НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

XLIV
НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ МОЛОДИХ ВЧЕНИХ ТА СПЕЦІАЛІСТІВ ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА НАН УКРАЇНИ

ПРИСВЯЧЕНА ДНЮ НАУКИ В УКРАЇНІ

Збірник матеріалів конференції
20 травня 2026 р.

Київ – 2026

УДК 621.3 + 004 + 519.6 : 620.9

Рекомендовано до друку Вченою радою
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
(протокол №5 від 30 квітня 2026 р.)

Організаційний комітет:
В.В. Мохор, В.О. Артемчук, А.В. Яцишин та ін.

Програмний комітет:
В.В. Мохор, В.О. Артемчук, О.О. Попов та ін.

Відповідальний за випуск:
В.О. Артемчук

Collection of materials of the XLIV Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 20, 2026 / PIMEE of NAS of Ukraine. - 2026. - 97 p.

Збірник матеріалів XLIV Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 20 травня 2026 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2026. – 97 с.

ЗМІСТ

O.O. Tsypliak, Y.S. Dmytruk, V.O. Artemchuk

EUROPEAN DIGITAL INNOVATION HUB WEB PLATFORMS DEVELOPMENT AS DOMAIN

1. Introduction

“European Digital Innovation Hubs” (EDIHs) stands for the network of organizations in Europe [1]. Co Founded and financed by European Union (EU) and local governments since 2016 in scope of following global EU strategy **“Digital Europe Programme work programme”** [2] to organize provision of free services for local public sector organizations and small medium private businesses (later in text clients) to boost their productivity and competitiveness [3], this process is called **“Digital Transformation Acceleration”** or simpler “digitalization”.

Each individual EDIH finds a set of partner organizations (later in text service providers) that will be providing services to clients for free at 50% cost from the EU and 50% cost from local government following EU approved standard guideline [4]. Key Performance Indicator (KPI) of the cooperation between client and service is measurement of **“client digital maturity”**, a complex metric that identifies the ability of a single organization to remain competitive and productive considering current technological progress in the field of its work.

When local EDIH can’t provide required service it can cooperate with any other EDIH in Europe. As of May 2026 there are 462 EDIHs on the European continent including Ukraine [5].

From the definition of what is single EDIH, its individual performance is hard to measure. According to previous research [6], official key performance indicators from EU to assess performance can be found in Table 1.

Table 1. All official EDIH KPIs

KPI Category	Indicator	Target/Notes
Outreach	Number of SMEs/public sector entities contacted	Shows awareness-raising success.
	Number of events/workshops organized	Measures outreach activities.
Client Engagement	Number of clients served (SMEs/public sector)	Key measure of hub reach and utility.
	Number of first-time users	Demonstrates ability to engage new clients.
Service Provision	Number of Test Before Invest (TBI) services delivered	Shows technological support provided.
	Number of digital maturity assessments conducted	Assesses client readiness and areas for improvement.

	Number of clients receiving skills/training services	Reflects support for digital skill-building.
	Number of clients supported in accessing finance	Shows facilitation of investment for digitalization.
	Number of services provided related to innovation ecosystem & networking	Reflects collaboration with other hubs and stakeholders.
Impact	Number of clients adopting digital technologies after support	Direct measure of transformation impact.
	Estimated jobs created or maintained due to EDIH support	Socio-economic impact metric.
Collaboration & Network	Number of joint actions with other EDIHs or networks (e.g., EEN, clusters)	Indicates cooperation within the digital ecosystem.
	Number of referrals to other EDIHs or initiatives	Shows integration and inter-hub cooperation.
Satisfaction & Quality	Client satisfaction score (survey-based)	Quality of service delivery.
Administrative	Reports delivered on time	Compliance indicator.

Multidimensional analysis of all those KPIs by individual EDIH is not possible based on public data. In December 2023, EU made public simplified metrics that would allow to judge individual EDIHs performance. System of badges [7] related to key countable achievements assigned to individual EDIH see Picture 1.

Picture 1 - Individual EDIH assigned badges representing their performance in key activity areas

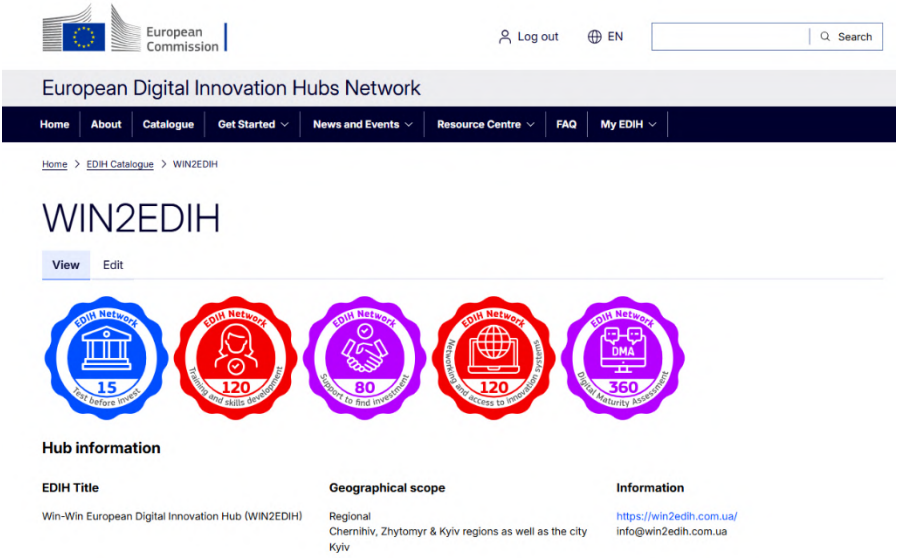
Being public service organizations themselves EDIHs performance is impacted by quality of there representation in global web. Assumption is that the higher quality has the platform of individual EDIH – the better would be its performance.

Let's check this hypothesis, analyze and outline common features of the individual EDIH web platforms. Even enlisting common features of the most performant platforms will be useful in optimization of EDIH platforms.

2. Analysis

To formalize performance of each EDIH and represent as single number let's check each EDIH page and record level of 5 types of badges awarded, counting each badge from 0 (if EDIH has no badge in selected dimension) to 5 (maximal stage) and then calculating total score as single number. Assuming all 5 dimensions of badges award as equally important.

As example, let's assess one of EDIHs profiles - WIN2EDIH [8] coordinated by Kyiv National Economic University see Picture 2.

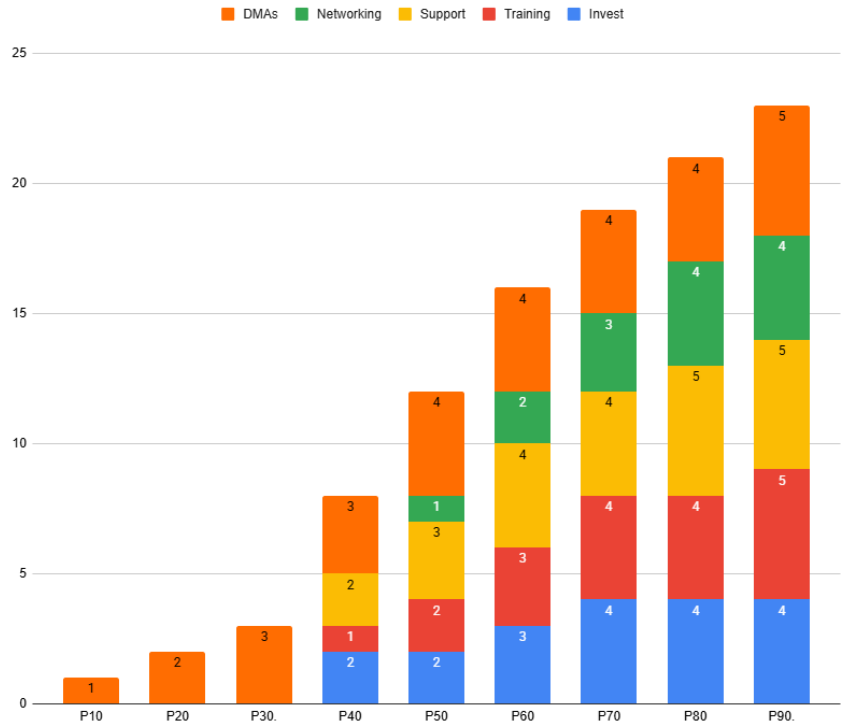


Picture 2 - WIN2EDIH profile page

According to badges types and levels form picture 1, this EDIH has all 5 types of badges: stage 1 for "Test before Invest", stage 4 for "Training and skills development" and so on. Leading its total score to $1 + 4 + 5 + 4 + 5 = 19$.

According to public EU EDIHs catalogue [5] and EU profiles of EDIHs, 82 % of all 462 has their own web platforms mentioned in their public profiles on EU official site. Among those 18% organizations without own web platforms only 27% have total score over 0 (at least one badge). Overall, 40% of all organizations earned at least 1 badge.

Badges earn statistics among EDIH, that have at least one badge showed different value of each metric. Let's calculate percentiles (see Picture 3) and the weight (see Picture 4) of each metric with the reverse proportion total score by each metric – where the least badges given in specific dimensions, the more valuable they are considered.



Picture 3 – Percentiles of metrics by EDIHs

3. Limitations and results

Using collected statistics and weight of each metric, top 8 most performant EDIHs as of May 2026 are in table 2. But before getting into common features of those platforms worth mentioning, that according to multiple researches related to e-commerce and consulting web user experience and user interfaces that any platform informational architecture design is iterative process basically started with functional requirements verification and user needs validation (see picture 5). But on later stages optimization key is user experience data analysis.

Unfortunately for this research we have no access to user experience data of platforms mentioned in table 2. So, the conclusions will be based on attempt of requirements reverse engineering.

According to Digital Europe program, EU keeps funding only under condition of achieving specific number of KPIs from table 1. Reasonable to assume that non-functional requirements design starts with covering KPI by specific features that will intend to maximize specific indicator.

Analysis results of top EDIHs from table 2 are depictured in table 3.

Table 2. Most performant EDIHs, common features

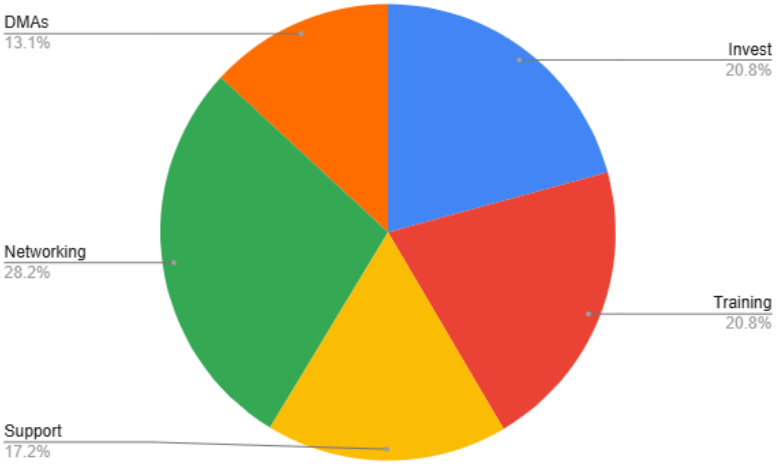
Name	Description	Number of occurrences among top 8 EDIHs
Landing page	Distinguishable marketing-focused long home page	8
Services catalogue	Structured catalogue describing available services and support options	8
Detailed site header section	Extended header with navigation menu, quick links, and action buttons	8
Home page infographics	Visual presentation of achievements, services, focus areas, or statistics	7
About us separate page with call to action	Dedicated organizational overview page encouraging user engagement	7
English localization	Platform allows switching to English	6
News section	Dedicated section with latest updates, announcements, and publications	6
Contact us section	Separate page or block with contacts, addresses, forms, and references	6
Social media references	Links to official social media platforms and communication channels	6
Site map in footer	Footer section containing structured navigation links to site pages	6
Newsletter subscription section	Form allowing users to subscribe for updates and news	5
Upcoming events calendar	Section displaying planned events, workshops, webinars, or trainings	5
Partners reference	Section presenting partner organizations, sponsors, or stakeholders	5
Video presentation	Embedded promotional or informational videos about the hub	4
Success stories/projects portfolio	Showcase of implemented projects, collaborations, or client success cases	4
FAQ section	Collection of frequently asked questions and answers for visitors	2

4. Conclusion

Individual EDIH web platform development is complex business analysis task. But this task can be handled via official numeric KPIs mapping to reverse engineered non-functional requirements from the one hand. And from using

ecommerce and consulting sites iterative approach to web user experience and user interfaces optimization.

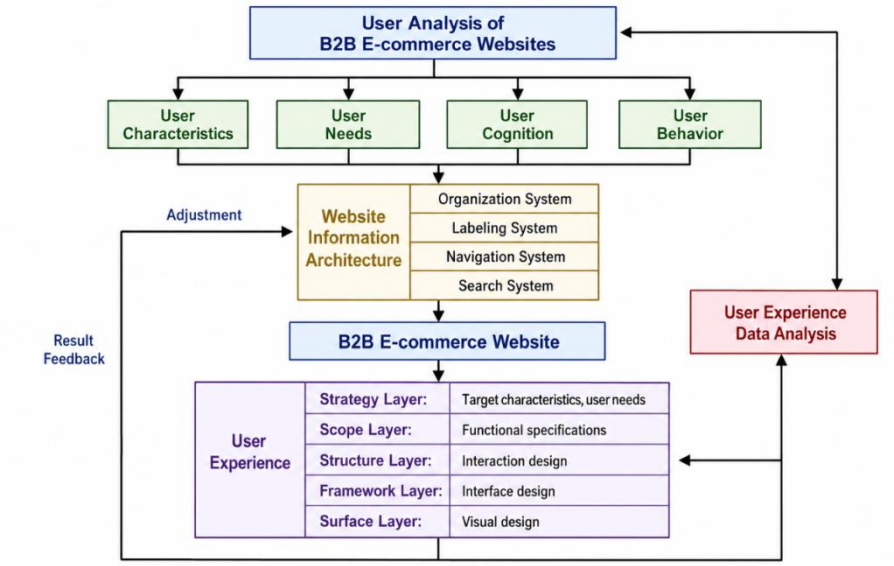
Current work was focused on identification of most performant EDIHs and their common features analysis. Prospect of further work on EDIHs web platform are in end user data analysis and prototyping of new features intended to target specific KPIs from table 1.



Picture 4 – Weight of metrics based on each of them total score

Table 3. Most performant EDIHs, May 2026

EDIH Title	**Simplified Description**	**Country**
AgroDigiRise [9]	Focuses exclusively on the digital and green transformation of the agri-food sector within the South Central region of Bulgaria.	Bulgaria
AI and Gaming [10]	Distinguishes itself through a specialized focus on game development, gamification, and blockchain to boost the Adriatic region's economy.	Croatia
CROatian Industry and Society Boosting [11]	Acts as a national excellence ecosystem specifically centered on the triple integration of AI, Cybersecurity, and High-Performance Computing.	Croatia
AI and Robotics Estonia [12]	Concentrates on increasing the digital maturity of the Estonian manufacturing industry through dedicated AI and robotics demo projects.	Estonia
Location Innovation Hub [13]	Stands out by using geospatial data and precise positioning technologies as the core driver for cross-sector innovation.	Finland
Robocoast [14]	Differentiates itself as a leading cybersecurity hub for the manufacturing industry, supported by a massive network of 9,000 specialists.	Finland
Wallachia eHub [16]	Focuses on "twin transition" services for an "Emerging Innovator" region, emphasizing GIS and Building Information Modelling (BIM).	Romania
EDIH MADRID REGION [15]	Functions as a government-led regional decision center that integrates EEN and Startup Europe services for a high-density urban economy.	Spain



Picture 5 – E-commerce website user experience improvement process [17]

[1] European Digital Innovation Hubs. (n.d.). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/edihs

[2] The DIGITAL Europe Programme – Work programmes. (n.d.). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital

[3] Get to know us | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/get-know-us#:~:text=EDIHs%20work%20as%20one-stop,their%20path%20towards%20digital%20transformation

[4] Cooperation guidelines for a seamless digitalization support to European SME. (n.d.). In https://european-digital-innovation-hubs.ec.europa.eu/system/files/2023-11/20231116_DTA_CooperationGuidelines_EDIH_EEN_Clusters_final.pdf.

[5] EDIH Catalogue | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/edih-catalogue

[6] Tsypliak O.O., Dmytruk Y.S., Cheban O.O., Artemchuk V.O. (2025). European digital innovation hub optimization using generative artificial intelligence tools. Collection of materials of the XLIII Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 14, 2025 / PIMEE of NAS of Ukraine. - 2025. - p. 32-38.

[7] Badges programme for the EDIH network – Guidelines | European Digital Innovation Hubs Network. (n.d.). https://european-digital-innovation-hubs.ec.europa.eu/knowledge-hub/guidance-documents/badges-programme-edih-network-guidelines

[8] WIN2EDIH | European Digital Innovation Hubs Network. (n.d.). https://european-

digital-innovation-hubs.ec.europa.eu/edih-catalogue/win2edih
[9] EDIH web platform, AgroDigiRise. https://edih.agrohub.bg/
[10] EDIH web platform, AI and Gaming. https://gaming-edih.hr/en/homepage/
[11] EDIH web platform, CROatian Industry and Society Boosting. https://crobohub.fer.hr/
[12] EDIH web platform, AI and Robotics Estonia, https://aire-edih.eu/en/
[13] EDIH web platform, Location Innovation Hub. https://locationinnovationhub.eu/en/home/
[14] EDIH web platform, Robocoast. https://robocoast.eu/
[15] EDIH web platform, EDIH MADRID REGION. https://www.edihmadrid.es/
[16] EDIH web platform, Wallachia eHub, https://wallachiaehub.ro/
[17] Li, Y., & Zhou, P. (2011). Research on B2B e-commerce site information architecture based on user experience. In 2011 International Conference on E-Business and E-Government (ICEE) (pp. 1–4). IEEE. 2011 International Conference on E-Business and E-Government (ICEE). https://doi.org/10.1109/icebeg.2011.5886889

В.С. Ракович, Г.В. Чурсін, О.М. Прокопець, В.В. Цуркан

ПРОТОТИП ПРОГРАМНОГО ЗАСТОСУНКУ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Дієвість забезпечування кібербезпеки ускладнюється без обміну інформацією між усіма зацікавленими сторонами. Його важливість підтверджується як міжнародними, регіональними, національними [1], так і вітчизняними нормативними документами [2]. Зокрема в [2] введено поняття про Національну систему обміну інформацією про кіберінциденти, кібератаки, кіберзагрози. Усе це вказує на важливість процесу обміну інформацією про події кібербезпеки.

Обмін інформацією про будь-яку подію кібербезпеки, яку виявлено працівником, починається з моменту фіксування її ознак та проявів, Як наслідок, початку процесу повідомляння за встановленим відповідним механізмом (процедурою) [3]. Залежно від зафіксованих ознак і проявів подія кібербезпека інтерпретується як кіберінцидент.

Процес обміну передбачає наявність середовища розповсюдження, яким буде пересилатися інформація про подію кібербезпеки. До того ж способу її передавання від однієї зацікавленої сторони до іншої. Відповідно до міжнародних, регіональних, національних [4] та вітчизняних нормативних документів [5, 6] у сфері кібербезпеки таким середовищем обміну інформацією про події кібербезпеки здебільшого є глобальна мережа Інтернет. Тоді як основним способом передавання – електронна пошта [5, 6]. Виокремлений спосіб має як переваги, так і недоліки. До переваг можна віднести перш за все простоту створювання та передавання повідомлення про подію кібербезпеки. До недоліків – складність забезпечування безпеки процесу повідомляння через недостатню упроваджуваність відповідних заходів і засобів. Крім того, складність процесу обробляння повідомлень з огляду на відсутність або складність налаштування автоматичного режиму його реалізування.

Разом з тим, міжнародними, регіональними, національними нормативними документами у сфері кібербезпеки пропонується використання декількох способів повідомляння про події кібербезпеки [4]. Цим зумовлено проведення дослідження відомих їх реалізування: електронна пошта, телефон, факс, вебсайт, мобільний застосунок. Серед них одним з найкращих є спосіб повідомляння за допомогою спеціалізованого мобільного застосунку. Його реалізування узгоджується з настановами міжнародних, регіональних, національних нормативних документів у сфері кібербезпеки [1] та характеризується перевагами порівняно з іншими способами повідомляння про події кібербезпеки, наприклад: безпечністю, надійністю, зручністю.

Рисунок 1 – Схематичне представлення порівняльного аналізу відомих способів повідомляння про подію кібербезпеки

Отже, проаналізовано передумови ініціювання обміну інформацією про виявлені працівником події кібербезпеки. За результатами зіставляння відомих способів повідомляння виокремлено використання спеціалізованого мобільного застосунку. Насамперед вибір даної альтернативи обумовлений його перевагами порівно з проаналізованими варіантами. До того ж це дозволить як реалізувати, так і автоматизувати механізм (процедуру) повідомляння про події кібербезпеки об’єктів критичної інфраструктури.

[1] International Organization for Standardization. (2023). I Information technology – Information security incident management – Part 1: Principles and process (ISO/IEC Standard No. 27035:2023)

[2] Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури» № 4336-IX (2025, 27 березня). https://zakon.rada.gov.ua/laws/show/4336-20#Text.

[3] Цуркан В. В., Ракович В. С. (2026). Механізм повідомляння про події кібербезпеки об’єктів критичної інфраструктури. Кібербезпека : освіта, наука, техніка. *4* (32). 1002–1014. https://doi.org/10.28925/2663-4023.2026.32.1200.

[4] ENISA. Good Practice Guide for Incident Management. https://enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf

[5] Наказ Адміністрації Державної служби спеціального. зв'язку та захисту інформації України «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» № 94 (2008, 10 Червня; зі змінами 2023, 10 січня). https://zakon.rada.gov.ua/laws/show/z0603-08#Text.

[6] Наказ Адміністрації Державної служби спеіального. зв'язку та захисту інформації України «Про затвердження Порядку повідомлення про інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних» (2024, 20 листопада). https://zakon.rada.gov.ua/laws/show/z1820-24#Text.

А.В. Ковилін

ЕКСПЕРИМЕНТАЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ НЕВІДОМИХ КІБЕРАТАК У ЦИФРОВИХ ПІДСТАНЦІЯХ

Цифрові підстанції є важливими елементами сучасної енергетичної інфраструктури, у яких функції моніторингу, керування, автоматизації та захисту значною мірою залежать від мережевої взаємодії між інтелектуальними електронними пристроями, серверами, комунікаційними шлюзами та системами диспетчерського керування. Використання стандартизованих промислових протоколів і мережевих сервісів підвищує ефективність обміну даними, але водночас розширює поверхню потенційних кібератак.

Одним із перспективних напрямів підвищення кіберстійкості цифрових підстанцій є застосування систем виявлення вторгнень, побудованих на основі методів машинного навчання. Такі системи здатні аналізувати параметри мережевого трафіку, виявляти відхилення від нормальної поведінки та класифікувати потенційно шкідливу активність. У сучасних дослідженнях ML-based IDS розглядаються як важливий компонент захисту smart grid та підстанційних середовищ [4], [7]. Разом із тим значна частина експериментальних досліджень оцінює моделі за умов, коли приклади всіх типів атак уже присутні у навчальній вибірці. У таких сценаріях supervised-моделі можуть демонструвати високі значення точності, однак це не завжди означає їхню здатність виявляти нові або модифіковані атаки. У сучасних роботах із zero-day detection для цифрових підстанцій підкреслюється, що узагальнення моделей на novel або unseen attacks залишається складним дослідницьким завданням [5], [6]. Також у роботах з anomaly detection для IEC 61850/GOOSE-комунікацій звертається увага на обмеженість розмічених атакувальних даних, проблему class imbalance та необхідність оцінювання моделей у більш складних сценаріях [7], [8].

Саме тому метою даної роботи є експериментальний аналіз моделей машинного навчання для виявлення невідомих кібератак у мережевому трафіку цифрових підстанцій на основі processed IEC104 частини датасету SANDI-2024.[1-2]

Для досягнення поставленої мети було реалізовано такі завдання: проаналізовано структуру processed IEC104 частини датасету SANDI-2024; підготовлено дані для задачі бінарного виявлення атак; сформовано базовий сценарій оцінювання моделей на відомих атаках; реалізовано сценарій leave-one-attack-out, у якому окремий тип атаки виключається з навчальної вибірки; порівняно supervised-моделі різних класів; оцінено anomaly-based моделі, навчені лише на нормальному трафіку; проаналізовано вплив порогу прийняття рішення на виявлення найскладнішої невідомої атаки;

сформульовано практичні висновки щодо застосування ML-based IDS у цифрових підстанціях.

Для експериментального дослідження використано датасет SANDI-2024, який містить сирі та попередньо оброблені мережеві дані, охоплює протоколи IEC 61850, IEC 60870-5-104, NTP і PTP, а також поєднує реальний безпечний трафік із лабораторними сценаріями атак [1-2]. Першим етапом експерименту було формування базового сценарію виявлення відомих атак. У цьому режимі навчальна та тестова вибірки містили приклади всіх типів атак. Такий сценарій відповідає традиційному підходу до оцінювання IDS, коли модель навчається на прикладах нормального та атакувального трафіку і тестується на даних із тим самим набором класів.

Таблиця 1 – Середні результати оцінювання якості моделей для виявлення невідомих атак на базі датасету SANDI-2024

Невідома атака	Recall	Precision	F1 -score	Balanced Accuracy	FPR	ROC-AUC
NTP DDoS	0.425	0.993	0.587	0.707	0.011	0.869
mitmattack	0.984	0.981	0.981	0.988	0.008	0.992
portscanattack	0.996	0.997	0.996	0.993	0.009	0.999
iec104starvationattack	0.999	0.997	0.998	0.994	0.011	1
dosattack	1	0.997	0.998	0.994	0.011	1
floodattack	1	0.992	0.996	0.994	0.011	1
fuzzyattack	1	0.997	0.998	0.994	0.011	1

Основним сценарієм дослідження був leave-one-attack-out. Його суть полягає в тому, що один тип атаки повністю виключається з навчальної вибірки та використовується лише на етапі тестування. Наприклад, якщо як невідома атака розглядається NTP DDoS - модель навчається на нормальному трафіку та всіх інших атаках, але не отримує жодного прикладу NTP DDoS під час навчання. Після цього модель тестується на суміші нормального трафіку та виключеної з даних інформації про атаку. Така постановка є ближчою до практичної ситуації, коли IDS стикається з новим або модифікованим типом шкідливої активності, і узгоджується з сучасними дослідженнями zero-day та unseen attack detection у цифрових підстанціях [5], [6]. У роботі порівнювалися дві групи моделей: supervised-моделі та anomaly-based моделі. Такий набір дозволяє порівняти лінійні, метричні, імовірнісні та

ансамблеві підходи до бінарного виявлення атак. На відміну від supervised-моделей, anomaly-based моделі навчалися лише на нормальному трафіку attackfree, після чого тестувалися на сумішах нормального трафіку та окремих атак.

Аналіз результатів за моделями показав, що найкращий середній результат серед supervised-моделей у сценарії leave-one-attack-out продемонструвала Extra Trees. Вона досягла Recall = 0.942, F1-score = 0.964 та Balanced Accuracy = 0.971 за False Positive Rate = 0.000. Це свідчить про високу придатність ансамблевих моделей для виявлення більшості невідомих атак у flow-based IEC104-трафіку цифрових підстанцій.

Random Forest, HistGradientBoosting, Linear SVM та Logistic Regression показали близькі результати за Balanced Accuracy, однак поступилися Extra Trees за Recall і F1-score. Це означає, що зазначені моделі можуть розглядатися як сильні альтернативи, проте для складних unseen-атак, зокрема NTP DDoS, потребують додаткового аналізу порогу прийняття рішення. KNN показав порівняно високий Recall, але мав підвищений рівень хибних спрацювань, що є небажаним для практичного використання в IDS. Gaussian Naive Bayes продемонструвала найнижчий середній Recall серед supervised-моделей, тому її доцільніше розглядати як простий baseline, а не як основну модель для захисту цифрових підстанцій.

