НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

03 червня 2026 року

Київ – 2026

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 06 від 28 травня 2026 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 03 червня 2026 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2026. 170 с.

B-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, June 03, 2026. Kyiv: PIMEE NAS of Ukraine, 2026. 170 p.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, професор,
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

Ф.О. Коробейніков

КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ В УМОВАХ HILP-РИЗИКІВ: БЮДЖЕТ НЕВИЗНАЧЕНОСТІ ТА АРХІТЕКТУРА АДАПТИВНОЇ СТРАТЕГІЇ

Кібербезпека енергетичного сектору досягла межі застосовності класичної парадигми. Наявні підходи залишаються необхідними, однак вони переважно спрямовані на загрози, для яких уже існує категоріальна форма розпізнавання: назва, статистична історія, сценарний опис, місце в матриці оцінювання ризиків організації. Проте за межами цієї матриці розташований клас високодеструктивних подій із низькою ймовірністю реалізації (*High-Impact Low-Probability*, *HILP*). Його радикальним виявом є ризики нульового прецеденту (*зіропрецедентні*, *zero-precedent*) [1], позбавлені не лише історичних аналогів, а й самої категоріальної форми попереднього розпізнавання, – втілення найтівської невизначеності (*knightian uncertainty*) [2] (рис. 1).

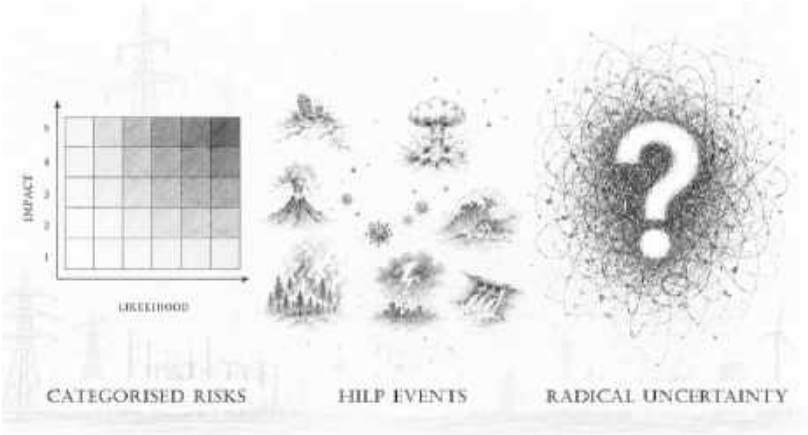


Рисунок 1 – Від категоризованих ризиків до радикальної невизначеності: епістемічна дуга управління ризиками

Історія української енергетики останнього десятиліття дає емпіричну ілюстрацію досягнення цієї межі: кібератака *BlackEnergy* на «*Прикарпаттяобленерго*» у грудні 2015 року [3], *Industroyer* у 2016 році [4], *Industroyer2* – у квітні 2022 року [5]. Кожна з цих подій, хоча й не була зіропрецедентною в термінологічно строгому значенні [1], але до моменту реалізації перебувала поза полем розпізнавання. *Іберійський блекаут* 28 квітня 2025 року – перше у світовій історії каскадне відключення, спричинене перенапругою в системі з високою часткою відновлюваної

генерації [6], – розширює цю картину: HILP-події виникають і поза межами кібератак, природних катастроф та воєнних дій. Вони випливають із самої логіки ускладнення сучасного світу та посилення взаємопов'язаності систем.

Класична логіка управління ризиками ефективна щодо загроз, які вже відомі й проаналізовані. Однак вона ґрунтується на припущенні, що простір можливих подій піддається статистичному опису, а ймовірність і збитки – бодай апроксимативному прогнозуванню та розрахунку. Для HILP-ризиків це припущення порушується: проблема полягає не в нестачі даних, а у відсутності самої категоріальної форми, яка дала б змогу заздалегідь розпізнати загрозу [2].

Бюджети кібербезпеки: концептуальна та управлінська рамка. Із цього обмеження випливає методологічна та практична необхідність розмежування загального бюджету кібербезпеки на два самостійні бюджети з різною логікою обґрунтування.

Бюджет ризику спрямований на загрози, внесені до матриці оцінювання ризиків організації. Його логіка – оптимізаційна: зіставлення вартості захисних заходів з очікуваним зниженням збитків у межах заданої моделі загроз. У цій царині залишаються чинними формальні моделі обґрунтування інвестицій, зокрема запропонована авторами раніше опціонна *інтерпретація формули Блека–Шоулза* [8, 9], за якої захисні заходи функціонують як *пут-опціон* на захищуваний актив, що обмежує глибину падіння його функціональної, економічної чи операційної вартості. Але, за всіх переваг цієї моделі – математичної строгості та зрозумілої економічної інтерпретації, вона має одне принципове обмеження: за межами матриці оцінювання ризиків ця модель незастосовна.

Бюджет невизначеності охоплює ризики, не відображені в матриці. Об'єктом цього бюджету є *адаптаційний потенціал* – сукупність ресурсів, якостей і спроможностей, завдяки яким організація змінює спосіб свого функціонування за зміни умов [7]. Для *функціонально зумовлених соціотехнічних систем* – систем, ідентичність яких задана функцією, закріпленою ззовні, та зберігається через її безперервне виконання, – цей потенціал набуває форми функціональної *трансморфності*: здатності зберігати ідентичність через адаптивну зміну способів реалізації критично важливих функцій [7]. Енергетична компанія залишається собою доти, доки виконує свої функції в енергосистемі. Зміна операційної форми їх реалізації припустима, припинення самих функцій – ні.

