Харків, 61022, Україна. ORCID: 0000-0002-2148-8645; e-mail: vasylecz.ty@uipa.edu.ua;

Vasileys Tetiana – Candidate of Technical Sciences Associate Professor of the Department of Automation, Metrology and Energy-Efficient Technologies; V.N. Karazin Kharkiv National University, Svobody Square, 4, Kharkiv, 61022, Ukraine. ORCID: 0000-0002-2148-8645; e-mail: vasylecz.ty@uipa.edu.ua;

Будь ласка, посилайтесь на цю статтю наступним чином:

Мезеря А.Ю., Антоненко Н.С., Князєва В.М., Близниченко О.М., Василець Т.Ю. Вплив вологості на якість теплоізоляції паропроводів. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 67-73. doi:10.20998/2413-4295.2026.02.09.

Please cite this article as:

Mezerya A., Antonenko N., Kniazieva V., Bliznichenko O., Vasilets T. The effect of moisture on the quality of steam pipeline thermal insulation. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 67–73, doi:10.20998/2413-4295.2026.02.09.

Надійшла (received) 17.04.2026
Прийнята (accepted) 08.05.2026
Опублікована (published) 05.06.2026

УДК 621.311:621.317:004.89 doi: 10.20998/2413-4295.2026.02.10

СЕМАНТИЧНА МОДЕЛЬ ДОСТУПУ ДО ДАНИХ МОНІТОРИНГУ ЯКОСТІ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ В АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

***В. М. ПАВЛЕНКО*[1]*, *А. В. ПЕТРЕНКО*[1], *Л. В. МАРТИНЮК*[1], *М. І. БУНТОВ*[1], *С. Г. АФІНОВИЧ*[1]**

[1] Кафедра інженерії енергосистем, Національний університет біоресурсів і природокористування України, Київ, УКРАЇНА
**e-mail: v.pavlenko@nubip.edu.ua*

АНОТАЦІЯ. *Показано, що цифровий моніторинг якості електричної енергії в автоматизованих інформаційно-вимірювальних системах формує великі масиви часових рядів напруги та струму, показників гармонійних спотворень, несиметрії, провалів, перенапруг і переривань. Акцентовано увагу на двох проблемах: втраті семантичного контексту під час прямого доступу інтелектуальних модулів до таблиць бази даних та недостатній відтворюваності класифікації збурень без фіксації метаданих вимірювання. Запропоновано семантичну модель доступу до даних моніторингу якості електричної енергії, побудовану на використанні сервера Model Context Protocol як контрольованого шару між вимірювальним пристроєм, базою даних PostgreSQL і модулем інтелектуального аналізу. Метод розроблення моделі включає декомпозицію предметної області на вісім сутностей, формування контракту доступу, порівняння з REST API та OWL/RDF-онтологіями, а також введення механізму аудиту запитів. Розглянуто узгодження моделі з підходами Common Information Model та профілями IEC 61970. Наведено розрахункову модель для середньоквадратичної напруги, коефіцієнта гармонійних спотворень, глибини провалу і коефіцієнта несиметрії. Для контрольного сценарію отримано глибину провалу 30,0 %, залишкову напругу 70,0 %, THD 4,39 % і коефіцієнт несиметрії 2,75 %. Додано приклад JSON-структури MCP-запиту та відповіді, що демонструє відтворюваність результату через фіксацію ідентифікатора події, алгоритму та версії обробки. Результати можуть бути використані в системах цифрового моніторингу, SCADA/ADMS, навчальних лабораторіях з якості електроенергії та в дослідженнях за спеціальностями G7, G6 і F6.*

Ключові слова: *якість електричної енергії; Model Context Protocol; семантична модель; цифровий моніторинг; інформаційно-вимірювальна система; Common Information Model; відтворюваність*

SEMANTIC ACCESS MODEL FOR POWER QUALITY MONITORING DATA IN AUTOMATED INFORMATION-MEASUREMENT SYSTEMS

***V. PAVLENKO*[1]*, *A. PETRENKO*[1], *L. MARTYNIUK*[1], *M. BUNTOV*[1], *S. AFINOVYCH*[1]**

[1] Department of Power Systems Engineering, National University of Life and Environmental Sciences of Ukraine, Kyiv, UKRAINE
**e-mail: v.pavlenko@nubip.edu.ua*

ABSTRACT *It is shown that digital power quality monitoring in automated information-measurement systems produces large volumes of voltage and current time series, harmonic distortion indicators, unbalance parameters, voltage dips, swells and interruptions. Two key problems are emphasized: the loss of semantic context when intelligent modules directly access database tables and the limited reproducibility of disturbance classification when measurement metadata are not fixed. A semantic access model for power quality monitoring data is proposed. The model uses a Model Context Protocol server as a controlled layer between a measuring device, a PostgreSQL database and an intelligent analysis module. The development method includes decomposition of the domain into eight entities, construction of an access contract, comparison with REST API and OWL/RDF ontology approaches, and introduction of request audit mechanisms. The model is aligned with the Common Information Model approach and IEC 61970 profiles. A calculation model is presented for root mean square voltage, total harmonic distortion, voltage dip depth and unbalance coefficient. For the control scenario, the obtained values are a 30.0 % voltage dip depth, 70.0 % retained voltage, 4.39 % THD and 2.75 % approximate unbalance coefficient. A JSON-based MCP request and response example is added to demonstrate reproducibility through event identifier, algorithm name and processing version. The results can be used in digital monitoring systems, SCADA/ADMS, educational laboratories on power quality and interdisciplinary research within G7 automation, G6 information-measurement technologies and F6 information systems.*

Keywords*: power quality; Model Context Protocol; semantic model; digital monitoring; information-measurement system; Common Information Model; reproducibility*

Вступ

Якість електричної енергії є одним із ключових параметрів функціонування сучасних електроенергетичних систем, оскільки відхилення напруги, гармонійні спотворення, несиметрія, провали, перенапруги й короткочасні переривання впливають на промислове обладнання, цифрову автоматику, перетворювачі, системи релейного захисту та засоби промислового Інтернету речей. Стандарт IEC 61000-4-30 визначає методи вимірювання параметрів якості електричної енергії у системах змінного струму 50 або 60 Гц [1].

Актуальність задачі посилюється розвитком відновлюваної генерації, мікромереж, нелінійних навантажень і силової електроніки. Сучасні дослідження вказують, що інтеграція відновлюваних джерел і розподіленої генерації підвищує частоту

появи збурень якості електроенергії, зокрема провалів, перенапруг, гармонік та флікеру [5, 6].

У промислових автоматизованих інформаційно-вимірювальних системах проблема полягає не лише у точності вимірювання, а й у коректному поданні даних для подальшого аналізу. Якщо інтелектуальний модуль отримує тільки фрагмент таблиці з часовим рядом, без відомостей про точку моніторингу, клас приладу, одиниці, часові межі та версію алгоритму, виникає ризик помилкової інтерпретації. Саме тому в цій роботі сервер Model Context Protocol розглядається як семантичний шар доступу до даних, а не як звичайний інтерфейс виклику функцій [4].

Аналіз останніх досліджень і публікацій

Методи моніторингу якості електроенергії регламентуються IEC 61000-4-30, IEC 62586-1, IEEE Std 1159-2019 та EN 50160 [1–3, 10]. Водночас сучасні публікації дедалі більше зосереджуються на інтелектуальній класифікації збурень. Огляд Jain та ін. систематизує ML/DL-рішення для оцінювання збурень якості електроенергії та підкреслює важливість цифрової обробки сигналів і відтворюваних наборів ознак [5].

У роботі Anwar та ін. запропоновано поєднання smoothed pseudo Wigner-Ville distribution і Vision Transformer для виявлення та класифікації збурень; автори отримали точність 98,94 % на синтетичних сигналах, сформованих відповідно до IEEE 1159 [6]. Подібні результати демонструють потенціал AI-моделей, але не знімають проблеми формалізованого доступу до даних та метаданих у реальних системах моніторингу.

Для енергетичних інформаційних систем важливим суміжним стандартом є IEC 61970. Він описує підходи Common Information Model для обміну даними в енергетичних системах, а IEC 61970-401:2022 визначає правила створення профілів на основі Canonical CIM і допускає використання UML, RDFS або OWL для опису профілів [11]. Отже, запропонована MCP-модель має узгоджуватися з CIM-логікою на рівні сутностей і метаданих.

У профілях авторів наявні сучасні публікації, що підтримують прикладний контекст цифрової енергетики, відновлюваної генерації та локальних мікроенергетичних систем. У статті використано роботи авторського колективу лише як допоміжний контекст, без підміни ними основної доказової бази та без перевищення допустимої частки самоцитування [13, 14].

Мета роботи

Метою роботи є розроблення семантичної моделі доступу до даних моніторингу якості електричної енергії в автоматизованій інформаційно-вимірювальній системі на основі сервера Model Context Protocol з урахуванням вимог відтворюваності, безпеки доступу та сумісності з підходами CIM/IEC 61970.

Виклад основного матеріалу

Постановка проблеми

У роботі розглядаються дві основні проблеми. Перша проблема – втрата семантичного контексту даних якості електроенергії. Часові ряди, гармоніки, події провалів і перенапруг мають інженерний зміст лише за умови збереження інформації про точку моніторингу, канал, клас приладу, часове вікно, одиниці вимірювання та алгоритм обробки.

Друга проблема – недостатня відтворюваність автоматизованої класифікації збурень. Якщо ознаки події, часові межі, версія алгоритму та метадані вимірювання не зберігаються у формалізованому вигляді, результати класифікації складно перевірити, повторити або використати як навчальний приклад.

Метод розроблення семантичної моделі

Метод розроблення моделі включає чотири етапи: предметну декомпозицію даних якості електроенергії; формування мінімального набору операцій MCP-контракту; визначення обов'язкових метаданих для відтворюваності; порівняння MCP-підходу з REST API та OWL/RDF-онтологією. На першому етапі дані подано через вісім сутностей: об'єкт моніторингу, точку вимірювання, сеанс, канал, часовий ряд, показник якості, подію збурення та метадані.

REST API забезпечує просту інтеграцію, але не задає предметної семантики відповіді без додаткової документації. OWL/RDF-онтологія є потужною для формального логічного виведення, але потребує складнішої інфраструктури. MCP-сервер займає проміжну позицію: він не замінює CIM або онтології, але надає контрольований інтерфейс для AI-модуля, у якому операції мають предметні назви, фіксовані схеми параметрів і обмежені права доступу.

Таблиця 1 – Порівняння підходів доступу до даних моніторингу якості електричної енергії

Підхід	Переваги	Обмеження	Роль у роботі
REST API	Простота реалізації	Семантика часто винесена в документацію	Базова альтернатива
OWL/RDF	Формальна онтологія, логічне виведення	Складність впровадження для лабораторної АІВС	Перспективне розширення
CIM / IEC 61970	Стандартизована модель енергетичних даних	Орієнтація на профілі обміну та EMS/DMS	Семантичний орієнтир
MCP-сервер	Контрольований доступ AI до даних і інструментів	Потребує аудиту, авторизації та обмеження інструментів	Запропоноване рішення

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Архітектура системи та семантичний контракт

Запропонована архітектура включає вимірювальний рівень, комунікаційний рівень, рівень зберігання, семантичний рівень, аналітичний рівень і прикладний інтерфейс (рис. 1). Вимірювальний рівень формують цифровий аналізатор якості електроенергії або smart meter. Комунікаційний рівень передає телеметрію через Ethernet/MQTT. Рівень зберігання реалізується на основі PostgreSQL або сумісного сховища часових рядів. Семантичний рівень утворює MCP-сервер, який надає AI-модулю не таблиці, а предметні сутності.

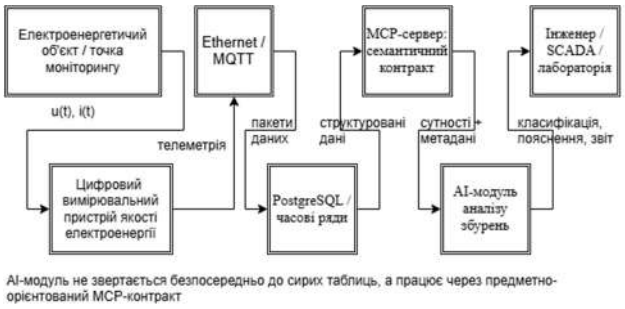


Рис. 1 – Архітектура автоматизованої системи семантичного доступу до даних якості електричної енергії

Семантична модель даних включає ієрархію сутностей, наведену на рис. 2. Метадані мають поперечний характер і пов'язуються з кожним рівнем, оскільки без них неможливо відтворити процедуру аналізу. До обов'язкових метаданих віднесено клас приладу, частоту дискретизації, одиниці вимірювання, часову зону, версію алгоритму, ідентифікатор події та контрольну суму вибірки.