Anomaly-based моделі показали інший характер поведінки. Local Outlier Factor досягла Recall = 1.000, F1-score = 0.946 та Balanced Accuracy = 0.914 за FPR = 0.171. One-Class SVM також забезпечила повне виявлення атак, однак мала дещо вищий рівень хибних спрацювань. Isolation Forest показала нижчий FPR, але поступилася за Recall, що означає можливий пропуск частини атакувальних прикладів. Таким чином, anomaly-based моделі демонструють високу чутливість до нетипової активності, однак їх практичне використання потребує контролю рівня хибних тривог.

Практичне застосування отриманих результатів полягає у можливості побудови більш реалістичної IDS-логіки для цифрових підстанцій. Extra Trees може використовуватися як основний supervised-класифікатор, оскільки забезпечує найкраще співвідношення між повнотою виявлення атак, F1-score та відсутністю хибних спрацювань. Local Outlier Factor може виконувати роль додаткового anomaly-based компонента для виявлення нетипової активності, яка не була представлена в навчальних даних. Аналіз порогів, виконаний для NTP DDoS, може бути використаний для налаштування рівнів тривоги IDS залежно від поточного ризику, типу трафіку або режиму роботи підстанційної мережі. Отримані результати підтверджують, що стандартний сценарій оцінювання на відомих атаках може переоцінювати практичну ефективність ML-based IDS. Сценарій leave-one-attack-out дозволяє виявити приховані обмеження моделей, зокрема різну складність окремих unseen-атак і залежність результатів від порогу прийняття рішення. Найбільш збалансованою supervised-моделлю в проведених експериментах є Extra Trees, тоді як Local Outlier Factor є перспективним додатковим засобом

anomaly-based контролю. Подальші дослідження доцільно спрямувати на перевірку отриманих результатів для IEC61850/GOOSE-трафіку, міжпротокольну переносимість моделей, аналіз сирих PCAP/PCAPNG-даних та розроблення адаптивних порогів IDS для зменшення ризику пропуску нових кібератак.

[1] Gutiérrez Mlot, E. D., Saldana, J., Rodríguez, R. J., Kotsiuba, I., & Gañán, C. (2024). A dataset to train intrusion detection systems based on machine learning models for electrical substations. Data in Brief, 57, Article 111153. https://doi.org/10.1016/j.dib.2024.111153

[2] Gutiérrez Mlot, E. D., Saldana, J., Rodríguez, R. J., Kotsiuba, I., & Hernández Gañán, C. (2024). Dataset to train intrusion detection systems based on machine learning models for electrical substations [Data set]. Zenodo. https://doi.org/10.5281/zenodo.15487636

[3] Gutiérrez Mlot, E. D. (n.d.). cybersecurity-datasets: Tools to process network captures in PCAP format from IEC61850 or IEC60870-5-104 [Computer software]. GitHub. Retrieved April 28, 2026, from https://github.com/esguti/cybersecurity-datasets

[4] Sahani, N., Zhu, R., Cho, J.-H., & Liu, C.-C. (2023). Machine learning-based intrusion detection for smart grid computing: A survey. ACM Transactions on Cyber-Physical Systems. https://doi.org/10.1145/3578366

[5] Manzoor, F., Khattar, V., Liu, C.-C., & Jin, M. (2024). Zero-day attack detection in digital substations using in-context learning. In 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (pp. 220–225). IEEE. https://doi.org/10.1109/SmartGridComm60555.2024.10738025

[6] Manzoor, F., Khattar, V., Herath, A., Black, C., Nielsen, M. C., Hong, J., Liu, C.-C., & Jin, M. (2025). Detecting zero-day attacks in digital substations via in-context learning. arXiv. https://doi.org/10.48550/arXiv.2501.16453

[7] Nhung-Nguyen, H., Girdhar, M., Kim, Y.-H., & Hong, J. (2024). Machine-learning-based anomaly detection for GOOSE in digital substations. Energies, 17(15), Article 3745. https://doi.org/10.3390/en17153745

[8] Tobar-Rosero, O. A., et al. (2024). GOOSE Secure: A comprehensive dataset for in-depth analysis of GOOSE spoofing attacks in digital substations. Energies, 17(23), Article 6098. https://doi.org/10.3390/en17236098

Р.І. Драгунцов, Є.В. Кочелаб

ПІДХІД ДО ОЦІНКИ ЯКОСТІ ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ НА ОСНОВІ ФУНКЦІОНАЛЬНОЇ ДЕКОМПОЗИЦІЇ

Управління інцидентами кібербезпеки є безперервним процесом, що потребує регулярного вдосконалення процедур та технологічних засобів. Готовність до кіберінцидентів в той же час складно оцінити якісно та кількісно, навіть за умови наявних формалізованих планів реагування та регулярних аудитів або навчань. Метою дослідження є формалізація методу регулярної перевірки заходів реагування через декомпозицію процесу реагування на атомарні функції, визначення для них очікуваних результатів та побудову відповідних функцій верифікації.

Процес управління інцидентами кібербезпеки не має короткого циклу зворотного зв'язку [1]. Факт успішного закриття інциденту не є достатньою підставою для висновку про технічну ефективність реагування, оскільки результат може бути зумовлений неповнотою атаки, зовнішніми обмеженнями дій порушника, ручною компенсацією недоліків або відсутністю повторної перевірки стану об'єкта після виконання дії. Крім того, ефективність розробленого плану, окремих стадій, або впроваджених засобів активного реагування неможливо оцінити до настання [2]. Під активним реагуванням визначаються дії, що безпосередньо змінюють стан суб'єкта, об'єкта, мережевого з'єднання, облікового запису або сервісу: блокування облікового запису, ізоляція кінцевої системи, тощо [3]. Варто зазначити, що до активного реагування включається не лише безпосередні технічні заходи, а і супроводжуючі адміністративні процеси.

В якості заходів перевірки спроможностей для реагування на кіберінциденти використовуються:

- Командно-штабні навчання;
- Стресс-тестування систем (Penetration Testing, RedTeaming);
- Системи симуляції загроз (Breach and Attack Simulation - BAS)

Командно-штабні навчання дають змогу оцінити організаційну готовність: розподіл ролей, ескалацію, комунікацію, узгодженість рішень і повноту документації. Водночас вони не забезпечують перевірки фактичної можливості реагування та дійсності результатів реагування.

Стресс-тестування, тобто моделювання дій порушника спеціалізованою командою мають вищу практичну цінність для виявлення технічних недоліків [4]. Однак такі підходи є ресурсоємними, потребують окремого планування та ускладнюють формальне визначення покриття перевірених процедур [5].

Після завершення тестування складно встановити, які саме елементарні дії реагування були перевірені, для яких класів об’єктів, з якими аргументами та за яких обмежень часу, також складно забезпечити повну повторюваність та регулярність перевірки.

Пропонується підхід, що ґрунтується на декомпозиції процесу реагування на атомарні функції активного реагування, зокрема в форматі наведеному в . Атомарною функцією реагування є мінімальна керована дія, що має визначені вхідні аргументи, виконавця, умови застосування та перевірюваний результат. Наприклад, функція ізоляції робочої станції визначається аргументом імені робочої станції, а результат перевіряється як відсутність можливості для робочої станції здійснювати мережеві комунікації з референтним переліком зовнішніх мережевих ресурсів. Кожна атомарна функція реагування подається як відображення множини детермінованих аргументів у очікуваний стан системи. Тобто, очікуваним результатом є формально визначений стан. Виконавцем функції реагування може бути людина, програмний бот або агент штучного інтелекту. У межах запропонованої моделі тип виконавця не змінює специфікацію функції, але впливає на показники часу виконання, відтворюваності, частоти помилок.

На основі атомарних функцій формується реєстр функцій реагування. Для кожного запису реєстру визначаються назва функції, область застосування, допустимі класи об’єктів, обов’язкові аргументи, передумови виконання, очікуваний результат, допустимий час виконання, тип виконавця, джерело командного впливу, джерело перевірки та обмеження безпечного застосування.

Кожній функції реагування ставиться у відповідність функція перевірки результату. Функція перевірки є незалежною процедурою, що встановлює відповідність фактичного стану системи очікуваному результату. Її вихідним значенням може бути бінарний результат або кількісна оцінка якості виконання. Бінарна оцінка застосовується для дій із чітким цільовим станом, наприклад успішне або неуспішне блокування облікового запису. Кількісна оцінка доцільна для дій із градацією якості, наприклад часткова ізоляція вузла, неповне покриття мережевих маршрутів або затримка появи подій у системі моніторингу, також кількісна оцінка може використовуватись для введення в розрахунок коефіцієнта часових параметрів реагування.

Функція перевірки повинна реалізовувати практичну логіку контролю результату, а не спиратися лише на повідомлення засобу реагування про успішне виконання команди. Для перевірки можуть засовуватись автоматизовані, зокрема агентні рішення, що розгортаються в інфраструктурі, зокрема на системах, що підлягають тестуванню. Час реагування має розглядатися як параметр функції перевірки, якщо цінність дії залежить від своєчасності. У такому разі позитивний результат встановлюється лише за

умови досягнення очікуваного стану в межах заданого часовго інтервалу, що відокремлює технічну можливість виконання дії від її операційної придатності.

Пара «функція реагування — функція перевірки» застосовується для регулярного автоматизованого тестування спроможностей реагування. Тестування виконується для всіх визначених типів об'єктів, до яких застосовна відповідна дія. Кумулятивна оцінка якості реагування розраховується на основі результатів функцій перевірки для всіх функцій реагування і всіх визначених об'єктів перевірки. Така оцінка може враховувати частку успішних виконань, середній і граничний час досягнення цільового стану, частку часткових результатів, кількість недоступних об'єктів, кількість помилкових впливів на суміжні об'єкти та вагу критичності активів. Формально це переводить оцінювання реагування з описового рівня у вимірювану модель технічної готовності.

Нехай $F = \{f_i\}_{i=1}^{m}$— множина атомарних функцій реагування, $O = \{o_j\}_{j=1}^{n}$— множина об'єктів перевірки, $A \subseteq F \times O$— відношення застосовності функції до об'єкта, $r_{ij} \in [0,1]$— результат функції перевірки для пари (f_i, o_j), $q_{ij} = \mathbb{I}(t_{ij} \leq \tau_i)$— ознака виконання часової вимоги. Тоді інтегральна оцінка технічної готовності реагування визначається як (1):

$$R = \frac{1}{|A|} \sum_{(i,j)\in A} r_{ij}\, q_{ij} \quad \#(1)$$

де $R \in [0,1]$, **0** відповідає відсутності підтвердженої спроможності реагування для всіх застосовних пар, а **1**— повному та своєчасному досягненню очікуваного результату для кожної застосовної пари «функція реагування — об'єкт».

Запропонований підхід також має навчальний ефект для команди реагування. Регулярне виконання атомарних дій у контрольованих умовах формує практичну перевірку повноважень, маршрутів ескалації, коректності інструкцій, доступності інструментів і відповідності інвентаризаційних даних фактичному стану системи. Водночас навчання не підміняє вимірювання, оскільки результат кожної дії фіксується через функцію перевірки.

Висновок

Запропонована модель розглядає активне реагування на інциденти кібербезпеки як множину формалізованих атомарних функцій із визначеними аргументами, очікуваними результатами та незалежними функціями перевірки, що створює об'єктивну базу для регулярного оцінювання технічної спроможності реагування, що не забезпечується іншими існуючими методами. Практичний результат полягає у виявленні недоступних, повільних, неповних або організаційно заблокованих дій реагування, а також у формуванні кількісної оцінки готовності системи та персоналу до

виконання активних заходів під час інциденту для визначення пріоритетів для покращення результатів та кіберзахисту в цілому.

[1] Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, 103309. https://doi.org/10.1016/j.cose.2023.103309

[2] Chiarini, F., Sacher-Boldewin, D., Wilkins, L., & Zajicek, M. (2023, 29 травня). Security Incident Timing Metrics version 1.0. FIRST.org. https://www.first.org/global/sigs/metrics/Security-Incident-Timing-Metrics_v1.0.pdf

[3] Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident response recommendations and considerations for cybersecurity risk management : National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/nist.sp.800-61r3

[4] Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment. Cyber Security and Applications, 3, 100077. https://doi.org/10.1016/j.csa.2024.100077

[5] Kleijmeer, R., Prenio, J., & Yong, J. (2019, листопад). FSI Insights on policy implementation No 21 Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions. bis.org. https://www.bis.org/fsi/publ/insights21.pdf

R.A. Vasylyshyn

COMPUTER MODELING IN THE FIELD OF SECURITY OF NUCLEAR FACILITIES

The modern shift to digital data is inevitable. It helps to process data quickly and sufficiently, analyze previous mistakes and define potential risks. Computer modeling enhanced level of nuclear facilities security. Despite this, cyberattacks have become more widespread and sophisticated. The threats to both organizations and individuals have become more striking. Hackers are constantly changing their attack strategies and seeking to maintain an advantage in cyberspace.

How should defense organizations act to establish security? N. Srivastava and U. C. Jaiswal see preventive measures as focusing attention on several stages. The main task is to create a direct channel for reporting on the methodology of hacker attacks to cybersecurity directors. It is necessary to reduce the time between the broadcast of the threat signal and the implementation of preventive measures as much as possible.

This can be achieved by improving the quality of the information collection process, risk assessment, establishment of a system for detecting potential dangers, and communication networks [4, p.582]. At each of the above levels, violations can occur that lead to vulnerability. Computer modeling helps to solve this problem at each of stages.

The key process is the collection of information from various networks. This includes Internet traffic, data on previous user downloads, assessment of user behavior during previous downloads, and a report on previous actions.

If there are changes in patterns compared to the past login to the system, one can suspect the presence of a threat due to a violation of cybersecurity. In addition, other factors should be considered: geographical, political and economic, the history of previous armed conflicts between different states. The presence of nuclear weapons in the country should also be reviewed. This serves as an important factor in preventing a nuclear attack, since the consequences of a potential mutual exchange of blows are realized.

In general, the level of development of nuclear preemption is constantly changing, in accordance with changes in international relations and political narratives.

This information is then used in the analysis of potential nuclear threats and theoretical models. For example, Game Theory studies the history of previous military conflicts. And on their basis, predictive algorithms for future wars and the probability of the attacks performed on nuclear objects were developed [1]. Game Theory has given rise to other systematic approaches.

Predictive models have been successful in identifying weaknesses in nuclear deterrence. In particular, Monte Carlo simulation systems are often used in cybersecurity assessments. They involve creating thousands of models of theoretically probable attack scenarios through the information space. This allows organizations to assess potential losses in the event of a hit. At the same time, Bayesian systems are more relevant to real-world cyberspace threat indicators.

Their peculiarity is that the algorithm considers the "parent" initial patterns of behavior, from which further options for the development of algorithmic variants of events are already based. Bayesian systems also represent the internal interaction between several factors, which significantly brings the results of simulations closer to the real data obtained.

Initially, supporters of Game Theory in the classical approach consider scenarios of variants of behavioral patterns of "players" in the form of linear projections that depend on specific factors. Therefore, errors when comparing with historical data are more common [2, p. 1559-1560].

P. Weiland and J. S. Lustosa conduct analysis using Bayesian networks in areas such as workplace and environmental safety; hiring practices; customers, products and business practices; physical assets; business and systems; execution, delivery and process management; internal and external fraud; public trust.

A Bayesian network (BN) graphically represents the cause-and-effect relationship between events, which allows for an easy and quick intuitive understanding of the situation as a whole and, therefore, supports the risk-based decision-making process.

A Bayesian network provides a logical, integrated structure that allows for a better examination of all operational risks and the probability of their occurrence. A BN can be regularly updated in real time by managers to consider new information. A Bayesian network acts as an early warning system: whenever a risk is determined to be unacceptably high, action must be taken to avoid the risk.

This model encourages discussion between pairs to reach a consensus on the relative importance of operational risks. However, it should start with a simplified algorithm and gradually make it more complex so as not to break the logic of events. Also, the simulation does not work if there are missing initial inputs [5]

P.R. Saey and co-authors express doubts about the possibility of fully automating the process of the analysis of risks of nuclear safety. Therefore, the probability of technical errors that will contribute to the emergence of irreparable consequences is extremely high. Human intervention is necessary for control [3, p.769].

As a conclusion, computer modeling in the sphere of nuclear facilities security is a complex phenomenon that requires thorough analysis. It also becomes obvious that with the development of new technologies, the issue of compliance

with the moral norms of humanity in accordance with the time frame in which they were approved becomes relevant.

[1] Epifanovskaya, L.W.E. & Lakkaraju, K. et al. (2018) Toward a Quantitative Approach to Data Gathering and Analysis for Nuclear Deterrence Policy, U.S. Department of Energy Office of Scientific and Technical Information, Retrieved May 11, 2026, from https://doi.org/10.1007/978-3-319-96661-8_26

[2] Ferreira, D. J., Mateus-Coelho, N. and Mamede, H. S. (2023) 'Methodology for Predictive Cyber Security Risk Assessment (PCSRA)', Procedia Computer Science, 219, pp. 1555–1563. doi: 10.1016/J.PROCS.2023.01.447.

[3] Saey, P.R.J.& De Geer (2005) Notes on radioxenon measurements for CTBT verification purposes, Applied radiation and Isotopes, 63 (5-6), 765-773.

[4] Srivastava, N. and Jaiswal, U. C. (2019) Big data analytics technique in cyber security: A review, Proceedings of the 3rd International Conference on Computing Methodologies and Communication, pp. 579–585.

[5] Wieland, P., Lustosa, S.J. (2009) Modeling operational risks of the nuclear industry with the Bayesian networks, International Nuclear Atlantic Conference, Retrieved May 11, 2026, from https://inis.iaea.org/records/nk2t3-kpk62

З.В. Іванов

АКТУАЛЬНІ ПИТАННЯ ВІДНОВЛЕННЯ ДЖЕРЕЛА РАДІОАКТИВНОГО ВИКИДУ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Одним із ключових елементів аварійної готовності та реагування у сфері ядерної та радіаційної безпеки є моделювання атмосферної дисперсії радіоактивних аерозолів для оцінки територій, де потребується проведення контрзаходів. Фундаментальним вхідним параметром таких розрахунків є джерело радіоактивного викиду (Source Term), яке і є основним вкладником у прогнозовані дози опромінення. Якщо для вибору метеоданих (локальні вимірювання чи чисельні прогнози NWP) та програмного забезпечення (наприклад, системи підтримки прийняття рішень (СППР) JRODOS, ARGOS, HotSpot [1]) експерти мають стандартизований алгоритм дій, то оперативна оцінка самого джерела викиду залишається найбільш складною та ресурсомісткою задачею.

Для проведення первинної оцінки джерела під час реальної аварії або тренувань залучається група експертів, яка аналізує стан ядерної установки. Паралельно експерти з радіаційних наслідків виконують серії розрахунків дисперсії на основі гіпотетичних сценаріїв. Цей процес є вкрай ітеративним: обчислення одного сценарію в класичних СППР може займати від 10 хвилин. В умовах стрімкого розвитку аварії метод ітеративного перебору (forward modeling) стикається як з проблемою людського фактору, так і з критичною втратою часу, необхідного для прийняття рішень.

Більше того, як демонструє досвід міжнародного проєкту BARCO [2], навіть за умови фіксованого (відомого) джерела викиду, використання різних джерел метеорологічних даних та моделей призводить до значної розбіжності результатів і доз опромінення населення на відстанях понад 100 км. В умовах же невідомого джерела ця невизначеність зростає експоненціально.

Розв’язання оберненої задачі – відновлення параметрів викиду за фактом радіаційного забруднення територій – можливе шляхом використання даних радіаційного моніторингу. Проте, враховуючи просторову розрідженість постів радіаційного моніторингу в Україні [3], обмежений доступ до даних із зон спостереження атомних електричних станцій (АЕС), загальний доступ до яких наразі відсутній з міркувань безпеки, та відсутність щільних альтернативних мереж, реконструкція джерела викиду подібним класичним математичним методом може бути невирішуваною через обмежену кількість даних для аналізування.

Загалом, проблема оцінки джерела викиду включає три основні групи невизначеностей:

- метеорологічні – відповідність прогнозних даних реальній складній аеродинаміці повітряних мас в близькій зоні (100 кілометрів) від аварійної АЕС;

- невизначеності даних моніторингу – похибки результатів вимірювань, просторова розрідженість постів радіаційного моніторингу, відсутність загальної встановленої концепції до ідеального поста радіаційного моніторингу;
- невизначеності параметрів джерела викиду – невідомі активність джерела викиду, його радіонуклідний, зміни інтенсивності викиду в часі.

Для подолання цих викликів перспективною є розробка та створення швидкої сурогатної нейромережевої моделі. Ця модель навчатиметься на масиві статистичних розрахунків, попередньо згенерованих СППР JRODOS на основі багаторічних локальних метеорологічних баз. Після навчання, така модель зможе на основі поточного прогнозу погоди надавати результати попередніх оцінок зон проведення контрзаходів та потенційних напрямків руху радіоактивних аерозолів за короткий час. Цей підхід концептуально наслідує інноваційну архітектуру глобальних погодних ШІ-моделей від Google (GraphCast [4] / WeatherNext), які навчалися на десятиліттях даних реаналізу метеорологічних даних, що підготовані та зберігаються на ресурсах ECMWF ERA5 [5].

Зниження невизначеності даних радіаційного моніторингу можливо реалізувати шляхом попередньої нормалізації показників постів радіаційного моніторингу (зокрема значень потужності амбієнтного еквівалента дози) до еталонних умов, які генерує JRODOS, з урахуванням висотних коефіцієнтів послаблення гамма-випромінювання [6] та топології місць встановлення постів радіаційного контролю [7]. В перспективі, модель буде здатна приймати за вхідні дані результати вимірювань потужності амбієнтного еквівалента дози будь-де в зоні, на якій проводилось навчання моделі.

Запропонований підхід до вирішення проблеми відновлення джерела радіоактивного викиду забезпечить експертів кризових центрів можливістю проводити оперативну реконструкцію джерела викиду в умовах глибокої невизначеності, відсутності щільної моніторингової мережі та жорстких часових обмежень.

[1] Balashevska, Y., Kyrylenko, Y., Pecherytsia, O., Shevchenko, I., & Bogorad, V. (2020). Гармонізація методичних підходів та засобів прогнозування радіаційних наслідків у реальному часі. Ядерна та радіаційна безпека, (2(86), 20–26. https://doi.org/10.32918/nrs.2020.2(86).03;

[2] Yu. Balashevska, Yu. Kyrylenko, Z. Ivanov, F. Rocchi, A. Cervone, A. Guglielmelli, M. Ilvonen, J. Rossi, A. Slavickas, H. Thielen (2024), «Comparative analysis of the dispersion modeling and dose projection results performed under BARCO international project», Journal of Environmental Radioactivity, Volume 279, October 2024, 107513, https://doi.org/10.1016/j.jenvrad.2024.107513;

[3] Yu Kyrylenko, Yu Balashevska, Z Ivanov, A Myshkovska, I Shevchenko, O Pecherytsia, Yu Yesypenko and K Siegien (2025), «Expanding the radiation monitoring network as an effective approach to reducing uncertainties in emergency response preparedness during armed conflict», Journal of Radiological Protection, Volume 45, Number 4. https://doi.org/10.1088/1361-6498/ae10c3;

[4] Lam, Remi & Sanchez-Gonzalez, Alvaro & Willson, Matthew & Wirnsberger, Peter & Fortunato, Meire & Pritzel, Alexander & Ravuri, Suman & Ewalds, Timo & Alet, Ferran & Eaton-Rosen, Zach & Hu, Weihua & Merose, Alexander & Hoyer, Stephan & Holland, George & Stott, Jacklynn & Vinyals, Oriol & Mohamed, Shakir & Battaglia, Peter. (2022). GraphCast: Learning skillful medium-range global weather forecasting. 10.48550/arXiv.2212.12794.

[5] H. Hersbach, B. Bell, P. Berrisford, S. Hirahara, A. Horányi, J. Muñoz-Sabater, J. Nicolas, C. Peubey, R. Radu, D. Schepers, et al. The era5 global reanalysis. Quarterly Journal of the Royal Meteorological Society, 146(730):1999–2049, 2020.

[6] Szegvary, T., Conen, F., Stöhlker, U., Dubois, G., Bossew, P., & de Vries, G. (2007). Mapping terrestrial -dose rate in Europe based on routine monitoring data. Radiation Measurements, 42(9), 1561–1572. doi:10.1016/j.radmeas.2007.09.002.

[7] D9.7 – Report on uncertainty reduction in exposure assessment based on environmental monitoring data, including concept for identifying critically exposed groups. EJP-CONCERT European Joint Programme for the Integration of Radiation Protection Research H2020 – 662287.

К.В. Васильєв

ІДЕНТИФІКАЦІЯ ТА ДІАГНОСТИКА ЕЛЕКТРОТЕХНІЧНИХ СИСТЕМ: ПОРІВНЯЛЬНИЙ АНАЛІЗ КЛАСИЧНИХ І ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ

Теорія ідентифікації систем, систематизована Л. Льюнгом, спирається на три компоненти: вибір структури моделі, метод оцінювання параметрів і процедуру валідації [9, с. 1]. Поява керованих силових перетворювачів, гібридних мереж і систем зі стохастичною відновлюваною генерацією зробила лінійне наближення недостатнім для більшості промислово важливих задач [5, с. 7]. Zhao та ін. показали, що невідповідність між обсягом накопичених у SCADA-системах даних і можливостями класичних алгоритмів стала головним стимулом для інтеграції методів глибокого навчання у промислову діагностику [11, с. 1].

Електротехнічні системи поділяються на два рівні: функціональний (перетворення/передача vs. споживання енергії) і за характером процесів (лінійні/нелінійні, стаціонарні/нестаціонарні) [2, с. 33]. Для асинхронних двигунів лінійна модель, побудована при номінальному навантаженні, при частковому завантаженні 30–40% від номіналу дає похибку прогнозу струму до 25–35% — критично для систем векторного керування [3, с. 75]. Силова електроніка є гібридним неперервно-дискретним класом: ключі комутують на частоті 10–200 кГц, що на 2–3 порядки перевищує постійні часи навантаження, тому усереднені моделі не відображають поведінки поблизу частоти комутації [4, с. 55]. Smart Grid потребує розподілених адаптивних методів, здатних опрацьовувати потоки даних від тисяч вимірювальних точок у режимі реального часу [6, с. 3].

Похибка параметрів асинхронного двигуна в 10% призводить до відхилення кута потоку на 5–8° в алгоритмах векторного керування; для синхронних двигунів аналогічна похибка спричиняє вдвічі менше відхилення [2, с. 85]. Нагрів обмотки від 20°C до 80°C збільшує активний опір статора на ~24% (0,4%/°C) — ігнорування цього ефекту є типовою причиною систематичних похибок ідентифікації [3, с. 40]. Гармонічний склад струмів несе унікальну сигнатуру класу навантаження: діодні випрямлячі генерують непарні гармоніки 5-го, 7-го і 11-го порядків, насичені трансформатори — 3-тю і 5-ту, що є основою технології NILM [16, с. 16838].

Класичний МНК при порушенні умов незміщеності (системи зі зворотним зв'язком) замінюють інструментальними змінними або узагальненим МНК. Рекурсивний МНК (RLS) із $\lambda = 0.98$ підтримує «вікно пам'яті» ~50 кроків і скорочує обчислювальні витрати з $O(n^3)$ до $O(n^2)$ [1, с. 95]. Sigma-point фільтр (UKF) демонструє нижчу похибку оцінки параметрів порівняно з лінеаризованим EKF у нелінійних режимах пуску і гальмування [10, с. 187]. За методом DGA для трансформаторів перевищення концентрації

ацетилену понад 35 мкл/л сигналізує про дуговий розряд; трикутник Дюваля класифікує тип дефекту з похибкою 10–15% [7, с. 25].

Традиційні методи мають сім системних обмежень: (1) лінійне наближення неадекватне для асинхронного двигуна в широкому діапазоні навантаження; (2) критерії AIC/BIC не гарантують правильного вибору порядку моделі для коротких вибірок [9, с. 490]; (3) умова стійкості збудження (PE) порушується при природному вузькосмуговому навантаженні вентиляторів і насосів [1, с. 140]; (4) масштабованість — кількість параметрів MIMO-моделей зростає як $n^2 \cdot m$; (5) ручне проектування ознак: якість діагностики цілком залежить від досвіду інженера; (6) відсутність накопичення досвіду між сесіями ідентифікації; (7) неможливість використання великих ретроспективних масивів SCADA для навчання [11, с. 1].