Розрізнення бюджетів має прямий управлінський сенс. Бюджет ризику відповідає на: «скільки необхідно витратити, щоб знизити очікувані збитки від відомого набору загроз». Бюджет невизначеності – на принципово інше запитання: «якими ресурсами повинна володіти система, щоб продовжувати роботу, якщо набір урахованих загроз виявився неповним, основний

цифровий контур недоступний, довіру до зовнішніх сервісів утрачено, а звичні процедури відновлення – незастосовні». Ці бюджети не конкурують: їхні предмети є різними, і одна шкала оцінювання не може одночасно діяти в зоні вимірюваного ризику та за її межами.

Концентрація залежностей як структурна проблема сучасної кібербезпеки. *Уразливість* – властивість компонента: вона піддається виявленню, класифікації, усуненню або компенсації. *Залежність* – властивість зв'язку між компонентами, платформами, сервісами, юрисдикціями, каналами довіри та організаційними практиками. Якщо уразливість закривається патчем, то залежність потребує інших методів – аналізу самої архітектури відносин, через які система зберігає здатність діяти.

В енергетичних компаніях концентрація потенційно деструктивних залежностей проявляється передусім на *п'яти основних рівнях: (i) хмарна інфраструктура великих глобальних провайдерів*; *(ii) централізовані системи ідентифікації та керування доступом; (iii) промислові вендори й канали оновлень; (iv) аутсорсинг сервісів IT та кібербезпеки; (v) зовнішні комунікаційні платформи*. Кожен із цих виборів організації окремо буде раціональним – бо він забезпечує масштабованість, економічну ефективність і професійну експертизу. Але їхня сукупність утворює архітектуру єдиної точки відмови нового типу – структуру концентрованих залежностей, у якій принципово різні процеси сходяться до обмеженого набору платформ, постачальників і довірених інфраструктур.

Цей тип *структурної крихкості* перестав бути гіпотетичним. 19 липня 2024 року помилка в рядку коду автоматичного оновлення endpoint-захисту за кілька годин паралізувала близько 8,5 мільйона систем у всьому світі – авіацію, банки, лікарні, екстрені служби. Сукупні втрати оцінено в 5–10 мільярдів доларів [10]. Залежність, що в нормальному режимі сприймається як звичайний сервісний зв'язок, у момент кризи виявилася точкою відмови, формально не представленою на жодній архітектурній діаграмі.

До структурної концентрації залежностей додається ще один чинник – *ерозія внутрішніх компетенцій*. Перенесення технічної та аналітичної функцій кібербезпеки до зовнішніх сервісів (керовані SOC, комерційні платформи аналізу загроз) є раціональним у нормальному режимі: професійний зовнішній центр обробляє події швидше й дешевше. Однак аутсорсинг призводить до того, що внутрішні фахівці поступово втрачають компетенції. У момент, коли зовнішній сервіс недоступний, скомпрометований чи не розпізнає новий клас атаки, перенесені за периметр компетенції залишаються за цим периметром.

Парадокс сучасного стану галузі полягає в тому, що її раціональність обертається її крихкістю. *Сума локальних оптимізацій не дорівнює глобальній*

ефективності – вона дорівнює глобальній залежності. Це не докір окремим рішенням і не аргумент проти аутсорсингу як такого. Це діагноз структурного характеру: модель безпеки, що захищає лише нормальний режим, у момент його втрати залишається взагалі без моделі.

Підсилення атак штучним інтелектом і межа людської швидкості реагування. Ситуація різко загострюється з розвитком атак, підсилених штучним інтелектом. Середній час від першого проникнення до латерального переміщення в атакованій мережі у 2025–2026 роках скоротився до десятків хвилин, а в найшвидших випадках – до секунд. Зафіксовано інциденти, коли один атакувальник, спираючись на автоматизований інструмент, проексплуатував відому уразливість на тисячах вузлів за лічені хвилини [11]. Сторона нападу дедалі частіше діє не як група операторів, а як сукупність автоматизованих та напівавтоматизованих агентів, які паралельно ведуть розвідку, готують комунікації, шукають точки входу та підлаштовують сценарій атаки під реакцію захисту.

Змінюється сам темп протиборства в кібердомені. Людина дедалі частіше не встигає пройти повний цикл виявлення, аналізу, узгодження та реагування до того, як атака переходить у наступну фазу. Низька швидкість реагування стає перешкодою для ефективного захисту: людський цикл ухвалення рішень дедалі частіше поступається швидкості машинного циклу атаки, і значну частину роботи – як із захисту, так і з нападу – у недалекому майбутньому виконуватимуть ШІ-системи. Це вже не питання ймовірності чи галузевого вибору. *ШІ проти ШІ – наша реальність найближчих років*.