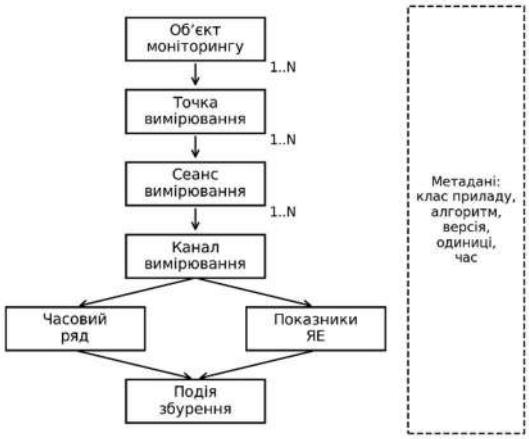


Рис. 2 – Ієрархія семантичних сутностей даних моніторингу якості електричної енергії

Розрахункова модель і відтворюваність

Для дискретного сигналу напруги середньоквадратичне значення визначається як

$$U_{\mathrm{RMS}} = \sqrt{\frac{1}{N}\sum_{i=1}^{N} u_i^2}, \tag{1}$$

де U_{RMS} – середньоквадратичне значення напруги; N – кількість відліків; u_i – миттєві значення напруги.

Коефіцієнт гармонійних спотворень напруги визначається за виразом

$$\mathrm{THD}_U = \frac{\sqrt{\sum_{h=2}^{H} U_h^2}}{U_1} \cdot 100 \tag{2}$$

де THD_U – коефіцієнт гармонічних спотворень напруги; U_h – діюче значення h-ої гармоніки напруги; U_1 – діюче значення основної гармоніки напруги; H – номер найвищої врахованої гармоніки.

Глибина провалу напруги визначається як

$$D_{\mathrm{sag}} = \left(1 - \frac{U_{\min}}{U_{\mathrm{nom}}}\right) \cdot 100 \tag{3}$$

де D_{sag} – глибина провалу напруги; $U_{\min}$ – мінімальне значення діючої напруги під час провалу; U_{nom} – номінальна діюча напруга.

Для прикладної оцінки несиметрії використано наближену форму

$$K_{\mathrm{unb}} = \frac{\max\left|U_k - U_{\mathrm{avg}}\right|}{U_{\mathrm{avg}}} \cdot 100 \tag{4}$$

де K_{unb} – коефіцієнт несиметрії напруги; U_k – діюче значення фазної напруги фази k; U_{avg} – середнє значення фазних напруг.

Формула (4) використовується лише як швидка діагностична оцінка для лабораторного прикладу. Для метрологічно коректної оцінки несиметрії у трифазних мережах доцільно використовувати метод симетричних складових, де коефіцієнт несиметрії визначається через відношення напруги зворотної послідовності до напруги прямої послідовності. Це застереження введено для уникнення підміни стандартизованої процедури спрощеним індикатором.

Для контрольного сценарію прийнято:

U_{nom} = 230 В; $U_{\min}$ = 161 В;

гармонічні складові

U_5 = 8 В, U_7 = 5 В, U_{11} = 3 В, U_{13} = 2 В;

фазні напруги

U_A = 231 В, U_B = 224 В, U_C = 236 В.

Отримано: залишкова напруга – 70,0 %, глибина провалу – 30,0 %, THD_U – 4,39 %, середнє фазне значення – 230,33 В, наближений коефіцієнт несиметрії – 2,75 %.

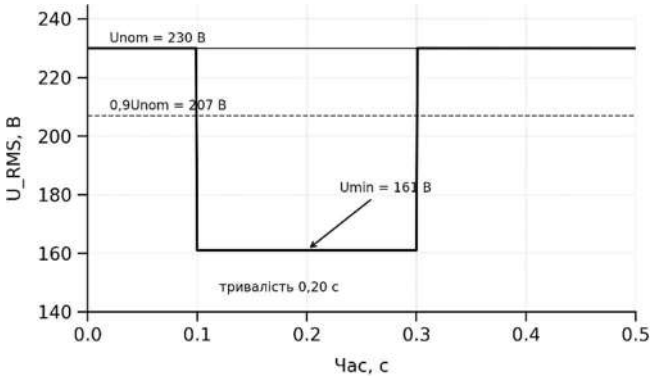


Рис. 3 – Приклад часової діаграми провалу напруги

Приклад MCP-запиту та відповіді

Приклад 1 – Фрагмент MCP-контракту для відтворюваного отримання події ЯЕ

Запит:

{"tool":"getPowerQualityEvent","arguments":{"event_id":"PQE-2026-00017","include_timeseries":true,"include_metadata":true}}

Відповідь:

{"event_id":"PQE-2026-00017","point_id":"MP-10kV-01","channel":"Ua_RMS","time_start":"2026-05-25T10:00:00.100Z","time_end":"2026-05-25T10:00:00.300Z","event_type":"voltage_dip","U_nom_V":230,"U_min_V":161,"retained_voltage_pct":70.0,"dip_depth_pct":30.0,"THD_pct":4.39,"algorithm":"PQ-basic-v1","algorithm_version":"1.0.3","sample_hash":"sha256:..."}

Наявність event_id, algorithm_version і sample_hash забезпечує повторюваність: повторний запит до того самого ідентифікатора повертає однакові часові межі, однаковий набір відліків або контрольну суму та однакову версію алгоритму. У разі зміни алгоритму формується нова версія результату, а попередня залишається доступною для аудиту.

Безпека MCP-інтеграції

Для промислового застосування MCP-сервер має розглядатися як межа довіри. OWASP MCP Top 10 виділяє ризики керування токенами, розширення привілеїв, отруєння інструментів, недостатньої автентифікації та авторизації, відсутності аудиту і телеметрії, а також надмірного поширення контексту [12]. Для запропонованої системи мінімальний набір заходів включає рольову авторизацію, заборону довільних SQL-запитів, реєстрацію всіх викликів інструментів, контроль версій контракту та розділення доступу до сирих даних і похідних показників.

Обговорення результатів

Порівняно з прямим доступом до таблиць бази даних запропонована модель зменшує ризик помилкової інтерпретації, оскільки кожна відповідь містить не лише числові значення, а й контекст вимірювання. Це особливо важливо для AI-модулів, які можуть формувати висновки природною мовою або автоматично обирати інструменти аналізу.

Порівняно з повноцінною онтологією OWL/RDF MCP-підхід є простішим для впровадження у лабораторній або прототипній системі. Водночас він не суперечить CIM/IEC 61970, оскільки може використовувати CIM-подібні назви сутностей і метаданих. Перспективним напрямом є створення мапінгу між сутностями MCP-контракту та профілем CIM для розподільної мережі.

Академічна доброчесність та використання цифрових інструментів

Автори підтверджують, що поданий матеріал є результатом власного наукового опрацювання; усі використані джерела належним чином процитовані; результати інших авторів відокремлені від авторських положень. Під час підготовки рукопису використовувалися цифрові інструменти для технічного структурування, мовного редагування та перевірки узгодженості тексту. Змістові наукові положення, добір джерел, інженерна інтерпретація, розрахунки, висновки та відповідальність за достовірність матеріалу належать авторам. Зображення у статті не є результатами експериментальних вимірювань, а подані як схеми та діаграми для відтворення архітектури і логіки запропонованої моделі.

Висновки

Запропоновано семантичну модель доступу до даних моніторингу якості електричної енергії, що поєднує вимірювальний пристрій, базу даних, MCP-сервер і AI-модуль у межах автоматизованої інформаційно-вимірювальної системи.

Враховано дві ключові проблеми: втрату семантичного контексту вимірювань та недостатню відтворюваність автоматизованої класифікації збурень.

Додано методологічне обґрунтування вибору MCP через порівняння з REST API, OWL/RDF і CIM/IEC 61970, а також розширено статтю блоком безпеки MCP-інтеграції.

Розрахунковий приклад підтвердив можливість формування структурованих ознак події: глибина провалу 30,0 %, залишкова напруга 70,0 %, THD 4,39 %, наближений коефіцієнт несиметрії 2,75 %.

Для всіх рисунків наведено детальні текстові описи, достатні для відтворення схем у зовнішніх графічних застосунках. Тематика відповідає спеціальностям G7, G6 і F6.

Декларації та уточнення щодо академічної доброчесності

Декларація академічної доброчесності. Автори підтверджують, що рукопис підготовлено з дотриманням принципів академічної доброчесності: використані джерела наведено у списку літератури, результати інших авторів відокремлено від авторських положень, наведений розрахунковий приклад

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

позначено як контрольний сценарій, а не як результат промислового експерименту. Автори несуть відповідальність за достовірність наведених тверджень, розрахунків, джерел і висновків відповідно до вимог Закону України «Про академічну доброчесність» [15].

Декларація щодо використання штучного інтелекту. Під час підготовки рукопису цифрові інструменти штучного інтелекту могли використовуватися лише для технічного структурування тексту, мовного редагування, перевірки логіки викладу та формування допоміжних описів рисунків. Змістові наукові положення, інженерна інтерпретація, вибір джерел, розрахунки та остаточні висновки перевірені й затверджені авторами. Така декларація введена з огляду на вимогу повідомляти про використання об'єктів або результатів, згенерованих штучним інтелектом, в академічному творі [15].

Список літератури

1. IEC 61000-4-30:2025. Electromagnetic compatibility (EMC) – Part 4-30: Testing and measurement techniques – Power quality measurement methods. Geneva: International Electrotechnical Commission, 2025.
2. IEC 62586-1:2017. Power quality measurement in power supply systems – Part 1: Power quality instruments. Geneva: International Electrotechnical Commission, 2017.
3. IEEE Std 1159-2019 Recommended Practice for Monitoring Electric Power Quality 2. IEEE Power and Energy Society. New York: IEEE, 2019. URL: https://www.scribd.com/document/857784798/IEEE-Std-1159-2019-Recommended-Practice-for-Monitoring-Electric-Power-Quality-2 (дата звернення: 25.05.2026).
4. Model Context Protocol. Specification. 2025. URL: https://modelcontextprotocol.io/specification/2025-11-25 (дата звернення: 25.05.2026).
5. Jain S., Satsangi A., Kumar R., Panwar D., Amir M. Intelligent assessment of power quality disturbances: A comprehensive review on machine learning and deep learning solutions. Computers and Electrical Engineering. 2025. Vol. 123. Article 110275. doi:10.1016/j.compeleceng.2025.110275.
6. Anwar M. H., Baig M. M. A., Shaikh A. J., Abro A. G. Detection and classification of power quality disturbances: Vision transformers vs. CNN. AIMS Energy. 2025. Vol. 13, no. 5. P. 1052–1075. doi:10.3934/energy.2025039.
7. Albalooshi F. A., Qader M. R. Deep Learning Algorithm for Automatic Classification of Power Quality Disturbances. Applied Sciences. 2025. Vol. 15, no. 3. Article 1442. doi:10.3390/app15031442.
8. Pan S., Nie X., Zhai X., Wang B., Ge H., He C., Ding Z. Classification of Power Quality Disturbances Using ResNet with Channel Attention Mechanism. arXiv. 2024. doi:10.48550/arXiv.2407.04739.
9. de Sousa E. L., de Oliveira R. A., Neto A. F., et al. Development of a Low-Cost Wireless Smart Meter with Power Quality Measurement for Smart Grid Applications. Sensors. 2023. Vol. 23, no. 16. Article 7210. doi:10.3390/s23167210.
10. EN 50160:2022. Voltage characteristics of electricity supplied by public electricity networks. Brussels: CENELEC, 2022.
11. IEC 61970-401:2022. Energy management system application program interface (EMS-API) – Part 401: Profile framework. Geneva: International Electrotechnical Commission, 2022.
12. OWASP Foundation. OWASP MCP Top 10. 2025. URL: https://owasp.org/www-project-mcp-top-10/ (дата звернення: 25.05.2026).
13. Shvedchykova I., Trykhlieb A., Trykhlieb S., Demishonkova S., Pavlenko V. Determining the efficiency of restored photovoltaic modules under natural lighting conditions. Eastern-European Journal of Enterprise Technologies. 2024. Vol. 6, no. 8(132). P. 16–24. doi:10.15587/1729-4061.2024.317829
14. Каплун В. В., Макаревич С. С., Петренко А. В., Кругляк Г. В., Кулибаба Є. О. Адаптивне управління електроспоживанням в локальній мікроенергетичній системі з полігенерацією на основі кластеризації умовного динамічного тарифу. Енергетика: економіка, технології, екологія. 2023. Вип. 1. С. 22–29. DOI: https://doi.org/10.20535/1813-5420.1.2023.275929
15. Закон України «Про академічну доброчесність» від 18.12.2025 № 4742-IX. URL: https://zakon.rada.gov.ua/laws/show/4742-20 (дата звернення: 26.05.2026).