CNN при застосуванні до вейвлет-спектрограм вібраційних сигналів підшипників забезпечує точність класифікації несправностей 98–99% проти 90–93% у класичного SVM — Lei та ін. пов'язують різницю зі здатністю CNN виявляти тонкі міжчастотні залежності [8, с. 8]. LSTM і GRU точніше відтворюють перехідні процеси при різких змінах навантаження, де лінеаризована модель систематично відхиляється від реальної траєкторії [12, с. 374]. Трансформерна архітектура через механізм self-attention динамічно зосереджується на найбільш інформативних часових сегментах незалежно від відстані у послідовності [13, с. 5998].

Physics-Informed Neural Networks (PINN) навчаються одночасно мінімізувати похибку на вимірюваних даних і нев'язку диференціальних рівнянь об'єкта; Raissi та ін. довели здатність PINN розв'язувати обернені задачі ідентифікації з вищою точністю при значно меншій кількості вимірювань [15, с. 686]. Переносне навчання (TL) скорочує потрібний обсяг розмічених прикладів несправностей на 1–2 порядки [11, с. 15]. Методи без учителя — автоенкодери та GAN — вирішують проблему відсутності розмічених прикладів дефектів: GAN генерують синтетичні несправності для балансування малих навчальних вибірок. LIME (Ribeiro та ін., 2016) забезпечує локальне пояснення рішень складних класифікаторів — критична умова для практичного впровадження в системах безпеки [14, с. 1135].

Порівняльний аналіз виявляє чіткий розподіл зон ефективності. RLS із температурною компенсацією для асинхронних двигунів малої потужності дає похибку ідентифікації менше 3–5% без навчання — прийнятний результат для лінійних об'єктів [5, с. 230]. Методи глибокого навчання принципово ефективніші при нелінійній нестаціонарній поведінці і великих ретроспективних масивах, але чисто data-driven підходи страждають від низької узагальнюючої здатності при зміні конфігурації об'єкта. PINN через вбудовані фізичні обмеження долають цей недолік і є найбільш перспективним гібридним напрямком [15, с. 686].

Відкритими залишаються: стандартизація оцінки якості PINN-моделей для конкретних класів електромеханічних об'єктів; кількісна характеристика невизначеності прогнозів (uncertainty quantification); розроблення методів

пояснення для критичної інфраструктури. Наукова задача: розроблення гібридних методів ідентифікації та діагностики електротехнічних систем, що поєднують аналітичні методи теорії ідентифікації з алгоритмами машинного навчання і забезпечують підвищену точність оцінки параметрів, автоматичне вилучення ознак, навчання за обмеженими вибірками і фізичну інтерпретованість рішень [1, с. 230].

[1] Tangirala A. K. Principles of System Identification: Theory and Practice. Boca Raton : CRC Press, 2015. 560 p.
[2] Keesman K. J. System Identification: An Introduction. London : Springer, 2011. 333 p.
[3] Chatzi E., Papadimitriou C. Identification Methods for Structural Health Monitoring. Cham : Springer, 2016. 302 p.
[4] Kutsenko O., Bezmenov M. Identification of Linear Dynamic Systems in the Environment of Polynomial Signals. Kharkiv : NTU «KhPI», 2022. 180 p.
[5] Nelles O. Nonlinear System Identification. 2nd ed. Cham : Springer, 2020. 785 p.
[6] Morello S. A., De Donno M. C. Smart Grid Technologies. IEEE Industrial Electronics Magazine. 2019. Vol. 13, No. 1. P. 1–10.
[7] CIGRE Working Group A2.34. Guide for Transformer Maintenance. Paris : CIGRE, 2011. 200 p.
[8] Lei Y. et al. Applications of Machine Learning to Machine Fault Diagnosis. Mechanical Systems and Signal Processing. 2020. Vol. 138. P. 1–39.
[9] Ljung L. System Identification: Theory for the User. 2nd ed. Upper Saddle River : Prentice Hall, 1999. 672 p.
[10] Simon D. Optimal State Estimation. Hoboken : Wiley, 2006. 552 p.
[11] Zhao R. et al. Deep Learning and Its Applications to Machine Health Monitoring. Mechanical Systems and Signal Processing. 2019. Vol. 115. P. 1–20.
[12] Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 775 p.
[13] Vaswani A. et al. Attention Is All You Need. NeurIPS. 2017. Vol. 30. P. 5998–6008.
[14] Ribeiro M. T., Singh S., Guestrin C. «Why Should I Trust You?». Proc. 22nd ACM SIGKDD. 2016. P. 1135–1144.
[15] Raissi M., Perdikaris P., Karniadakis G. E. Physics-Informed Neural Networks. Journal of Computational Physics. 2019. Vol. 378. P. 686–707.
[16] Zoha A. et al. Non-Intrusive Load Monitoring: A Survey. Sensors. 2012. Vol. 12, No. 16. P. 16838–16866.

О.В. Згуровець, Д.С. Матушкін

ІМІТАЦІЙНА МОДЕЛЬ АКУМУЛЯТОРНОЇ СИСТЕМИ НАКОПИЧЕННЯ ЕНЕРГІЇ

В умовах воєнного стану та підвищених ризиків пошкодження енергетичної інфраструктури актуальним є завдання забезпечення безперервного електроживлення критичних споживачів, особливо об'єктів, для яких короткочасне зникнення напруги призводить до порушення технологічних процесів, втрати даних та зупинки обладнання.

Традиційні рішення резервного живлення на основі дизель-генераторів або класичних джерел безперебійного живлення обмежено забезпечують одночасне досягнення швидкодії, автономності та якості вихідної напруги за прийнятного ресурсу акумуляторних батарей. Найбільш критичними є режими з різкими змінами навантаження, короткочасними піковими струмами та переходом від мережевого живлення до автономного. Для таких режимів застосовують модульні накопичувачі енергії з проміжною ланкою постійного струму, інверторним перетворювачем та можливістю інтеграції суперконденсаторного буфера для покриття швидких перехідних процесів [1-3].

Необхідним етапом розроблення таких систем є імітаційне моделювання, яке дає змогу дослідити електромагнітні процеси в акумуляторному накопичувачі, проміжній ланці постійного струму, інверторі та навантаженні без ризику для реального обладнання. Моделювання дає змогу оцінити працездатність структури накопичувача, характер перехідних процесів у разі втрати зовнішнього живлення, здатність акумуляторної батареї підтримувати напругу проміжної ланки та якість вихідної напруги інвертора в автономному режимі. Воно також є основою для вибору раціональної структури модульного накопичувача та синтезу алгоритмів керування й розподілу енергії, спрямованих на забезпечення тривалої та надійної роботи системи [4,5].

Метою роботи є побудова та дослідження імітаційної моделі акумуляторної системи накопичення енергії для оцінювання сценаріїв живлення навантаження в мережевому та автономному режимах.

На рис. 1 наведено імітаційну модель акумуляторної системи накопичення енергії. Модель складається з чотирьох функціональних підсистем: підсистеми акумуляторного накопичувача, підсистеми зовнішньої мережі, інверторної підсистеми та підсистеми навантаження.

Акумуляторна підсистема реалізована на основі $LiFePO_4$-батареї та двонапрямленого перетворювача постійної напруги, який забезпечує енергетичний обмін між батареєю та проміжною ланкою постійного струму інверторного блоку. За наявності зовнішнього живлення перетворювач може працювати в напрямі заряджання акумуляторної батареї, а у разі його зникнення або дефіциту енергії в ланці постійного струму – у напрямі

розряджання батареї з підтриманням напруги проміжної ланки. Керування напрямом потоку енергії здійснюється сигналами *charge_mode* та *discharge_mode*.

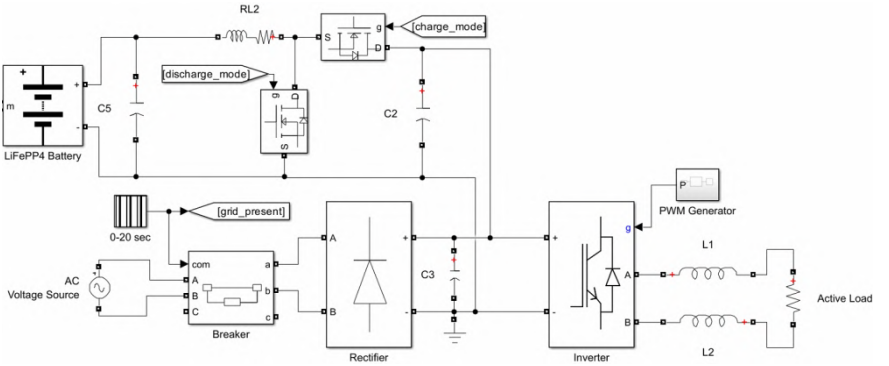


Рисунок 1 – Імітаційна модель акумуляторної системи накопичення енергії в середовищі MATLAB/Simulink

Підсистема зовнішньої мережі представлена джерелом змінної напруги та вимикачем, який використовується для імітації наявності або зникнення мережевого живлення. Сигнал *grid_present* задає режим роботи вимикача і дає змогу моделювати як перехід системи до автономного живлення, так і подальшу автономну роботу. Далі змінна напруга подається на інверторну підсистему.

Інверторна підсистема містить випрямляч, ланку постійного струму, інверторний перетворювач і генератор сигналів широтно-імпульсної модуляції. Випрямляч перетворює змінну напругу мережі в постійну напругу проміжної ланки, а інвертор виконує зворотне перетворення – постійної напруги в змінну для живлення навантаження. Формування керуючих імпульсів широтно-імпульсної модуляції здійснюється блоком *PWM Generator* на основі синусоїдального опорного сигналу.

Підсистема навантаження має активний характер, що дає змогу використати модель як базовий тестовий варіант для первинної оцінки працездатності системи, без додаткового впливу реактивної або нелінійної складової споживання.

У межах моделі досліджуються три характерні режими роботи:

- мережевий режим – живлення активного навантаження від зовнішньої мережі через випрямляч та інвертор з одночасним заряджанням акумуляторної батареї;
- перехідний процес – відключення зовнішнього джерела та перемикання системи на живлення від акумуляторної батареї;
- автономний режим – підтримання напруги ланки постійного струму від акумуляторної батареї та живлення активного навантаження.

Основними контрольованими параметрами є напруга акумуляторної батареї, струм батареї, стан заряду, напруга та струм у ланці постійного струму, вихідна напруга інвертора та струм навантаження.

У такій постановці модель дає змогу оцінити узгодженість роботи акумуляторної батареї, випрямляча, ланки постійного струму та інверторного перетворювача. Особливий інтерес становлять перехідні процеси під час зміни джерела живлення, оскільки саме в ці моменти визначається здатність накопичувача підтримувати напругу ланки постійного струму та забезпечувати безперервність живлення активного навантаження.

Розроблена модель є основою для подальшого розвитку системи, що передбачає введення додаткових елементів, зокрема суперконденсаторного буфера та нелінійних навантажень, а також ускладнення алгоритмічного забезпечення в частині пріоритезації навантажень та узгодженого керування потоками енергії між накопичувальними елементами.

[1] Jing, W., Lai, C. H., Wong, W. S. H., & Wong, M. L. D. (2017). Battery-supercapacitor hybrid energy storage system in standalone DC microgrids: A review. IET Renewable Power Generation, 11(4), 461–469. https://doi.org/10.1049/iet-rpg.2016.0500

[2] Lahyani, A., Venet, P., Guermazi, A., & Troudi, A. (2013). Battery/supercapacitors combination in uninterruptible power supply (UPS). IEEE Transactions on Power Electronics, 28(4), 1509–1522. https://doi.org/10.1109/TPEL.2012.2210736

[3] Khalid, M. (2019). A review on the selected applications of battery-supercapacitor hybrid energy storage systems for microgrids. Energies, 12(23), 4559. https://doi.org/10.3390/en12234559

[4] Sinha, S., & Bajpai, P. (2020). Power management of hybrid energy storage system in a standalone DC microgrid. Journal of Energy Storage, 30, 101523. https://doi.org/10.1016/j.est.2020.101523

[5] Bharatee, A., Ray, P. K., Subudhi, B., & Ghosh, A. (2022). Power management strategies in a hybrid energy storage system integrated AC/DC microgrid: A review. Energies, 15(19), 7176. https://doi.org/10.3390/en15197176

В.В. Станиціна

ОБҐРУНТУВАННЯ СТАВКИ ДИСКОНТУ ПРИ ВИЗНАЧЕННІ СЕРЕДНЬОЗВАЖЕНОЇ СОБІВАРТОСТІ ТЕПЛОВОЇ ЕНЕРГІЇ ЗА ЖИТТЄВИЙ ЦИКЛ ДЛЯ ТЕПЛОПОСТАЧАННЯ УКРАЇНИ

Теплопостачання є важливою складовою енергетики України, яка нині зазнає суттєвих технологічних, економічних та організаційних змін. Для порівняння різнорідних теплогенеруючих технологій у системах теплопостачання дедалі ширше застосовується показник середньозваженої собівартості теплової енергії за життєвий цикл (Levelised Cost of Heat - LCOH). Його методична перевага полягає в тому, що різночасові капітальні, паливні, експлуатаційні та інші витрати приводяться до єдиної розрахункової одиниці теплової енергії, що дає змогу порівнювати технології з різною структурою витрат.

У міжнародних джерелах LCOH застосовується для оцінювання теплогенеруючих технологій різної потужності та різного типу теплопостачання: як для систем централізованого теплопостачання з біомасовим водогрійним котлом тепловою потужністю 20 МВт [1], для побутових теплових насосів типу «повітря–повітря» і «повітря–вода» у порівнянні з газовими котлами [2], так і для систем із розрахунковим тепловим навантаженням 1 МВт та змінним профілем навантаження від 0,2 до 1 МВт [3].

У методичних матеріалах JASPERS з оцінювання проєктів теплопостачання розрізняють фінансовий та соціально-економічний LCOH [1]. Фінансовий LCOH розраховується у ринкових цінах і відображає витрати, які несе інвестор або теплопостачальне підприємство: капітальні вкладення, експлуатаційні витрати, витрати на паливо чи електроенергію, а також передбачені платежі за викиди. Для когенераційних установок додатково можуть враховуватися доходи від продажу електроенергії [1]. Такий показник доцільний для оцінювання вартості варіанта з позиції підприємства або власника проєкту.

Соціально-економічний LCOH розраховується з позиції суспільства і, крім прямих витрат, може враховувати зовнішні ефекти: вартість викидів CO_2, SO_2, NO_x, твердих частинок, ризики енергетичної безпеки та економічну цінність супутньої електроенергії у разі когенерації [1]. Тому цей показник доцільний для порівняння варіантів розвитку систем теплопостачання, коли важливо оцінити не лише витрати підприємства, а й ширші наслідки для економіки, довкілля та суспільства.

Фінансовий LCOH може слугувати орієнтовним індикатором економічно необхідної вартості теплової енергії, однак не є тотожним тарифу. Тариф визначається за окремими регуляторними правилами, що відрізняються від методики розрахунку LCOH за порядком урахування амортизації, прибутку, джерел фінансування інвестицій, грантової чи

бюджетної підтримки, а для когенерації – також розподілу витрат між виробництвом теплової та електричної енергії [1]. Тому LCOH доцільно застосовувати передусім для порівняльного оцінювання варіантів розвитку систем теплопостачання.

Один із параметрів, що істотно впливає на результат розрахунку LCOH, – це ставка дисконтування. Вона використовується для приведення майбутніх витрат до вартості у базовому році розрахунку. При цьому ставка дисконтування має відповідати тому, у яких цінах подано витрати. Якщо витрати наведено у постійних цінах базового року, без урахування майбутньої інфляції, застосовують реальну ставку дисконтування. Якщо ж у розрахунку використовують прогнозні ціни майбутніх років, які вже включають очікувану інфляцію, застосовують номінальну ставку дисконтування [4-5]. Невідповідність між видом цін і типом ставки дисконтування може спотворювати приведену вартість витрат за життєвий цикл.

У джерелах, що безпосередньо стосуються оцінювання вартості тепла, використовуються різні ставки дисконтування залежно від типу об'єкта та мети оцінювання. У методичних матеріалах JASPERS для систем централізованого теплопостачання LCOH використовується як інструмент порівняння технологічних варіантів, а фінансовий і соціально-економічний LCOH розглядаються як окремі показники оцінювання [1]. Міжнародне енергетичне агентство для порівняння вартості тепла від теплових насосів і газових котлів використовує ставку 3%, однак без чіткого уточнення, чи вона є реальною, чи номінальною [2]. Національна лабораторія відновлюваної енергетики США у розрахунках LCOH для відновлюваних теплових систем і теплового навантаження 0,2–1 МВт застосовує 10%, що доцільно трактувати як фінансове припущення для високоризикової технології [3].

Для вибору типу ставки важливими є також загальні методичні джерела з оцінювання енергетичних та інфраструктурних проєктів. Європейська Комісія для розрахунків у постійних цінах рекомендує застосовувати 4% реальної фінансової ставки дисконтування для фінансового аналізу інвестиційних проєктів, а для соціально-економічного аналізу – 5% для держав-членів ЄС, що отримують підтримку в межах політики згуртування ЄС, і 3% – для інших держав-членів ЄС [4]. У США Національний інститут стандартів і технологій та Федеральна програма енергоменеджменту для аналізу вартості життєвого циклу енергетичних проєктів у федеральних будівлях у 2025 р. наводять обидва значення: 3,0% реальної та 4,5% номінальної ставки дисконтування [5]. У Канаді Секретаріат Ради казначейства для аналізу вигід і витрат регуляторних пропозицій використовує 7% реальної ставки як оцінку альтернативної вартості капіталу, а для окремих соціально значущих ефектів допускає нижчу соціальну ставку, близьку до 3% [6]. Це підтверджує, що вибір між реальною та номінальною ставкою має залежати не від типу технології, а від виду цін у розрахунку.

Для України спеціальної нормативно встановленої ставки дисконтування саме для розрахунку LCOH у теплопостачанні наразі не

виявлено. Водночас у матеріалах JASPERS щодо економічного оцінювання публічних інвестицій в Україні зазначено, що для оцінювання проєктів застосовується соціальна ставка дисконтування 5% [7]. Крім того, Міжнародне енергетичне агентство у розрахунках економії енергетичних витрат для заходів з енергоефективності типової багатоквартирної будівлі в Україні використовує період 20 років і ставку дисконтування 5% [8]. Це дає підстави розглядати 5% реальної ставки дисконтування як можливий базовий орієнтир для соціально-економічної оцінки проєктів у сфері теплопостачання України.

Для оцінювання витрат варіантів розвитку відновлюваної енергетики, зокрема у теплопостачанні, IRENA у регіональному дослідженні для Центральної та Південно-Східної Європи 2020 р., до якого включено Україну, використовує соціальну ставку дисконтування 4%, а в аналізі чутливості додатково розглядає ставки 9% і 14% [10]. У попередньому дослідженні IRENA для України 2015 р. для оцінювання вартості заміщення у секторах, зокрема у теплопостачанні, використовувалася ставка 10% [9]. Оскільки розрахунки у дослідженні 2015 р. подано у доларах США у цінах 2010 року, застосована ставка 10% за змістом ближча до реальної ставки дисконтування, хоча її тип прямо не визначено.

Проведені розрахунки LCOH за різних реальних ставок дисконту [11-12] показали, що вплив цього параметра істотно залежить від структури витрат теплогенеруючої технології. Для котельних установок на органічному паливі та біопаливі, у яких основну частку витрат формує паливо, підвищення ставки дисконтування з 5 до 10% призводить лише до помірного зростання LCOH – до 5%. Натомість для теплових насосів різного типу, де значною є інвестиційна складова, таке саме підвищення ставки може збільшувати LCOH на 20–70% залежно від типу установки, її потужності, вартості обладнання та умов експлуатації.

Таким чином, вибір ставки дисконтування особливо суттєво впливає на оцінювання капіталомістких технологій, насамперед теплових насосів. Оскільки такі технології є енергоефективними та можуть сприяти скороченню споживання органічного палива, а також зменшенню прямих викидів CO_2 і забруднюючих речовин у місці виробництва теплової енергії, вибір ставки дисконтування для них потребує окремого обґрунтування, а аналіз чутливості доцільно розглядати як необхідний елемент такого оцінювання.

У розрахунках LCOH для систем теплопостачання доцільно не лише обґрунтовувати розмір ставки дисконтування, а й чітко зазначати її тип – реальна чи номінальна. Для соціально-економічної оцінки варіантів розвитку теплопостачання в Україні можливим орієнтиром може бути реальна ставка в діапазоні 4–5%, що узгоджується з підходами, використаними у матеріалах JASPERS, IEA та IRENA. Вищі значення доцільно розглядати як сценарії підвищеної вартості капіталу, інвестиційного ризику або як елементи аналізу чутливості. Особливо важливим обґрунтування це є для капіталомістких технологій, зокрема теплових насосів, для яких зміна розміру ставки

дисконтування істотно впливає на LCOH і висновки щодо конкурентоспроможності та доцільності впровадження.

[1] JASPERS. (2024). JASPERS guide to decarbonisation of district heating systems. European Investment Bank. https://jaspers.eib.org/files/library/2024/jaspers-guide-to-decarbonisation-of-district-heating-systems.pdf

[2] International Energy Agency. (2022). Levelised cost of heating for air-to-air and air-to-water heat pumps and gas boilers for selected countries, and sensitivity to fuel prices, H1 2021–H1 2022. IEA, Paris.

[3] Akar, S., Kurup, P., Belding, S., McTigue, J., Cox, J., Boyd, M., McMillan, C., Lowder, T., & Baldwin, S. (2022). Renewable thermal energy systems designed for industrial process solutions in multiple industries: Preprint (NREL/CP-7A40-81147). National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy22osti/81147.pdf

[4] European Commission. (2014). Guide to cost-benefit analysis of investment projects: Economic appraisal tool for Cohesion Policy 2014–2020. Publications Office of the European Union. https://ec.europa.eu/regional_policy/sources/studies/cba_guide.pdf

[5] Kneifel, J., Parekh, P., & Lavappa, P. (2025). Energy price indices and discount factors for life-cycle cost analysis – 2025: Annual supplement to NIST Handbook 135 (NIST IR 85-3273-40). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.85-3273-40

[6] Treasury Board of Canada Secretariat. (2022). Canada's cost-benefit analysis guide for regulatory proposals. Government of Canada. https://publications.gc.ca/collections/collection_2022/sct-tbs/BT58-5-2022-eng.pdf

[7] JASPERS. (2024). Ukraine: Economic appraisal and public investment management. European Investment Bank. https://jaspers.eib.org/files/activities/2024/5-ukraine-economic-appraisal-and-public-investment-management-martin-pospisil.pdf

[8] International Energy Agency. (2025). Energy cost savings and upfront investments for different energy efficiency upgrades in a typical multi-family building in Ukraine under current energy tariffs. IEA, Paris.

[9] International Renewable Energy Agency. (2015). REmap 2030: Renewable energy prospects for Ukraine. IRENA.

[10] International Renewable Energy Agency. (2020). Renewable energy prospects for Central and South-Eastern Europe Energy Connectivity (CESEC). IRENA.

[11] Stanytsina, V., Horskyi, V., Danyliv, S., Zaporozhets, A., Kovtun, S., Maevsky, O., Garbuz, I., & Artemchuk, V. (2025). Comparative analysis of levelized cost of heat in implemented and calculated heat supply systems with heat pumps in Ukraine. Energies, 18(5), 1110. https://doi.org/10.3390/en18051110

[12] Станиціна, В. В., Куц, Г. О., Тесленко, О. І., & Маляренко, О. Є. (2020). Порівняльний аналіз середньої вартості теплової енергії, виробленої в котельнях різної потужності, з урахуванням екологічної складової. Енерготехнології та ресурсозбереження, (2), 55–62. https://doi.org/10.33070/etars.2.2020.07

О.В. Матухно, В.В. Станиціна, В.О. Артемчук

ОЦІНЮВАННЯ КЛІМАТИЧНОЇ ПОЛІТИКИ ДЛЯ РІШЕНЬ У СФЕРІ ЕНЕРГЕТИЧНОГО ПЕРЕХОДУ

Низьковуглецева трансформація енергетики потребує не лише визначення кліматичних цілей, а й створення інструментів для їх прозорого оцінювання, порівняння та моніторингу. У цьому контексті особливого значення набувають системи підтримки прийняття рішень, які дають змогу поєднувати різнорідні показники кліматичної політики, енергетичного переходу, інституційної спроможності та економічних механізмів у єдину систему оцінювання.

Методологічні засади побудови такого оцінювання мають спиратися на загальні принципи формування композитних індикаторів: визначення мети оцінювання, відбір показників, нормування даних, вибір вагових коефіцієнтів, агрегування часткових оцінок і перевірку стійкості результатів [1]. Водночас вибір методів вагування й агрегування може істотно впливати на підсумкові оцінки, тому система оцінювання не повинна бути «чорним ящиком», а має забезпечувати прозорість розрахунків і можливість інтерпретації внеску окремих складових [2].

Наявні міжнародні підходи до оцінювання кліматичної політики, зокрема Climate Change Performance Index [3], Climate Action Tracker [4], Climate Laws, Institutions and Measures Index [5] та Climate Policy Measure Index [6], охоплюють різні аспекти її результативності. Одні з них більшою мірою орієнтовані на фактичні результати скорочення викидів, розвиток відновлюваної енергетики й енергоефективність, інші – на відповідність кліматичних цілей міжнародним зобов'язанням, якість інституційної рамки або застосування ринкових інструментів. Отже, для підтримки управлінських рішень доцільним є не механічне використання одного індексу, а формування інтегрованого підходу до оцінювання, який поєднує результативні, інституційні, інструментальні та фінансові характеристики політики.

Запропонований підхід ґрунтується на тому, що ефективність кліматичної політики не можна оцінювати лише за одним показником, наприклад за обсягами скорочення викидів або наявністю вуглецевого ціноутворення. Для більш збалансованої оцінки доцільно враховувати п'ять груп характеристик: фактичні результати у сфері викидів парникових газів; зміни в енергетичному секторі, зокрема розвиток відновлюваної енергетики та підвищення енергоефективності; якість законодавчої та інституційної основи кліматичної політики; наявність економічних інструментів, зокрема вуглецевого ціноутворення; а також фінансові, адаптаційні та міжнародні умови її реалізації. Такий підхід дозволяє оцінювати не лише досягнуті результати, а й спроможність країни забезпечувати довгострокову реалізацію кліматичної політики.

Практична реалізація запропонованого підходу передбачає кілька

послідовних процедур. Спочатку формується набір вхідних показників, які характеризують як кількісні результати кліматичної політики, так і якісні умови її реалізації. До кількісних показників можуть належати обсяги викидів парникових газів, вуглецева та енергетична інтенсивність економіки, частка відновлюваних джерел енергії, рівень вуглецевого ціноутворення та обсяги кліматичного фінансування. Якісні показники відображають наявність кліматичного законодавства, стратегічних планів, відповідальних інституцій, механізмів координації, громадського залучення та міжнародної співпраці. Для України доцільним є також урахування екологічних витрат у блоці енергоефективності та ресурсної оцінки, оскільки такі витрати можуть впливати на розрахунок показників енергетичної ефективності та потенціалів енергозбереження [7].

Після відбору показників вони мають бути приведені до порівнюваного вигляду, наприклад до шкали від 0 до 1, із урахуванням напряму бажаної зміни: для одних показників кращими є вищі значення, для інших – нижчі [1]. Далі визначаються правила вагування та агрегування, тобто спосіб поєднання окремих показників у блокові та узагальнені оцінки. Водночас для системи підтримки прийняття рішень доцільно не обмежуватися лише підсумковим балом, а зберігати профіль оцінювання за окремими складовими, щоб бачити сильні й слабкі сторони кліматичної політики. Завершальним етапом є перевірка стійкості результатів за різних схем вагування, складу показників, базових років або джерел даних, що відповідає вимогам до робастності композитних індикаторів [2].