В основі цієї проблеми – відсутність як обов'язкових нормативних обмежень щодо наступального застосування ШІ, так і дієвих засобів впливу на порушників. Індустрія декларує розвиток етичних норм застосування та методів безпечного навчання моделей (*AI alignment, constitutional AI, RLHF*), однак моделі та агентні системи фактично використовуються в дослідницьких лабораторіях подвійного призначення, на тренувальних полігонах, у red-team-практиках та реальних воєнних операціях. Асиметрія між зусиллями з безпечного розвитку ШІ та можливостями його наступального застосування сама стає чинником системного ризику для критичної інфраструктури та, у ширшому вимірі, екзистенційного ризику для цивілізації загалом.

Архітектурна відповідь: MVDO та автономний аналітичний контур. Із сукупності чотирьох чинників: *технічної залежності, втрати внутрішніх компетенцій унаслідок аутсорсингу аналітики, ШІ-прискорення атак та відсутності нормативних обмежень* – випливає, що нинішня стратегія побудови та захисту інформаційної інфраструктури енергетичних компаній вже не відповідає вимогам часу. Однак відмова від хмарних платформ, комерційних сервісів захисту та промислових вендорів була б економічно й

технологічно нереалістичною. Пропонована авторами архітектурна відповідь полягає в доповненні основного контуру диверсним контуром, що має іншу природу та іншу логіку обґрунтування.

Теоретичною основою такого контуру виступає *концепція мінімально життєздатної цифрової операційності* (minimum viable digital operability, MVDO), розроблена в рамках цього дослідження. MVDO – це заздалегідь підготовлений, диверсний, регулярно перевірюваний цифровий контур, що підтримує виконання критично важливих функцій тоді, коли основний контур є недостатнім, недоступним, скомпрометованим чи таким, що втратив довіру. *Диверсність* у строгому розумінні, згідно з класичною теорією відмовостійкості [12], – це принципова відмінність шляхів реалізації однієї й тієї самої функції, що виключає спільні причини відмови. Це поняття тонше, ніж «технологічне розмаїття» в управлінському сенсі: кілька рішень від різних вендорів, побудованих на одній архітектурній парадигмі та одних каналах довіри, диверсної архітектури не утворюють.

Архітектура MVDO ґрунтується на п’яти вимогах: *диверсність щодо основної інфраструктури*; *активний режим експлуатації*, за якого контур постійно використовується, щоб не виявитися непридатним у момент кризи; *функціональна оптимальність* – мінімально необхідний обсяг без амбіції дублювати основний контур; *процедурна готовність до перемикання* – чіткі правила активації; та *фракталізація диверсності* – принцип, за яким кожен резервний контур повинен мати власний резерв іншої природи, оскільки, ставши основним, він сам перетворюється на можливу точку відмови.

Диверсність не може бути одноразовою властивістю вихідної архітектури – вона повинна відтворюватися заново за кожного перемикання на резервний контур. Принцип фракталізації робить адаптивну безпеку не набором резервних контурів, а безперервною здатністю системи породжувати умови власної виживаності на кожному рівні розгортання.

Особливого значення для MVDO набувають відкриті технологічні рішення. Окрім економічної доступності, вони дають організації можливість перевіряти код, адаптувати функціональність, зберігати керованість і тоді, коли зовнішній постачальник недоступний або втратив довіру. Open source-ядро MVDO формує мінімальний суверенний шар операційності та водночас знижує впізнаваність інфраструктури ззовні, зменшуючи цінність попереднього OSINT-профілювання і ускладнюючи побудову точної мапи залежностей цілі.

MVDO обов'язково має бути доповнено *автономним аналітичним контуром* – це локально розгорнута SIEM-інфраструктура, контрольована організацією та здатна виконувати мінімально необхідний аналіз подій безпеки без звернення до зовнішнього постачальника послуг. Якщо MVDO відповідає за збереження дії, то автономний аналітичний контур відповідає за збереження розуміння. Його завдання полягає не в тому, щоб перевершити

комерційні платформи за повнотою охоплення загроз: саме поняття повноти застосовне до зони бюджету ризику, тоді як HILP-події належать до іншої зони, де повнота заздалегідь недосяжна. Контур існує для того, щоб організація не втратила здатність розуміти власний стан і мала можливість коректно перемикатися на диверсну інфраструктуру, коли основна недоступна, втратила довіру чи структурно сліпа до нового класу атак.

Контур складається з локальної SIEM, засобів аналізу уразливостей та обробки індикаторів компрометації, інфраструктури виявлення та обману (ханіпотів) [13], – і локально розгорнутих ШІ-моделей. Останні посідають особливе місце: саме вони дають шанс наблизити швидкість аналізу до швидкості сторони нападу. Ідеться не про створення власних фундаментальних моделей, а про використання відкритих або перевірюваних моделей, розгорнутих усередині інфраструктури й донавчених на допустимих наборах даних. При цьому локальний ШІ не повинен ставати самостійним суб'єктом ухвалення рішень: в енергетиці ціна помилки надто висока, щоб передавати критичні рішення автоматизованій моделі. Поки що людина має залишатися в контурі відповідальності.

Практичні рекомендації.

Розмежування бюджету. Сформувати у структурі витрат на кібербезпеку дві самостійні статті: *бюджет ризику* та *бюджет невизначеності* – з різною логікою обґрунтування та різними метриками успішності. Бюджет невизначеності повинен становити окрему захищувану категорію, що не підлягає скороченню в межах стандартних оптимізаційних процедур.