References

1. IEC 61000-4-30:2025. Electromagnetic compatibility (EMC) – Part 4-30: Testing and measurement techniques – Power quality measurement methods. Geneva, International Electrotechnical Commission, 2025.
2. IEC 62586-1:2017. Power quality measurement in power supply systems – Part 1: Power quality instruments. Geneva, International Electrotechnical Commission, 2017.
3. IEEE Std 1159-2019 Recommended Practice for Monitoring Electric Power Quality 2. IEEE Power and Energy Society. New York: IEEE, 2019. URL: https://www.scribd.com/document/857784798/IEEE-Std-1159-2019-Recommended-Practice-for-Monitoring-Electric-Power-Quality-2 (accessed 25.05.2026).
4. Model Context Protocol. Specification. 2025. Available at: https://modelcontextprotocol.io/specification/2025-11-25 (accessed 25.05.2026).
5. Jain S., Satsangi A., Kumar R., Panwar D., Amir M. Intelligent assessment of power quality disturbances: A comprehensive review on machine learning and deep learning solutions. Computers and Electrical Engineering, 2025, vol. 123, article 110275, doi:10.1016/j.compeleceng.2025.110275.
6. Anwar M. H., Baig M. M. A., Shaikh A. J., Abro A. G. Detection and classification of power quality disturbances: Vision transformers vs. CNN. AIMS Energy, 2025, vol. 13, no. 5, pp. 1052–1075, doi:10.3934/energy.2025039.
7. Albalooshi F. A., Qader M. R. Deep Learning Algorithm for Automatic Classification of Power Quality Disturbances. Applied Sciences, 2025, vol. 15, no. 3, article 1442, doi:10.3390/app15031442.
8. Pan S., Nie X., Zhai X., Wang B., Ge H., He C., Ding Z. Classification of Power Quality Disturbances Using ResNet with Channel Attention Mechanism. arXiv, 2024, doi:10.48550/arXiv.2407.04739.
9. de Sousa E. L., de Oliveira R. A., Neto A. F., et al. Development of a Low-Cost Wireless Smart Meter with

Power Quality Measurement for Smart Grid Applications. Sensors, 2023, vol. 23, no. 16, article 7210, doi:10.3390/s23167210.
10. EN 50160:2022. Voltage characteristics of electricity supplied by public electricity networks. Brussels, CENELEC, 2022.
11. IEC 61970-401:2022. Energy management system application program interface (EMS-API) – Part 401: Profile framework. Geneva, International Electrotechnical Commission, 2022.
12. OWASP Foundation. OWASP MCP Top 10. 2025. Available at: https://owasp.org/www-project-mcp-top-10/ (accessed 25.05.2026).
13. Shvedchykova I., Trykhlieb A., Trykhlieb S., Demishonkova S., Pavlenko V. Determining the efficiency of restored photovoltaic modules under natural lighting conditions. Eastern-European Journal of Enterprise Technologies, 2024, vol. 6, no. 8(132), pp. 16–24, doi:10.15587/1729-4061.2024.317829.
14. Kaplun V. V., Makarevych S. S., Petrenko A. V., Kruhliak H. V., Kulybaba Ye. O. Adaptyvne upravlinnia elektrospozhyvanniam v lokalnii mikroenerhetychnii systemi z poliheneratsiieiu na osnovi klasteryzatsii umovnoho dynamichnoho taryfu [Adaptive control of electricity consumption in a local microenergy system with polygeneration based on clustering of a conditional dynamic tariff]. Enerhetyka: ekonomika, tekhnolohii, ekolohiia, 2023, issue 1, pp. 22–29. DOI: https://doi.org/10.20535/1813-5420.1.2023.275929
15. Zakon Ukrainy «Pro akademichnu dobrochesnist» vid 18.12.2025 no. 4742-IX [Law of Ukraine "On Academic Integrity" dated 18.12.2025 no. 4742-IX]. Available at: https://zakon.rada.gov.ua/laws/show/4742-20 (accessed 26.05.2026).

Відомості про авторів

Павленко Володимир Миколайович – кандидат технічних наук, доцент, Національний університет біоресурсів і природокористування України, доцент кафедри інженерії енергосистем, м. Київ, Україна; ORCID: https://orcid.org/0000-0003-2163-8508; e-mail: v.pavlenko@nubip.edu.ua.

Pavlenko Volodymyr – Candidate of Technical Sciences (Ph. D.), Docent, National University of Life and Environmental Sciences of Ukraine, Associate Professor, Department of Power Systems Engineering, Kyiv, Ukraine; ORCID: https://orcid.org/0000-0003-2163-8508; e-mail: v.pavlenko@nubip.edu.ua.

Петренко Андрій Володимирович – кандидат технічних наук, доцент, Національний університет біоресурсів і природокористування України, доцент кафедри інженерії енергосистем, м. Київ, Україна; ORCID: https://orcid.org/0000-0002-8246-4911; e-mail: petrenko@nubip.edu.ua

Petrenko Andrii – Candidate of Technical Sciences (Ph. D.), Docent, National University of Life and Environmental Sciences of Ukraine, Associate Professor, Department of Power Systems Engineering, Kyiv, Ukraine; ORCID: https://orcid.org/0000-0002-8246-4911; e-mail: petrenko@nubip.edu.ua.

Мартинюк Лілія Володимирівна – Національний університет біоресурсів і природокористування України, старший викладач кафедри інженерії енергосистем, м. Київ, Україна; ORCID: https://orcid.org/0009-0007-3852-5610; e-mail: martyniuklilia@nubip.edu.ua

Martyniuk Liliia – National University of Life and Environmental Sciences of Ukraine, Senior Lecturer, Department of Power Systems Engineering, Kyiv, Ukraine; ORCID: https://orcid.org/0009-0007-3852-5610; e-mail: martyniuklilia@nubip.edu.ua

Бунтов Матвій Іванович – Національний університет біоресурсів і природокористування України, аспірант, м. Київ, Україна; ORCID: https://orcid.org/0009-0009-3872-0517; e-mail: matt.buntov@nubip.edu.ua.

Buntov Matvii – National University of Life and Environmental Sciences of Ukraine, Postgraduate Student, Kyiv, Ukraine;ORCID: https://orcid.org/0009-0009-3872-0517; e-mail: matt.buntov@nubip.edu.ua.

Афінович Сергій Григорович – Національний університет біоресурсів і природокористування України, аспірант, м. Київ, Україна, ORCID: https://orcid.org/0009-0007-9788-3696; e-mail: s.afinovych@nubip.edu.ua.

Afinovych Serhii – National University of Life and Environmental Sciences of Ukraine, Postgraduate student, Kyiv, Ukraine, ORCID: https://orcid.org/0009-0007-9788-3696; e-mail: s.afinovych@nubip.edu.ua

Будь ласка, посилайтесь на цю статтю наступним чином:

Павленко В. М., Петренко А. В., Мартинюк Л. В., Бунтов М. І., Афінович С. Г. Семантична модель доступу до даних моніторингу якості електричної енергії в автоматизованих інформаційно-вимірювальних системах. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях.* – Харків: НТУ «ХПІ». 2026. № 2(28). С. 74–79. doi:10.20998/2413-4295.2026.02.10.

Please cite this article as:

Pavlenko V., Petrenko A., Martyniuk L., Buntov M., Afinovych S. Semantic access model for power quality monitoring data in automated information-measurement systems. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 74–79, doi:10.20998/2413-4295.2026.02.10.

Надійшла (received) 18.05.2026
Прийнята (accepted) 25.05.2026
Опублікована (published) 05.06.2026

UDC 004.89:621.79:681.5 doi:10.20998/2413-4295.2026.02.11

3D PRINTING AS AN ALTERNATIVE TO SPARE PARTS FOR FIELD REPAIR OF RADIO-ELECTRONIC EQUIPMENT

***I. IV. KLYUCHNYK*[1*], *V. NEBRAT*[2], *I. IG. KLIUCHNYK*[3], *O. DEGTIAROV*[3], *T. HEUEIS*[4]**

[1]*Department of Electronic Devices Design and Operation, Kharkiv National University of Radio Electronics, Kharkiv, UKRAINE*
[2]*Department of Microelectronics, Electronic Devices and Devices, Kharkiv National University of Radio Electronics, Kharkiv, UKRAINE*
[3]*Department of Information and Measurement Technology, Kharkiv National University of Radio Electronics, Kharkiv, UKRAINE*
[4]*Mühlbauer+Partner, Technische Dokumentation GmbH & Co. KG, Unterschleißheim, GERMANY*
[*]*e-mail: ihor.kliuchnyk@nure.ua*

ABSTRACT *The application of three-dimensional printing technologies for the rapid restoration of radio-electronic equipment in field conditions, in cases of limited access to logistics infrastructure and as an alternative to traditional spare parts kits is considered. The technical and economic aspects of choosing three-dimensional printer models are analyzed depending on the level of structural complexity of radio-electronic equipment, the dimensions of parts and the features of their operation. It is shown that the use of three-dimensional printing technologies allows the manufacture of not only individual parts of equipment structures, but also elements of its fastening to the corresponding installation objects, parts, assembly units of installation objects and components for the printing devices themselves. The main stages of preparing products for manufacturing by the three-dimensional printing method are considered. The possibilities of automatic selection of materials, formation of technological parameters of printing, verification of model geometry, preparation of control programs and control of the manufacturing process of products are analyzed. An experimental study of the effectiveness of using artificial intelligence to prepare parts of the field radio station housing for manufacturing was conducted. A comparison of printing parameters proposed by experienced specialists and the artificial intelligence system was carried out. A high degree of compliance of the received recommendations with the requirements for strength, reliability and durability of the product was confirmed. The timing of preparatory operations was carried out and it was established that the use of artificial intelligence provides a significant reduction in the time of preparation for printing due to the automation of analytical and calculation procedures. The feasibility of using artificial intelligence to increase the efficiency of field repairs and reduce the requirements for the level of personnel training was confirmed. The prospects of combining the technologies of three-dimensional printing, reuse of polymer materials, multi-material printing and manufacturing of metal parts by the cold spraying method for further development of the concept of operational restoration of radio-electronic equipment directly at the places of its operation were shown.*
Key words*: 3DP-SP, additive manufacturing, field repair, print preparation, spare parts, artificial intelligence.*

3D-ДРУК ЯК АЛЬТЕРНАТИВА ПОШУКУ ЗАПЧАСТИН ПРИ РЕМОНТІ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ В ПОЛЬОВИХ УМОВАХ

***І. І. КЛЮЧНИК*[1*], *В. В. НЕБРАТ*[2], *І. ІГ. КЛЮЧНИК*[3], *О. В. ДЕГТЯРЬОВ*[3], *Т. ГЕУАЙС*[4]**

[1] кафедра проектування та експлуатації електронних апаратів, Харківський національний університет радіоелектроніки, Харків, УКРАЇНА
[2] кафедра мікроелектроніки, електронних приладів та пристроїв, Харківський національний університет радіоелектроніки, Харків, УКРАЇНА
[3] кафедра інформаційно-вимірювальних технологій, Харківський національний університет радіоелектроніки, Харків, УКРАЇНА
[4] компанія *Mühlbauer+partner, Technische Dokumentation GmbH&Co. KG, Унтершляйсгаймі, НІМЕЧЧИНА*
[*] *e-mail: ihor.kliuchnyk@nure.ua*

АНОТАЦІЯ *Розглянуто застосування технологій тривимірного друку для оперативного відновлення радіоелектронної апаратури у польових умовах, в випадках обмеженого доступу до логістичної інфраструктури та як альтернативи традиційним комплектам запасних частин. Проаналізовано технічні та економічні аспекти вибору моделей тривимірних принтерів залежно від рівня конструктивної складності радіоелектронних засобів, габаритів деталей та особливостей їх експлуатації. Показано, що використання технологій тривимірного друку дозволяє виготовляти не лише окремі деталі конструкцій апаратури, а й елементи її кріплення на відповідні об'єкти установлення, деталі, монтажні вузли об'єктів установлення та комплектуючі для самих друкувальних пристроїв.Розглянуто основні етапи підготовки виробів до виготовлення методом тривимірного друку. Проаналізовано можливості автоматичного вибору матеріалів, формування технологічних параметрів друку, перевірки геометрії моделей, підготовки керуючих програм та контролю процесу виготовлення виробів. Проведено експериментальне дослідження ефективності використання штучного інтелекту для підготовки до виготовлення деталі корпусу польової радіостанції. Виконано порівняння параметрів друку, запропонованих досвідченими фахівцями та системою штучного інтелекту. Підтверджено високий ступінь відповідності отриманих рекомендацій вимогам до міцності, надійності та довговічності виробу. Проведено хронометраж підготовчих операцій та встановлено, що застосування штучного інтелекту забезпечує суттєве скорочення часу підготовки до друку*

завдяки автоматизації аналітичних та розрахункових процедур. Підтверджено доцільність використання штучного інтелекту для підвищення ефективності польового ремонту та зниження вимог до рівня підготовки персоналу. Показано перспективність поєднання технологій тривимірного друку, повторного використання полімерних матеріалів, багатоматеріального друку та виготовлення металевих деталей методом холодного напилення для подальшого розвитку концепції оперативного відновлення радіоелектронної апаратури безпосередньо в місцях її експлуатації.
Ключові слова: *ЗІП-принтер, 3D-друк, польовий ремонт, підготовка до друку, запасні частини, ШІ*

.