Практичне значення запропонованого підходу полягає у можливості його використання як основи для створення інформаційно-аналітичного модуля оцінювання кліматичної політики для рішень у сфері енергетичного переходу. Такий модуль може забезпечувати введення й оновлення даних, автоматизоване нормування показників, розрахунок блокових та інтегральних оцінок, візуалізацію профілю кліматичної політики, а також тестування альтернативних сценаріїв вагування. Зв’язок оцінювання кліматичної політики з інструментами моделювання управлінських рішень може бути проілюстрований дослідженнями, у яких регулювання викидів парникових газів розглядається як взаємодія джерел викидів і регулятора в межах ігрової моделі [8].

Отже, запропонований підхід до оцінювання кліматичної може розглядатися як крок від порівняльного аналізу міжнародних індексів до створення прикладних систем підтримки прийняття рішень. Він дозволяє поєднати різнорідні показники у прозору аналітичну структуру, забезпечити зіставність оцінок, виявити сильні та слабкі сторони кліматичної політики, а також підвищити обґрунтованість рішень щодо низьковуглецевої трансформації енергетики.

[1] OECD, & European Commission Joint Research Centre. (2008). Handbook on constructing composite indicators: Methodology and user guide. OECD Publishing. https://doi.org/10.1787/9789264043466-en

[2] Greco, S., Ishizaka, A., Tasiou, M., & Torrisi, G. (2019). On the methodological framework of composite indices: A review of the issues of weighting, aggregation, and robustness. Social Indicators Research, 141, 61–94. https://doi.org/10.1007/s11205-017-1832-9

[3] Burck, J., Uhlich, T., Bals, C., Höhne, N., & Nascimento, L. (2023). Climate Change Performance Index 2024: Results. Germanwatch, NewClimate Institute, & Climate Action Network International. https://ccpi.org/download/climate-change-performance-index-2024/

[4] Climate Action Tracker. (2024). CAT rating methodology. Climate Analytics & NewClimate Institute. https://climateactiontracker.org/methodology/cat-rating-methodology/

[5] Steves, F., & Teytelboym, A. (2013). Political economy of climate change policy (Smith School Working Paper No. 13-02). University of Oxford. https://doi.org/10.2139/ssrn.2456538

[6] Dieler, J. (2016). Effectiveness of climate policies: Empirical methods and evidence (ifo Beiträge zur Wirtschaftsforschung, Vol. 68). ifo Institute. https://www.ifo.de/DocDL/ifo_Beitraege_z_Wifo_68.pdf

[7] Станиціна В.В. (2012). Врахування екологічних витрат при визначенні показників енергетичної ефективності та потенціалів енергозбереження в галузях та регіонах. Проблеми загальної енергетики, 1 (28), 62-68. https://systemre.org/index.php/journal/article/view/450

[8] Maevsky, O., Kovalchuk, M., Brodsky, Y., Stanytsina, V., & Artemchuk, V. (2024). Game-theoretic modeling in regulating greenhouse gas emissions. Heliyon, 10(9), e30549. https://doi.org/10.1016/j.heliyon.2024.e30549

А.А. Ублінських

ВИКОРИСТАННЯ БЛОКЧЕЙНУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА ПРОЗОРОСТІ ДАНИХ У СИСТЕМАХ PEER-TO-PEER ТОРГІВЛІ ЕЛЕКТРОЕНЕРГІЄЮ

Цифрова трансформація енергетики пов'язана з переходом від централізованої моделі електропостачання до більш гнучких і децентралізованих систем. Поширення відновлюваних джерел енергії, локальних сонячних електростанцій, систем накопичення та розумних лічильників сприяє появі активних споживачів, які можуть одночасно виробляти й споживати електроенергію. Таких учасників часто називають prosumer-учасниками.

Одним із практичних середовищ для розвитку цієї моделі є micro-grid. Micro-grid можна розглядати як локальну енергетичну систему, що об'єднує споживачів, виробників, накопичувачі енергії, засоби обліку та цифрову платформу керування. У межах такої системи можлива peer-to-peer торгівля електроенергією, коли учасники продають надлишкову електроенергію іншим учасникам локальної мережі без повної залежності від централізованого посередника [1].

Основна проблема такої моделі полягає в необхідності довіри до даних. Для коректної роботи P2P-торгівлі потрібно точно фіксувати обсяги виробництва, споживання, заявки на купівлю та продаж, умови угод, час виконання транзакцій і результати фінансових розрахунків. Якщо ці дані можна непомітно змінити або якщо учасники не мають можливості перевірити історію операцій, виникають ризики неправильних нарахувань та втрати довіри до всієї системи.

Метою роботи є обґрунтування ідеї використання блокчейну для забезпечення цілісності, прозорості та перевірюваності даних у системах peer-to-peer торгівлі електроенергією в micro-grid.

Блокчейн у такій системі може виконувати роль розподіленого реєстру енергетичних транзакцій. До нього можуть записуватися факти укладення P2P-угод, підсумкові дані про купівлю-продаж електроенергії, часові мітки, результати розрахунків і дії смартконтрактів. Головна цінність блокчейну полягає в тому, що після додавання запису його складно змінити непомітно для інших учасників. Це створює основу для прозорого аудиту та незалежної перевірки операцій [2].

Запропонована ідея не передбачає зберігання всіх технічних даних безпосередньо в блокчейні. Дані з розумних лічильників можуть бути великими за обсягом і чутливими з погляду приватності. Тому доцільним є комбінований підхід: детальні вимірювання зберігаються поза блокчейном, а в блокчейн записується хеш, підтвердження або підсумкова транзакція. Це дозволяє зменшити навантаження на систему та водночас зберегти можливість перевірити, чи не були змінені вихідні дані.

Смартконтракти можуть бути використані як програмний механізм автоматизації правил торгівлі. Вони здатні реєструвати заявки на продаж і купівлю електроенергії, перевіряти умови угоди, фіксувати факт її укладення, розраховувати вартість електроенергії та записувати результат у блокчейн. У micro-grid це дозволяє зменшити потребу в ручному адмініструванні та підвищити прозорість взаємодії між незалежними учасниками [3].

Узагальнена модель може працювати так: розумні лічильники фіксують виробництво та споживання електроенергії; учасники формують заявки на купівлю або продаж; цифрова платформа передає умови угоди до смартконтракту; смартконтракт перевіряє правила операції; після підтвердження транзакція або її криптографічне підтвердження записується в блокчейн. У результаті кожен учасник може перевірити історію операцій і переконатися в цілісності записів.

Перевагами такого підходу є підвищення прозорості P2P-торгівлі, захист історії транзакцій від непомітної зміни, можливість незалежної перевірки даних, автоматизація розрахунків і зменшення залежності від єдиного центру довіри. Водночас блокчейн не усуває всіх ризиків. Практичне впровадження потребує достовірних даних від розумних лічильників, захисту персональної інформації, безпечного проєктування смартконтрактів, урахування масштабованості та відповідності енергетичному регулюванню. Питання кібербезпеки micro-grid залишаються критично важливими, оскільки компрометація первинних пристроїв може вплинути на якість усіх подальших цифрових записів [4].

Отже, використання блокчейну в системах peer-to-peer торгівлі електроенергією на основі micro-grid є перспективною ідеєю для підвищення довіри, прозорості та інформаційної безпеки локальних енергетичних ринків. Блокчейн у цьому випадку слід розглядати не як заміну фізичної енергетичної інфраструктури, а як цифровий рівень фіксації, перевірки та аудиту даних, необхідних для справедливої взаємодії між учасниками.

[1] Tushar, W., Saha, T. K., Yuen, C., Smith, D., & Poor, H. V. (2020). Peer-to-Peer Trading in Electricity Networks: An Overview. IEEE Transactions on Smart Grid, 11(4), 3185–3200. https://doi.org/10.1109/tsg.2020.2969657

[2] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143–174. https://doi.org/10.1016/j.rser.2018.10.014

[3] Vieira, G., & Zhang, J. (2021). Peer-to-peer energy trading in a microgrid leveraged by smart contracts. Renewable and Sustainable Energy Reviews, 143, 110900. https://doi.org/10.1016/j.rser.2021.110900

[4] Jamil, N., Qassim, Q. S., Bohani, F. A., Mansor, M., & Ramachandaramurthy, V. K. (2021). Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research. Applied Sciences, 11(21), 9812. https://doi.org/10.3390/app11219812

В.В. Шкарупило, В.В. Душеба, Т.А. Зайко, В.В. Шкарупило

МОДЕЛЬНО-ОРІЄНТОВАНА МЕТОДИКА ОЦІНЮВАННЯ РЕЗИЛІЄНТНОСТІ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Триваюче неспровоковане повномасштабне вторгнення країни-агресора обумовлює значимість розвинення теоретичних засад забезпечення резилієнтності критичних інфраструктур, у тому числі таких, на основі яких забезпечується належне функціонування електроенергетичної системи держави. Стосовно означеного доречно зауважити, що небажаний системний деструктивний вплив на електроенергетичну систему України охоплює і фізичний [1], і кібернетичний рівні [2]. Це, у свою чергу, слугує обґрунтуванням важливості розроблення і застосування дієвих інструментальних засобів оцінювання показників резилієнтності критичних систем. У складі таких засобів варто виокремити комп'ютерну модель електроенергетичної системи України, яку вже було успішно застосовано у якості дієвого програмного засобу оцінювання резилієнтності [3].

За результатами проведеного аналізу існуючих напрацювань у частині розвинення резилієнтності критичних систем було підсумовано, що відповідні засоби, підходи, рішення можна узагальнити наступним чином: такі, що полягають у доопрацюванні і забезпеченні структурної мінливості електроенергетичних систем [4], і рішення, що полягають у впровадженні на регіональному, загальнодержавному і міжнародному рівнях відповідних політик та/або стратегій [5]. Окремої уваги заслуговує залучення засобів глибинного навчання у контексті уніфікованої моделі резилієнтності для отримання оціночних значень відповідних показників [6].

Згідно раніше представленої тривимірної концепції аналізу ризиків, що постають у наші дні перед критичною електроенергетичною інфраструктурою [7], розроблено модельно-орієнтовану методику оцінювання резилієнтності. Методика базується на кількісному оцінюванні здатності до поглинання (absorption) системою небажаного деструктивного впливу. Вона полягає у проведенні імітаційного моделювання на основі згаданої вище комп'ютерної моделі [3]. Розглядається множина генеруючих вузлів у складі енергосистеми держави. Ітераційним шляхом проводиться переведення елементів даної множини у неактивний стан. Таке переведення, у свою чергу, інтерпретується як наслідок небажаного деструктивного впливу на генеруючі потужності – фізичного чи кібернетичного. Мета – встановлення граничної кількості неактивних генеруючих вузлів, за якої функційна безпечність системі продовжує зберігатися – у частині надання споживачам напруги живлення у відповідності до заданих обмежень.

Дослідження проведено у рамках вирішення задач наступних науково-дослідних робіт, виконуваних в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: НДР № 0125U000326 «Розвинення

теоретичних засад формалізації подань процесів опрацювання оперативної інформації в енергетиці» (2025–2029 рр.); 0125U002837 «Розвинення теоретичних засад забезпечення резильєнтності критичної енергетичної інфраструктури» (2025–2026 рр.); «Методи та засоби управління інформаційними активами об'єктів критичної інфраструктури як основа забезпечення їх кібербезпеки» (Грант НАН України дослідницьким лабораторіям/групам молодих вчених НАН України для проведення досліджень за пріоритетними напрямами розвитку науки і техніки 2026–2027 рр.); у рамках наукової роботи «Методологія та інструментарій формальної перевірки несуперечливості артефактів проєктування критичних систем», поданої на конкурс на призначення іменних стипендій Верховної Ради України імені Бориса Патона для молодих учених – докторів наук на 2026 рік.

[1] Nikolaieva, I. & Zwijnenburg, W. (2022). *Risks and impacts from attacks on energy infrastructure in Ukraine*. PAX report. https://paxforpeace.nl/wp-content/uploads/sites/2/import/2023-01/PAX_Ukraine_energy_infrastructure_FIN.pdf

[2] Шкарупило, В. В., Душеба, В. В., Зайко, Т. А., & Шкарупило, В. В. (2026). Формалізація кібернетичної складової енергетичної інфраструктури як шлях забезпечення резилієнтності. *Міжнародна науково-практична конференція «Енергетичний фронт: шостий театр воєнних дій: стратегія захисту, управління та відновлення»* (с. 100–102). ІПМЕ ім. Г.Є. Пухова НАН України. https://ipme.kiev.ua/konferencii/energy-front-2026/

[3] Sanginov, A. & Chemeris, A. (2023). Resilience of Ukrainian energy system: behavioral simulation of the war influence. Proc. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, IEEE, Athens, Greece. https://doi.org/10.1109/DESSERT61349.2023.10416478

[4] Saukh, S. Ye. (2023). Concept of building a structurally variable power system of Ukraine. *Technical Electrodynamics*, 5, 48–54. https://doi.org/10.15407/techned2023.05.048

[5] Shkarupylo, V., Chemerys, O., Artemchuk, V., Alsayaydeh, J., Kudermetov, R., & Polska, O. (2024). Comprehensive stratified approach to energy resilience solutions taxonomy: a Ukraine scenario. Proc. *14th International Conference on Dependable Systems, Services and Technologies, (DESSERT)* (pp. 1–8). IEEE, Athens, Greece. https://doi.org/10.1109/DESSERT65323.2024.11122234

[6] Artemchuk, V., Garbuz, I., Alsayaydeh, J. A. J., Shkarupylo, V., Oliinyk, A., Yusof, M. F., & Herawan, S. G. (2025). Unified resilience model using deep learning for assessing power system performance, *Heliyon*, 11(4), e42802. https://doi.org/10.1016/j.heliyon.2025.e42802

[7] Шкарупило, В. В., Чемерис, О. А., Зайко, Т. А., Дімітрієва, Д. О., & Шкарупило, В. В. (2025). Тривимірна концепція аналізу ризиків критичної енергетичної інфраструктури. *Електронне моделювання*, 47(1), 101–115. https://doi.org/10.15407/emodel.47.01.101

Є.А. Чичикало, Ю.В. Парфененко

ПІДХІД ДО ЗБЕРІГАННЯ ДАНИХ ЦИФРОВИХ ДВІЙНИКІВ ЕНЕРГЕТИЧНИХ МІКРОМЕРЕЖ

Сучасні енергетичні мікромережі з фотоелектричною генерацією чи іншими альтернативними джерелами енергії та системами накопичення енергії постійно формують великі обсяги різнорідних даних. Саме вони є необхідним ресурсом для реалізації цифрового двійника та систем інтелектуального керування електрозабезпеченням [1]. До таких даних можна віднести телеметричні показники сенсорів і контролерів, параметри генерації та споживання електроенергії, стани акумуляторних систем, результати прогнозування, а також сценарії керування режимами роботи мікромережі. Для ефективного функціонування цифрового двійника необхідна реалізація багаторівневої системи зберігання даних, яка зможе забезпечити підтримку моніторингу, аналізу, прогнозування та прийняття рішень [2]. Для даного підходу основною проблемою є необхідність одночасної роботи з високочастотними потоками телеметричних даних і структурованою інформацією, що використовується для довготривалого аналітичного опрацювання.

У роботі пропонується підхід до організації зберігання даних цифрових двійників енергетичних мікромереж, який реалізує розділення оперативного рівня збору телеметричних даних і рівня аналітичного зберігання агрегованої інформації. Для накопичення високочастотних даних моніторингу доцільно використовувати нереляційні структури даних, орієнтовані на часові ряди, зокрема спеціалізовані NoSQL-рішення [3]. У таких структурах можуть зберігатися сирі телеметричні дані від інверторів, BMS-систем акумуляторних батарей, розумних лічильників та IoT-пристроїв. Це можуть бути миттєві значення напруги, струму, потужності, температури, рівня заряду акумуляторів, параметри навколишнього середовища, часові мітки подій і журнали роботи обладнання. Використання нереляційних сховищ дає змогу забезпечити високу швидкість запису потокових даних, масштабованість системи та ефективну обробку великих масивів часових рядів у режимі реального часу [4].

Перед додаванням даних для довготривалого зберігання варто проводити попередню обробку та агрегацію шляхом фільтрації аномальних значень, усереднення значень за обрані часові інтервали, синхронхронізації часових міток та підтвердження цілісності отриманої інформації. Також на цьому етапі може виконуватися обчислення проміжних показників ефективноості роботи системи на основі телеметрії. Попередня обробка даних дозволить зменшити надлишковість об’єму даних і забезбечити підготовку чітко структурованих наборів даних для подальшого використання.

Для довготривалого зберігання та аналітичного опрацювання інформації

слід використовувати реляційну базу даних як основу цифрового двійника енергетичної мікромережі. У реляційній структурі доцільно зберігати агреговані та семантично значущі дані, які будуть сформовані після попереднього оброблення телеметричних наборів даних [5]. До них належать характеристики фізичних компонентів системи, параметри фотоелектричних масивів, інформація про акумуляторні батареї, усереднені значення генерації та споживання енергії за визначені часові інтервали, стани системи, результати прогнозування та сценарії керування. Крім того, реляційна база даних може містити інформацію про ефективність роботи обладнання, енергетичні баланси, виявлені аномалії, історію прийнятих рішень і результати їх реалізації. Такий підхід дозволяє суттєво зменшити обсяг довготривалого сховища, підвищити узгодженість інформаційної моделі та забезпечити ефективне використання даних у прогнозних і оптимізаційних алгоритмах цифрового двійника.

Запропонований підхід забезпечує логічне розмежування рівнів збору та зберігання інформації, підвищує масштабованість системи та створює передумови для інтеграції інтелектуальних методів аналізу й підтримки прийняття рішень. Поєднання нереляційних структур для оперативного моніторингу з реляційною базою даних для зберігання агрегованої інформації дозволяє використати переваги обох підходів до організації даних. Така архітектура забезпечує можливість довготривалого накопичення інформації про роботу енергетичної мікромережі, підтримує побудову прогнозних моделей і створює інформаційну основу для ефективного функціонування цифрових двійників у системах інтелектуального керування електрозабезпеченням.

[1] Lai, Y., Fan, L., Zheng, W., Han, R., & Liu, K. (2024). Construction of a digital twin model for incremental aggregation of multi type load information in hybrid microgrids under integrity constraints. Energy Informatics, 7. https://doi.org/10.1186/s42162-024-00404-5

[2] Han, J., Feng, X., Zhao, H., Chen, Z., & Hu, P. (2024). Multi-granularity signal processing method for digital twin power grids via graph representation learning. Transmission & Distribution, 41(3), 1263–1270. https://doi.org/10.18280/ts.410315

[3] Khan, W., Kumar, T., Zhang, C., Raj, K., Roy, A. M., & Luo, B. (2023). SQL and NoSQL database software architecture performance analysis and assessments—A systematic literature review. Big Data and Cognitive Computing, 7(2), 97. https://doi.org/10.3390/bdcc7020097

[4] Ward, R., Choudary, R., Singh, M. J., Roumpani, F., Lazauskas, T., & Yong, M. (2023). The challenges of using live-streamed data in a predictive digital twin. Journal of Building Performance Simulation, 16(5), 609–630. https://doi.org/10.1080/19401493.2023.2187463

[5] Ocheretnyi, V., Vadurin, K., Perekrest, A., Shekhovets, M., & Zozulia, L. (2025). Modeli baz danykh v systemakh munitsypalnoho enerhetychnoho ta ekolohichnoho monitorynhu [Database models in municipal energy and environmental monitoring systems]. Visnyk of Kremenchuk Mykhailo Ostrohradskyi National University, 2(151), 9. [in Ukrainian]. https://doi.org/10.32782/1995-0519.2025.2.9

Н.В. Заїка, І.В. Мартинюк, М.Ю. Комаров, О.М. Лаурейссенс

КЛАСИФІКАЦІЯ СТАНУ ІТ-СИСТЕМ НА ОСНОВІ ДАНИХ МОНІТОРИНГУ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Забезпечення надійності та безперервності функціонування ІТ-систем є одним із ключових завдань сучасного управління інформаційною інфраструктурою. Зростання складності розподілених обчислювальних середовищ, збільшення обсягів телеметричних даних та постійна еволюція кіберзагроз обумовлюють необхідність використання автоматизованих підходів до моніторингу та аналізу стану систем [1, 2].

Традиційні методи порогового моніторингу, що базуються на статично визначених граничних значеннях параметрів, демонструють обмежену ефективність у середовищах із динамічним навантаженням та складними нелінійними залежностями між метриками системи. У зв'язку з цим методи машинного навчання розглядаються як перспективний інструмент аналізу та класифікації станів ІТ-інфраструктури, оскільки дозволяють враховувати багатовимірний характер даних моніторингу та адаптуватися до змін у поведінці системи [2].

У сучасних підходах до забезпечення кібербезпеки моніторинг розглядається як безперервний процес спостереження за мережевою інфраструктурою, серверами, кінцевими пристроями та журналами подій з метою своєчасного виявлення загроз і реагування на них. Відповідно до рекомендацій National Institute of Standards and Technology, викладених у NIST SP 800-137, безперервний моніторинг інформаційної безпеки повинен забезпечувати організацію актуальною інформацією про стан активів, вразливості та ефективність засобів контролю безпеки, що дозволяє підтримувати необхідний рівень кіберстійкості [1].

Перехід від реактивного до проактивного підходу у сфері кібербезпеки обумовлений зростанням масштабу сучасних кіберзагроз та збільшенням фінансових втрат від кібератак. У зв'язку з цим особливої актуальності набуває застосування методів аналізу даних та алгоритмів машинного навчання для автоматизованого виявлення аномалій і прогнозування стану інформаційних систем [3].

Алгоритми класифікації K-Nearest Neighbours, Support Vector Machine, Decision Tree, Random Forest та AdaBoost, активно досліджуються у задачах виявлення аномалій та аналізу стану складних технічних систем [3, 4]. Результати порівняльних досліджень свідчать, що ансамблеві методи (Random Forest та AdaBoost), у багатьох випадках демонструють кращу узагальнюючу здатність порівняно з окремими класифікаторами, хоча їх ефективність залежить від характеристик набору даних та структури ознак [3].

Метою даної роботи є порівняльний аналіз методів машинного навчання

для класифікації стану ІТ-системи на основі даних моніторингу обсягом 10 000 записів, а також визначення найбільш ефективного підходу за метриками Accuracy, Precision, Recall та F1-score. Окрему увагу приділено оцінюванню придатності алгоритмів машинного навчання до використання у задачах безперервного моніторингу та виявлення аномалій у середовищах із підвищеними вимогами до кібербезпеки.

Перспективні напрями розвитку систем моніторингу ІТ-інфраструктури з використанням КЗІ. Отримані результати порівняльного аналізу алгоритмів машинного навчання для класифікації стану ІТ-систем підтверджують доцільність подальших досліджень у напрямі інтеграції засобів криптографічного захисту інформації (КЗІ) у системи безперервного моніторингу. Зростання складності інформаційної інфраструктури, поширення розподілених обчислювальних середовищ та збільшення кількості кіберзагроз обумовлюють необхідність поєднання методів аналізу даних із криптографічними механізмами захисту [5-7].

Одним із перспективних напрямів є автоматизована криптографічна інвентаризація активів. У сучасних ІТ-середовищах криптографічні компоненти, включаючи ключовий матеріал, алгоритми шифрування та протоколи захищеного обміну даними, часто розподілені між різними програмними й апаратними компонентами системи. Дослідження показують, що відсутність централізованого обліку таких компонентів ускладнює управління криптографічною інфраструктурою та своєчасне оновлення засобів захисту [7]. У цьому контексті перспективним є застосування алгоритмів машинного навчання для автоматизованого виявлення та класифікації криптографічних активів у гетерогенних середовищах моніторингу.

Іншим важливим напрямом є забезпечення крипто-спритності (crypto-agility), що передбачає здатність системи оперативно адаптувати криптографічні механізми у відповідь на появу нових загроз або компрометацію алгоритмів. В умовах переходу до постквантової криптографії ця проблема набуває особливої актуальності, оскільки інформаційні системи повинні підтримувати можливість оновлення криптографічних протоколів без критичного впливу на функціонування сервісів [8-10]. У зв’язку з цим перспективним є створення модулів моніторингу стану криптографічних протоколів у реальному часі з автоматизованим виявленням застарілих або потенційно вразливих алгоритмів.

Подальший розвиток систем моніторингу пов’язаний із впровадженням постквантових криптографічних алгоритмів. Відповідно до рекомендацій National Institute of Standards and Technology, стандартизація алгоритмів CRYSTALS-Kyber та CRYSTALS-Dilithium розглядається як один із базових етапів переходу до квантово-стійких систем захисту [7]. У межах систем моніторингу це відкриває можливість застосування постквантових механізмів для захисту каналів передачі телеметричних даних між агентами моніторингу та серверами збору метрик.

Окремий інтерес становить моніторинг захищених каналів передачі даних. Сучасні системи кібербезпеки дедалі частіше працюють із зашифрованим мережевим трафіком, що ускладнює використання традиційних методів аналізу пакетів. У зв'язку з цим перспективним напрямом є розроблення гібридних моделей, які поєднують алгоритми класифікації стану системи з аналізом метаданих зашифрованого трафіку без порушення конфіденційності інформації. Такий підхід дозволяє зберегти баланс між вимогами до безпеки та необхідністю своєчасного виявлення аномальної активності.

Важливого значення набуває також моніторинг IoT та кіберфізичних систем із використанням КЗІ. Сучасні дослідження у сфері промислових кіберфізичних систем демонструють потенціал застосування квантових фізично неклонованих функцій (QPUF) для формування унікальних криптографічних відбитків апаратних компонентів [11]. Поєднання таких механізмів із методами машинного навчання створює передумови для побудови систем виявлення аномалій у захищених каналах IoT-пристроїв та промислових систем керування.

Подальший розвиток систем моніторингу також пов'язаний із використанням ШІ-орієнтованих підходів до забезпечення кібербезпеки. У сучасних дослідженнях наголошується на доцільності побудови інтегрованих систем, що поєднують алгоритми машинного навчання з апаратно підтримуваними засобами криптографічного захисту [8]. Така інтеграція дозволяє забезпечити контроль цілісності моніторингових даних та підвищити достовірність результатів аналізу.

Таким чином, перспективи розвитку систем моніторингу IT-інфраструктури пов'язані з інтеграцією методів машинного навчання, криптографічних механізмів та технологій безперервного моніторингу у єдину архітектуру. Поєднання КЗІ, постквантових алгоритмів та адаптивних моделей аналізу даних створює основу для побудови кіберстійких систем моніторингу, здатних функціонувати в умовах динамічного розвитку сучасних кіберзагроз.

Методика дослідження та результати класифікації стану IT-системи. Для проведення дослідження було використано вибірку, що містить 10 000 записів моніторингових метрик IT-системи. Кожен запис включав набір параметрів, які характеризують поточний стан системи, показники завантаження процесора, використання оперативної пам'яті, параметри мережевого трафіку та характеристики дискової підсистеми. Цільова змінна відображала клас стану системи як нормальний або проблемний. Такий підхід відповідає сучасним методам аналізу стану IT-інфраструктури на основі телеметричних даних [2].

Попередня обробка даних включала нормалізацію числових параметрів, усунення пропущених значень та кодування категоріальних ознак. Для оцінювання якості моделей вибірку було розділено на навчальну та тестову у співвідношенні 80:20, що відповідає поширеним практикам побудови моделей машинного навчання [3].

У роботі досліджено п’ять алгоритмів класифікації: K-Nearest Neighbours (KNN), Kernel Support Vector Machine (SVM), Decision Tree, Random Forest та AdaBoost. Вибір зазначених моделей обумовлений їх широким застосуванням у задачах класифікації, виявлення аномалій та аналізу стану складних технічних систем [2]. KNN реалізує класифікацію на основі відстані до найближчих сусідів у просторі ознак, Kernel SVM використовує ядрові перетворення для розділення нелінійних класів, тоді як Decision Tree, Random Forest та AdaBoost належать до групи деревоподібних та ансамблевих методів машинного навчання [3-4].

Оцінювання якості моделей здійснювалось за метриками Accuracy, Precision, Recall та F1-score. В умовах дисбалансу класів найбільш інформативною метрикою розглядалась F1-score, оскільки вона забезпечує збалансоване врахування точності та повноти класифікації [11-13]. Результати порівняльного аналізу моделей наведено у таблиці 1.