Аудит концентрації залежностей. Провести структурний аудит усіх рівнів концентрованих залежностей – технологічних, операційних, кадрових, юрисдикційних, etc., з чіткою кваліфікацією кожної за критеріями диверсності.

Розгортання MVDO. Спроєктувати та розгорнути резервний адаптивний контур для критично важливих функцій згідно з п'ятьма вимогами, включно з принципом *фракталізації диверсності*. Контур повинен перебувати в активній експлуатації – не як архівний резерв, а як частина операційного середовища.

Впровадження автономного аналітичного контуру. На базі локальних донавчених ШІ-моделей створити SIEM-інфраструктуру, здатну розпізнавати слабкі сигнали та формувати сценарії загроз за відсутності прецедентів у темпі, близькому до темпу сторони нападу, за збереження людини в контурі відповідальності та процедурного зв'язку із MVDO.

Відновлення внутрішніх компетенцій через перманентне оновлення MVDO. Закласти в операційну модель кібербезпеки *безперервний* цикл пошуку, оцінювання та впровадження нових технологічних рішень для MVDO. Резервний контур, спроєктований одноразово, із часом втрачає диверсність щодо еволюціонуючого основного контуру. Необхідні

регулярний технологічний моніторинг *open source* рішень, SIEM-інструментів і локально розгорнутих моделей; пілотні середовища для перевірки нових рішень; планова заміна застарілих вузлів; і – як умова всього переліченого – утримання внутрішньої аналітичної компетенції та мотивації персоналу.

Головний висновок. У світі, де епістемічна межа ризику безперервно зміщується, захищеною виявляється не та організація, що підготувалася лише до відомих загроз, а та, що зберегла можливість залишатися собою перед лицем ще не названих.

1. Korobeynikov, F., Matviev, S., & Mokhor, V. (2026). High-impact low-probability risks and the limits of anticipation: From known knowns to zero-precedent uncertainty. Electronic Modeling, 48(2), 87–105. https://www.emodel.org.ua/images/em/48-2/48-2-5.pdf.
2. Knight, F. H. (1921). Risk, uncertainty and profit. Houghton Mifflin.
3. Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid: Defense use case. E-ISAC; SANS ICS. https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
4. Cherepanov, A. (2017). Win32/Industroyer: A new threat for industrial control systems ESET https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf.
5. ESET Research. (2022, April 12). Industroyer2: Industroyer reloaded. WeLiveSecurity. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
6. ENTSO-E Expert Panel. (2026). Final report on the 28 April 2025 Iberian blackout. https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/.
7. Korobeynikov, F., & Mokhor, V. (2026). Adaptive security: Strategic principles for complex socio-technical systems. Royal Society Open Science, 13(1), 251481. https://doi.org/10.1098/rsos.251481.
8. Korobeynikov, F. (2025). Justifying investment in information security: An interpretation of the Black–Scholes formula. Nuclear and Radiation Safety, 107(3), 69–75. https://doi.org/10.32918/nrs.2025.3(107).06.
9. Black, F., & Scholes, M. (1973). The pricing of options and corporate liabilities. Journal of Political Economy, 81(3), 637–654. https://doi.org/10.1086/260062.
10. CrowdStrike. (2024). External technical root cause analysis – Channel file 291. CrowdStrike Holdings. https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf
11. Booz Allen Hamilton. (2026). Threat report: When cyberattacks happen at AI speed. https://www.boozallen.com/expertise/cybersecurity/threat-report-when-cyberattacks-happen-at-ai-speed.html.
12. Avižienis, A., & Kelly, J. P. J. (1984). Fault tolerance by design diversity: Concepts and experiments. Computer, 17(8), 67–80. https://doi.org/10.1109/MC.1984.1659219.
13. Spitzner, L. (2002). Honeypots: Tracking hackers. Addison-Wesley.

В.В. Коваль, О.В. Самков, В.І. Вакась, О.М. Піскун, Б.О. Самков

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ СИСТЕМ СИНХРОНІЗАЦІЇ ОБ'ЄКТІВ ЕНЕРГЕТИКИ ТА МОБІЛЬНОГО ЗВ'ЯЗКУ

Трансформація енергетики відбувається через побудову багатовекторних інтегрованих інтелектуальних систем та мікромереж. Атомна генерація, сонячні станції чи теплові потужності – усе це працює задля ефективних енергетичних послуг, що відповідають відомій «концепції 3D»: Decarbonization, Decentralization, Digitalization [1-3]. Примітно, що ключовою високотехнологічною складовою цього процесу є діджиталізація, де процеси синхронізації сигналів відіграють вирішальну роль [3, 4]. Такі системи є фундаментом не лише для енергетики, а й для цифрових телекомунікацій мобільного зв'язку та оборонних технологій. Жорсткі вимоги до точності сигналів роблять питання їх відмовостійкості першочерговим [3, 4].

Україна має унікальний шанс – трансформувати енергосистему на базі сучасних цифрових стандартів, оминувши етап застарілих рішень [1-5]. Основою такої модернізації стають концепції Smart Grid, системи глобального моніторингу WAMS та WAMPAC [1-3]. Технологія синхронізованих вимірювань, стандарти IEC 61850 та IEEE-1588 PTP, використання приладів PMU та кіберзахищених IP/MPLS-мереж – усе це формує новий технологічний ландшафт. Досвід партнерів із ЄС підтверджує: поєднання цих елементів суттєво покращує надійність та стійкість систем [2]. Для України це не просто питання технологічного розвитку, це необхідна умова для інтеграції в європейський енергопростір та забезпечення власної безпеки.