Introduction

Radio-electronic equipment (REE) is an important component in almost any sphere of activity of modern society. During its operation, for various reasons, situations may arise in which it becomes necessary to carry out appropriate repair work. Usually, the availability of service support, spare parts and qualified personnel allows you to avoid significant inconveniences with repairs, but under certain circumstances (impossibility of timely delivery of damaged or failed parts, complete lack of communication or transport links, etc.) the equipment may partially or completely cease to perform its functions for a long time. Such risks should be considered, for example, when using REE on spacecraft, submarines and surface boats, Arctic stations, during military operations, etc.

In such situations, as an alternative to searching for spare parts, the use of 3D printing technologies can be proposed, which to date have already achieved certain successes in the manufacture of products with satisfactory quality characteristics for many applications [1-7]. An objective need exists to improve repair methodologies for equipment with rare earth elements. The most promising solution is the use of 3D printing to manufacture spare parts on-site, directly at the equipment operation locations.

Objective

The objective of this work is to enhance the efficiency of field repair of radio-electronic equipment through the use of 3D printing technologies and artificial intelligence.

Core of the work

3DP-SP printer selection options

Modern 3D printers have a wide range of technical characteristics [8-11], which can be used to make a reasonable choice of the appropriate model, which is actually included in the set of radio-electronic equipment instead of a certain number of spare parts, typical replacement elements or structural parts with a regulated service life or those that work in difficult operating conditions. At the same time, the printer itself is easily disassembled and in this state does not take up much space. However, the list of parts potentially suitable for printing is significantly affected by the size of the printer's working field – the printing platform. Such a limitation also determines the economic feasibility of using 3D printing as an alternative to the traditional set of spare tools and accessories (SPA), since the price of 3D printers is proportional to the size of their printing area [12, 13]. In turn, a comparison of the minimum and maximum possible sizes of parts that can be printed on a 3DP-SP printer and typical sizes for radio electronic equipment (REE) indicates that at present such a repair concept applies, first of all, to structural parts of REE of the first and second levels of the hierarchy in a conventional or on REM1, REM2 in a modular design. For the above-mentioned conditions of use, which are mostly characterized by the presence of restrictions on the size of the volumes for placing equipment, available 3DP-SP printers provide printing of structural parts of equipment of such levels of complexity. In addition, it should be noted that the concept of 3DP-SP printers can be extended to the repair and manufacture of structural parts that are associated with the fastening and installation of REE on installation objects, as well as to the manufacture of some parts of such objects. For example, these may be original brackets for mounting video equipment and additional power sources on UAVs, the number of models of which already exceeds hundreds today [14-18]. The lack of standardization of such design solutions will keep such tasks relevant for a long time. In these cases, the cost-effectiveness of using a spare parts printer increases significantly.

The quality of parts and products using 3D printing technology is largely determined by the properties of the materials used. The raw materials are filaments, granules, powders from the most common materials: ABS; PLA; PETG, nylon, as well as secondary plastics.

With a long autonomous stay at remote stations, etc., it is especially advisable to use recycled used or secondary plastic material. Products made from recycled material without its purification and stabilization of characteristics have lower quality indicators than from original materials. However, equipment for implementing the recycling process for 3D printing already today reaches satisfactory indicators and continues to be improved. This indicates the possibility of combining both printing and recycling functions in 3D printers in the near future, which will reduce material costs, energy consumption, and increase environmental friendliness.

The implementation of the concept of 3DP-SP printers is also facilitated by the simplification of the printing preparation process, which includes all stages from creating a sketch of the part to generating and saving the G-code that controls the operation of the 3D printer. A typical preparation process consists of the following operations: object modeling – creating a three-dimensional model using CAD software (for example, Blender, Fusion 360, SolidWorks); object optimization – checking for errors: models are checked for holes,

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

polygon intersections or incorrect geometry; model export - saving the model in formats supported by 3D printers (the most common: STL, OBJ, 3MF); settings in the slicer program – importing the model into a layer-by-layer slicing program, for example, Cura, Prusa Slicer, Simplify3D, setting up print parameters, as well as cutting the model into layers (slicing) and saving it in G-code format; 3D printer preparation – cleaning and calibrating the printing platform, loading the material; uploading G-code to the 3D printer via SD card, USB or Wi-Fi. After that, the model is printed.

Reducing the duration of the preparation process can be achieved by using a 3D scanner at the modeling stage. For scanning medium and large objects (REM1, REM2), the most promising are portable (hand-held) laser scanners, which are especially effective for objects with complex geometry (Artec Eva, Creality CR-Scan Lizard). Scanning takes several minutes (15–30 min) for those parts of REE structures, the manual design of which takes hours (5–15 hours). In this case, the verification stage is minimized and the export stage is not required, a ready-to-print STL or OBJ model is automatically generated.

The role of AI in prepress

In addition, a significant reduction in work can be achieved by involving the capabilities of artificial intelligence (AI) at all stages of preparing the model for printing. At the stage of object modeling, AI can simplify the process of creating a 3D model by automatically correcting errors in geometry, optimizing topology, and even generating models based on a text description. For example, generative AI can quickly create a model adapted for printing based on drawings or technical requirements.

At the stage of object optimization, using analysis algorithms, AI can check the model for holes, polygon intersections, incorrect geometry and offer automatic correction. In addition, the system can evaluate the mechanical characteristics of the part and adjust its shape to increase strength.

When exporting a model, AI can automatically determine the best file format for export, taking into account the features of the printer and the type of material used.

To the greatest extent, artificial intelligence helps at the stage of setting up in the slicing program (slicer). It can automatically select printing parameters (layer height, printing speed, infill density, extruder and platform temperature, etc.) taking into account the characteristics of the material, the complexity of the model geometry and the features of the printer. Chat GPT-4o, for example, can instantly generate optimal settings and warn about possible problems associated with printing a specific part.

At the stage of preparing a 3D printer, AI can be used to calibrate the printing platform, diagnose the printer and assess the condition of the material (for example, warn about possible filament moisture, which can affect print quality). AI can also be used to predict printer maintenance to avoid unexpected failures.

When loading G-code and starting printing, artificial intelligence can be tasked with checking the generated G-code for errors, as well as providing recommendations for changes to improve printing efficiency. In addition, AI can monitor the printing process in real time, identifying defects and suggesting parameter corrections during printing.

The feasibility of using AI increases when replacing the printer model with one that has different characteristics, printing platform dimensions, active thermal camera, etc.; when changing the printing material or increasing the number of controlled parameters. The use of Chat GPT-4o and similar systems demonstrates the effectiveness of integrating AI into the 3D printing process, which allows reducing preparation time, improving product quality, and automating the control process.

Discussion

As an experimental confirmation of the possibility of using AI in the process of preparing models for 3D printing, a request will be formulated for Chat GPT-4o to determine the settings of printing parameters for one of the parts of the REE design. According to the parameters generated by AI in the response, the part was manufactured, the timing of all operations was carried out, the recommendations received were compared with the conclusion of an expert with extensive experience in the field of 3D printing, and the quality of the resulting part was assessed.

User request to AI

The part is the back cover of the field radio station case with printed circuit board mounting clips. It is used to protect the internal components of the radio station from dust, moisture and mechanical damage, as well as to fix the printed circuit board in the case. Ensures the tightness and structural integrity of the device when operating in field conditions.

Operating conditions:

1) Temperature range: from –20 °C to +50 °C (extreme temperatures typical of field conditions, including winter and summer).

2) Mechanical stability: the part must withstand shocks, falls, vibrations and other loads typical of mobile equipment.

3) Fastening: integrated latches are provided for fixing the board, which must be sufficiently flexible, but not brittle.

4) Weight: it is important to maintain the lightness of the design, especially for portable equipment.

Tables 1-3 show the results of comparing the parameters set by an expert engineer in 3D printing (Table 1) and those generated using AI (Table 2), as well as estimates of the time spent on performing the relevant work by the expert and AI according to prepared queries (Table 3).

Table 1 – Parameters recommended by an expert engineer in 3D printing

Parameter	Value	Expert's comment
Material	PETG	It has good chemical resistance to oils, moisture, dust, is not brittle, and withstands loads well.
Printing temperature	230 °C	Optimal range for PETG, provides reliable interlayer adhesion.
Layer thickness	0.2 mm	The balance between surface quality, detail and strength is optimal for technical parts.
Wall thickness	1.5+ mm	Provides the necessary rigidity and strength of the body part.
Filling	30 %	Sufficient level for mechanical resistance without excessive material consumption.
Form to fill out	Hexagonal structure	Optimal shape to achieve high strength with minimal weight.
Alternating walls and filling	Active	Increases the contact area between the outer walls and the inner filling, increases rigidity.

Table 2 – Parameters generated using AI

Parameter	Value	AI Commentary
Material	PETG	Recommended for field conditions due to its combination of flexibility and chemical resistance.
Printing temperature	235 °C	Provides an optimal compromise between layer adhesion and thread prevention.
Layer thickness	0.22 mm	A slightly thicker thickness speeds up printing while maintaining sufficient detail.
Wall thickness	2.0 mm	A reliable solution to ensure structural integrity during vibrations.
Filling	28 %	The system recommends slightly reducing the infill to save material without losing quality.
Form to fill out	Hexagonal structure (hex-grid)	High efficiency in terms of weight and strength. Hexagrid is chosen as a universal solution.
Alternating walls and filling	3 exterior walls before filling	The additional layer increases the strength of the outer shell and reduces the risk of delamination.

Table 3 – Results of the timing

The stage of preparation for 3D printing	AI can be implemented	Time (AI), min	Time (expert), min	Comment
Formulation of requirements for the part	+	1	5	AI can collect and structure the technical requirements of a typical product specified by the operator.
Material selection	+	1	5	AI selects the optimal material according to operating conditions.
Generating print settings	+	2	15	AI quickly generates parameters based on the database.
Part design analysis	Part	1	10	AI can provide a basic assessment, but an expert does the in-depth analysis.
Model preparation	Part	3	5	AI can configure a slicer or suggest G-code.
Preparing to print (printer settings)	Part	2	5	AI hints on parameters, but manual intervention is still necessary.
Visual inspection before printing	–	–	5	This stage is performed only manually.
Total time		10	50	AI significantly reduces training time, especially in the early analytical stages.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

General comment of an engineer-expert in 3D printing, regarding the printing parameters generated by AI: the data generated by AI is correct and meets the requirements for the part. PETG is the optimal material for the case of a field radio station, and the recommended printing parameters provide the necessary strength and durability of the part.

Even more useful may be the use of AI in the manufacture of parts using multifilament 3D printing technology, which uses interchangeable heads with materials with different properties, colors, etc. When changing the hotend, AI allows you to optimize printing parameters almost instantly.

This approach not only reduces the time for performing the preparatory stage, but also provides the opportunity to involve less qualified workers without reducing the requirements for the quality of the parts being manufactured.

The design process can also be shortened by using ready-made 3D models from available libraries (Thingiverse, MyMiniFactory).

But the greatest effect when implementing repair work according to the concept of a spare parts printer can be provided by the timely creation of G-code libraries for all parts of the REE structures at the design stage and during their prototyping, which in modern conditions usually occurs using 3D printers. In this case, the set of radio equipment supplied to the user, in addition to the 3DP-SPprinter, should also include a pre-created G-code library for all parts of the REE structures. This allows you to minimize the preparation period for printing parts to two stages – loading the G-code and preparing the 3D printer.

Conclusion

Thus, the implementation of the concept of rapid printing of parts when they need to be replaced at the place of operation of the REE (field repair) may be appropriate, firstly, in conditions of impossibility of timely delivery of spare parts, secondly, when reducing the time spent on preparing the necessary parts for printing by using laser scanners, artificial intelligence or libraries of ready-made G-code for all parts, the replacement of which is provided for by the operating regulations, or/and those that may be damaged during their operation.

The prospects for implementing this approach are increasing due to the decrease in prices for 3D printers, which can be used as spare parts printers, as well as due to their integration with devices for processing secondary plastics, which reduces the cost of materials and, accordingly, products made from them and expands the areas of application of 3D printing technologies in general (including multifilament 3D printing technology). An important aspect is also the possibility of printing replacement parts for the spare parts printer itself, if necessary, for its repair or for the purpose of its modernization. The decrease in the cost of 3D printers with cold spraying technology for the rapid production of metal parts opens up even greater prospects for the implementation of this method.The comparison of the estimates of the technological parameters of the 3D printing process, recommended by two independent experts and proposed by artificial intelligence, conducted in the work comprehensively confirms the effectiveness of the use of AI and indicates even greater prospects for the application of AI in this area with its further improvement.