Таблиця 1 – Порівняння результатів класифікації

Модель	Accuracy	Precision	Recall	F1-score
KNN	0.998342	0.916002	0.777611	0.832918
Random Forest	0.998010	0.999004	0.666667	0.749501
AdaBoost	0.998010	0.999004	0.666667	0.749501
Kernel SVM	0.994362	0.666499	0.941783	0.741007
Decision Tree	0.970481	0.532096	0.819029	0.551900

Отримані результати свідчать, що всі досліджені моделі забезпечують високий рівень загальної точності класифікації. Водночас порівняння за метрикою F1-score показало суттєві відмінності між алгоритмами. Найкращий збалансований результат продемонстрував алгоритм K-Nearest Neighbours із показником F1-score ≈ 0.83, що свідчить про ефективне поєднання точності та повноти виявлення проблемних станів системи [2].

Моделі Random Forest та AdaBoost характеризуються високими значеннями Accuracy і Precision, однак демонструють нижчий Recall, що може призводити до пропуску частини проблемних станів системи. Подібна поведінка є прийнятною для задач із низькою вартістю хибнонегативних помилок, проте є менш ефективною для сценаріїв раннього виявлення критичних відхилень [4]. Kernel SVM, навпаки, показав високу повноту класифікації при нижчій точності, що може збільшувати кількість хибнопозитивних спрацьовувань. Найменш стабільний результат отримано для Decision Tree, що узгоджується з відомою схильністю цього алгоритму до перенавчання на навчальних даних [3].

Отримані результати підтверджують перспективність застосування методів машинного навчання у задачах моніторингу IT-інфраструктури та автоматизованого виявлення проблемних станів системи. Інтеграція таких

підходів із системами безперервного моніторингу створює передумови для переходу від реактивного реагування до проактивного управління кібербезпекою, що є особливо актуальним для середовищ із підвищеними вимогами до надійності та кіберстійкості.

У роботі проведено порівняльний аналіз методів машинного навчання для класифікації стану IT-системи на основі даних моніторингу обсягом 10 000 записів. Досліджено ефективність алгоритмів KNN, Kernel SVM, Decision Tree, Random Forest та AdaBoost за метриками Accuracy, Precision, Recall та F1-score.

Встановлено, що всі досліджені моделі демонструють високий рівень загальної точності класифікації, однак найбільш інформативною метрикою в умовах дисбалансу класів є F1-score [11]. Найбільш ефективним алгоритмом виявився K-Nearest Neighbours, який забезпечив найкраще співвідношення між точністю та повнотою виявлення проблемних станів системи.

Результати дослідження підтверджують доцільність використання методів машинного навчання для автоматизованого моніторингу IT-інфраструктури та раннього виявлення аномальних станів, що створює основу для подальшого розвитку інтелектуальних систем безперервного кібербезпекового моніторингу.

[1] Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137. National Institute of Standards and Technology, 2011. https://doi.org/10.6028/NIST.SP.800-137

[2] Chandola, V., Banerjee, A., & Kumar, V. Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58, 2009. https://doi.org/10.1145/1541880.1541882

[3] Fernández-Delgado, M., Cernadas, E., Barro, S., & Amorim, D. Do we need hundreds of classifiers to solve real world classification problems? Journal of Machine Learning Research, 15(1), 3133–3181, 2014. https://jmlr.org/papers/v15/delgado14a.html

[4] Freund, Y., & Schapire, R. E. A decision-theoretic generalization of on-line learning and an application to boosting. Journal of Computer and System Sciences, 55(1), 119–139, 1997. https://doi.org/10.1006/jcss.1997.1504

[5] Dempsey, K., Pillitteri, V., Baer, C., Niemeyer, R., Rudman, R., & Urban, S. Assessing Information Security Continuous Monitoring (ISCM) Programs. NIST Special Publication 800-137A. National Institute of Standards and Technology, 2020. https://csrc.nist.gov/pubs/sp/800/137/a/final

[6] FBI Internet Crime Complaint Center (IC3). Internet Crime Report 2024. Federal Bureau of Investigation, 2025. https://www.ic3.gov/AnnualReport

[7] Näther, M. et al. Detecting cryptographically relevant software packages with collaborative LLMs. arXiv preprint, 2025. https://arxiv.org/abs/2603.07204

[8] National Institute of Standards and Technology. Post-Quantum Cryptography Standards (FIPS 203, 204, 205), 2024. https://csrc.nist.gov/projects/post-quantum-cryptography

[9] IBM Security. IBM Cybersecurity Predictions for 2025. IBM Think Insights, 2024. https://www.ibm.com/think/insights/cybersecurity-trends-ibm-predictions-2025

[10] Dempsey, K. et al. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137, 2011. https://doi.org/10.6028/NIST.SP.800-137

[11] Quantum Physical Unclonable Functions for Industrial Cyber-Physical Systems. Cryptography, 9(2), MDPI, 2025. https://www.mdpi.com/2410-387X/9/2

[12] Bishop, C. M. Pattern Recognition and Machine Learning. Springer, 2006.

[13] Géron, A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (3rd ed.). O'Reilly Media, 2022.

Ю.Г. Сапсай, А.О. Запорожець

ГІБРИДНІ МЕТОДИ ДІАГНОСТИКИ ТЕХНІЧНОГО СТАНУ ЛІТІЙ-ІОННИХ АКУМУЛЯТОРІВ: СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ

Розширення сфер застосування літій-іонних акумуляторів (ЛІА) та посилення вимог до надійності й безпеки їх експлуатації обумовлюють потребу в точному оцінюванні параметрів технічного стану акумуляторної комірки — насамперед ступеня заряджання (State of Charge, SOC), стану здоров'я (State of Health, SOH) та залишкового ресурсу (Remaining Useful Life, RUL) [1].

Складність діагностики ЛІА зумовлена нелінійністю електрохімічних процесів, залежністю характеристик від температури і режимів навантаження та варіативністю старіння окремих комірок. При цьому класичні модельні підходи характеризуються високою обчислювальною складністю та чутливістю до точності параметризації, а суто інтелектуальні методи на основі даних мають низьку інтерпретованість та обмежену здатність до узагальнення. Зазначене актуалізує задачу побудови гібридних методів, що поєднують фізико-математичні моделі акумулятора з методами машинного навчання (machine learning, ML) [2].

Гібридні методи діагностики технічного стану ЛІА ґрунтуються на узгодженому поєднанні двох джерел знань: фізико-математичної моделі акумулятора (як приклад еквівалентні електричні схеми заміщення - Thevenin 1C/2C) та експериментальних даних циклування (струм, напруга, температура, ємність), які опрацьовуються алгоритмами машинного навчання. Завдання методу полягає в тому, щоб алгоритм навчався на даних, водночас узгоджуючись з фізичними законами, що забезпечує підвищення точності прогнозу та його фізичну несуперечність за межами навчальної вибірки [3].

У науковій літературі останніх років сформувалися два основні напрями реалізації цього підходу.

Першим із них є фізико-орієнтовані нейронні мережі (Physics-Informed Neural Networks, PINN) є архітектурою глибокого навчання, у якій рівняння, що описують поведінку акумулятора, додаються як штрафний доданок до функції втрат. У разі відхилення прогнозу від фізичних законів мережа отримує додатковий штраф, що змушує її одночасно мінімізувати похибку та задовольняти диференціальні рівняння. Як фізична основа найчастіше використовуються модель одиничної частинки (Single Particle Model, SPM) та псевдодвовимірна модель Doyle — Fuller — Newman (P2D) [4]. За даними дослідження [5], PINN-модель забезпечує оцінювання SOH із середньою абсолютною відсотковою похибкою (MAPE) на рівні 0,87 % при валідації на 387 комірках.

Другий напрям становлять послідовно-каскадні архітектури «модель + ML-коректор» передбачають двоетапну схему: спочатку фізична модель (зазвичай еквівалентна схема заміщення першого або другого порядку) з онлайн-ідентифікацією параметрів через фільтр Калмана (Extended/Unscented Kalman Filter) формує базовий прогноз, після чого алгоритм машинного навчання — рекурентна нейронна мережа (LSTM, GRU) або ансамблевий метод (Gradient Boosting, Random Forest) — компенсує залишкову систематичну похибку. Така схема поєднує обчислювальну простоту і фізичну прозорість моделі з гнучкістю інтелектуальних алгоритмів [6; 7].

Інтеграція фізичних моделей із методами машинного навчання забезпечує синергетичний ефект, недосяжний при застосуванні кожного підходу окремо. Передусім, сучасні гібридні архітектури демонструють підвищену точність прогнозування — похибка оцінювання SOH становить 0,5–1,5 % за метрикою MAPE, що значно перевершує показники класичних алгоритмів. Включення фізичних обмежень у структуру нейронної мережі покращує її узагальнювальну здатність, зменшуючи перенавчання та забезпечуючи адекватне функціонування моделі в режимах, не представлених у навчальній вибірці. Водночас гібридні моделі також частково усувають проблему «чорної скриньки», оскільки їхні внутрішні параметри (коефіцієнт дифузії, опір SEI-плівки, ємність активного матеріалу) зберігають фізичний зміст і піддаються інженерному аналізу. Використання апріорних знань дозволяє суттєво зменшити обсяг експериментальних даних, необхідних для досягнення прийнятної точності, а також забезпечує можливість одночасного оцінювання кількох параметрів — SOC, SOH і RUL — у межах єдиної моделі [2;3;5].

Незважаючи на досягнутий прогрес, низка задач у цій галузі залишається відкритою. Подальше підвищення якості гібридних методів безпосередньо пов’язане з удосконаленням фізичних моделей, що покладені в їхню основу — зокрема, перспективним є застосування моделей дробового порядку, які краще описують пам’ятозалежні процеси старіння [8]. Не менш важливим завданням є адаптація моделей, навчених у лабораторних умовах, до реальних режимів експлуатації з варіативними навантаженнями та температурою [3]. Окремим напрямом виступає реалізація гібридних алгоритмів безпосередньо у вбудованих обчислювальних платформах систем BMS, що вимагає оптимізації обчислювальної складності через стиснення моделей, квантизацію ваг та побудову спрощених сурогатів [4]. Також, актуальним залишається перехід від діагностики окремої комірки до рівня батарейного блоку з урахуванням неоднорідності старіння послідовно-паралельно з’єднаних елементів [7].

Проведений аналіз засвідчує, що гібридні методи є одним із найбільш перспективних напрямів розвитку засобів діагностування технічного стану літій-іонних акумуляторів, оскільки забезпечують ефективне поєднання методологічних переваг фізико-математичного моделювання та інтелектуального опрацювання даних. Інтеграція рівнянь електрохімічної

моделі акумулятора з алгоритмами машинного навчання забезпечує підвищення точності визначення SOC і SOH, поліпшення інтерпретованості результатів та скорочення обсягу експериментальних даних, необхідних для калібрування. Подальші дослідження доцільно зосередити на розробленні адаптивних гібридних алгоритмів, спроможних до самонавчання в умовах реальної експлуатації та придатних до реалізації на вбудованих обчислювальних платформах. Отримані результати можуть бути покладені в основу побудови інформаційно-вимірювальної системи діагностування технічного стану літій-іонних акумуляторів.

[1] Demirci, O., Taskin, S., Schaltz, E., & Acar Demirci, B. (2024). Review of battery state estimation methods for electric vehicles – Part I: SOC estimation. Journal of Energy Storage, 87, 111435. https://doi.org/10.1016/j.est.2024.111435

[2] Aykol, M., Gopal, C. B., Anapolsky, A., Herring, P. K., van Vlijmen, B., Berliner, M. D., Bazant, M. Z., Braatz, R. D., Chueh, W. C., & Storey, B. D. (2021). Perspective—Combining physics and machine learning to predict battery lifetime. Journal of The Electrochemical Society, 168(3), 030525. https://doi.org/10.1149/1945-7111/abec55

[3] Thelen, A., Lui, Y. H., Shen, S., Laflamme, S., Hu, S., Ye, H., & Hu, C. (2022). Integrating physics-based modeling and machine learning for degradation diagnostics of lithium-ion batteries. Energy Storage Materials, 50, 668–695. https://doi.org/10.1016/j.ensm.2022.05.047

[4] Hassanaly, M., Weddle, P. J., King, R. N., De, S., Doostan, A., Randall, C. R., Dufek, E. J., Colclasure, A. M., & Smith, K. (2024). PINN surrogate of Li-ion battery models for parameter inference, Part II: Regularization and application of the pseudo-2D model. Journal of Energy Storage, 98, 113104. https://doi.org/10.1016/j.est.2024.113104

[5] Wang, F., Zhai, Z., Zhao, Z., Di, Y., & Chen, X. (2024). Physics-informed neural network for lithium-ion battery degradation stable modeling and prognosis. Nature Communications, 15, 4332. https://doi.org/10.1038/s41467-024-48779-z

[6] Wang, C., Li, R., Cao, Y., & Li, M. (2024). A hybrid model for state of charge estimation of lithium-ion batteries utilizing improved adaptive extended Kalman filter and long short-term memory neural network. Journal of Power Sources, 235272. https://doi.org/10.1016/j.jpowsour.2024.235272

[7] Su, L., Xu, Y., & Dong, Z. (2024). State-of-health estimation of lithium-ion batteries: A comprehensive literature review from cell to pack levels. Energy Conversion and Economics, 5(4), 224–242. https://doi.org/10.1049/enc2.12125

[8] Dang, L., & Wang, Z. (2025). Fractional differential equation physics-informed neural network and its application in battery state estimation. arXiv preprint arXiv:2512.12285. https://arxiv.org/abs/2512.12285

А.І. Швайка, Д.І. Швайка, В.О. Артемчук

АВТОМАТИЗОВАНЕ ПРОЄКТУВАННЯ IOT-РІШЕНЬ НА ОСНОВІ БАГАТОАГЕНТНОЇ АРХІТЕКТУРИ З ВИКОРИСТАННЯМ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Проєктування та конфігурування рішень Інтернету речей (IoT) залишаються складними інженерними завданнями, які потребують значного експертного досвіду й ручної роботи [1]. Сучасні IoT-архітектури виходять за межі простого збирання даних і базуються на багаторівневих розподілених моделях, що поєднують хмарні, граничні (edge) та прикладні компоненти обробки. Великі мовні моделі (LLM) демонструють потужні можливості у природномовному розумінні та логічному міркуванні, проте їхня стохастична природа обмежує пряме застосування в інженерії промислових IoT-систем, де необхідна сувора структурна коректність та відтворюваність результатів. Існуючі дослідження здебільшого використовують LLM як агентів часу виконання або аналітичні компоненти [2, 3], тоді як комплексна детермінована оркестрація конфігурацій IoT-платформи на основі природномовних вимог залишається відкритою задачею [4].

Метою роботи є розробка детермінованого оркестраційного підходу, який дозволяє перетворювати природномовні описи IoT-системи на перевірені, готові до виконання конфігурації платформи з явним розділенням імовірнісних міркувань на етапі проєктування та детермінованого виконання. Підхід реалізовано та апробовано на платформі ThingsBoard [5].

Запропонований підхід. Представлено схемно-керовану генеративну структуру, що інтегрує LLM у конвеєр з трьох послідовних етапів. Реалізація побудована на екосистемі Java 21 з використанням кастомізованого форку LangChain4j [6] як шару координації агентів та великої мовної моделі Google Gemini 3.0 Flash.

Етап 1 — Детермінована початкова конфігурація. Природномовні вимоги перетворюються на строго типізований конвеєр обробки за принципом покрокового міркування (Chain-of-Thought), обмеженого заздалегідь визначеними JSON-схемами [7]. Агент Бізнес-аналітика працює у двох режимах взаємодії: у стані IN_PROGRESS він формує обмежений набір припущень та уточнюючих запитань, після чого переходить у стан READY і формує структурований JSON-опис рішення. Виділені агенти будують онтологію системи (профілі CUSTOMER, USER, DEVICE, ASSET), застосовують топологічні обмеження та формують політики рольового контролю доступу. Бізнес-логіка (метрики, сигнали тривоги) формується паралельно: кожен тип обчислень (геофенсинг, агрегація часових рядів, алгебраїчні розрахунки) делегується спеціалізованому агенту, а механізм інвертованого розв’язання залежностей забезпечує доповнення схеми необхідними полями.

Етап 2 — Ітеративне уточнення та узгодження стану. Агент-планувальник, який має доступ читання/запису до опису рішення, інтерпретує запити на модифікацію через семантичний аналіз відмінностей і формує План змін з атомарних CRUD-операцій (створення, читання, оновлення, видалення). Це забезпечує локальні оновлення без повного перебудовування конфігурації.

Етап 3 — Формування інтерфейсу користувача та налаштування панелей керування. Перевірена серверна конфігурація транслюється у клієнтський інтерфейс візуалізації за принципом орієнтації на користувацькі ролі: адміністративні представлення зосереджуються на адмініструванні та керуванні життєвим циклом, операційні — на моніторингу телеметрії.

Розгортання виконується Java-оркестратором рішень, який створює сутності, налаштовує бізнес-логіку та компоненти інтерфейсу через API платформи у транзакційному режимі. Повне відокремлення процесу розгортання від роботи LLM гарантує виконання без галюцинацій моделі.

Результати. Експериментальна перевірка проводилась на сценарії побудови рішення для відстеження автопарку. На Етапі 1 BA-агент коректно обробляє неповний запит, переходячи у стан IN_PROGRESS з обмеженим набором припущень та уточнюючих запитань (рис. 1). Після надання уточнень формується структурований опис рішення з профілями сутностей, схемами телеметрії та логічними визначеннями.

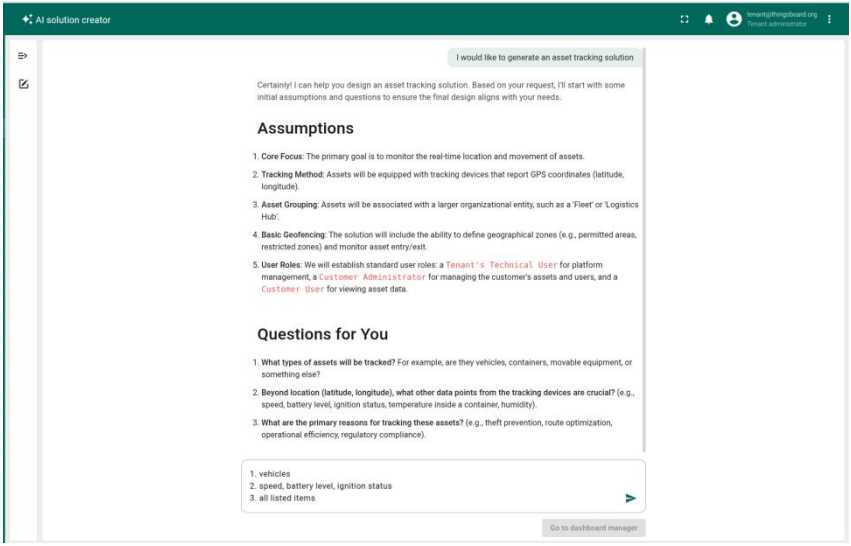


Рисунок 1 – Початкова елісітація вимог у стані IN_PROGRESS

На Етапі 2 запит на модифікацію (додавання нової зони геофенсингу) обробляється локально без повного перебудовування конфігурації:

формується План змін з атомарних CRUD-операцій, які перевіряються щодо існуючої схеми та об'єднуються з головним описом рішення (рис. 2).

Після розгортання система демонструє повну операційну функціональність. Панель керування Fleet Management інтегрує просторову візуалізацію, таблиці стану активів та зони геофенсингу в єдиний робочий простір (рис. 3). Зони restricted, allowed та no-parking відображаються відповідно до сформованої конфігурації.

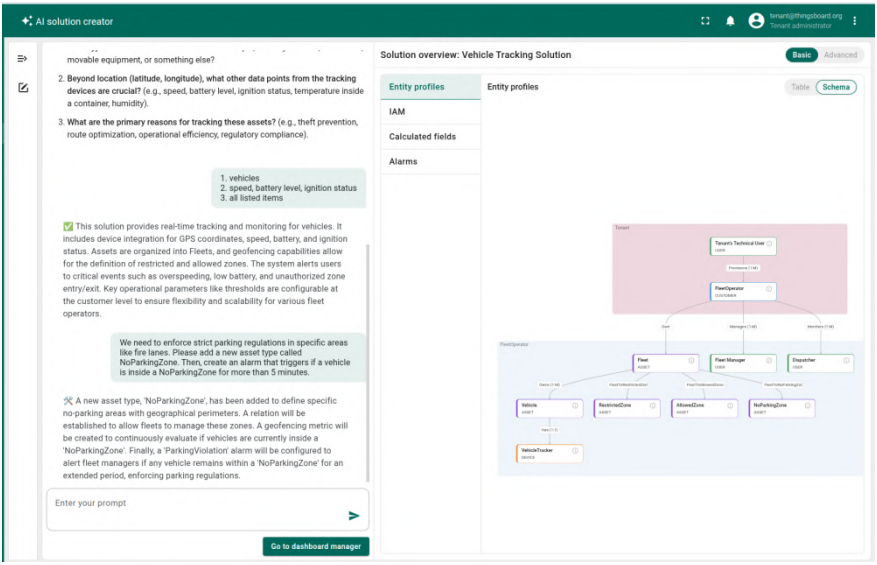


Рисунок 2 – Ітеративне уточнення рішення Агентом-планувальником

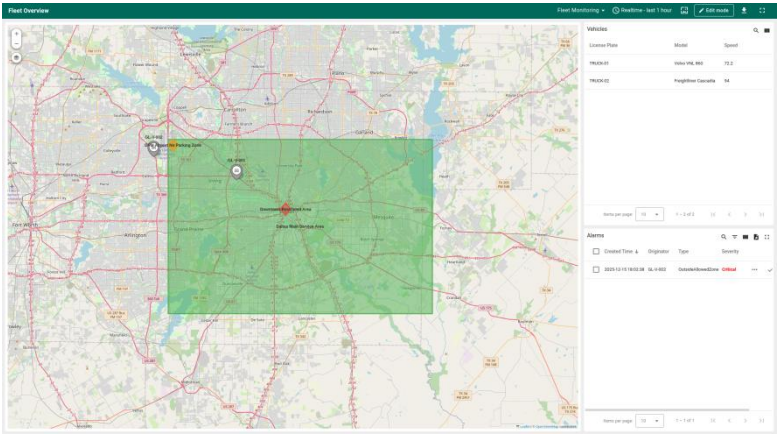


Рисунок 3 – Панель керування Fleet Management з геофенсингом та станом активів

Детальне представлення стану транспортного засобу підтверджує коректну роботу телеметрії, обчислюваних полів та сигналів тривоги в реальному часі (рис. 4): відображаються швидкість, рівень заряду, статус запалювання, історія змін показників та активний сигнал тривоги геофенсингу.

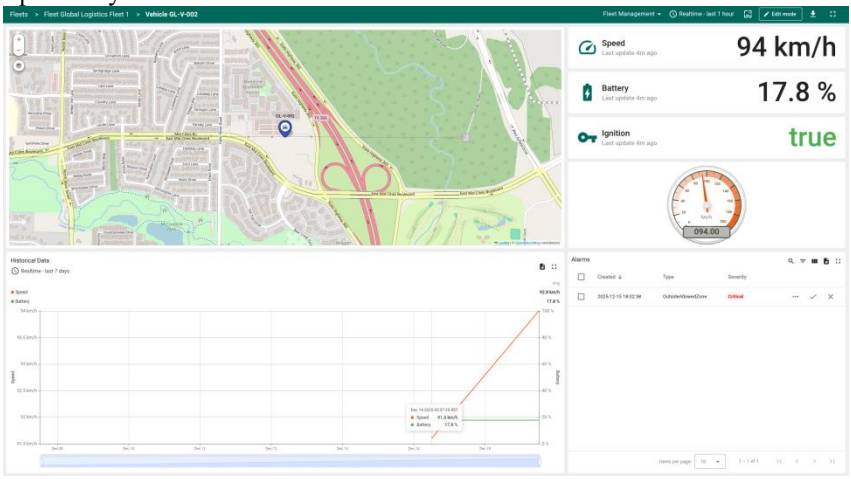


Рисунок 4 – Детальний стан транспортного засобу з активним сигналом тривоги

Обговорення. На відміну від програмних каркасів агентів часу виконання [2, 3], запропонований підхід обмежує застосування LLM етапом проєктування, що повністю усуває ризик галюцинацій моделі під час виконання — критичну вимогу для промислової безпеки. Структура працює на рівні класу (профілів), а не екземпляра, що забезпечує масштабованість. Перевага декларативних обчислюваних полів над імперативними ланцюгами правил дозволяє відокремити масштабованість часу виконання від процесу генерації за допомогою LLM, оскільки виконання логіки делегується оптимізованому ядру платформи, здатному обробляти телеметрію мільйонів пристроїв [8]. Підхід зміщує необхідний набір навичок з технічної конфігурації платформи до природномовного опису вимог, знижуючи бар'єр входу для прикладних доменів. Подальша робота передбачає введення спеціалізованого Агента оптимізації зв'язності, який автоматично налаштовуватиме оптимальну структуру корисного навантаження пристроїв, зокрема з використанням бінарних форматів та інтеграції з TBMQ [9].

Висновки. Запропоновано детерміновану декларативну оркестраційну структуру для інтеграції великих мовних моделей у процес проєктування IoT-рішень. Поєднання обмеженого схемою покрокового міркування (Chain-of-Thought) з багатоагентною оркестрацією дозволяє ефективно використовувати LLM для семантичної інтерпретації на етапі проєктування

за умов збереження детермінованого виконання. Первинна цінність LLM у складних IoT-системах полягає в інтерпретації вимог та декларативному формуванні конфігурації, а не у прийнятті рішень під час виконання.

[1] Dauda, A., Flauzac, O., & Nolot, F. (2024). A survey on IoT application architectures. Sensors, 24(16), 5320. https://doi.org/10.3390/s24165320

[2] Du, Y., Yang, Q., Wang, L., Lin, J., Cui, H., & Liew, S. C. (2025). LLMind 2.0: Distributed IoT automation with natural language M2M communication and lightweight LLM agents (arXiv:2508.13920). arXiv. https://arxiv.org/abs/2508.13920

[3] Rivkin, D., Hogan, F., Feriani, A., Konar, A., Sigal, A., Liu, X., & Dudek, G. (2025). AIoT smart home via autonomous LLM agents. IEEE Internet of Things Journal, 12(3), 2458–2472. https://doi.org/10.1109/JIOT.2024.3471904

[4] De Vito, G., Palomba, F., & Ferrucci, F. (2025). The role of large language models in addressing IoT challenges: A systematic literature review. Future Generation Computer Systems, 171, 107829. https://doi.org/10.1016/j.future.2025.107829

[5] ThingsBoard Inc. (2025). ThingsBoard: Open-source IoT platform. https://thingsboard.io/

[6] LangChain4j Contributors. (2024). LangChain4j: Java LLM orchestration framework. GitHub. https://github.com/langchain4j/langchain4j

[7] Qiu, L., Ye, Y., Gao, Z., Zou, X., Chen, J., Gui, Z., Huang, W., Xue, X., Qiu, W., & Zhao, K. (2025). Blueprint first, model second: A framework for deterministic LLM workflow (arXiv:2508.02721). arXiv. https://arxiv.org/abs/2508.02721

[8] Швайка, Д. І., Швайка, А. І., & Артемчук, В. О. (2024). Advancing IoT interoperability: Dynamic data serialization using ThingsBoard. Journal of Edge Computing, 3(2), 126–135. https://doi.org/10.55056/jec.745

[9] Shvaika, A., Shvaika, D., Landiak, D., et al. (2025). A distributed architecture for MQTT messaging: The case of TBMQ. Journal of Big Data, 12, 224. https://doi.org/10.1186/s40537-025-01271-x

М.С. Кондратенко

ВИКОРИСТАННЯ КАСКАДНИХ БЛОКЧЕЙН-РЕЄСТРІВ ДЛЯ ЗАХИСТУ ЖУРНАЛІВ КОНФІГУРАЦІЙ SCADA-СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ

У сучасних умовах цифрової трансформації енергетичного сектору України особливого значення набуває впровадження децентралізованих рішень як компонентів концепції «Smart Grid» [1]. Системи диспетчерського управління та збору даних (SCADA) є фундаментом керування складними технічними об’єктами, проте традиційні централізовані архітектури мають суттєві вразливості, зокрема ризик несанкціонованої підміни історії записів [3]. Використання блокчейн-технологій дозволяє створити ієрархічні структури для захисту державної інформації, що є критично важливим для забезпечення надійності зберігання даних.