В сучасних WAMS наявність точних сигналів синхронізації дозволяє операторам здійснювати захист, керування та детальний аналіз подій. Проте, погіршення відмовостійкості сигналу неминуче веде до зниження його якості. Це спричиняє похибки у вимірюванні векторів напруги та струму, що може спровокувати хибне прийняття рішення в процесі керування [3, 5].

Основне джерело синхронізації сьогодні – глобальні навігаційні супутникові системи GNSS [4, 5]. Однак перебої у прийомі цих сигналів, викликані навмисними завадами, джамінгом або спуфінгом, створюють серйозні ризики для стабільної роботи систем. За цих обставин традиційні методи вже не гарантують необхідного рівня відмовостійкості. Система повинна бути не лише автоматизованою, а й стійкою до кібератак та фізичних пошкоджень інфраструктури. Це критично для прифронтових регіонів, а під час повітряних тривог – для всієї території України [4].

Підвищення вімовостійкості вимагає поєднання різних методів [2-5]. Метод комплексного багаторівневого резервування охоплює кілька рівнів: апаратне дублювання, використання незалежних джерел сигналу та альтернативних каналів, застосування протоколів передачі сигналів синхронізації. Важливо, що обладнання синхронізації у разі зникнення опорного сигналу, може певний час утримувати стабільність у режимі Holdover, проте це лише тимчасовий захід [3-5]. З метою подолання такого обмеження можуть використовуватись новітні цезієві генератори Cesium Clock з функціоналом фазової синхронізації, що входять до складу обладнання ePRTC [4, 5]. Калібрування таких генераторів відбувається при стабільному сигналі GNSS, причому його фізичні властивості дозволяють робити це рідко, приблизно 1-2 рази на місяць, без втрати необхідної точності вихідного сигналу.

Розроблено експериментальний комплекс для перевірки роботи цезієвого генератора в польових умовах на базі обладнання базової станції мобільного зв'язку стандарту LTE [4]. Результати вимірювання параметру MAFE показали, що отримані значення повністю вкладаються в шаблон HRM-1 [4]. Важливо зазначити, що навіть при переході на роботу від власного генератора (в режимі Holdover), попри певні стрибки по фазі, якість сигналу залишається цілком прийнятною для роботи базової станції мобільного зв'язку стандарту LTE [4].

Окрім того, пропонується система інтелектуального моніторингу (CIM), що забезпечує безперервний багатоканальний контроль та гібридний синтез сигналів синхронізації [3, 5]. Використання CIM дозволяє не лише оцінювати параметри в реальному часі, але й прогнозувати деградацію опорних джерел.

Також пропонується перехід до розподіленої архітектури – це крок від вразливих централізованих вузлів до гнучкої та стійкої системи. В умовах України доцільно розгорнути 3-4 Cesium Clock на вузлах з верхньою ієрархією мережі синхронізації [4]. Передача до споживачів має відбуватися за протоколом PTP, зокрема за профайлами PTP G.8275.1 та G.8275.2. Розроблені лабораторні зразки PTP-грандмайстру та PTP-слейву для дослідження характеристик сигналів синхронізації при трансляції через IT-мережу.

Пропонується використовувати цифрові технології, які дозволяють суттєво підвищити точність за рахунок адаптивної фільтрації та компенсації затримок, а також ресурси Системи координатно-часового та навігаційного забезпечення України. Зокрема, технологія RTK, що працює через мережу контрольно-коригувальних станцій, дає змогу отримувати координати з сантиметровою точністю. Це не тільки покращує параметри синхросигналів, а й створює фундамент для формування просторової надлишковості джерел часу. Мережа контрольно-коригувальних станцій RTK компенсує втрати у

випадку виходу з ладу окремих її елементів, що дозволяє виявляти аномалії, такі як спуфінг і значно покращити відновлення після збоїв.

Варто врахувати результати інтеграцію систем частотно-часового забезпечення з цифровою інформаційною інфраструктурою, що вимагає надійного кіберзахисту. Для підтвердження достовірності навігаційних повідомлень у відкритому сервісі Galileo пропонується використовувати сервіс OSNMA. Він базується на криптографічних методах та схемі TESLA, що дозволяє перевіряти автентичність повідомлень. Для автоматизованих систем це є надійним бар'єром проти підміни сигналів.

Відмовостійкість синхронізації – складна, багатофакторна задача. Впровадження багаторівневого резервування, розподілених архітектур та інтелектуального моніторингу відкриває шлях до систем нового покоління. Інтеграція RTK-мереж, цезієвих генераторів та сервісу OSNMA забезпечує синергетичний ефект, підвищуючи точність і відмовостійкість електроенергетичних й телекомунікаційних систем мобільного зв'язку у складних умовах.