References

1. Nebrat V.V., Klyuchnyk I.Iv., Galkin P.V., Romanchuk V.S., Kliuchnyk I.Ig. Accuracy evaluation of manufacturing parts using 3D printing technology. *Metrology and Instruments*. 2025. No. 1. P. 73–78. doi:10.30837/2663-9564.2025.1.11
2. Mecheter A., Pokharel S., Tarlochan F. Additive Manufacturing Technology for Spare Parts Application: A Systematic Review on Supply Chain Management. *Applied Sciences*. 2022. Vol. 12, No. 9. Art. 4160. doi:10.3390/app12094160.
3. Naghshineh B., Fragoso M., Carvalho H. Rethinking Additive Manufacturing for Spare Parts Supply Chain Management. *Industrial Management*. 2023. Vol. 65, No. 4. P. 38–47. doi:10.1080/08956308.2023.2207970.
4. van Oudheusden A., Faludi J., Balkenende R. Facilitating the Production of 3D-Printed Spare Parts in the Design of Plastic Parts: A Design Requirement Review. *Sustainability*. 2024. Vol. 16, No. 21. Art. 9203. doi:10.3390/su16219203.
5. van Oudheusden A., Faludi J., Balkenende R. 3D Printing for Repair: An Approach for Enhancing Repair. *Sustainability*. 2023. Vol. 15, No. 6. Art. 5168. doi:10.3390/su15065168.
6. Thomsen M.R., Nicholas P., Chiujdea R.-S., Nielsen S.D., Sonne K., Eppinger C. Additive Manufacturing for Repair: Continual Construction Through Bio-Based Materials. *3D Printing and Additive Manufacturing*. 2025. Vol. 12, No. 2. doi:10.1089/3dp.2023.0344.
7. Lee T., Du Preez W., Ferreira R. Towards Foundational AI Models for Additive Manufacturing: Language Models for G-Code Debugging, Manipulation, and Comprehension. *arXiv*. 2023. № arXiv: 2309.02465. doi:10.48550/arXiv.2309.02465.
8. 3D printers make ageing army vehicles fighting fit again. *The Times*. 2024. URL: https://www.thetimes.co.uk/article/3d-printers-make-ageing-army-vehicles-fighting-fit-again-h26nmxn63 (Last accessed: 05.06.2026).
9. Alzyoud S., et al. A Review of Machine Learning (ML) and Explainable Artificial Intelligence (XAI) Methods in Additive Manufacturing (3D Printing). *Materials Today Communications*. 2024. Vol. 41. Art. 110294. doi:10.1016/j.mtcomm.2024.110294.
10. Zaidi A.A., Asif M., Aljabri A., Khan S.Z. Intelligent Composite 3D Printing: The Role of Artificial Intelligence, Machine Learning, and In-Situ Monitoring in Next-Generation Additive Manufacturing. *Frontiers in Mechanical Engineering*. 2026. Vol. 12. doi:10.3389/fmech.2026.1774757.
11. Zaman S., Mahmud M.S., Mollick A.A., Lhaden T. Artificial Intelligence in Additive Manufacturing: Advances in Smart Materials, Lattice Optimization, and Process

Intelligence. *International Journal of Advanced Manufacturing Technology*. 2026. doi:10.1007/s00170-026-18072-y.
12. How this Darwin invention is supporting Ukrainian war effort. *Courier Mail*. 2024. URL: https://www.couriermail.com.au/news/northern-territory/darwin-company-spee3d-contributes-to-ukraine-war-effort/news-story/e244c095914706f4c2195202af9b0f8a (Last accessed: 05.06.2026).
13. Зіненко М.С., Ключник І.Іг., Галкін П.В., Бондаренко О.Ю., Ключник І.Ів. Сучасні стратегії захисту літаючих сенсорних мереж від радіоелектронного впливу. *Бізнес і безпека*. № 1 (154). 2024. С. 77–82.
14. Нестеров Д.О., Ключник І.Іг., Небрат В.В., Ключник І.І. Польове 3-D моделювання деталей РЕА. *Радіоелектроніка та молодь у XXI столітті* : матеріали 29-го Міжнар. молодіж. форуму (Харків, 16-19 квітня 2025 р.). Харків: ХНУРЕ, Т. 2. 2025. С. 49–51. URL: https://drive.google.com/file/d/1nNDWQGeezzw070hGQRh0QO3WNgZu0oZo/view (дата звернення: 05.06.2026).
15. Бачинський В., Шкурпіт О., Гнатюк О. Розробка методу вибору моделі 3D-принтера для виготовлення деталей для ремонту і модернізації безпілотних літальних апаратів в умовах бойових дій. *Збірник наукових праць Національної академії державної прикордонної служби України. Серія: Військові та технічні науки*. 2024. № 2(95). С. 150–157. doi:10.32453/3.v95i2.1667.
16. Ivanov-Kosteckyy S.O., Gumennyk I., Voronkova I. Ways of applying 3D printing technologies in the creation of modern architectural objects. *Scientific Architecture (SA)*. 2022. Vol. 4, No. 1. P. 54–64. doi:10.23939/sa2022.01.054.
17. США передали Україні 3D-принтери для друку запчастин. URL: https://mil.in.ua/uk/news/ssha-peredaly-ukrayini-3d-pryntery-dlya-druku-zapchastyn (дата звернення: 05.06.2026).
18. Закревський А. Формування авіаційних конструкцій методом 3D-друку. *Науково-технічний журнал авіаційно-космічна техніка та технологія*. Харків : ХНУПС, 2018. № 3. С. 13–21. doi:10.32620/aktt.2018.3.02

References (transliterated)

1. Nebrat V.V., Klyuchnyk I.Iv., Galkin P.V., Romanchuk V.S., Kliuchnyk I.Ig. Accuracy evaluation of manufacturing parts using 3D printing technology. *Metrology and Instruments*. 2025. No. 1. P. 73–78. doi:10.30837/2663-9564.2025.1.11
2. Mecheter A., Pokharel S., Tarlochan F. Additive Manufacturing Technology for Spare Parts Application: A Systematic Review on Supply Chain Management. *Applied Sciences*. 2022. Vol. 12, No. 9. Art. 4160. doi:10.3390/app12094160.
3. Naghshineh B., Fragoso M., Carvalho H. Rethinking Additive Manufacturing for Spare Parts Supply Chain Management. *Industrial Management*. 2023. Vol. 65, No. 4. P. 38–47. doi:10.1080/08956308.2023.2207970.
4. van Oudheusden A., Faludi J., Balkenende R. Facilitating the Production of 3D-Printed Spare Parts in the Design of Plastic Parts: A Design Requirement Review. *Sustainability*. 2024. Vol. 16, No. 21. Art. 9203. doi:10.3390/su16219203.
5. van Oudheusden A., Faludi J., Balkenende R. 3D Printing for Repair: An Approach for Enhancing Repair. *Sustainability*. 2023. Vol. 15, No. 6. Art. 5168. doi:10.3390/su15065168.
6. Thomsen M.R., Nicholas P., Chiujdea R.-S., Nielsen S.D., Sonne K., Eppinger C. Additive Manufacturing for Repair: Continual Construction Through Bio-Based Materials. *3D Printing and Additive Manufacturing*. 2025. Vol. 12, No. 2. doi:10.1089/3dp.2023.0344.
7. Lee T., Du Preez W., Ferreira R. Towards Foundational AI Models for Additive Manufacturing: Language Models for G-Code Debugging, Manipulation, and Comprehension. arXiv. 2023. № arXiv: 2309.02465. doi:10.48550/arXiv.2309.02465.
8. 3D printers make ageing army vehicles fighting fit again. *The Times*. 2024. URL: https://www.thetimes.co.uk/article/3d-printers-make-ageing-army-vehicles-fighting-fit-again-h26nmxn63 (Last accessed: 05.06.2026).
9. Alzyoud S., et al. A Review of Machine Learning (ML) and Explainable Artificial Intelligence (XAI) Methods in Additive Manufacturing (3D Printing). *Materials Today Communications*. 2024. Vol. 41. Art. 110294. doi:10.1016/j.mtcomm.2024.110294.
10. Zaidi A.A., Asif M., Aljabri A., Khan S.Z. Intelligent Composite 3D Printing: The Role of Artificial Intelligence, Machine Learning, and In-Situ Monitoring in Next-Generation Additive Manufacturing. *Frontiers in Mechanical Engineering*. 2026. Vol. 12. doi:10.3389/fmech.2026.1774757.
11. Zaman S., Mahmud M.S., Mollick A.A., Lhaden T. Artificial Intelligence in Additive Manufacturing: Advances in Smart Materials, Lattice Optimization, and Process Intelligence. International Journal of Advanced Manufacturing Technology. 2026. doi:10.1007/s00170-026-18072-y.
12. How this Darwin invention is supporting Ukrainian war effort. *Courier Mail*. 2024. URL: https://www.couriermail.com.au/news/northern-territory/darwin-company-spee3d-contributes-to-ukraine-war-effort/news-story/e244c095914706f4c2195202af9b0f8a (Last accessed: 05.06.2026).
13. Zinenko M.S., Klyuchnyk I.Ig., Halkin P.V., Bondarenko O.Yu., Klyuchnyk I.Iv. Suchasni stratehii zakhystu litaichykh sensornykh merezh vid radioelektronnoho vplyvu [Modern strategies for protecting flying sensor networks against electronic warfare effects]. *Biznes i bezpeka* [Business and Security], 2024, no. 1(154), pp. 77–82.
14. Nesterov D.O., Klyuchnyk I.Ig., Nebrat V.V., Klyuchnyk I.Iv. Polove 3-D modeliuvannia detalei REA [Field 3D modeling of radio-electronic equipment parts]. Radioelektronika ta molod u XXI stolitti: materialy 29-ho Mizhnarodnoho molodizhnoho forumu [Radio Electronics and Youth in the XXI Century: Proceedings of the 29th International Youth Forum], Kharkiv, April 16–19, 2025. Kharkiv, KhNURE, vol. 2, 2025, pp. 49–51. Available at: https://drive.google.com/file/d/1nNDWQGeezzw070hGQRh0QO3WNgZu0oZo/view (accessed 05.06.2026).
15. Bachynskyi V., Shkurpit O., Hnatiuk O. Rozrobka metodu vyboru modeli 3D-pryntera dlia vyhotovlennia detalei dlia remontu i modernizatsii bezpilotnykh litalnykh aparativ v umovakh boiovykh dii [Development of a method for selecting a 3D printer model for manufacturing parts for repair and modernization of unmanned aerial vehicles under combat conditions]. *Zbirnyk naukovykh prats Natsionalnoi akademii derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia: Viiskovi ta tekhnichni nauky* [Collection of Scientific Works of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences], 2024, no. 2(95), pp. 150–157, doi:10.32453/3.v95i2.1667.
16. Ivanov-Kosteckyy S.O., Gumennyk I., Voronkova I. Ways of applying 3D printing technologies in the creation of

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

modern architectural objects. *Scientific Architecture (SA)*. 2022. Vol. 4, No. 1. P. 54–64. doi:10.23939/sa2022.01.054.

17. SSHA peredaly Ukraini 3D-pryntery dlia druku zapchastyn [The United States transferred 3D printers to Ukraine for spare parts production]. Available at: https://mil.in.ua/uk/news/ssha-peredaly-ukrayini-3d-pryntery-dlya-druku-zapchastyn (accessed 05.06.2026).
18. Zakrevskyi A. Formuvannia aviatsiinykh konstruktsii metodom 3D-druku [Formation of aircraft structures using 3D printing technology]. *Aviatsiino-kosmichna tekhnika ta tekhnolohiia* [Aerospace Engineering and Technology], Kharkiv, KhNUPS, 2018, no. 3, pp. 13–21, doi:10.32620/aktt.2018.3.02...

Відомості про авторів (About authors)

Klyuchnyk Igor – PhD, Associate Professor, professor of the Department of Electronic Devices Design and Operation, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; ORCID: 0000-0002-9352-5716, e-mail: ihor.kliuchnyk@nure.ua.

Ключник Ігор Іванович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри проектування та експлуатації електронних апаратів; м. Харків, Україна; ORCID: 0000-0002-9352-5716, e-mail: ihor.kliuchnyk@nure.ua.

Nebrat Viacheslav – PhD student, Department of Microelectronics, Electronic Devices and Devices, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; ORCID: 0009-0009-2384-3813, e-mail: viacheslav.nebrat@nure.ua.

Небрат В'ячеслав Валерійович – аспірант, кафедра мікроелектроніки, електронних приладів та пристроїв, Харківський національний університет радіоелектроніки; м. Харків, Україна; ORCID: 0009-0009-2384-3813, e-mail: viacheslav.nebrat@nure.ua.

Kliuchnyk Igor – PhD student, Department of Information and Measurement Technology, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; ORCID: 0009-0000-3718-0584, e-mail: ihor.kliuchnyk1@nure.ua.

Ключник Ігор Ігорович – аспірант, кафедра інформаційно-вимірювальних технологій, Харківський національний університет радіоелектроніки; м. Харків, Україна; ORCID: 0009-0000-3718-0584, e-mail: ihor.kliuchnyk1@nure.ua.

Degtiarov Oleksandr – PhD, Associate Professor, Department of Information and Measurement Technology, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine; ORCID: 0000-0002-3187-1621, e-mail: oleksandr.degtiarov@nure.ua.