Для розв'язання проблем масштабованості та безпеки пропонується перехід до гібридних розподілених інфраструктур, що поєднують переваги локального контролю та хмарної гнучкості [2]. Каскадна модель реєстрів передбачає використання операційних сайдчейнів для швидкої фіксації конфігурацій та державного мейнчейну як глобального джерела правди. Такий підхід забезпечує функціональний розподіл обов’язків між рівнями мережі, мінімізуючи навантаження на основний ланцюг при збереженні математично доведеної незмінності історії транзакцій.

Особливу увагу при розробці таких систем слід приділити алгоритмічному забезпеченню стійкості. Протокол Proof-of-Proof *(PoP)* дозволяє сайдчейну «публікувати» свої блоки у мейнчейні, що фактично передає безпеку потужнішої мережі менш потужній. Це критично для індустріальних об'єктів, де локальні обчислювальні ресурси обмежені. Математична модель дворівневого блокчейну враховує ненульовий час синхронізації мережі для чесних учасників та можливість зловмисника ігнорувати мережеві затримки. Застосування ітераційних алгоритмів для визначення мінімально необхідної кількості блоків підтвердження (z) гарантує, що ймовірність успішної атаки підміни даних (Q) не перевищуватиме встановленого порогу надійності [2].

Аналіз результатів імітаційного моделювання показує, що при поєднанні PoS-сайдчейнів із PoW-мейнчейном вдається досягти високої пропускної здатності операційного шару при експоненціальному зростанні складності для потенційного атакувальника. Для захисту SCADA-систем це означає, що кожна зміна у налаштуваннях критичного обладнання стає частиною незмінного ланцюга подій. Навіть у випадку компрометації локального адміністративного вузла, зловмисник не зможе видалити сліди своєї діяльності в минулому, оскільки відповідні хеш-відбитки вже зафіксовані у «якірному» мейнчейні з кроком *n* блоків [4].

Додатковим напрямком підвищення резильєнтності системи є інтеграція методів штучного інтелекту для аналізу транзакційних потоків. Гібридна архітектура дозволяє реалізувати шари попереднього аналізу на рівні Edge Computing (Fog infrastructure), де легковагові вузли (lightweight nodes) здійснюють первинну фільтрацію аномалій в поведінці системи. Використання швидких сховищ (fast storage) для логування активних змін у поєднанні з архівними сховищами (slow storage) для мейнчейну дозволяє збалансувати навантаження на мережеву інфраструктуру та забезпечити доступність даних навіть в умовах часткової втрати зв'язку між підстанціями [3].

Перспективи впровадження каскадних реєстрів також пов'язані з правовим регулюванням смартконтрактів. Математично доведена стабільність блоку в блокчейні є фундаментом для визнання записів юридично значущими. Це створює умови для автоматизованого виконання цивільно-правових угод у сфері енергетики, де смартконтракт виступає не лише як програмний код, а й як засіб гарантування виконання зобов'язань між виробниками та споживачами електроенергії. Таким чином, каскадні структури забезпечують не лише технічну, а й регуляторну стійкість системи.

Впровадження каскадних реєстрів дозволяє створити ефективний інструментарій для захисту журналів конфігурацій SCADA-систем. Завдяки механізму якірного закріплення, будь-яке втручання в налаштування обладнання залишає незмінний слід у глобальному ланцюзі, що унеможливлює приховану модифікацію даних адміністратором чи зовнішнім зловмисником. Це створює надійну базу для подальшого аудиту та моніторингу стану критичної інфраструктури в режимі реального часу. Отримані результати сприятимуть розвитку національної кібербезпеки та модернізації державних інформаційних систем в умовах євроінтеграції.

[1] Denysiuk S., Bielokha H. (2024), “Decentralized Electricity Systems as Component Implementations of the 'Smart Grids' Concept”, System Research in Energy, №4 (80), p.26-40. https://doi.org/10.15407/srenergy2024.04.026

[2] Кондратенко М.С, Ковальчук Л.В., Кучинська Н.В. (2024) “Визначення кількості блоків підтвердження у дворівневому блокчейні з протоколом консенсусу Proof-of-Proof за різних типів консенсусу у мейнчейні/сайдчейні для запобігання атаці подвійної витрати. I. PoS у мейнчейні та PoW у сайдчейні”, Кібернетика та Системний Аналіз, 60(4), с.156–167, https://doi.org/10.34229/KCA2522-9664.24.4.12

[3] Zubok V., Kondratenko M. (2026) “Formulating requirements for hybrid distributed computing systems: An infrastructure perspective”, Electronics and Control Systems, №2 (88), p.77-85, http://jrnl.nau.edu.ua/index.php/ESU

[4] Кондратенко М.С., (2023), “Використання технології блокчейну для побудови ієрархічної структури на множині державних реєстрів з метою захисту від підробки інформації”, Електронне моделювання, 45(3), с.43-56, https://doi.org/10.15407/emodel.45.03.043

А.В. Тіменко, В.В. Шкарупило, Н.А. Куликовська

МОДЕЛЬ ФОРМАЛІЗАЦІЇ ВИМОГ У ЧАСТИНІ КОНТРОЛЮ СУМІСНОСТІ КОМПОНЕНТІВ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

Сучасний стан розвитку енергетичної галузі характеризується переходом до децентралізованих моделей управління на основі концепції мікромереж що виступають стратегічним інструментом забезпечення резилієнтності енергосистем. Функціонування таких автономних кластерів базується на використанні розвиненої інфраструктури Інтернету речей, де велика кількість інтелектуальних пристроїв забезпечує моніторинг та балансування навантаження у реальному часі. Критичним аспектом стабільності мікромережі є координація взаємодії між гетерогенними сенсорами, актуаторами та контролерами, що потребує впровадження надійних методів забезпечення їхньої сумісності.

Забезпечення сумісності між різними компонентами систем Інтернету речей стає актуальним завданням на тлі стрімкого розвитку технологій та їхнього впливу на різноманітні сфери життя [1]. Особливо важливим це є у контексті розроблення та інтеграції систем з високим рівнем різнорідності та динамічності. Питання сумісності компонентів розглядається на прикладному рівні семирівневої моделі відкритих систем, де за основу береться комунікаційні протоколи, такі як MQTT (Message Queuing Telemetry Transport). Для уникнення непередбачуваних сценаріїв взаємодії та відмов пропонується підхід, заснований на засобах темпоральної логіки дій TLA (Temporal Logic of Actions) [2]. Цей підхід призначений для автоматизованої перевірки сумісності між компонентами шляхом формальної верифікації, що вже знайшло своє практичне застосування у великих хмарних інфраструктурах [3].

Розроблена модель формалізації зв'язків між компонентами будується на математичному апараті структури Кріпке. Для оцінювання корисного ефекту опрацьовується специфікація протоколу MQTT, а саме – підтримувані ним рівні якості обслуговування повідомлень. При описі моделі використовуються концепції дії (Action) та поведінки (Behavior) логіки TLA.

У запропонованій моделі механізм формування специфікацій переходів реалізовано на основі тернарного оператора, що дозволяє одержувати послідовності станів та формалізувати властивості системи. Процес верифікації зводиться до топологічного співставлення графів, де аналізуються кількості станів (вершин) та глибини обходів графів. Якщо означені параметри графів для специфікацій різних компонентів співпадають, то відповідні компоненти характеризуються як сумісні на рівні протоколів взаємодії (рис. 1).

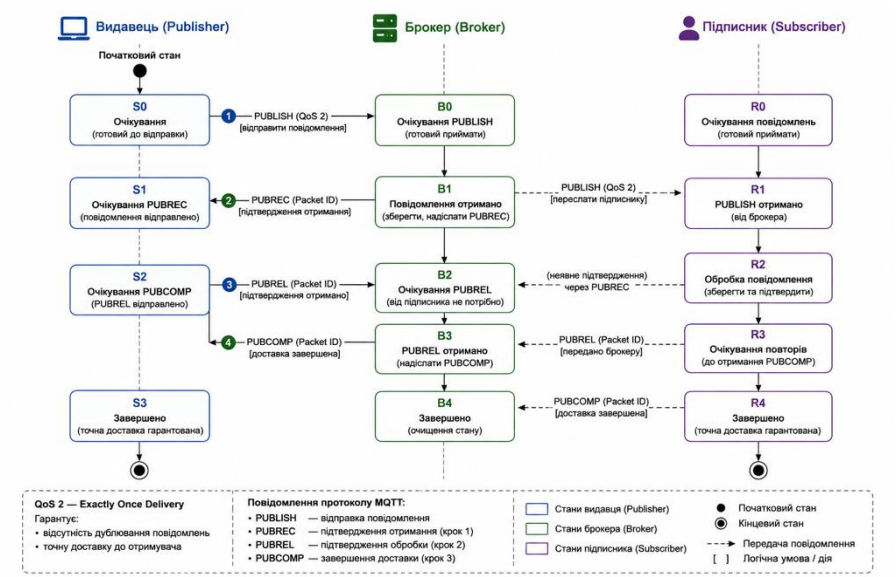


Рисунок 1 – Схема взаємодії компонентів згідно протоколу MQTT на рівні QoS 2

У межах дослідження формалізовано сценарій, за якого визначені компоненти системи підтримують взаємодію виключно на рівні QoS 2 (Quality of Services). Було створено формальні специфікації. Їх відповідність було підтверджено експериментальним шляхом. Проведено оцінювання часових витрат, супутніх процесу їх верифікації (табл. 1).

Таблиця 1 – Результати оцінювання часових витрат

Кількість компонентів	Часові витрати, с
П'ять сервісів	1,2
Десять сервісів	247,0
П'ятнадцять сервісів	1843,0

Отримані результати підтверджують експоненційний характер зростання обчислювальної складності вирішення задачі формальної верифікації методом перевірки на моделі зі збільшенням кількості залучених компонентів [1]. Водночас результати верифікації підтвердили узгодженість взаємодії компонентів для всіх розглянутих сценаріїв функціонування системи. Запропонована модель забезпечує модульність подання формалізованого опису та можливість реконфігурування специфікацій при зміні технічних вимог, без необхідності повного перепроєктування

архітектурної складової програмної системи. Корисний ефект від застосування розробленої моделі полягає у наступних позиціях:

– виявлення потенційних несумісностей компонентів на рівні протоколів взаємодії вже на ранніх етапах процесу розроблення системи;

– можливість залучення вже наявного інструментарію автоматизації процесу формальної верифікації методом перевірки на моделі TLC (TLA Checker);

– отримання кількісних оцінок сумісності компонентів розроблюваної системи вже на етапі її проєктування.

Вбачається, що застосування розробленої моделі сприятиме підвищенню резилієнтності гетерогенних систем критичного призначення, у тому числі таких, що забезпечують стале функціонування електроенергетичної інфраструктури.

[1] Тіменко А. В. та ін. Формальна модель перевірки сумісності компонентів IoT системи. Вчені записки ТНУ імені В.І. Вернадського. Серія Технічні науки. 2025. Том 36. № 5 частина 2. С. 352-358.

[2] Lamport L. The Temporal Logic of Actions. ACM Transactions on Programming Languages and Systems. 1994. Vol. 16, No. 3. P. 872–923.

[3] Newcombe C., Rath T., Zhang F., Munteanu B., Brooker M., Deardeuff M. How Amazon web services uses formal methods. Communications of the ACM. 2015. Vol. 58, No. 4. P. 66-73.

В.Р. Герасимов, В.В. Душеба

ВИЯВЛЕННЯ АГРЕГАТНИХ МЕЖ НА ОСНОВІ ORM-МЕТАДАНИХ ПРИ МІГРАЦІЇ РЕЛЯЦІЙНИХ СТРУКТУР ДО ДОКУМЕНТНО-ОРІЄНТОВАНИХ БАЗ ДАНИХ

Міграція реляційних даних до документно-орієнтованих баз даних є актуальною задачею для інформаційних систем, у яких необхідно підвищити ефективність доступу до даних і зменшити кількість складних з'єднань між таблицями [1]. Одним із ключових етапів такої міграції є визначення агрегатних меж, тобто встановлення того, які сутності доцільно зберігати в межах одного документа, а які — як окремі об'єкти з посиланнями [2].

Традиційні схемоорієнтовані підходи до міграції спираються переважно на аналіз таблиць, атрибутів, первинних і зовнішніх ключів [3]. Проте реляційна схема не завжди відображає прикладну семантику зв'язків. Однакові за структурою зв'язки можуть мати різне значення на рівні програмного застосунку: одна сутність може бути частиною основного об'єкта, інша — незалежним ресурсом.

Додатковим джерелом прикладної семантики можуть бути ORM-метадані. Вони містять відомості про типи зв'язків між сутностями, каскадні операції, стратегії завантаження, ознаки володіння та життєвий цикл об'єктів. Це дозволяє точніше обирати між вкладенням даних у документ (Embedding) та збереженням через посилання (Referencing). Такий підхід узгоджується з принципами модельно-керованої інженерії, де трансформація даних має спиратися не лише на фізичну схему, а й на модель предметної області [4].

Наприклад, наявність каскадного видалення або параметра orphanRemoval може свідчити, що сутність не має самостійного життєвого циклу і повинна бути частиною основного агрегату. Натомість незалежний життєвий цикл, повторне використання сутності в різних контекстах або її роль як довідника вказують на доцільність використання посилання.

Як приклад можна розглянути інформаційну систему обліку споживання електроенергії. У реляційній моделі сутності Consumer, Meter, MeterReading, Tariff та Substation можуть бути представлені окремими таблицями. Аналіз ORM-метаданих дозволяє визначити, що MeterReading має тісний зв'язок із конкретним Meter і може бути згрупований у межах документа лічильника або окремого агрегату періодичних вимірювань. Водночас Tariff має незалежний життєвий цикл, застосовується до багатьох споживачів або груп обліку та змінюється незалежно від конкретних показників, тому його доцільніше зберігати окремо через посилання.

Substation також є незалежним інфраструктурним об'єктом, пов'язаним із багатьма споживачами або лічильниками, тому її повне вкладення в кожен документ призвело б до дублювання даних. Натомість технічні параметри конкретного Meter, які мають спільний життєвий цикл із ним і часто використовуються разом із показниками, можуть бути включені до

відповідного документа.

Таким чином, ORM-метадані дозволяють уникнути формального перенесення реляційної структури до NoSQL без урахування логіки роботи застосунку. Перспективним є поєднання такого підходу з інтелектуальними методами аналізу програмного коду, зокрема великими мовними моделями, які можуть використовуватися як допоміжний інструмент для виявлення семантичних ознак у програмних системах [5], [6].

Висновки: Визначення агрегатних меж є важливим етапом міграції реляційних даних до документно-орієнтованих баз даних. Реляційна схема містить структурні зв'язки, але не завжди відображає їх прикладну семантику. ORM-метадані можуть виступати додатковим джерелом такої семантики та допомагати у виборі між стратегіями Embedding і Referencing. Подальші дослідження доцільно спрямувати на формалізацію правил використання ORM-ознак для автоматизованого визначення агрегатних меж.

[1] Sadalage P. J., Fowler M. NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence. — Boston : Addison-Wesley, 2012. — 192 p.

[2] Akoka J., Comyn-Wattiau I. Roundtrip engineering of NoSQL databases // Enterprise Modelling and Information Systems Architectures (EMISAJ). — 2018. — Vol. 13. — DOI: https://doi.org/10.18417/emisa.si.hcm.22

[3] El Alami A., Khourdifi Y., Ait El Mouden Z., Lahmer M., Hasnaoui M. L. Migrating Relational Databases to NoSQL-Oriented Documents Using Object-Oriented Concepts // International Journal of Intelligent Engineering and Systems. — 2024. — Vol. 17, No. 4. — DOI: https://doi.org/10.22266/ijies2024.0831.48

[4] 4. Chebotko A., Kashlev A., Lu S. A Big Data Modeling Methodology for Apache Cassandra // Proceedings of the IEEE International Congress on Big Data (BigData Congress 2015). — IEEE, 2015. — P. 238–245. — DOI: https://doi.org/10.1109/BigDataCongress.2015.41

[5] Brambilla M., Cabot J., Wimmer M. Model-Driven Software Engineering in Practice. — 2nd ed. — Springer, 2017. — DOI: https://doi.org/10.1007/978-3-031-02549-5

[6] Linares-Vásquez M., Bavota G., Bernal-Cárdenas C., Di Penta M., Oliveto R., Poshyvanyk D. Documenting Database Usages and Schema Constraints in Database-Centric Applications // Proceedings of the 25th ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2016). — ACM, 2016. — P. 270–281. — DOI: https://dl.acm.org/doi/10.1145/2931037.2931072

С.Ф. Гончар

АНАЛІЗ БЕЗПЕКОВИХ АСПЕКТІВ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ КЕРУВАННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стрімкий розвиток цифрових технологій зумовлює необхідність пошуку нових інструментів захисту та управління об’єктами критичної інфраструктури (ОКІ). Впровадження інтелектуальних систем дозволяє автоматизувати складні процеси, проте вимагає ретельного аналізу безпекових ризиків [1, 2].

За результатами аналізу сучасних наукових досліджень та міжнародних звітів встановлено, що інтеграція штучного інтелекту (ШІ) в системи керування та безпеки ядерних установок та інших об’єктів критичної інфраструктури (ОКІ) є неминучим етапом еволюції галузі [3]. Проте успішність такої трансформації залежить від обраної моделі впровадження.

Впровадження ШІ на об'єктах критичної інфраструктури має свої незаперечні переваги а також може створювати критичні ризики, що потребують контролю.

Переваги, що домінують:

- швидкість реагування: ШІ здатен аналізувати тисячі технологічних параметрів за мілісекунди, що фізично неможливо для людини-оператора. У критичних сценаріях (наприклад, швидка зміна реактивності або різке падіння тиску) це дозволяє запобігти аварійним ситуаціям;

- превентивність: перехід від стратегії «ремонту за фактом поломки» до «прогнозного обслуговування» значно знижує ймовірність техногенних збоїв за рахунок раннього виявлення деградації обладнання [4].

Критичні ризики, що потребують контролю:

- непередбачуваність «чорної скриньки»: основний ризик полягає у складності верифікації рішень ШІ. Для ОКІ, зокрема енергетичної галузі, це є критичним фактором. Впровадження має супроводжуватися технологіями Explainable Artificial Intelligence (XAI). На відміну від класичних моделей ШІ, які видають лише фінальний результат, XAI дозволяє оператору зрозуміти логіку алгоритму: які саме параметри (температура, тиск, мережевий трафік тощо) стали причиною спрацювання системи [5]. Це забезпечує прозорість прийняття рішень та дозволяє оператору вчасно виявити помилкове спрацювання алгоритму;

- кібервразливість: ШІ створює нову «поверхню атаки». Зловмисники можуть використовувати методи маніпулювання вхідними даними, щоб змусити систему «не помітити» реальну загрозу або згенерувати хибний сигнал тривоги [6].

Запропонована концептуальна модель (рис. 1) демонструє ієрархічний підхід до управління, де модуль пояснювального штучного інтелекту (XAI) виступає аналітичним посередником між автоматизованими алгоритмами та

оператором. Це забезпечує прозорість прийняття рішень та гарантує виконання принципу людського контролю у межах ізольованого безпекового контуру.

Окремим аспектом безпеки є забезпечення фізичної ізоляції критичних сегментів мережі. Навчання та оновлення моделей ШІ має відбуватися в ізольованих середовищах ("air-gapped" zones). Це унеможливлює прямий доступ зовнішніх зловмисників до навчальних вибірок та запобігає несанкціонованій зміні параметрів нейронних мереж через глобальну мережу.

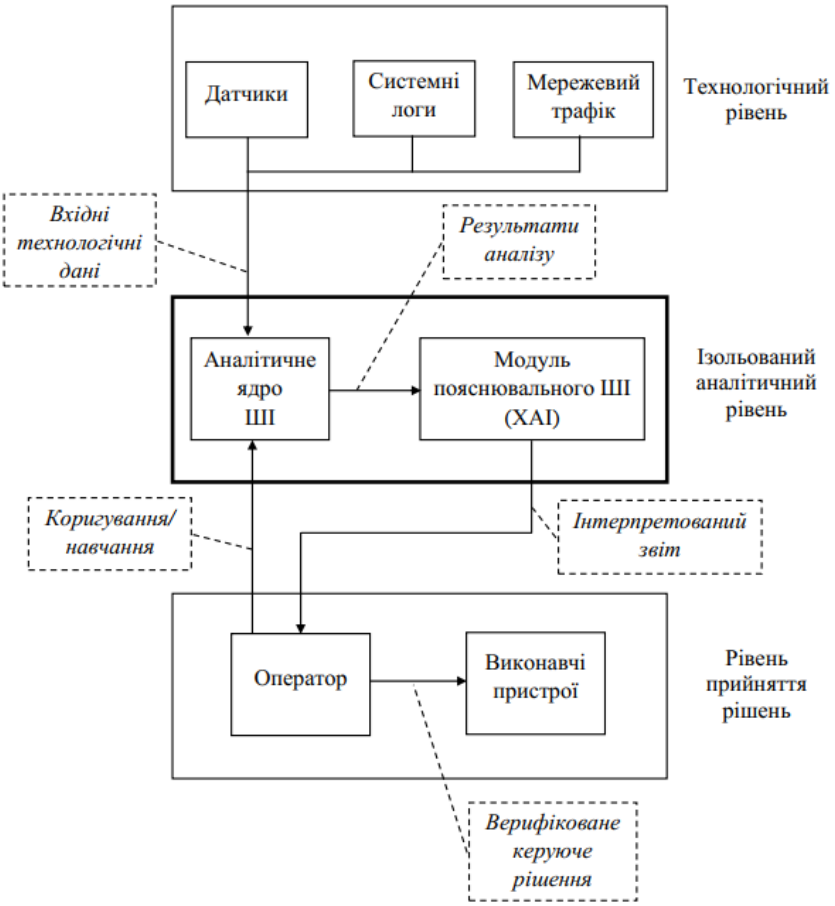


Рис. 1. Архітектура безпечного управління ОКІ з використанням ізольованого аналітичного контуру ШІ

Таким чином, на даному етапі розвитку технологій переваги ШІ перевищують потенційні ризики лише за умови суворого дотримання принципу «Людина в контурі управління». ШІ має виступати як потужна інтелектуальна підтримка, а не як автономний суб'єкт прийняття остаточних рішень на критичних етапах.

Впровадження ШІ на об'єктах критичної інфраструктури має відбуватися поетапно: від моніторингу допоміжного обладнання до систем підтримки прийняття рішень, і лише після тривалих випробувань – до автоматизованого керування основними технологічними процесами. При цьому обов'язковою умовою є використання ізольованих зон для обробки даних, що гарантує цілісність алгоритмів та захищає критичну інфраструктуру від віддалених кібератак.

[1] Гончар С.Ф. Методологія оцінки ризиків кібербезпеки інформаційної системи об’єктів критичної інфраструктури. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. 2019. Том 30(69). Ч.1. С.40 – 43.

[2] Alguliyev, R., Aliguliyev, R., & Fataliyev, T. (2023). Cyber-physical systems security: Challenges and opportunities of artificial intelligence. Journal of Cyber Security Technology, 7(1), 1–24.

[3] IAEA. (2021). Computer security for nuclear facilities (Nuclear Security Series No. 42-G). International Atomic Energy Agency.

[4] OECD/NEA. (2024). Artificial intelligence in the nuclear sector: Opportunities and challenges. OECD Publishing.

[5] Islam, M. R., Ahmed, M. U., Barua, S., & Begum, S. (2024). Explainable artificial intelligence (XAI) for next-generation industrial automation: A review. IEEE Access, 12, 15432–15455.

[6] Клевцов, О. Л. (2022). Питання кібербезпеки інформаційних та керуючих систем атомних електричних станцій. Ядерна та радіаційна безпека, 1(93), 44–53.

К.В. Середюк, С.В. Суровцев

ЦИФРОВІЗАЦІЯ ТА МОДЕЛЮВАННЯ ПРОЦЕСІВ УПРАВЛІННЯ ВИТРАТАМИ НА ПЕРСОНАЛ У СИСТЕМІ СТАЛОГО РОЗВИТКУ ЕНЕРГЕТИЧНИХ ПІДПРИЄМСТВ

Трансформаційні процеси, що відбуваються в енергетичному секторі України, зумовлюють необхідність пошуку нових підходів до управління підприємствами в умовах воєнної економіки, цифровізації та посилення вимог до сталого розвитку. Сучасні енергетичні підприємства функціонують в умовах високого рівня ризиків, нестабільності зовнішнього середовища та дефіциту трудових ресурсів, що актуалізує проблему ефективного управління витратами на персонал.

У системі сучасного менеджменту людський капітал розглядається не лише як ресурс, а як стратегічний фактор забезпечення конкурентоспроможності, економічної стійкості та резильєнтності підприємства. Саме тому питання цифровізації HR-процесів, використання аналітичних платформ, автоматизації кадрового управління та економіко-математичного моделювання кадрових витрат набувають особливого значення для енергетичної галузі.

Актуальність теми посилюється необхідністю адаптації систем управління персоналом до сучасних викликів, зокрема до змін ринку праці, міграції кадрів, професійного вигорання працівників та необхідності забезпечення безперервності функціонування критичної інфраструктури. У таких умовах цифровізація процесів управління витратами на персонал стає важливим інструментом підтримки сталого розвитку енергетичних підприємств та підвищення ефективності управлінських рішень.

Теоретичним підґрунтям дослідження є сучасні концепції цифрової економіки, сталого розвитку, управління людським капіталом та адаптивного менеджменту. Особливу увагу приділено застосуванню методів економічного моделювання, HR-аналітики та цифрових платформ у системі управління персоналом енергетичних підприємств.

Сучасний етап розвитку енергетичної галузі України характеризується високим рівнем невизначеності, цифровою трансформацією бізнес-процесів та необхідністю забезпечення безперервного функціонування критичної інфраструктури. За таких умов особливого значення набуває ефективне управління витратами на персонал як одним із ключових напрямів забезпечення економічної стійкості енергетичних підприємств [1].

У науковій літературі витрати на персонал розглядаються як сукупність витрат підприємства, пов’язаних із забезпеченням трудової діяльності працівників, включаючи оплату праці, соціальні виплати, професійне навчання, охорону праці та розвиток людського капіталу [2]. Водночас сучасні підходи до управління персоналом передбачають перехід від традиційної кадрової роботи до використання цифрових систем управління

людськими ресурсами (HRM-систем), які забезпечують автоматизацію кадрових процесів та аналітичну підтримку прийняття управлінських рішень [3].

Для енергетичних підприємств, зокрема Групи ДТЕК, людський капітал є стратегічним ресурсом, що визначає ефективність функціонування виробничих систем та рівень резильєнтності компанії в умовах кризових викликів. У зв'язку з цим особливої актуальності набуває впровадження інструментів цифровізації управління персоналом, спрямованих на оптимізацію витрат та підвищення продуктивності праці.

Теоретичною основою цифровізації процесів управління витратами на персонал є концепції сталого розвитку, цифрової економіки та data-driven management, відповідно до яких управлінські рішення повинні базуватися на аналізі великих масивів даних, прогнозуванні та моделюванні економічних процесів [4]. Застосування HR-аналітики дозволяє оцінювати взаємозв'язок між рівнем витрат на персонал, продуктивністю праці, рівнем плинності кадрів та ефективністю функціонування підприємства.

У межах дослідження доцільно використовувати економіко-математичну модель оцінювання ефективності управління витратами на персонал:

$$E = f * (W, P, T, R) \quad (1)$$

де:

E — ефективність управління витратами на персонал;

W — витрати на оплату праці;

P — продуктивність праці;

T — рівень плинності кадрів;

R — рівень цифровізації HR-процесів.

Запропонована модель дозволяє визначати вплив цифрових технологій на оптимізацію кадрових витрат та ефективність використання трудових ресурсів. Практичне застосування таких моделей на енергетичних підприємствах забезпечує можливість прогнозування потреби у персоналі, оцінювання ефективності кадрової політики та формування сценаріїв управлінських рішень.