1. Kyrylenko, O. V., Denysiuk, S. P., & Blinov, I. V. (2023). Digital transformation of the energy industry: Current trends and task. *Praci Institutu Elektrodinamiki Nacionalnoi Akademii Nauk Ukraini, 2023*(65), 5–14. https://doi.org/10.15407/publishing2023.65.005.
2. Dondossola G., Terruggia R., Todeschini M.G. (2024). D2 – Cybersecurity in the loop for multi energy infrastructures. *CIGRE Science & Engineering*. *2024. №035.* 1–16.
3. Коваль, В. В., Самков, О. В., Вакась, В. І., Пилипенко, Ю. В., Яніцький, І. Я., & Лавінський, Д. С. (2024). *Відмовостійкі системи синхронізації часу інтелектуальних електричних мереж*. Національний університет біоресурсів і природокористування України.
4. Самков, О., Коваль, В., Вакась, В., Рибіна, О., Самков, Б., & Піскун, О. (2025). Improving the resilience of synchroinformation systems of smart power grids and mobile communications networks under wartime conditions. *Vidnovluvana energetika*, (3(82)), 39–47. https://doi.org/10.36296/1819-8058.2025.3(82).39-47.
5. Коваль, В. В., Самков, О. В., Тітко, В. О., Вакась, В. І., Яніцький, І. Я., Осінський, О. Л., Самков, Б. О., & Піскун, О. М. (2025). *Автоматизовані системи синхронізації сигналів з підвищеною відмовостійкістю*. Академперіодика.

В.М. Горбачук, В.М. Большаков, Д.І. Ніколенко,
О.С. Шаталов, А.О. Камуз

ПРИНЦИП НУЛЬОВОЇ ДОВІРИ ДЛЯ МЕРЕЖ ПРОДУКТІВ JIT

Документ [1] був розроблений з метою сприяння місіям Агентства національної безпеки (АНБ; NSA (National Security Agency)) з кібербезпеки, включаючи обов'язки АНБ щодо виявлення та поширення загроз, а також розроблення та видання специфікацій і запобіжних заходів з кібербезпеки для національних систем безпеки (National Security Systems (NSSs)), інформаційних систем Міністерства війни (Department of War (DoW)), оборонно-промислової бази (Defense Industrial Base (DIB)) США, а також для широкого поширення інформації з метою охоплення всіх відповідних зацікавлених сторін [2]. В цій справі АНБ і Директорат кібербезпеки визнають цінний внесок і підтримку директора з інформаційних технологій (Chief Information Officer (CIO)) Офісу менеджменту портфеля (Portfolio Management Office (PfMO)) нульової довіри (Zero Trust (ZT)) DoW.

ZT являє собою фундаментальне покращення в кібербезпеці [3]. Не покладаючись на захист периметра, ZT наголошує на безперервній автентифікації та авторизації кожного користувача чи кожної особової сутності (Person Entity (PE)), кожного пристрою чи кожної неособової сутності (Non-Person Entity (NPE)), кожного застосунку, працюючи за принципами «ніколи не довіряй, завжди перевіряй» та «припускай порушення» (assume breach). Підхід ZT має вирішальне значення для захисту конфіденційних даних, систем і послуг від дедалі складніших кіберзагроз [4].

Згідно з Виконавчим наказом (Executive Order (EO)) 14028 «Поліпшення кібербезпеки країни» (Improving the Nation's Cybersecurity), уряд Сполучених Штатів (United States Government (USG)) для досягнення ZT розробив кілька відповідних стратегій, які включають структури (frameworks), настанови, моделі зрілості, спроектовані для допомоги організаціям у впровадженні ZT. Ключові основоположні документи, що окреслюють архітектуру, моделі зрілості, настанови на підтримку цих зусиль, включають: Національний інститут стандартів і технологій (National Institute of Standards and Technology (NIST)), Zero Trust Architecture Special Publication (SP) 800-207, серпень 2020 р.; Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency (CISA)), Zero Trust Maturity Model, Version 2.0, січень 2022 р.; DoW, Zero Trust Reference Architecture, Version 2.0, липень 2022 р.; DoW, Zero Trust Strategy, Version 1.0, жовтень 2022 р.

Згідно з EO 14347, DoW є повноважним вторинним титулом Міністерства оборони (Department of Defense (DoD)) США.

АНБ, використовуючи свої повноваження з кібербезпеки та роль Національного менеджера (National Manager (NM)) для NSSs США,

розробило Настанови впровадження нульової довіри (Zero Trust Implementation Guidelines (ZIGs)), використовуючи опубліковані рекомендації NIST та DoW. ZIGs призначені для того, щоб допомогати DoW, DIB, NSSs та афілійованим організаціям у впровадженні принципів ZT у свої процеси, уможливлюючи досягнення ними цільового рівня (Target-level) ZT, як описано в DoW ZT Framework з DoW ZT Strategy.