Дегтярьов Олександр Валентинович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри інформаційно-вимірювальних технологій; м. Харків, Україна; ORCID: 0000-0002-3187-1621, e-mail: oleksandr.degtiarov@nure.ua.

Heueis Tilman – Technical Editorand 3D Designer, Mühlbauer+partner, Technische Dokumentation GmbH&Co. KG, Unterschleißheim, Germany; ORCID: 0009-0003-7364-9986, e-mail: t.heueis@gmail.com.

Геуайс Тільман – технічний редактор і 3D-дизайнер, компанії Mühlbauer+partner, Унтершляйсгаймі, Німеччина; ORCID: 0009-0003-7364-9986, e-mail: t.heueis@gmail.com.

Please cite this article as:

Klyuchnyk I. Iv., Nebrat V., Kliuchnyk I. Ig., Degtiarov O., Heueis T. 3D printing as an alternative to spare parts for field repair of radio-electronic equipment. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology.* – Kharkiv: NTU "KhPI", 2026, no. 4(22), pp. 80–86, doi:10.20998/2413-4295.2026.02.11.

Будь ласка, посилайтесь на цю статтю наступним чином:

Ключник І. І., Небрат В. В., Ключник І. Іг., Дегтярьов О. В., Геуайс Т. 3D-друк як альтернатива пошуку запчастин при ремонті радіоелектронної апаратури в польових умовах. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 4 (22). С. 80-86. doi:10.20998/2413-4295.2026.02.11.

Надійшла (received) 25.05.2026
Прийнята (accepted) 28.05.2026
Опублікована (published) 05.06.2026

УДК 004.896 doi:10.20998/2413-4295.2026.02.12

МОДЕЛЮВАННЯ ДИНАМІКИ МОБІЛЬНИХ РОБОТІВ В УМОВАХ НЕВИЗНАЧЕНОСТІ

А. О. НОСОВ[1*], М. В. КОРЖИК[1]

[1]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, УКРАЇНА
**e-mail: andriinosov91@gmail.com*

АНОТАЦІЯ *Сучасні автономні мобільні роботи функціонують у середовищах із суттєвою невизначеністю, що виникає внаслідок неточностей динамічних моделей, стохастичних збурень, невідомих параметрів взаємодії з поверхнею та непередбачуваних зовнішніх впливів. Метою роботи є розробка конкретизованої математичної моделі адаптивної ідентифікації динаміки мобільних роботів з явною специфікацією архітектур нейромережевих компонент, функцій втрат та методів навчання, а також верифікація працездатності через чисельний експеримент з аналізом чутливості. На основі аналізу наукових публікацій 2018–2025 років виконано порівняння дев'яти методологічних підходів за критеріями точності, обчислювальної складності, здатності до кількісного оцінювання невизначеності та придатності для роботи в реальному часі. Запропоновано гібридну модель, що інтегрує номінальну модель Ейлера–Лагранжа з ансамблевим фільтром Калмана (N = 50) для параметричної адаптації, нейромережеву корекцію на основі Deep Lagrangian Network (двошарова повнозв'язна мережа з 128 нейронами та функцією втрат з енергетичним регуляризатором) для компенсації структурної невизначеності, а також контекстно-залежну адаптивну стохастичну компоненту. Розроблено трирівневу архітектуру (PLC → Edge GPU → Edge CPU) з формалізованими інтерфейсами OPC UA та ROS2 DDS, що забезпечує час циклу 4,8 мс/крок та режим graceful degradation. Працездатність підтверджено чисельним експериментом на задачі моделювання динаміки диференціального робота на трьох поверхнях (суха, мокра, промаслена): показано зниження RMSE позиції у 5,9 разів (з 0,142 м до 0,024 м) та підвищення каліброваності 95 % довірчого інтервалу з 62,3 % до 94,1 % порівняно з детермінованою моделлю.*
Ключові слова: *моделювання динаміки; мобільні роботи; стохастичні диференціальні рівняння; фільтр Калмана; Deep Lagrangian Network; цифрові двійники; невизначеність.*

MODELING DYNAMICS OF MOBILE ROBOTS UNDER UNCERTAINTY

A. O. NOSOV[1], M. V. KORZHYK[1]

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, UKRAINE

ABSTRACT *Modern autonomous mobile robots operate in environments with significant uncertainty arising from inaccuracies in dynamic models, stochastic disturbances, unknown surface interaction parameters, and unpredictable external influences. The aim of the work is to develop a specified mathematical model of adaptive identification of mobile robot dynamics with explicit specification of neural network component architectures, loss functions and training methods, and to verify performance through a numerical experiment with sensitivity analysis. Based on the analysis of scientific publications from 2018–2025, a comparison of nine methodological approaches was performed according to criteria of accuracy, computational complexity, ability to quantitatively assess uncertainty, and suitability for real-time operation. A hybrid model is proposed that integrates a nominal Euler–Lagrange model with an Ensemble Kalman Filter (N = 50) for parametric adaptation, a neural network correction based on Deep Lagrangian Network (two-layer fully connected network with 128 neurons and a loss function with energy regularization) to compensate for structural uncertainty, and a context-dependent adaptive stochastic component. A three-level architecture (PLC → Edge GPU → Edge CPU) with formalized OPC UA and ROS2 DDS interfaces has been developed, providing a cycle time of 4.8 ms/step and a graceful degradation mode. Performance is confirmed by a numerical experiment on the problem of modeling the dynamics of a differential robot on three surfaces (dry, wet, oiled): a 5.9-fold reduction in position RMSE (from 0.142 m to 0.024 m) and an increase in 95 % confidence interval calibration from 62.3 % to 94.1 % are demonstrated compared to a deterministic model.*
Keywords: *dynamics modeling; mobile robots; stochastic differential equations; Kalman filter; Deep Lagrangian Network; digital twins; uncertainty.*

Вступ

Сучасне виробництво активно впроваджує мобільні роботи для автоматизації логістичних та технологічних операцій. Ефективність автономної навігації та керування рухом критично залежить від якості математичних моделей динаміки, які описують зв'язок між керуючими сигналами та реальним переміщенням платформи. У практичних умовах динамічні моделі завжди є наближеними: параметри тертя, зчеплення коліс із поверхнею, маса вантажу та зовнішні збурення залишаються частково або повністю невідомими.

Об'єктом дослідження є процеси математичного моделювання динаміки промислових мобільних роботів в умовах параметричної, структурної та стохастичної невизначеності. Існуючі детерміновані моделі не враховують випадкових збурень і відхилень

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

параметрів, що призводить до систематичних похибок у прогнозуванні руху та зниження ефективності контурів керування.

Проблема ускладнюється тим, що різні джерела невизначеності потребують принципово різних математичних інструментів: стохастичні диференціальні рівняння для процесних збурень, баєсівські методи для параметричної невизначеності, нейромережеві апроксиматори для структурної невизначеності. Комплексне моделювання, що охоплює всі типи невизначеності у єдиній архітектурі з конкретизованими методами та експериментальним підтвердженням, залишається недостатньо дослідженим.

Аналіз стану питання

Для систематизації методів моделювання динаміки мобільних роботів в умовах невизначеності проведено аналіз дев'яти основних підходів за п'ятьма критеріями. Результати систематизовано у табл. 1.

Стохастичні моделі на основі СДР (стохастичне диференціальне рівняння) [1] забезпечують фундаментальну основу для опису випадкових збурень, поєднуючи безперервну динаміку з дискретними переключеннями режимів через марковські ланцюги. Проте вони не адресують структурну невизначеність – невідомі нелінійні ефекти (тертя Штрібека, деформації коліс), для яких аналітичний вираз принципово відсутній.

Інваріантні фільтри Калмана [2] на основі теорії груп Лі забезпечують збіжність, незалежну від траєкторії, що є принциповою перевагою над стандартними EKF. Диференційовані ансамблеві фільтри Калмана [10] розширюють цей підхід, уможливлюючи спільне навчання моделей спостереження та динаміки фільтра з даних, але обидва класи фільтрів працюють лише зі стохастичною невизначеністю та потребують зовнішньої моделі динаміки.

Фізично-інформовані нейронні мережі (PINN) [3] та, зокрема, їх структурні підкласи – Deep Lagrangian Networks (DeLaN) [11] і Hamiltonian Neural Networks (HNN) [12] – вбудовують фізичні закони збереження безпосередньо у архітектуру мережі. DeLaN параметризує функцію Лагранжа, а HNN – гамільтоніан, що обмежує простір рішень до фізично правдоподібних. Проте ці методи не надають явної оцінки невизначеності прогнозу.

Гаусові процеси (GP) [4] забезпечують калібровану ймовірнісну оцінку як прогнозу, так і його невизначеності, але мають обчислювальну складність $O(n^3)$, що обмежує масштабованість. Цифрові двійники [5] створюють «живу» модель, що еволюціонує разом із системою, але потребують значних інфраструктурних витрат. Адаптивне ковзне керування [6] гарантує стійкість за обмежених збурень, але не забезпечує ймовірнісного оцінювання. Баєсівське глибинне навчання [7] надає довірчі інтервали, але є занадто ресурсозатратним для реального часу. Рандомізація динаміки [8] забезпечує робастність до сімейства можливих динамік, але лише неявно. Поліноміальний хаос-розклад [9] дає гарантовані межі, але застосовний лише для параметричної невизначеності.

Комплексний огляд методів квантифікації невизначеності [13] систематизує підходи (баєсівські мережі, ансамблі, Monte Carlo dropout) та підтверджує, що жоден окремий метод не забезпечує одночасно високу точність, калібровану оцінку невизначеності та обчислювальну ефективність для роботи в реальному часі, що мотивує запропоновану інтеграцію.

Таблиця 1 – Порівняльна характеристика методів моделювання динаміки

Метод	Тип	Оц.	Скл.	Дані	Час
СДР + марков. перекл. [1]	Стохаст., парам.	Так (розподіл)	Низька	Мінім.	Так
InEKF на групах Лі [2]	Стохастична	Так (коваріація)	Низька	Мінім.	Так
PINN / DeLaN [3, 11]	Структурна	Неявна	Середня	Середня	Так (інф.)
GP + MPC [4]	Структ., парам.	Так (дисперсія)	Сер.–вис.	Середня	Обмежено
Цифровий двійник [5]	Стохаст., парам.	Через спостер.	Висока (сист.)	Онлайн	Так
Адапт. ковзне керув. [6]	Парам., зовн.	Ні (обмеж.)	Низька	Мінім.	Так
Баєсівське глиб. н. [7]	Структ., парам.	Так (довірчі)	Висока	Велика	Ні
Рандоміз. динаміки [8]	Парам., структ.	Неявна	Висока (навч.)	Велика (сим.)	Так (інф.)
Полін. хаос-розклад [9]	Параметрична	Так (межі)	Середня	Мінім.	Ні

Аналіз табл. 1 виявляє три закономірності. По-перше, жоден метод не адресує одночасно параметричну, стохастичну та структурну невизначеність із кількісним оцінюванням у реальному часі. По-друге, існує компроміс між багатством моделі та обчислювальною вартістю. По-третє, спостерігається тенденція до гібридизації, що мотивує розробку інтегрованої архітектури.

Мета роботи

Розробка конкретизованої математичної моделі адаптивної ідентифікації динаміки мобільних роботів з явною специфікацією архітектур нейромережевих компонент, функцій втрат та методів навчання, а також верифікація працездатності через чисельний експеримент з аналізом чутливості до гіперпараметрів.

Постановка задачі. Загальна динамічна модель колісного мобільного робота диференціального приводу описується системою Ейлера–Лагранжа:

$$M(\mathbf{q})\ddot{\mathbf{q}} + C(\mathbf{q},\dot{\mathbf{q}})\dot{\mathbf{q}} + B\dot{\mathbf{q}} + \mathbf{d}(t) = \boldsymbol{\tau} \quad (1)$$

де q = [p_x, p_y, φ]^T – узагальнені координати; M(q) – матриця інерції; C(q, q̇) – матриця коріолісових та відцентрових сил; B – матриця в'язкого тертя; d(t) – вектор невідомих збурень; τ – вектор узагальнених сил від приводів. Невизначеність формалізується через три компоненти:

– параметрична невизначеність: θ = {m, I, μ_s, μ_k, r} – маса, момент інерції, коефіцієнти тертя, радіус коліс відомі з точністю θ ∈ [θ_min, θ_max];

– стохастична невизначеність: d(t) = d_0(t) + σ_d(x)·ξ(t), де d_0 – систематична компонента, ξ(t) – білий шум;

– структурна невизначеність: Δf(x, u) – невраховані ефекти (нелінійне тертя Штрібека, деформація коліс), для яких аналітичний вираз невідомий.