На основі проведених досліджень у сфері управління персоналом, цифровізації бізнес-процесів, адаптації менеджменту до кризових умов та розвитку інноваційного потенціалу підприємств автором запропоновано комплекс рекомендацій для енергетичних компаній. Одним із ключових напрямів є впровадження інтегрованих цифрових HRM-систем, що передбачають створення єдиної цифрової платформи управління персоналом, яка об'єднуватиме кадровий облік, систему оцінювання ефективності працівників, аналітику витрат та інструменти прогнозування кадрових потреб.

Важливим напрямом удосконалення системи управління персоналом є використання predictive HR-аналітики. Доцільним є застосування

інструментів прогнозної аналітики для оцінювання ризиків плинності кадрів, визначення потреб у перекваліфікації персоналу та прогнозування ефективності витрат на оплату праці.

В умовах цифрової трансформації енергетичних підприємств особливого значення набуває розвиток цифрових компетентностей персоналу. Необхідним є системне навчання працівників цифровим навичкам, роботі з автоматизованими системами та сучасними інформаційними технологіями.

Для забезпечення резильєнтності енергетичних підприємств доцільним є використання сценарного моделювання кадрових витрат залежно від зміни економічних, безпекових та виробничих факторів. Такий підхід дозволить підвищити адаптивність системи управління персоналом до кризових умов.

Окрему увагу необхідно приділити формуванню адаптивної системи мотивації персоналу, що передбачає поєднання матеріальної та нематеріальної мотивації з урахуванням рівня професійного навантаження, психологічної стійкості працівників та специфіки роботи в умовах воєнної економіки.

Крім того, енергетичним підприємствам доцільно інтегрувати принципи сталого розвитку у кадрову політику шляхом впровадження ESG-підходів у систему управління персоналом, зокрема у сфері безпеки праці, підтримки добробуту працівників, розвитку інклюзивності та корпоративної соціальної відповідальності.

Запропоновані рекомендації сприятимуть підвищенню ефективності управління витратами на персонал, оптимізації кадрової політики та забезпеченню сталого розвитку енергетичних підприємств в умовах сучасних викликів.

Отже, в умовах цифрової трансформації економіки та посилення кризових викликів питання ефективного управління витратами на персонал набуває стратегічного значення для енергетичних підприємств. Проведене дослідження підтвердило, що цифровізація HR-процесів та використання економіко-математичного моделювання сприяють підвищенню ефективності кадрової політики, оптимізації витрат і забезпеченню адаптивності системи управління персоналом.

Визначено, що впровадження цифрових HRM-систем, HR-аналітики, прогнозних моделей управління кадровими ресурсами та сценарного моделювання дозволяє енергетичним підприємствам оперативно реагувати на зміни зовнішнього середовища, мінімізувати ризики втрати людського капіталу та підтримувати стабільність функціонування виробничих процесів. Особливого значення набуває інтеграція принципів сталого розвитку та ESG-підходів у систему управління персоналом, що забезпечує підвищення рівня резильєнтності підприємств в умовах воєнної економіки.

Практична цінність дослідження полягає у запропонованих рекомендаціях щодо розвитку цифрових компетентностей персоналу, удосконалення систем мотивації працівників, впровадження predictive HR-аналітики та створення інтегрованих цифрових платформ управління

персоналом. Реалізація запропонованих заходів сприятиме підвищенню конкурентоспроможності енергетичних підприємств, забезпеченню економічної стійкості та підтримці сталого розвитку енергетичної галузі України.

[1] Армстронг М. Практика управління людськими ресурсами. Київ : КНЕУ, 2021. 608 с.
[2] Колот А. М., Цимбалюк С. О. Управління персоналом : підручник. Київ : КНЕУ, 2020. 680 с.
[3] Цифрова трансформація економіки України : монографія / за ред. О. В. Криворучко. Харків : ХНЕУ, 2022. 340 с.
[4] OECD Digital Transformation and the Future of Work. Paris : OECD Publishing, 2022. 128 p.
[5] ДТЕК : офіційний сайт. URL: https://dtek.com (дата звернення: 11.05.2026).

А.В. Яцишин, Є.В. Кочелаб, В.О. Артемчук,
С.І. Скуратівський, Т.М. Яцишин

МАТЕМАТИЧНІ ПІДХОДИ ДО КОМПЛЕКСНОГО ОЦІНЮВАННЯ НЕРАДІАЦІЙНИХ ВИКИДІВ АЕС УКРАЇНИ

Під час оцінювання екологічної безпеки АЕС основна увага традиційно приділяється радіаційним чинникам. Водночас експлуатація АЕС супроводжується також нерадіаційними викидами, пов'язаними з роботою допоміжних енергетичних установок, дизель-генераторів, резервних котелень, транспортної інфраструктури, систем вентиляції та іншого технологічного обладнання. До таких викидів можуть належати оксиди азоту, діоксид сірки, оксид вуглецю, тверді частинки та інші забруднювальні речовини. Їхній вплив, як правило, є локальним або регіональним, однак для прилеглих територій він потребує окремого аналізу, особливо за умов тривалої експлуатації енергетичних об'єктів.

Актуальність розроблення математичних засобів для комплексної оцінки такого впливу зумовлена тим, що прямі інструментальні вимірювання не завжди дають повну картину просторового поширення домішок в атмосферному повітрі. Концентрації забруднювальних речовин залежать не лише від потужності джерела викиду, а й від висоти труби, температури та швидкості газоповітряної суміші, рельєфу, забудови, метеорологічних умов, сезонності й турбулентного стану атмосфери. Саме тому сучасна оцінка впливу промислових об'єктів на якість повітря значною мірою спирається на моделі атмосферного розсіювання, які використовуються як у регуляторній практиці, так і в епідеміологічних дослідженнях [1].

Для завдань, пов'язаних з АЕС України, доцільно формувати багаторівневу систему математичного оцінювання. Перший рівень має охоплювати інвентаризацію джерел нерадіаційних викидів і формування вхідних параметрів: координат джерел, висоти викиду, витрат газоповітряної суміші, температури, складу забруднювальних речовин і режимів роботи обладнання. Другий рівень повинен забезпечувати метеорологічну підготовку даних, зокрема врахування швидкості й напряму вітру, температурної стратифікації, атмосферної стійкості, висоти шару перемішування та опадів. Третій рівень передбачає власне моделювання розсіювання із застосуванням AERMOD, CALPUFF або інших моделей, залежно від масштабу території та характеру джерел.

Вибір моделі є принциповим елементом дослідження. AERMOD доцільно застосовувати для локальних оцінок впливу стаціонарних джерел за відносно однорідних умов, тоді як CALPUFF краще враховує змінні метеорологічні умови, складний рельєф і перенесення домішок на більші відстані. Порівняльні дослідження показують, що результати AERMOD і CALPUFF можуть суттєво відрізнятися залежно від типу джерела, метеорологічної ситуації та просторового масштабу моделювання [2, 3].

Окремі сучасні роботи також підтверджують важливість валідації моделей за фактичними спостереженнями, оскільки для площинних і складних джерел різні моделі можуть давати різну оцінку максимальних концентрацій і зон впливу [4].

Особливої уваги потребує поєднання дисперсійного моделювання з оцінкою ризиків для здоров'я населення. У такому разі розраховані приземні концентрації забруднювальних речовин можуть використовуватися для визначення зон потенційного впливу, порівняння з гранично допустимими концентраціями, оцінювання хронічного інгаляційного навантаження та визначення пріоритетних речовин для моніторингу. Подібний підхід використано в дослідженнях промислового забруднення, де моделі розсіювання поєднувалися з довгостроковою оцінкою ризику для населення [5]. Для українських АЕС це може бути корисним не лише для поточної екологічної оцінки, а й для планування санітарно-захисних зон, розміщення постів моніторингу та підготовки сценаріїв реагування у разі зміни режимів роботи обладнання.

Перспективним напрямом є інтеграція математичних моделей із фактичними даними спостережень. Зокрема, сучасні дослідження демонструють можливість поєднання інструментального моніторингу викидів SO_2 з подальшим моделюванням їх розсіювання за допомогою AERMOD (рис. 1) [6]. Такий підхід може бути адаптований і для об'єктів атомної енергетики: результати стаціонарного екологічного моніторингу, метеорологічних спостережень і розрахунків розсіювання мають розглядатися як взаємодоповнювальні джерела інформації, а не як ізольовані блоки оцінювання.

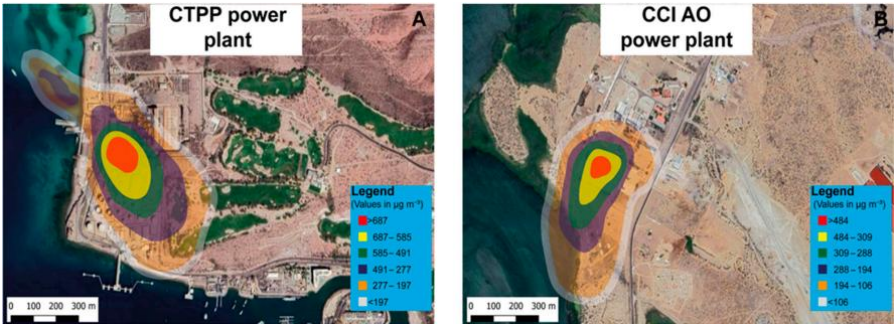


Рисунок 1 – Приклад моделювання розсіювання SO_2 від енергетичного об'єкта за допомогою AERMOD [6]

Окремий методичний інтерес становить комплексне оцінювання нерадіаційних викидів енергетичних об'єктів із застосуванням багатокритеріальних підходів. У дослідженні A.I. Chatzimouratidis та P.A. Pilavachi нерадіаційні викиди електростанцій розглянуто як один із важливих критеріїв порівняльної оцінки енергетичних технологій [7]. Для АЕС України це може бути використано під час формування інтегральної

системи показників, яка поєднує екологічні, санітарно-гігієнічні, технологічні та просторові характеристики впливу.

Отже, розроблення математичних засобів для комплексної оцінки впливу нерадіаційних викидів АЕС України має ґрунтуватися на поєднанні інвентаризації джерел, метеорологічного аналізу, дисперсійного моделювання, валідації результатів і оцінки потенційних ризиків для населення прилеглих територій. Такий підхід дає змогу перейти від формального контролю окремих показників до просторово обґрунтованої оцінки впливу, необхідної для підвищення екологічної безпеки, удосконалення моніторингу атмосферного повітря та прийняття управлінських рішень щодо зменшення нерадіаційного навантаження.

[1] Johnson, J. B. (2022). An introduction to atmospheric pollutant dispersion modelling. Environmental Sciences Proceedings, 19(1), 18. https://doi.org/10.3390/ecas2022-12826

[2] Jittra, N., Pinthong, N., & Thepanondh, S. (2015). Performance evaluation of AERMOD and CALPUFF air dispersion models in industrial complex area. Air, Soil and Water Research, 8, ASWR.S32781. https://doi.org/10.4137/ASWR.S32781

[3] Amoatey, P., Omidvarborna, H., Affum, H. A., & Baawain, M. (2018). Performance of AERMOD and CALPUFF models on SO2 and NO2 emissions for future health risk assessment in Tema Metropolis. Human and Ecological Risk Assessment: An International Journal, 25(3), 772–786. https://doi.org/10.1080/10807039.2018.1451745

[4] Tagliaferri, F., Rota, A., & Invernizzi, M. (2025). Area source emissions: A validation study of CALPUFF and LAPMOD models. Atmospheric Environment: X, 100348. https://doi.org/10.1016/j.aeaoa.2025.100348

[5] Bayraktar, O. M., & Mutlu, A. (2024). Analyses of industrial air pollution and long-term health risk using different dispersion models and WRF physics parameters. Air Quality, Atmosphere & Health, 17, 2277–2305. https://doi.org/10.1007/s11869-024-01573-8

[6] Schiavo, B., Stremme, W., Meza, J. V., Rangel-Rodríguez, R., Carbajal-Aguilar, C. C., Ortega-Flores, P. A., et al. (2025). Monitoring and dispersion of SO2 emissions from power plants using UV camera and AERMOD: A case study of Baja California Sur, Mexico. Atmosphere, 16(10), 1128. https://doi.org/10.3390/atmos16101128

[7] Chatzimouratidis, A. I., & Pilavachi, P. A. (2007). Objective and subjective evaluation of power plants and their non-radioactive emissions using the analytic hierarchy process. Energy Policy, 35(8), 4027–4038. https://doi.org/10.1016/j.enpol.2007.02.003

О. Фаррахов, В. Ковач, А. Запорожець, Ю. Хапко, Н. Лушнікова, Р. Галенда

ПРО НЕОБХІДНІСТЬ РОЗРОБЛЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОГО МЕТОДУ СВОЄЧАСНОГО ВИЯВЛЕННЯ МАЛИХ ТА НАДМАЛИХ БПЛА

Поширення малих та надмалих безпілотних літальних апаратів (БПЛА) суттєво ускладнює забезпечення безпеки об’єктів критичної інфраструктури, промислових підприємств, транспортних вузлів, енергетичних об’єктів і місць масового перебування людей. Такі апарати можуть застосовуватися для несанкціонованого спостереження, доставки небезпечних предметів, здійснення провокацій, диверсій або підготовки терористичних дій. Їх своєчасне виявлення ускладнюється незначними розмірами, низькою ефективною поверхнею розсіювання, здатністю рухатися на малих висотах і маскуватися на складному фоні місцевості. За таких умов стандартні засоби контролю повітряного простору не завжди забезпечують достатню надійність виявлення, що зумовлює потребу в розробленні спеціалізованих інформаційно-технічних підходів.

Необхідність такого дослідження зумовлена тим, що використання лише одного каналу спостереження, як правило, не забезпечує достатньої надійності виявлення та ідентифікації малорозмірних повітряних цілей. Радіолокаційні засоби дають змогу визначати просторові координати й параметри руху цілі, проте можуть мати труднощі з відокремленням малих БПЛА від птахів, фонових відбиттів або інших малорозмірних об’єктів. Радіочастотний моніторинг дає змогу виявляти ознаки каналів керування або передавання даних, але його ефективність залежить від режиму роботи БПЛА. Оптико-електронні та тепловізійні засоби корисні для підтвердження типу об’єкта, однак залежать від освітленості, погодних умов і видимості. Тому сучасні огляди з проблематики UAV detection підкреслюють переваги багатосенсорного підходу, у якому поєднуються радіолокаційні, радіочастотні, оптичні, інфрачервоні та акустичні дані [1].

Метою розроблення інформаційно-технічного методу є створення узгодженої процедури своєчасного виявлення малих та надмалих повітряних цілей на основі комплексного використання радіоелектронних засобів, подальшої обробки різнорідних даних і формування обґрунтованого попереджувального сигналу. Такий метод має бути орієнтований не лише на факт появи об’єкта в контрольованій зоні, а й на оцінювання його траєкторних, сигнальних і класифікаційних ознак. У цьому контексті важливою є не тільки технічна фіксація БПЛА, а й зменшення ймовірності хибних спрацювань, оскільки необґрунтована тривога може порушувати роботу об’єкта та призводити до неефективного використання сил реагування. У межах такого методу радіоелектронні засоби розглядаються не як окремі автономні канали спостереження, а як взаємопов’язані джерела

даних, результати яких узгоджуються в єдиному інформаційному контурі виявлення, класифікації та попередження.

Запропонований підхід доцільно будувати у вигляді кількох послідовних етапів. На першому етапі здійснюється аналіз об'єкта захисту, визначаються потенційні напрями появи малих повітряних цілей, особливості місцевості, наявність фонових перешкод, джерел радіовипромінювання та зон обмеженої видимості. На другому етапі формується склад радіоелектронних засобів спостереження з урахуванням завдань виявлення, супроводження та попередньої ідентифікації цілі. На третьому етапі відбувається збирання первинних даних, їх попередня фільтрація, синхронізація та приведення до єдиного інформаційного формату. На четвертому етапі застосовуються алгоритми об'єднання даних, які дають змогу зіставити просторово-часові, радіочастотні та класифікаційні ознаки об'єкта.

Особливе значення має мультисенсорне злиття даних. Як приклад реалізації концепції мультисенсорного злиття даних для виявлення БПЛА у тривимірному просторі на рис. 1 наведено відповідну структурну схему. У роботах, присвячених виявленню БПЛА у тривимірному просторі, показано, що поєднання різних джерел інформації дає змогу підвищити стійкість системи до перешкод і покращити розпізнавання цілей у складних умовах [2]. Для задач запобігання надзвичайним ситуаціям терористичного характеру це означає, що рішення не повинно ґрунтуватися лише на одному вимірювальному каналі. Більш надійним є варіант, коли попереджувальний висновок формується за сукупністю ознак: появою малорозмірної цілі, характером її руху, наявністю або відсутністю радіочастотних проявів, результатами класифікації та відповідністю траєкторії потенційно небезпечному сценарію.

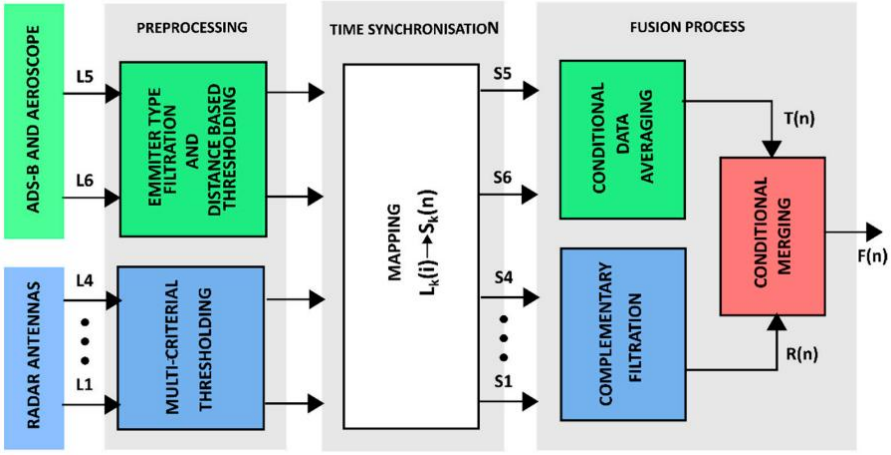


Рисунок 1 – Схема мультисенсорного злиття даних для виявлення БПЛА у тривимірному просторі [2]

Перспективним напрямом є використання методів штучного інтелекту для автоматизованого аналізу сигналів і зображень. Огляд досліджень із застосування глибинного навчання для виявлення БПЛА показує, що такі методи можуть бути ефективними для класифікації та розпізнавання малих повітряних об’єктів, однак потребують якісних навчальних наборів даних, перевірки в різних умовах спостереження та захисту від надмірної адаптації моделі до навчальних даних [3]. Тому для практичного застосування важливо передбачити не лише алгоритм класифікації, а й процедуру валідації результатів, оновлення бази ознак і контроль достовірності прийнятих рішень.

Науково-прикладне значення розроблення такого методу полягає в тому, що виявлення БПЛА розглядається не як робота окремого технічного засобу, а як узгоджена інформаційно-технічна процедура. Вона має поєднувати моніторинг повітряного простору, попередню обробку та фільтрацію сигналів, злиття даних із різних джерел, класифікацію об’єктів і формування попереджувального сигналу. Практичне застосування такого підходу може сприяти підвищенню безпеки об’єктів критичної інфраструктури, розвитку систем ситуаційної обізнаності та своєчасному реагуванню на загрози терористичного характеру.

[1] Semenyuk, V., Kurmashev, I., Lupidi, A., Alyoshin, D., Kurmasheva, L., & Cantelli-Forti, A. (2025). Advances in UAV detection: Integrating multi-sensor systems and AI for enhanced accuracy and efficiency. International Journal of Critical Infrastructure Protection, 49, 100744. https://doi.org/10.1016/j.ijcip.2025.100744

[2] Dudczyk, J., Czyba, R., & Skrzypczyk, K. (2022). Multi-sensory data fusion in terms of UAV detection in 3D space. Sensors, 22(12), 4323. https://doi.org/10.3390/s22124323

[3] Al-lQubaydhi, N., Alenezi, A., Alanazi, T., Senyor, A., Alanezi, N., Alotaibi, B., Alotaibi, M., Razaque, A., & Hariri, S. (2024). Deep learning for unmanned aerial vehicles detection: A review. Computer Science Review, 51, 100614. https://doi.org/10.1016/j.cosrev.2023.100614

Є. Пилипчук, В. Артемчук, В. Куценко, І. Мартинюк, К. Куценко

ІНТЕГРОВАНИЙ ПІДХІД ДО ВИВЧЕННЯ ГЕНЕРАЦІЇ, МІГРАЦІЇ ТА АКУМУЛЯЦІЇ ПРИРОДНОГО ВОДНЮ

Проблематика природного, або ендогенного, водню останніми роками набула особливої актуальності у зв'язку з пошуком низьковуглецевих джерел енергії та необхідністю розширення сировинної бази водневої енергетики. На відміну від промислового водню, що потребує значних енергетичних витрат на виробництво, природний водень формується в надрах Землі внаслідок геологічних, геохімічних і термодинамічних процесів. У сучасних оглядах з геологічного водню наголошується, що для його оцінювання потрібно розглядати не лише джерела генерації, а й шляхи міграції, умови збереження та можливі пастки акумуляції [1, 2]. Саме тому дослідження ендогенного водню доцільно проводити на основі узгодженого аналізу кількох груп даних – структурних, термічних і газогеохімічних. В роботі [2] прямо визначає джерела, міграційні шляхи й покришки як ключові компоненти геологічної водневої системи.

Основними механізмами генерації природного водню вважають серпентинізацію ультраосновних і основних порід, радіоліз води під впливом радіоактивного розпаду урану, торію та калію, дегазацію глибинних магматичних джерел, а також механохімічні реакції, що виникають під час руйнування силікатних порід у зонах тектонічної активізації. Для представницьких ділянок це означає необхідність виділення таких геологічних обстановок, де поєднуються відновні умови, наявність залізовмісних мінералів, глибинні розломи, підвищені теплові потоки й ознаки сучасної флюїдної активності. Особливу увагу варто приділяти рифтогенним структурам, зонам розущільнення кристалічного фундаменту, кільцевим структурам вибухового або вулканогенного походження, а також ділянкам перетину різноспрямованих розломів. Основні механізми утворення природного водню в геологічному середовищі узагальнено на рис. 1. У досліджені [3] серед джерел природного H_2 названо зміну Fe(II)-вмісних порід, радіоліз води, магматичну дегазацію та реакції за участю води під час механічного руйнування силікатних порід.

Структурний аналіз у межах таких досліджень має бути спрямований на встановлення просторового зв'язку між водневими проявами та тектонічними порушеннями. Розломні зони можуть виконувати подвійну роль: з одного боку, вони є каналами надходження глибинних флюїдів, а з іншого – ділянками підвищеної проникності, через які водень може швидко втрачатися. Тому перспективність ділянки визначається не тільки наявністю розломів, а й співвідношенням проникних зон, екранувальних товщ, літологічних бар'єрів і локальних пасток. Для України такий підхід є особливо важливим у межах Дніпровсько-Донецької западини, Українського щита та пов'язаних із ними структурно-тектонічних зон. У роботі [4] щодо

Дніпровсько-Донецького авлакогену підкреслено значення глибинних розломів, кільцевих структур і геофізичних ознак сучасної активізації для прогнозування ділянок підвищеного вмісту водню. Також вказано, що перспективність таких площ визначається не лише структурним положенням, а й сукупністю геофізичних, термічних, гідрогеологічних та геологічних показників.

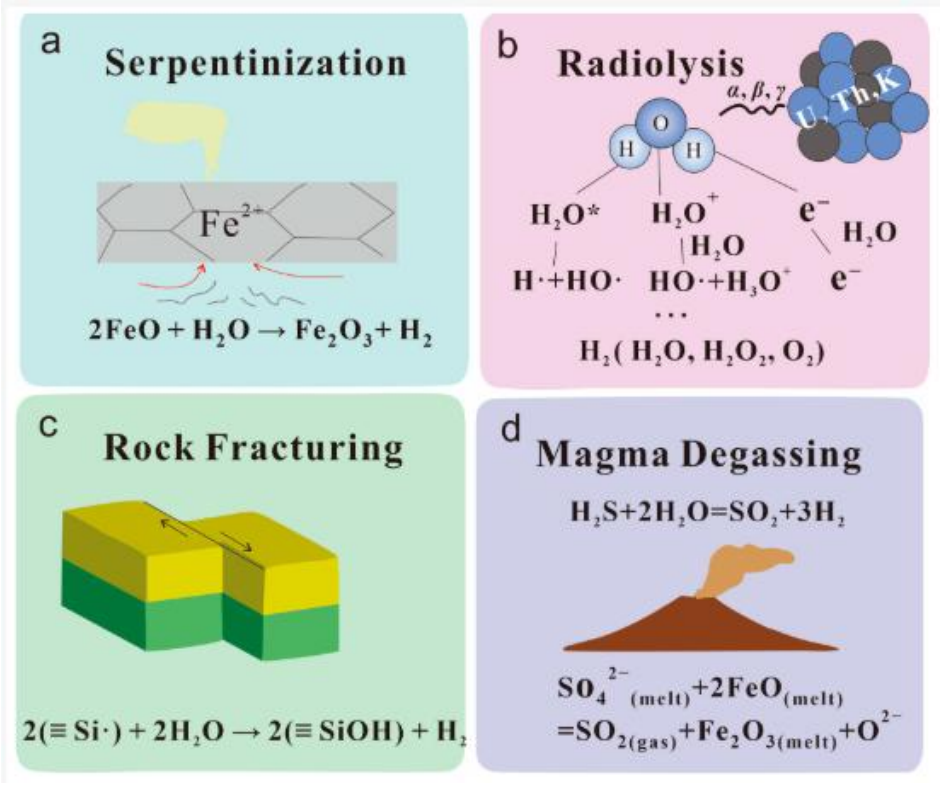


Рисунок 1 – Основні механізми генерації природного водню в геологічному середовищі [3]

Термічні дані є важливими для розуміння умов генерації та збереження водню. Підвищені температури можуть активізувати водо-породні реакції, сприяти флюїдній мобільності та інтенсифікувати дегазаційні процеси. Водночас надмірно висока проникність середовища або відсутність надійних покришок може призводити до розсіювання водню до поверхні. Тому аналіз теплового поля доцільно поєднувати з даними про глибину залягання фундаменту, склад порід, наявність зон тріщинуватості, гідрогеологічний режим і потенційні екрани. Такий підхід дає змогу перейти від фіксації окремих газових аномалій до побудови цілісної моделі водневої системи.

Газогеохімічні дослідження мають забезпечити виявлення просторових і часових закономірностей проявів H_2 у ґрунтовому повітрі, підземних водах, природних газах і свердловинних пробах. Важливими є не лише концентрації водню, а й співвідношення з іншими газами - метаном, гелієм, азотом, вуглекислим газом, радоном та легкими вуглеводнями. Такі співвідношення можуть відображати джерело газу, характер міграції, ступінь окиснення, вплив мікробіологічного споживання та глибину флюїдного живлення. Окреме значення має повторюваність вимірювань, оскільки водневі аномалії можуть мати нестійкий характер і залежати від сезонних, гідрологічних та барометричних умов. Дослідження ґрунтового газу на різних глибинах показують, що інтерпретація водневих аномалій потребує врахування вертикального перенесення H_2 та умов його взаємодії з приповерхневим середовищем [5].

Узгоджений аналіз структурних, термічних і газогеохімічних даних дає змогу виділити представницькі ділянки для детальнішого вивчення, ранжувати їх за перспективністю та сформувати пошукові критерії. Найбільш обґрунтованою є така схема дослідження: спочатку визначаються структурно-тектонічні передумови, далі оцінюється термічний режим і можливі джерела генерації, після цього проводиться газогеохімічне картування та зіставлення аномалій із геологічними структурами. Результатом має стати комплексна модель, яка пояснює, де водень може утворюватися, якими шляхами він мігрує і за яких умов здатний накопичуватися.

Дослідження процесів генерації, міграції та акумуляції ендогенного водню потребує не ізольованого аналізу окремих показників, а інтеграції різнорідних геологічних даних у єдину інтерпретаційну систему. У цьому контексті важливо враховувати, що ресурсний потенціал природного водню поки залишається недостатньо визначеним, а його оцінювання потребує подальшого уточнення геологічних критеріїв, пошукових моделей і методів перевірки водневих аномалій [6]. Такий підхід дає змогу підвищити достовірність прогнозування перспективних ділянок, зменшити ризик хибної інтерпретації газогеохімічних аномалій і сформувати наукову основу для подальших пошуково-розвідувальних робіт на природний водень.