У тісній співпраці з CIO DoW та з метою організації сумарно 152 заходів (activities) ZT, що містяться в DoW ZT Strategy, було розроблено 5 фаз (Відкриття (Discovery), Фаза 1 і Фаза 2, які є цільовим рівнем (91 захід), Фаза 3 і Фаза 4, які є передовим рівнем (Advanced-level) (61 захід)). Згадані фази дають структурований підхід до організації заходів ZT, допускаючи певні ініціативи при їх втіленні. Оскільки ZT є структурою, то за цією моделлю окреслені в ZIGs фази є модульними та можуть узгоджуватися з конкретним середовищем організації. Поточний набір ZIGs складається з Посібника (Primer) та трьох Настанов впровадження (Implementation Guidelines) ZT (Відкриття, Фаза 1 і Фаза 2), спроектованих для допомоги кваліфікованим (skilled) практикам в адаптуванні (adopting) та інтегруванні здатностей (capabilities) цільового рівня ZT (42) та заходів цільового рівня (91). ZIGs для Фаза 3 і Фаза 4 можуть розроблятися пізніше. Ці настанови забезпечують модульну структуру, дотримуючись в якості керівництва для впровадження напрямів (pillars), здатностей, заходів Рамкової програми (Framework) DoW ZT, а також згаданої публікації NIST SP 800-207. ZIGs відповідають пофазовому (phased) підходу впровадження DoW цільового рівня, причому цей ZIG (Фаза 1) охоплює 36 заходів, які підтримують 30 здатностей у Фазі 1. Заходи Фази 1 будуються на середовищі (середовищах) компонентів або вдосконалюють їх далі, щоб встановлювати безпечне підгрунтя, яке підтримує здатності ZT. Решта заходів і здатностей цільового рівня розглядається в інших ZIGs (Відкриття і Фаза 2) у сфері застосовності. ZIGs призначені для допомоги DoW і спільнотам NSS у впровадженні концепцій ZT для досягнення цільового рівня, як описано в DoW ZT Framework.

Передумовою Фази 1 є EO 14028, що зобов'язує агентства USG прийняти архітектуру нульової довіри (Zero Trust Architecture (ZTA)). Зокрема, для мереж NSS, Меморандум національної безпеки (National Security Memorandum) 8 (NSM-8) «Поліпшення кібербезпеки національної убезпеки» (Improving the Cybersecurity of National Security) [5], DoD і систем розвідувального співтовариства (Intelligence Community (IC)), реалізує вимоги до кібербезпеки, доручені EO 14028. NSM-8 зосереджується на вимогах до NSS, як вони визначені в 44 U.S.C § 3552(b)(6), а також всіма іншими системами DoD Міністерства оборони та IC, як описано в 44 U.S.C § 3553(e)(2) та 3553(e)(3). Ці директиви спрямовані на модернізацію позиції країни в галузі кібербезпеки у відповідь на постаючі загрози шляхом зміцнення цифрової інфраструктури, з'ясування критичних вразливостей,

посилення практик кібербезпеки, сприяння співпраці між державним і приватним секторами [6].

Мислення (mindset) ZT припускає, що весь трафік середовища, користувачі, пристрої, інфраструктура можуть бути скомпрометовані (compromised), що вимагає ретельного процесу автентифікації та авторизації для всіх запитів на доступ. Впровадження відповідних заходів посилює позицію безпеки державних мереж шляхом ретельної перевірки кожного запиту на доступ, що запобігає несанкціонованим змінам, зменшує ризик вставки (insertion) шкідливого (malicious) коду, забезпечує цілісність програмного забезпечення та ланцюгів постачання, зрештою зміцнюючи загальну кібербезпеку держави [7].

Прийняття менталітету ZT передбачає фундаментальну переоцінку та переосмислення того, як підходити до кібербезпеки в організації [8]. Такий менталітет доповнює традиційні периметральні (perimeter-based) моделі убезпеки, створюючи динамічніший підхід, за яким не можна довіряти будь-якій сутності за замовчуванням (by default), незалежно від її розташування, всередині даного середовища чи поза ним [9]. Щоб ефективно з'ясовувати сучасне динамічне середовище загроз, організації мають: впроваджувати скоординований та комплексний моніторинг, менеджмент і захисні операції системи для безперервного захисту; безперервно верифіковувати та перевіряти всі запити на ресурси та трафік середовища; безперервно верифіковувати та перевіряти позицію безпеки всіх пристроїв та інфраструктури; готуватися до швидкого реагування та відновлення, визнаючи притаманний (inherent) ризик, пов'язаний з усіма дозволами на доступ до критичних ресурсів [10].

Керівні принципи ZT, окреслені у згаданій публікації NIST SP 800-207, становлять ядро ZTA: завжди не довіряти, завжди перевіряти – ставитися як до ненадійного (untrusted) кожного користувача/PE/NPE, пристрою, програми/робочого навантаження, потоку даних; динамічно автентифіковувати та явно схвалювати всю діяльність, дотримуючись принципу найменших привілеїв (Least Privilege); припускати злам (breach) – працювати й захищати ресурси, припускаючи, що зловмисник вже має присутність у межах даного середовища; планувати заборону за замовчуванням (deny-by-default) і ретельно перевіряти (heavily scrutinize) всіх користувачів, всі пристрої, потоки даних, запити; безперервно вносити в журнал (log), інспектувати, вести моніторинг усіх змін конфігурації, доступів до ресурсів, трафіку середовища на наявність підозрілої діяльності; явно верифіковувати – безпечно та послідовно (consistently) верифіковувати доступ до всіх ресурсів, використовуючи кілька атрибутів (динамічних і статичних), щоб виводити рівні довіри для рішень щодо контекстного доступу (contextual access decisions) [11].

Електроенергія є прикладом продукту, який має постачатися у потрібному обсязі у потрібний час (just in time (JIT)). Принцип JIT для своїх ланцюгів постачання запропонувала компанія Toyota (заснована у 1937 р.; ТМ у лістингу біржі NYSE) у 1950-х роках. Цей принцип набув поширення в Японії та інших країнах світу у багатьох галузях . Актуальним є поширення принципу JIT в галузі електроенергетики України з урахуванням сучасних викликів і технологічних можливостей, зокрема можливостей цифровізації, електронного трейдингу, штучного інтелекту, а також євроінтеграції [12−14].