Методи дослідження. Конкретизована математична модель. Пропонується гібридна модель динаміки з трьома явно специфікованими компонентами:

$$\dot{\mathbf{x}}(t) = f_{\text{nom}}(\mathbf{x},\mathbf{u},\boldsymbol{\theta}_t) + \delta_{\text{DLN}}(\mathbf{x},\mathbf{u};\boldsymbol{\psi}) + \sigma(\mathbf{x},\boldsymbol{\xi}_t;\boldsymbol{\varphi})\cdot d\mathbf{W}(t) \quad (2)$$

Компонента 1: Номінальна фізична модель

Для диференціального робота з неголономними обмеженнями кінематика та динаміка мають вигляд:

$$\dot{p}_x = v\cos(\varphi), \quad \dot{p}_y = v\sin(\varphi), \quad \dot{\varphi} = \omega \quad (3)$$

$$\hat{m}_t\dot{v} = \frac{(\tau_R + \tau_L)}{\hat{r}_t} - \hat{\mu}_t v,$$
$$\hat{I}_t\dot{\omega} = (\tau_R - \tau_L)L/(2\hat{r}_t) - \hat{\mu}_{\omega,t}\,\omega \quad (4)$$

де v, ω – лінійна та кутова швидкості; τ_R, τ_L – моменти правого та лівого приводів; L – база робота. Параметри θ_t = {m̂_t, Î_t, μ̂_t, μ̂_ω,t, r̂_t} оновлюються онлайн через ансамблевий фільтр Калмана (EnKF) з N_ens = 50 членами ансамблю [10]:

$$\boldsymbol{\theta}_t = \boldsymbol{\theta}_{t-1} + K_t\big(\mathbf{y}_t - h(\hat{\mathbf{x}}_t)\big), \quad K_t = P_{\theta x}(P_{xx} + R)^{-1} \quad (5)$$

де K – калманівський виграш; P – кросковаріація та коваріація, обчислені за ансамблем; R – коваріація шуму вимірювань. Вибір EnKF обґрунтовано здатністю працювати з нелінійними моделями без обчислення якобіанів, можливістю паралелізації та підтвердженою ефективністю у робототехнічних застосуваннях [10].

Компонента 2: Нейромережева корекція на основі DeLaN

Для компенсації структурної невизначеності використовується Deep Lagrangian Network [11] – підклас фізично-інформованих нейронних мереж, що параметризує функцію Лагранжа. На відміну від загальних PINN [3], DeLaN вбудовує механіку Лагранжа безпосередньо у архітектуру, гарантуючи фізичну узгодженість. Альтернативний підхід – Hamiltonian Neural Networks [12] – зберігає симплектичну структуру через параметризацію гамільтоніана, але потребує канонічних координат, що ускладнює застосування для систем з обмеженнями.

Архітектура DeLaN: двошарова повнозв'язна мережа з ReLU-активацією, 128 нейронів у кожному шарі. Вхід: [q, q̇, u] ∈ $\mathbb{R}^9$. Мережа параметризує корекцію до функції Лагранжа ΔL(q, q̇; ψ), звідки корекційні сили обчислюються:

$$\delta_{\text{DLN}} = \frac{d}{dt}\left(\frac{\partial \Delta L}{\partial \dot{q}}\right) - \frac{\partial \Delta L}{\partial q} + D(\dot{q};\,\psi_D) \quad (6)$$

де D(q̇; ψ_D) – дисипативна компонента (одношарова мережа, 64 нейрони), що моделює неконсервативні сили [3, 11]. Лагранжева структура гарантує збереження енергії для консервативної частини.

Функція втрат:

$$\mathcal{L}(\boldsymbol{\psi}) = \lambda_1 \parallel \ddot{x}_{\text{pred}} - \ddot{x}_{\text{real}} \parallel^2 + \lambda_2 \parallel E_{\text{pred}} - E_{\text{real}} \parallel^2 + \lambda_3 \parallel \boldsymbol{\psi} \parallel^2 \quad (7)$$

де перший член – помилка прогнозу прискорень; другий – помилка зміни енергії (фізичний регуляризатор); третій – L2-регуляризація. Ваги λ_1 = 1,0, λ_2 = 0,1, $\lambda_3 = 10^{-4}$ підібрані за результатами крос-валідації. Навчання: Adam (lr = $3\cdot10^{-4}$, batch = 256, 500 епох) з подальшим онлайн-донавчанням на ковзному вікні K = 1000 спостережень.

Компонента 3: Адаптивна стохастична модель

Матриця дифузії параметризується контекстно-залежною функцією:

$$\sigma(\mathbf{x},\boldsymbol{\xi}_t;\boldsymbol{\varphi}) = \sigma_0 \cdot \mathrm{diag}(1 + \varphi_v|v|,\ 1 + \varphi_v|v|,\ 1 + \varphi_\omega|\omega|,\ \varphi_a,\ \varphi_a) \quad (8)$$

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

де σ_0 – базова інтенсивність; $\varphi = \{\varphi_v, \varphi_\omega, \varphi_a\}$ – параметри чутливості, оцінювані офлайн через EM-алгоритм. Контекстний вектор $\xi_t = [|v|, |\omega|, s\_terrain, \eta\_load, e\_recent]^T$, де s_terrain – тип поверхні, визначений пропріоцептивним класифікатором на основі сигналів IMU та енкодерів коліс [15]; η_load – завантаженість; e_recent – середня похибка за останні 100 кроків.

Адаптивне зважування критеріїв

Якість моделі оцінюється за N = 3 критеріями: L_1 – RMSE координат; L_2 – RMSE швидкостей; L_3 – каліброваність 95 %-го довірчого інтервалу. Адаптивні ваги:

$$\alpha_i(\boldsymbol{\xi}_t) = \frac{\exp(\beta_i\, g_i(\xi_t))}{\sum_{j=1}^{N} \exp(\beta_j\, g_j(\xi_t))} \qquad (9)$$

де $g_i(\xi_t) = w_i^T \cdot \xi_t + b_i$ – лінійна функція контексту з навченими параметрами. При русі по слизькій поверхні зростає вага L_1, при високих швидкостях – вага L_2. Параметри w_i, b_i, β_i навчаються методом крос-валідації на калібрувальному наборі.

Цифрові двійники та проблема переходу Sim-to-Real. Запропонована модель природно інтегрується з парадигмою цифрових двійників (Digital Twin), яка створює двонаправлений зв'язок між фізичним роботом та його віртуальною копією. У роботі [5] побудовано систему цифрового двійника для мобільного робота з нелінійним спостерігачем розширеного стану, що оцінює збурення обох сутностей. Важливо, що збурення фізичного та віртуального об'єктів відрізняються, відображаючи reality gap. У контексті запропонованої моделі цифровий двійник реалізує безперервне оновлення параметрів θ (через компоненту 1) та донавчання δ_DLN (через компоненту 2) на основі потоку даних від фізичного робота, забезпечуючи «живу» модель, що еволюціонує разом із системою.

Суміжною проблемою є перенос моделей із симуляції у реальний світ (Sim-to-Real). Метод рандомізації динаміки [8] під час навчання варіює параметри симулятора у широких діапазонах, змушуючи LSTM-політику неявно ідентифікувати динаміку з історії спостережень. Запропонована модель доповнює цей підхід: рандомізація може використовуватись для офлайн-претренування DeLaN-компоненти у симуляції, після чого онлайн-адаптація (компоненти 1 та 3) компенсує залишковий reality gap на реальному обладнанні. Конформне прогнозування [14] надає додатковий інструмент для отримання гарантованих (а не лише каліброваних) довірчих інтервалів на прогнози моделі без припущень щодо розподілу – перспективне доповнення для сертифікації безпеки.

Архітектура системи моделювання. Об'єднання трьох компонент потребує ієрархічної архітектури з формалізованими інтерфейсами. Характеристики рівнів подано у табл. 2.

Таблиця 2 – Характеристики рівнів архітектури

Рівень	Модель	Платформа	Час, мс	Інтерф.
1. Фізична	f_nom(x, u, θ)	PLC Siemens S7-1500	1–5	{u, θ} → {x̂_nom, M, C}
2. Нейрокор.	δ_DLN(x, u; ψ)	Edge GPU (Jetson Orin)	5–20	{x, u, q, q̇} → {δ_DLN}
3. Оцінюв.	InEKF + EnKF	Edge CPU / GPU	10–50	{y, x̂, δ, σ} → {x̂, P, θ̂}

Рівень 1 (PLC) виконує номінальну модель із гарантованим часом циклу та реалізує аварійну логіку безпеки. Рівень 2 обчислює корекцію DeLaN; інференс мережі 9→128→128→3 потребує близько 2 мс на Jetson Orin Nano. Рівень 3 виконує EnKF (N = 50) для оцінювання стану та параметрів; складність $O(N \cdot n^2) \approx O(1250)$ операцій на крок.

Ключова особливість – graceful degradation: при відмові рівня 2 система працює на номінальній моделі; при відмові рівня 3 PLC використовує останні параметри θ у консервативному режимі. Обмін даними між рівнями здійснюється через OPC UA (рівні 1↔3, 10 Гц) та ROS2 DDS (рівні 2↔3, 50 Гц).

Результати чисельного моделювання. Для верифікації проведено чисельний експеримент: диференціальний робот (m = 15 кг, I = 0,5 кг·м², r = 0,05 м, L = 0,3 м) виконує S-подібний маневр (v = 0,5–1,5 м/с, 60 с) на трьох поверхнях: суха підлога (μ = 0,8), мокра плитка (μ = 0,3), промаслена поверхня (μ = 0,1). Додано стохастичні збурення (σ_0 = 0,05) та нелінійне тертя Штрібека як невідомий структурний ефект. Пропріоцептивний класифікатор поверхні [15] моделюється ідеальним з затримкою 0,2 с.

Порівняно три моделі: (A) детермінована Ейлера–Лагранжа з фіксованими параметрами; (B) адаптивна фізична модель з EnKF; (C) повна запропонована модель. Результати за 100 реалізацій Монте-Карло наведено у табл. 3.

Таблиця 3 – Результати чисельного експерименту (100 реалізацій МК)

Показник	(A)	(B)	(C)
RMSE позиції, м	0,142 ± 0,031	0,067 ± 0,018	0,024 ± 0,009
RMSE швидкості, м/с	0,098 ± 0,022	0,041 ± 0,012	0,016 ± 0,006
Каліброваність 95 %, %	62,3 ± 5,1	88,7 ± 3,2	94,1 ± 1,8
Час на крок, мс	0,3 ± 0,1	2,1 ± 0,4	4,8 ± 0,9

Повна модель знижує RMSE позиції у 5,9 разів порівняно з (A) та у 2,8 разів порівняно з (B). Каліброваність 94,1 % (проти 62,3 % у (A)) означає, що контролер матиме коректне уявлення про надійність прогнозів. Час 4,8 мс прийнятний для типового періоду дискретизації 20–50 мс. Додаткові експерименти з переключенням поверхонь показали виявлення зміни тертя за 0,5–1,0 с (25–50 кроків), після чого точність відновлюється.

Аналіз чутливості до гіперпараметрів

Для оцінки робастності результатів проведено аналіз чутливості моделі (C) до ключових гіперпараметрів. Результати у табл. 4.

Таблиця 4 – Аналіз чутливості (RMSE позиції, м) при варіації гіперпараметрів

Гіперпарам.	Знижене	Базове	Підвищене
N_ens: 20 / 50 / 100	0,031 ± 0,012	0,024 ± 0,009	0,022 ± 0,008
DeLaN шари: 64 / 128 / 256	0,029 ± 0,011	0,024 ± 0,009	0,023 ± 0,009
λ_2: 0,01 / 0,1 / 1,0	0,028 ± 0,010	0,024 ± 0,009	0,032 ± 0,013
K (вікно): 500 / 1000 / 2000	0,027 ± 0,010	0,024 ± 0,009	0,025 ± 0,009

Аналіз показує помірну чутливість до більшості гіперпараметрів: збільшення ансамблю з 50 до 100 дає лише 8 % покращення при подвоєнні обчислювальних витрат, що підтверджує обґрунтованість вибору N = 50. Найбільш чутливим є вага фізичного регуляризатора λ_2: при λ_2 = 1,0 (надмірний регуляризатор) RMSE зростає на 33 %, оскільки мережа занадто обмежена у компенсації структурних ефектів. При λ_2 = 0,01 (слабкий регуляризатор) RMSE зростає на 17 % через втрату фізичної узгодженості. Це підтверджує критичну роль балансу між точністю апроксимації та фізичним обмеженням у гібридних моделях.

Обговорення обмежень

Необхідно зазначити обмеження поточної роботи. По-перше, верифікація проведена лише у чисельному експерименті, а не у повноцінній симуляції (ROS/Gazebo) або на реальному обладнанні. Чисельний експеримент контролює всі змінні, що дозволяє ізолювати внесок кожної компоненти, але не відтворює повною мірою складності реального середовища (затримки комунікації, шуми датчиків, обмежена точність актуаторів). По-друге, гіперпараметри DeLaN (кількість шарів, нейронів, швидкість навчання) підібрані через крос-валідацію, але не через систематичний пошук (наприклад, баєсівську оптимізацію). Аналіз чутливості (табл. 4) показує помірну залежність від цих параметрів, що частково знімає це обмеження. По-третє, ансамбль із 50 членів може бути недостатнім для задач вищої розмірності (наприклад, маніпулятори з 6+ ступенями свободи). По-четверте, пропріоцептивний класифікатор поверхні [15] у експерименті моделюється ідеальним із затримкою 0,2 с; у реальній системі класифікація має власну похибку (близько 5–15 % за даними [15]), яка поширюється через контекстний вектор на адаптивні ваги.