[1] Cao, P., & Ning, F. (2025). Origins, migrations and accumulations of natural hydrogen. Applied Energy, 401, 126726. https://doi.org/10.1016/j.apenergy.2025.126726

[2] Mao, S., Yu, S., Xu, J., Chen, H., Zhao, W., Blunt, M. J., Kang, Q., Gross, M. R., Chen, B., Van Wijk, J. W., Yuan, Q., Gao, K., Kazi, S. R., & Mehana, M. Z. S. (2025). Geologic hydrogen: A review of resource potential, subsurface dynamics, exploration, production, transportation, and research opportunities. Energy & Environmental Science. https://doi.org/10.1039/D5EE02910D

[3] Wang, L., Jin, Z., & Wang, X. (2023). The origin and occurrence of natural hydrogen. Energies, 16(5), 2400. https://doi.org/10.3390/en16052400

[4] Shestopalov, V., Lukin, O., Starostenko, V., Ponomarenko, O., Tsvetkova, T., Koliabina, I., Makarenko, O., Usenko, O., Rud, O., Onoprienko, A., Saprykin, V., & Vardapelian, R. (2021). Prospects for exploration of hydrogen fields in riftogene structures of platforms (the case of the Dnieper-Donets Aulacogene). Geofizicheskiy Zhurnal, 43(5), 3–18. https://journals.uran.ua/geofizicheskiy/article/download/244038/242773/563008

[5] Patino, C., Piedrahita, D., Colorado, E., Aristizabal, K., & Moretti, I. (2024). Natural H2 transfer in soil: Insights from soil gas measurements at varying depths. Geosciences, 14(11), 296. https://doi.org/10.3390/geosciences14110296

[6] Etiope, G., Ellis, G. S., Ardakani, O. H., Boreham, C. J., Klitzke, P., Martín-Monge, A., Reis, H. L. S., Templeton, A. S., Kim, H. S., Gaucher, E., & Sissmann, O. (2026). Understanding the resource potential of natural hydrogen on Earth: Scientific gaps, uncertainties and recommendations. Earth-Science Reviews, 275, 105413. https://doi.org/10.1016/j.earscirev.2026.105413

Р. Мелещенко, В. Ковач, В. Куценко, Р. Драгунцов

ІНЖЕНЕРНО-ТЕХНІЧНИЙ ПІДХІД ДО РАННЬОГО ВИЯВЛЕННЯ ПОЖЕЖОНЕБЕЗПЕЧНИХ СТАНІВ У ПРИМІЩЕННЯХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення безпеки об'єктів критичної інфраструктури є одним із пріоритетних завдань у сфері техногенної безпеки, оскільки порушення їх функціонування може призвести до значних економічних збитків, загрози життю людей, зупинення важливих виробничих процесів і дестабілізації систем життєзабезпечення. Відповідно до Закону України «Про критичну інфраструктуру», такі об'єкти мають особливе значення для економіки, національної безпеки, оборони, функціонування суспільства та безпеки населення [1]. Саме тому для них необхідні не лише традиційні засоби реагування на пожежу, а й інженерно-технічні підходи раннього виявлення небезпечних змін у середовищі, які передують виникненню надзвичайної ситуації. Раннє виявлення пожежонебезпечних станів у приміщеннях об'єктів критичної інфраструктури розглядається як один із ключових елементів попередження надзвичайних ситуацій техногенного характеру, пов'язаних із пожежами та вибухами.

Актуальність дослідження пов'язана з тим, що традиційні системи пожежної сигналізації здебільшого спрацьовують після появи достатньо виражених ознак пожежі – задимлення, підвищення температури, відкритого полум'я або перевищення допустимих концентрацій небезпечних газів. Водночас на початковій стадії загоряння зміни параметрів повітряного середовища часто мають слабко виражений, нестійкий і нерівномірний характер. Це ускладнює їх своєчасне виявлення за допомогою окремих датчиків. Тому більш перспективним є підхід, за якого одночасно аналізуються кілька показників повітряного середовища, зокрема дим, температура, оксид і діоксид вуглецю, а також враховується динаміка їх змін у часі. Такий багатопараметричний контроль дає змогу підвищити надійність раннього виявлення пожежонебезпечних станів у приміщеннях. Зокрема, дослідження [2] підтверджує перспективність газосенсорних масивів для виявлення тління та горіння пластиків, а робота [3] обґрунтовує доцільність одночасного вимірювання диму, CO і CO_2 для скорочення часу спрацювання пожежного сповіщення. Як приклад технічної реалізації багатосенсорного підходу на рис. 1 наведено блок-схему прототипу системи раннього виявлення пожежі на основі масиву газових сенсорів, електроніку оброблення сигналів, платформу збору даних на базі Arduino Due та персональний комп'ютер для збереження й візуалізації результатів вимірювання [2].

Розроблення інженерно-технічного підходу до раннього виявлення пожежонебезпечних станів у приміщеннях об'єктів критичної інфраструктури базується на припущенні, що повітряне середовище

приміщення доцільно розглядати як складну нелінійну динамічну систему, стан якої визначається сукупністю небезпечних факторів: температурою, оптичною щільністю диму, концентрацією чадного газу та, за потреби, іншими газовими компонентами. У роботі [4] зазначено, що раннє загоряння змінює характер флуктуацій цих параметрів, а тому трансформація динаміки станів повітряного середовища може бути використана як інформативна ознака для виявлення загрози ще до переходу ситуації у фазу відкритої пожежі.

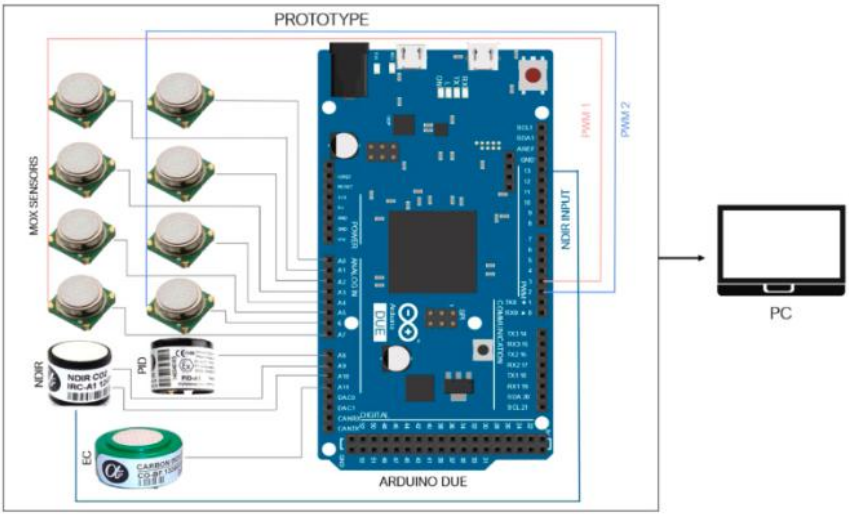


Рисунок 1 – Блок-схема прототипу системи раннього виявлення пожежі на основі масиву газових сенсорів [2]

Сутність запропонованого підходу полягає не лише у фіксації абсолютних значень контрольованих параметрів, а й у поточному аналізі їх прирощень, автокореляцій, взаємних кореляцій та ознак фрактальності. Такий підхід є важливим, оскільки на початковій стадії загоряння небезпечні фактори можуть не перевищувати нормативних або налаштованих порогів, але їх динамічна структура вже змінюється. Для цього доцільно використовувати поточні показники кореляційної розмірності та рекурентності станів. Методологічно такий підхід спирається на положення нелінійного аналізу часових рядів, зокрема алгоритм Grassberger–Procaccia [5] для оцінювання кореляційної розмірності та рекурентний аналіз, започаткований у працях J.-P. Eckmann, S. O. Kamphorst і D. Ruelle [6].

Практична реалізація інженерно-технічного підходу передбачає послідовне виконання кількох процедур. Спочатку здійснюється аналіз приміщень об'єкта критичної інфраструктури з погляду пожежного навантаження, наявності горючих матеріалів, вентиляційного режиму, технологічного обладнання та потенційних джерел займання. Далі

визначаються контрольовані параметри повітряного середовища й обґрунтовується вибір сенсорів. На наступному етапі проводиться безперервне вимірювання температури, диму, CO та інших показників із заданою дискретністю. Отримані сигнали використовуються для розрахунку прирощень станів повітряного середовища, після чого визначаються поточні значення кореляційної розмірності й міри рекурентності. У разі перевищення встановлених порогів система формує попереджувальний сигнал, який може бути використаний для активації інженерних, організаційних або автоматизованих заходів реагування.

Запропонований інженерно-технічний підхід до раннього виявлення пожежонебезпечних станів у приміщеннях об’єктів критичної інфраструктури може розглядатися як дієвий інструмент підвищення техногенної безпеки та попередження надзвичайних ситуацій. Поєднання багатосенсорного вимірювання, аналізу динаміки небезпечних факторів повітряного середовища, кореляційних характеристик і показників фрактальності дає змогу раніше та надійніше виявляти пожежну або вибухонебезпечну ситуацію.

[1] Верховна Рада України. (2021). Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. https://zakon.rada.gov.ua/laws/show/1882-20

[2] Solórzano, A., Eichmann, J., Fernández, L., Fonollosa, J., Marco, S., & Burgués, J. (2022). Early fire detection based on gas sensor arrays: Multivariate calibration and validation. Sensors and Actuators B: Chemical, 352, 130961. https://doi.org/10.1016/j.snb.2021.130961

[3] Chen, S.-J., Hovde, D. C., Peterson, K. A., & Marshall, A. W. (2007). Fire detection using smoke and gas sensors. Fire Safety Journal, 42(8), 507–515. https://doi.org/10.1016/j.firesaf.2007.01.006

[4] Мелещенко, Р. Г. (2021). Інженерно-технічні методи попередження надзвичайних ситуацій техногенного характеру на об'єктах критичної інфраструктури за допомогою оперативного контролю стану повітряного середовища [Дисертація доктора наук, Національний університет цивільного захисту України]. https://uacademic.info/ua/document/0521U000030

[5] Grassberger, P., & Procaccia, I. (1983). Measuring the strangeness of strange attractors. Physica D: Nonlinear Phenomena, 9(1–2), 189–208. https://doi.org/10.1016/0167-2789(83)90298-1

[6] Eckmann, J.-P., Kamphorst, S. O., & Ruelle, D. (1987). Recurrence plots of dynamical systems. Europhysics Letters, 4(9), 973–977. https://doi.org/10.1209/0295-5075/4/9/004

[7] Khan, F., Xu, Z., Sun, J., Khan, F. M., Ahmed, A., & Zhao, Y. (2022). Recent advances in sensors for fire detection. Sensors, 22(9), 3310. https://doi.org/10.3390/s22093310

А. Яцишин, О. Попов, М. Миронцов, О. Фаррахов, Є. Пилипчук

ПЕРСПЕКТИВИ РОЗРОБЛЕННЯ СОРБЕНТУ ВОДНЮ НА ОСНОВІ СИСТЕМИ «ФУЛЕРЕН-МЕТАЛОГІДРИД»

Розвиток водневої енергетики значною мірою залежить від наявності ефективних, безпечних і достатньо компактних способів зберігання водню. Газобалонне зберігання потребує застосування високого тиску та міцних конструкцій, тоді як кріогенний спосіб супроводжується значними енергетичними витратами на охолодження. У зв'язку з цим для автономних і мобільних джерел живлення доцільно розглядати твердофазні накопичувачі, в яких водень утримується в матеріалі-сорбенті та може вивільнятися за визначених температурно-баричних умов. Перспективним напрямом у цьому контексті є поєднання металогідридних матеріалів із вуглецевими наноструктурами, зокрема фулеритом, що дає змогу розглядати систему «фулерен-металогідрид» як одну з можливих основ для створення сучасного сорбенту водню.

Металогідриди відомі високою об'ємною щільністю зберігання водню та відносно безпечним режимом експлуатації порівняно з газобалонними системами. У сучасних дослідженнях зазначається, що металогідридні системи для мобільних застосувань мають різні термодинамічні характеристики, а їх ефективність значною мірою залежить від складу сплаву, кінетики сорбції-десорбції, тепловідведення та циклічної стабільності [1]. Саме ці характеристики є визначальними під час вибору металогідридної складової для накопичувача водню, оскільки матеріал має не лише поглинати достатню кількість водню, а й забезпечувати його контрольоване вивільнення без різких змін робочого режиму. Орієнтиром для оцінювання перспективності розроблюваного сорбенту «фулерен-металогідрид» можуть бути цільові показники гравіметричної та об'ємної ємності систем зберігання водню, наведені в табл. 1.

Таблиця 1 – Цільові показники гравіметричної та об'ємної ємності систем зберігання водню [1]

Показник	2020	2025	Кінцева ціль
Гравіметрична ємність	4,5 мас. %	5,5 мас. %	6,5 мас. %
Об'ємна ємність	30 г H_2/л	40 г H_2/л	50 г H_2/л

Фулерени та фулеритні структури привертають увагу завдяки великій питомій поверхні, наявності впорядкованої молекулярної структури та можливості взаємодії з молекулярним воднем. Теоретичні й експериментальні дослідження показують, що поверхня C_{60} може бути перспективною для адсорбції H_2, а розрахунки на основі DFT і молекулярної динаміки дають змогу оцінювати енергетику зв'язування та просторові конфігурації молекул водню на поверхні фулерену [2]. Водночас практичне

використання фулеренів як самостійного накопичувального матеріалу обмежується умовами сорбції, стабільністю отриманих гідридних форм і необхідністю керування процесами заряджання та розряджання.

У зв'язку з цим доцільним є створення комбінованого сорбенту, в якому фулерит виконує функцію структурно-нанодисперсної добавки, а металогідридна фаза забезпечує основне оборотне зв'язування водню. Така механічна суміш може мати кілька потенційних переваг: покращення міжфазної взаємодії, збільшення активної поверхні, підвищення рівномірності розподілу водню в робочому тілі та поліпшення кінетики сорбційних процесів. Дослідження дефектних фулеренів також показують, що структурні зміни вуглецевої матриці впливають на її здатність до зберігання водню, тому оптимізація дисперсності, дефектності та співвідношення компонентів у системі «фулерит-металогідрид» має бути окремим технологічним завданням [3].

Створення сорбенту типу «фулерен-металогідрид» має передбачати поетапне відпрацювання складу та технології його одержання. На першому етапі доцільно обґрунтувати вибір металогідридної основи з урахуванням робочого інтервалу температур і тиску, оборотної водневої ємності та стійкості матеріалу до багаторазових циклів заряджання і розряджання. Наступним етапом є визначення фулеритної складової, її оптимального вмісту в суміші, способу механічного змішування та умов активації матеріалу. Після виготовлення дослідних зразків необхідно провести їх атестацію за фазовим складом, структурними характеристиками, питомою поверхнею, водневою ємністю, швидкістю поглинання і десорбції водню, тепловими ефектами та стабільністю під час циклічних випробувань.

Окрему увагу слід приділити переходу від порошкової суміші до робочого твердого тіла накопичувача. Сорбент має бути технологічно придатним для розміщення в контейнері високого тиску, не руйнуватися під час циклічної експлуатації та забезпечувати достатній тепловий контакт із конструктивними елементами накопичувача. Це важливо тому, що процеси гідрування і дегідрування супроводжуються тепловими ефектами, а отже, ефективність накопичувача залежить не тільки від складу матеріалу, а й від конструкції тепловідведення, геометрії контейнера та режиму подавання водню.

Отже, система «фулерен-металогідрид» може розглядатися як перспективний напрям створення сучасного сорбенту водню для автономних енергетичних установок. Її науково-технічна цінність полягає у поєднанні переваг металогідридного зберігання з можливостями вуглецевих наноструктур щодо модифікації поверхні та кінетики сорбційних процесів. Подальші дослідження мають бути спрямовані на оптимізацію складу механічної суміші, встановлення зв'язку між структурою матеріалу та його водневою ємністю, а також перевірку працездатності сорбенту в складі реального накопичувача водню.

[1] Scarpati, G., Frasci, E., Di Ilio, G., & Jannelli, E. (2024). A comprehensive review on metal hydrides-based hydrogen storage systems for mobile applications. Journal of Energy Storage, 102, 113934. https://doi.org/10.1016/j.est.2024.113934

[2] Aziz, M. T., Gill, W. A., Khosa, M. K., Jamil, S., & Janjua, M. R. S. A. (2024). Adsorption of molecular hydrogen (H2) on a fullerene (C60) surface: Insights from density functional theory and molecular dynamics simulation. RSC Advances, 14, 36546–36556. https://doi.org/10.1039/D4RA06171C

[3] Doğan, M., Kalafat, M. Y., Kızılduman, B. K., Bicil, Z., Turhan, Y., Yanmaz, E., & Duman, B. (2025). Hydrogen storage analysis of fullerene and defective fullerenes: The first experimental study. Fuel, 390, 134705. https://doi.org/10.1016/j.fuel.2025.134705

V. Artemchuk, V. Zubok, V. Shkarupylo

RESILIENCE STRESS TESTING OF UKRAINE'S ENERGY AND DIGITAL INFRASTRUCTURE UNDER REPEATED SHOCKS

Russia's war against Ukraine has demonstrated that the resilience of critical infrastructure cannot be reduced only to protection against isolated physical or cyber incidents. Energy systems, telecommunication networks, data centres, fuel chains, and related digital services are exposed to repeated, combined, and cascading shocks. Under such conditions, it is necessary to assess not only system vulnerability, but also the ability of infrastructure to absorb disruptions, maintain essential services, recover, and adapt. This paper presents an approach to resilience stress testing of Ukraine's energy and digital infrastructure developed within the RRUA project. The proposed approach combines minimum viable supply chain modelling, incident-driven scenario design, cyber-physical co-simulation, and multi-phase resilience metrics. Critical infrastructure dependencies are represented as directed graph models that include key assets and services, such as power supply nodes, high-voltage equipment, fuel and biomass inputs, cross-border interconnectors, backbone fibre links, telecom nodes, and data-centre services.

A key component of the study is the use of real Ukrainian outage and incident data for 2022–2024. These data are harmonised and linked to the "Ukraine Energy" scenario catalogue, which allows selected attack waves and restoration processes to be replayed in a controlled simulation environment. For the communication layer, open-source tools such as ns-3, OMNeT++, and Mininet are considered, while power-system modelling relies on GridLAB-D-type and related simulation tools. Initial co-simulation templates make it possible to inject disruption scenarios into both the energy and communication layers and trace their combined effects. Preliminary pilot runs produce resilience curves showing performance degradation, recovery trajectories, and transitions between resilience phases. The interpretation of these results is based on the PARA logic, which treats resilience as a dynamic process covering preparation, absorption, recovery, and adaptation. The approach also supports the development of a practical cyber-maturity and resilience assessment instrument for universities and SMEs, linking infrastructure-level stress testing with organisational self-assessment and capacity building. The proposed methodology provides a basis for identifying critical nodes and dependencies, comparing recovery strategies, and supporting evidence-based decision-making for operators, regulators, and public authorities. Further work will focus on refining operator-action models, backup power assumptions, traffic rerouting mechanisms, and the scenario base for combined physical and cyber threats.

Research was supported by the U.S. National Academy of Sciences (NAS) and the Office of Naval Research (ONR) through the Science and Technology Center in Ukraine (STCU) under STCU contract number 7126 in the framework of the International Multilateral Partnerships for Resilient Education and Science System in Ukraine (IMPRESS-U).

Р.Ю. Донюк, А.В. Давидюк

КЛАСИФІКАЦІЯ МЕТОДІВ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК В УМОВАХ ВИКОРИСТАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Еволюція фішингу, на яку значно вплинув штучний інтелект (далі - AI), відображає загальну тенденцію у кібербезпеці, де акцент зміщується від підходів, що базуються на статичних правилах і шаблонах до контекстно-залежного та семантичного аналізу електронних листів із застосуванням технологій AI. Також відзначається, що кіберзагрози стають дедалі більш складними, а процеси їх реалізації - автоматизованими, що посилює проблеми традиційних підходів до їхнього виявлення та реагування. Зловмисники все частіше використовують механізми автоматичного створення листів та шкідливих програм, що дозволяють значно масштабувати кампанії для проведення атак на великі масиви адрес та обходити існуючі засоби захисту [1]. Зокрема, у [2] фіксується адаптація та автоматизація тактик зловмисників, які активно поєднують традиційні техніки соціальної інженерії з сучасними технологіями автоматизованого генерування контенту.

Листи, створені за допомогою генеративних моделей штучного інтелекту (далі - GenAI), знижують ефективність звичайних детекторів (традиційний класифікатор падає на 5–9% після переформулювання листів LLM [3]). Дослідники описують це як еру переходу від традиційних фішингових кампаній до GenAI фішингу [3-5,14]. Фішингові атаки, створенні з використанням LLM, становлять новий, сучасний клас загроз, що поєднує соціальну інженерію, автоматизацію та персоналізацію у вражаючих масштабах. До 82% атак електронного фішингу вже містять контент, згенерований LLM, а такі листи мають до 30% вищий показник переходів на шкідливі посилання порівняно з оригінальними [6-7].

Це провокує зміни та створює як виклики для команди захисників (Blue team) у контексті вдосконалення засобів та заходів захисту, так і нові можливості для досліджень у галузі застосування LLM для їхнього виявлення та аналізу.

Пропонується виокремити наступні рівні аналізу (див. Таблиця 1), за якими класифікуються методи детектування фішингових атак, кожен із яких характеризується різною глибиною аналізу даних, стійкістю до варіативності (різноманітності, мінливості) GenAI фішингу, обчислювальною складністю та інтерпретованістю результатів.

У таблиці 1 представлене узагальнене структуроване впорядкування існуючих методів виявлення фішингових атак за рівнями аналізу та додатковими критеріями порівняння, які стають критичними саме в умовах GenAI фішингу.

Таблиця 1 – Порівняння рівнів аналізу методів виявлення фішингових атак

Рівень аналізу та методи виявлення	Обчислювальна складність	Стійкість до GenAI фішингу	Інтерпретованість результатів
Структурний рівень (Structural Analysis): аналіз заголовків, SPF/DKIM/DMARC верифікація, аналіз репутації IP/domain/URL тощо	Низька	Низька	Висока
Синтаксичний рівень (Syntactic Analysis): аналіз на базі регулярних виразів, пошук за ключовими словами, нечіткий аналіз тощо	Середня	Низька	Висока
Статистичний рівень (Statistical Analysis): оцінка показника стандартного відхилення, оцінка метрик схожості, оцінка показника ентропії тощо	Середня	Середня	Середня
Семантичний рівень (Semantic (Deep Content) Analysis): векторні представлення, трансформерні моделі тощо	Висока	Висока	Низька
Поведінковий рівень (Behavioral Analysis): аналіз поведінкових патернів користувачів, виявлення поведінкових аномалій тощо	Висока	Висока	Середня
Гібридний рівень (Hybrid (Multi-Layered) Analysis): комбінування методів різних рівнів	Висока	Висока	Середня

Базові підходи до детектування, зокрема методи структурного та синтаксичного рівнів, орієнтовані на сигнатури або регулярні шаблони, є ефективними для виявлення класичного традиційного фішингу. Беручи до уваги роботи [8-14], можна зробити висновок, що для протидії GenAI фішинговим атакам необхідні інтелектуальні підходи, засновані на

міжподійній кореляції та багатокритеріальному контекстному аналізі, які функціонують на рівні латентного семантичного простору, виявляють приховану подібність і враховують поведінкові ознаки. Таким чином, еволюція фішингових атак не змінює фундаментальну логіку захисту, але підвищує вимоги до її адаптивності та стійкості.

Висновок. У результаті проведеного дослідження теоретично обґрунтовано, що можливість використання великих мовних моделей суттєво трансформувала характер фішингових атак. Тому захист від фішингу в умовах поширення GenAI вимагає еволюції аналітичних підходів та застосування єдиної, але багаторівневої архітектури детекції фішингу, а не створення ізольованих систем протидії виключно GenAI контенту.

Здійснено порівняння рівнів аналізу фішингових атак з урахуванням глибини аналізу даних, стійкості до варіативності GenAI контенту, обчислювальної складності та інтерпретованості результатів. Ключовим критерієм класифікації рівнів аналізу є стійкість методів до GenAI фішингу. Ця класифікація дозволяє оцінити поточний стан спроможностей організації з виявлення фішингу та спланувати стратегію подальшого їх нарощування.

[1] The Impact of AI on Cyber Threat. National Cyber Security Centre. URL: https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat (date of access: 06.04.2026).

[2] Російські кібероперації. Аналітика за І півріччя 2025. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=71278 (дата звернення: 06.04.2026).

[3] Phishing Detection in the Gen-AI Era: Quantized LLMs vs Classical Models / J. Thapa et al. arXiv. URL: https://arxiv.org/html/2507.07406v1 (date of access: 06.04.2026).

[4] Моделювання та реалізація атак соціальної інженерії / Н. Коршун та ін. Телекомунікаційні та інформаційні технології. 2026. Т. 90, № 1. С. 130–139. URL: https://doi.org/10.31673/2412-4338.2026.019013 (дата звернення: 06.04.2026).

[5] Інтелектуальні технології у кібербезпеці: аналіз потенціалу та викликів застосування штучного інтелекту / А. Ільєнко та ін. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2026. Т. 4, № 32. С. 711–723. URL: https://doi.org/10.28925/2663-4023.2026.32.1139. (дата звернення: 06.04.2026).

[6] A systematic literature review of large language models in phishing attack generation and detection / D. Sivaneswaran et al. Array. 2026. Vol. 30. P. 100775. URL: https://doi.org/10.1016/j.array.2026.100775 (date of access: 06.04.2026).

[7] Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities / M. A. Ferrag et al. Internet of Things and Cyber-Physical Systems. 2025. Vol. 5. P. 1–46. URL: https://doi.org/10.1016/j.iotcps.2025.01.001 (date of access: 06.04.2026).

[8] Lateral Phishing with Large Language Models: A Large Organization Comparative Study / M. BETHANY et al. arXiv. 2025. URL: https://arxiv.org/html/2401.09727v2 (date of access: 06.04.2026).

[9] Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects / F. Heiding et al. arXiv. 2024. URL: https://arxiv.org/pdf/2412.00586 (date of access: 06.04.2026).

[10] Schmitt, M., Flechais, I. Digital deception: generative artificial intelligence in social engineering and phishing. Artif Intell Rev 57, 324 (2024). https://doi.org/10.1007/s10462-024-10973-2 (date of access: 06.04.2026).

[11] Staying Ahead of Threat Actors in the Age of AI. Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/ (date of access: 06.04.2026).

[12] David versus Goliath: Can Machine Learning Detect LLM-Generated Text? A Case Study in the Detection of Phishing Emails / F. Greco et al. Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024), Salerno, 8–12 April 2024. URL: https://ceur-ws.org/Vol-3731/paper41.pdf (date of access: 06.04.2026).

[13] Carelli A. Finding Differences Between LLM-generated And Human-written Text: A Phishing Emails Case Study. 2024. URL: https://www.researchgate.net/publication/382648027_Finding_Differences_Between_LLM-generated_And_Human-written_Text_A_Phishing_Emails_Case_Study (date of access: 06.04.2026).

[14] Jabir R., Le J., Nguyễn C. Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. AI. 2025. Vol. 6. P. 174. URL: https://doi.org/10.3390/ai6080174 (date of access: 06.04.2026).

XLIV
НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ
МОЛОДИХ ВЧЕНИХ ТА СПЕЦІАЛІСТІВ
ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В
ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА НАН УКРАЇНИ

ПРИСВЯЧЕНА ДНЮ НАУКИ В УКРАЇНІ

Збірник матеріалів конференції
20 травня 2026 р.

Collection of materials of the XLIV Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 20, 2026 / PIMEE of NAS of Ukraine. - 2026. - 97 p.

Збірник матеріалів XLIV Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 20 травня 2026 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2026. – 97 с.

Інформаційна підтримка:

Сторінка конференції на сайті Інституту

Telegram канал РМВ НАН України