Висновки

Розроблено конкретизовану математичну модель адаптивної ідентифікації динаміки мобільних роботів, що інтегрує три компоненти: номінальну модель Ейлера–Лагранжа з ансамблевим фільтром Калмана (N = 50) для параметричної адаптації; Deep Lagrangian Network (2×128, функція втрат з енергетичним регуляризатором λ_2 = 0,1) для компенсації структурної невизначеності; та контекстно-залежну стохастичну модель для процесних збурень. Порівняльний аналіз дев'яти існуючих підходів виявив відсутність методу, що одночасно адресує всі три типи невизначеності із кількісним оцінюванням у реальному часі. Трирівнева архітектура (PLC → Edge GPU → Edge CPU) з інтерфейсами OPC UA / ROS2 DDS забезпечує час 4,8 мс/крок та graceful degradation. Чисельний експеримент на задачі з трьома поверхнями показав зниження RMSE позиції у 5,9 разів (0,024 м проти 0,142 м) та підвищення каліброваності 94,1 % проти 62,3 %. Аналіз чутливості підтвердив помірну залежність від гіперпараметрів та критичну роль фізичного регуляризатора (λ_2) у балансі точності та фізичної узгодженості. Перспективи подальших досліджень включають експериментальну верифікацію на платформі TurtleBot3 у ROS/Gazebo та на реальному обладнанні; розширення DeLaN до Hamiltonian Neural Network [12] для збереження симплектичної структури; інтеграцію з конформним прогнозуванням [14] для гарантованих довірчих інтервалів; дослідження масштабованості для маніпуляторів з 6+ ступенями свободи; впровадження диференційованого EnKF [10] для наскрізного навчання; та федеративне навчання DeLaN для флотів роботів.

Список літератури

1. Vesentini F., Di Persio L., Muradore R. A Brownian–Markov Stochastic Model for Cart-Like Wheeled Mobile Robots. European Journal of Control. 2023. Vol. 70. Article 100771. DOI: 10.1016/j.ejcon.2022.100771.
2. Hartley R., Ghaffari M., Eustice R. M., Grizzle J. W. Contact-Aided Invariant Extended Kalman Filtering for Robot State Estimation. The International Journal of Robotics Research. 2020. Vol. 39, № 4. P. 402–430. DOI: 10.1177/0278364919894385.

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

3. Liu J., Borja P., Della Santina C. Physics-Informed Neural Networks to Model and Control Robots: A Theoretical and Experimental Investigation. Advanced Intelligent Systems. 2024. Vol. 6, № 5. Article 2300385. DOI: 10.1002/aisy.202300385.
4. Hewing L., Kabzan J., Zeilinger M. N. Cautious Model Predictive Control Using Gaussian Process Regression. IEEE Transactions on Control Systems Technology. 2020. Vol. 28, № 6. P. 2736–2743. DOI: 10.1109/TCST.2019.2949757.
5. Zhao L., Nie Z., Xia Y., Li H. Virtual–Physical Tracking Control for a Car-Like Mobile Robot Based on Digital Twin Technology. IEEE Transactions on Industrial Electronics. 2024. Vol. 71, № 12. P. 16348–16356. DOI: 10.1109/TIE.2024.3387107.
6. Xie H., Zheng J., Sun Z., Wang H., Chai R. Finite-time tracking control for nonholonomic wheeled mobile robot using adaptive fast nonsingular terminal sliding mode. Nonlinear Dynamics. 2022. Vol. 110. P. 1437–1453. DOI: 10.1007/s11071-022-07682-2.
7. Zhou H., Ibrahim C., Zheng W. X., Pan W. Sparse Bayesian Deep Learning for Dynamic System Identification. Automatica. 2022. Vol. 144. Article 110489. DOI: 10.1016/j.automatica.2022.110489.
8. Peng X. B., Andrychowicz M., Zaremba W., Abbeel P. Sim-to-Real Transfer of Robotic Control with Dynamics Randomization. Proceedings of the 2018 IEEE ICRA. IEEE, 2018. P. 3803–3810. DOI: 10.1109/ICRA.2018.8460528.
9. Wang L., Yang G. An Interval Uncertainty Propagation Method Using Polynomial Chaos Expansion and Its Application in Complicated Multibody Dynamic Systems. Nonlinear Dynamics. 2021. Vol. 105. P. 837–858. DOI: 10.1007/s11071-021-06512-1.
10. Liu X., Clark G., Campbell J., Zhou Y., Ben Amor H. Enhancing State Estimation in Robots: A Data-Driven Approach with Differentiable Ensemble Kalman Filters. Proceedings of the 2023 IEEE/RSJ IROS. IEEE, 2023. DOI: 10.1109/IROS55552.2023.10341617.
11. Lutter M., Listmann K., Peters J. Deep Lagrangian Networks for End-to-End Learning of Energy-Based Control for Under-Actuated Systems. Proceedings of the 2019 IEEE/RSJ IROS. IEEE, 2019. P. 7718–7725. DOI: 10.1109/IROS40897.2019.8968268.
12. Greydanus S., Dzamba M., Yosinski J. Hamiltonian Neural Networks. Advances in Neural Information Processing Systems 32 (NeurIPS). 2019. P. 15353–15363. arXiv: 1906.01563.
13. Gawlikowski J. та ін. A Survey of Uncertainty in Deep Neural Networks. Artificial Intelligence Review. 2023. Vol. 56, Suppl. 1. P. 1513–1589. DOI: 10.1007/s10462-023-10562-9.
14. Lindemann L., Cleaveland M., Shim G., Pappas G. J. Safe Planning in Dynamic Environments Using Conformal Prediction. IEEE Robotics and Automation Letters. 2023. Vol. 8, № 8. P. 5116–5123. DOI: 10.1109/LRA.2023.3292071.
15. Vulpi F., Milella A., Marani R., Reina G. Recurrent and Convolutional Neural Networks for Deep Terrain Classification by Autonomous Robots. Journal of Terramechanics. 2021. Vol. 96. P. 119–131. DOI: 10.1016/j.jterra.2020.12.002.

References (transliterated)

1. Vesentini, F., Di Persio, L. and Muradore, R. (2023) “A Brownian–Markov Stochastic Model for Cart-Like Wheeled Mobile Robots,” European Journal of Control, 70, Art. 100771. DOI: 10.1016/j.ejcon.2022.100771.
2. Hartley, R., Ghaffari, M., Eustice, R. M. and Grizzle, J. W. (2020) “Contact-Aided Invariant Extended Kalman Filtering for Robot State Estimation,” The International Journal of Robotics Research, 39(4), pp. 402–430. DOI: 10.1177/0278364919894385.
3. Liu, J., Borja, P. and Della Santina, C. (2024) “Physics-Informed Neural Networks to Model and Control Robots: A Theoretical and Experimental Investigation,” Advanced Intelligent Systems, 6(5), Art. 2300385. DOI: 10.1002/aisy.202300385.
4. Hewing, L., Kabzan, J. and Zeilinger, M. N. (2020) “Cautious Model Predictive Control Using Gaussian Process Regression,” IEEE Transactions on Control Systems Technology, 28(6), pp. 2736–2743. DOI: 10.1109/TCST.2019.2949757.
5. Zhao, L., Nie, Z., Xia, Y. and Li, H. (2024) “Virtual–Physical Tracking Control for a Car-Like Mobile Robot Based on Digital Twin Technology,” IEEE Transactions on Industrial Electronics, 71(12), pp. 16348–16356. DOI: 10.1109/TIE.2024.3387107.
6. Xie, H., Zheng, J., Sun, Z., Wang, H. and Chai, R. (2022) “Finite-time tracking control for nonholonomic wheeled mobile robot using adaptive fast nonsingular terminal sliding mode,” Nonlinear Dynamics, 110, pp. 1437–1453. DOI: 10.1007/s11071-022-07682-2.
7. Zhou, H., Ibrahim, C., Zheng, W. X. and Pan, W. (2022) “Sparse Bayesian Deep Learning for Dynamic System Identification,” Automatica, 144, Art. 110489. DOI: 10.1016/j.automatica.2022.110489.
8. Peng, X. B., Andrychowicz, M., Zaremba, W. and Abbeel, P. (2018) “Sim-to-Real Transfer of Robotic Control with Dynamics Randomization,” Proceedings of the 2018 IEEE International Conference on Robotics and Automation, IEEE, pp. 3803–3810. DOI: 10.1109/ICRA.2018.8460528.
9. Wang, L. and Yang, G. (2021) “An Interval Uncertainty Propagation Method Using Polynomial Chaos Expansion and Its Application in Complicated Multibody Dynamic Systems,” Nonlinear Dynamics, 105, pp. 837–858. DOI: 10.1007/s11071-021-06512-1.
10. Liu, X., Clark, G., Campbell, J., Zhou, Y. and Ben Amor, H. (2023) “Enhancing State Estimation in Robots: A Data-Driven Approach with Differentiable Ensemble Kalman Filters,” Proceedings of the 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems, IEEE. DOI: 10.1109/IROS55552.2023.10341617.
11. Lutter, M., Listmann, K. and Peters, J. (2019) “Deep Lagrangian Networks for End-to-End Learning of Energy-Based Control for Under-Actuated Systems,” Proceedings of the 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems, IEEE, pp. 7718–7725. DOI: 10.1109/IROS40897.2019.8968268.
12. Greydanus, S., Dzamba, M. and Yosinski, J. (2019) “Hamiltonian Neural Networks,” Advances in Neural Information Processing Systems 32 (NeurIPS), pp. 15353–15363. arXiv: 1906.01563.
13. Gawlikowski, J. et al. (2023) “A Survey of Uncertainty in Deep Neural Networks,” Artificial Intelligence Review, 56(S1), pp. 1513–1589. DOI: 10.1007/s10462-023-10562-9.
14. Lindemann, L., Cleaveland, M., Shim, G. and Pappas, G. J. (2023) “Safe Planning in Dynamic Environments Using Conformal Prediction,” IEEE Robotics and Automation Letters, 8(8), pp. 5116–5123. DOI: 10.1109/LRA.2023.3292071.

15. Vulpi, F., Milella, A., Marani, R. and Reina, G. (2021) "Recurrent and Convolutional Neural Networks for Deep Terrain Classification by Autonomous Robots," Journal of Terramechanics, 96, pp. 119–131. DOI: 10.1016/j.jterra.2020.12.002.

Відомості про авторів (About authors)

Носов Андрій Олександрович – аспірант, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна; ORCID: https://orcid.org/0009-0009-7708-1295; e-mail: andriinosov91@gmail.com.

Nosov Andrii Oleksandrovych – PhD Student, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine; ORCID: https://orcid.org/0009-0009-7708-1295; e-mail: andriinosov91@gmail.com.

Коржик Михайло Володимирович – кандидат технічних наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна; ORCID: https://orcid.org/0000-0002-7636-4754; e-mail: korzhyk@kpi.ua.

Korzhyk Mykhailo Volodymyrovych – PhD, Associate Professor, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine; ORCID: https://orcid.org/0000-0002-7636-4754; e-mail: korzhyk@kpi.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Носов А. О., Коржик М. В. Моделювання динаміки мобільних роботів в умовах невизначеності. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 87-93. doi: 10.20998/2413-4295.2026.02.12

Please cite this article as:

Nosov A., Korzhyk M. Modeling dynamics of mobile robots under uncertainty. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 87–93, doi: 10.20998/2413-4295.2026.02.12.

Надійшла (received) 14.05.2026
Прийнята (accepted) 25.05.2026
Опублікована (published) 05.06.2026

ЗМІСТ

CONTENTS

НАУКОВЕ ВИДАННЯ

ВІСНИК НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ "ХПІ". СЕРІЯ: НОВІ РІШЕННЯ В СУЧАСНИХ ТЕХНОЛОГІЯХ

Збірник наукових праць

№ 2(28)’ 2026

АДРЕСА РЕДКОЛЕГІЇ ТА ВИДАВЦЯ: 61002, Харків, вул. Кирпичова, 2, НТУ «ХПІ».
тел. (057) 707-66-00, e-mail: vestnik.nsmt@khpi.edu.ua

Підп. до друку «29» травня 2026 р. Формат 60x84 1/8. Папір офсетний. Друк цифровий.
Гарнітура Таймс. Ум. друк. арк. 3,3. Облік.вид.арк. 3,0.
Тираж 50 прим. Зам. № 556. Ціна договірна.

Видавничий центр НТУ «ХПІ». Свідоцтво про державну реєстрацію
суб’єкта видавничої справи ДК №5478 від 21.08.2017
61002, Харків, вул. Кирпичова, 2