Принцип JIT відповідає принципу нульової довіри для мереж [15].

1. *Zero Trust Implementation Guideline Phase One. Cybersecurity Technical Report*. *Version 1.0.* U/OO/107297-26. PP-25-4750. Fort Meade, MD: National Security Agency, 2026, January. 368 p.
2. Горбачук В., Дунаєвський М. Енергетична резильєнтність України і конкурентоспроможність Європи в цілому. *Національна безпека і оборона*. 2026. 1−2 (201−202). С. 80−85. https://razumkov.org.ua/images/2026/04/20/NSD201-202_2025_ukr.pdf.
3. Kovalenko I.N., Savchuk M.N. On a statistical algorithm to decode heavily corrupted linear codes. *Applied Probability and Stochastic Processes*. J.G.Shanthikumar, U.Sumita (eds.). International Series in Operations Research & Management Science. V. 19. Boston, MA: Springer, 1999. P. 73−82. https://doi.org/10.1007/978-1-4615-5191-1_6.
4. Savchuk M. N. Works of the Kiev school of theoretical cryptography. *Cybernetics and Systems Analysis*. 2010. 46 (3). P. 386−404. https://doi.org/10.1007/s10559-010-9214-1.
5. Гінзбург М.Д., Бабенко В.О. Safety та Security − як це буде українською? *Стандартизація, сертифікація, якість*. 2016. 3 (200). С. 13−17. http://nbuv.gov.ua/UJRN/ssia_2016_3_4.
6. Gorbachuk V., Zaslavskyi V., Knopov P. Impacting equilibrium states by technologies and conflict factors. *Cybernetics and Systems Analysis*. 2022. 58 (6). P. 923−934. https://doi.org/10.1007/s10559-023-00526-w.
7. Evdokimov V., Polukhin A., Tsvilii D., Lukashevych Y., Havva O. P2P contracts as a mechanism for automating and decentralizing the modern energy market. *OIDA International Journal of Sustainable Development*. 2026. 19 (6). P. 39−48. https://doi.org/10.64211/oidaijsd190603.
8. Кіссінджер Г., Манді К., Шмідт Е. *Генезис. Штучний інтелект, надія та людський дух*. Stone Publishing, 2025. 224 с. ISBN 978-617-8144-79-1.
9. Kovalenko I. N. Influence of Boris V. Gnedenko's probabilistic-statistical school on the development of cybernetics and informatics. *Cybernetics and Systems Analysis*. 2017. 53 (6). P. 876−883. https://doi.org/10.1007/s10559-017-9989-4.
10. *Risk Taxonomy and Thresholds for Frontier AI Frameworks. Technical Report*. Palo Alto, CA: Frontier Model Forum. 2025, June 18. 13 p.
11. Горбачук В.М. Компоненти і динаміка Government AI Readiness Index України та сусідніх держав у 2019−2025 рр. *Сучасна кібернетика: Глушковські читання. XIV Міжнародна науково-практична конференція: Матеріали*. Київ: Інститут кібернетики імені В.М.Глушкова НАН України, 2025. Вип. 14. С. 28−38.

12. Gorbachuk V., Bespalov S. Regulations, international standards, indicators and digitalization of modern energy. *Transformation of the Economic System in the Context of Global and Regional Changes: Collective monograph*. R.Bendaravičienė, K.Shaposhnykov (eds.). Riga, Latvia: Jan Kochanowski University of Kielce; Baltija Publishing, 2026. P. 919–943. https://doi.org/10.30525/978-9934-26-670-6-39.
13. Горбачук В.М., Беспалов С.А. Виміри та індикатори врядування, інфраструктури, прийняття державним сектором штучного інтелекту. *Національні інтереси України*. 2026. 5 (22). С. 291–306. https://doi.org/10.52058/3041-1793-2026-5(22)-291-306.
14. Горбачук В.М., Камуз А.О., Товстенко Л.М. Індекс готовності уряду до штучного інтелекту та його індикатори політичної спроможності. *Наука і техніка сьогодні*. 2026. 4 (58). С. 3067–3079. https://doi.org/10.52058/2786-6025-2026-4(58)-3067-3079.
15. Горбачук В.М., Беспалов С.А. Резильєнтність у рівнях розвитку штучного інтелекту України та сусідніх держав 2020–2025 років. *Національні інтереси України*. 2026. 4 (21). С. 228–241. https://doi.org/10.52058/3041-1793-2026-4(21)-228-241.

V.M. Zvaritch, Yu.I. Gyzhko, L.B. Ostapchuk

SOME FEATURES RELATED TO THE DESIGN OF WIRELESS VIBRATION DIAGNOSTICS SYSTEMS FOR POWER EQUIPMENT

In the post-war era, the energy grid is not merely a rear infrastructure; it is a new theatre of operations, where traditional methods of centralised defence have become the primary vulnerability. As V.F. Zaluzhny noted in his report, 'the main lesson of modern warfare is that without energy, any technological system turns into a pile of scrap metal' [1].

Assessing the reliability of electrical equipment is of particular importance in the post-war period. The uninterrupted operation of electrical equipment is essential for the reliable functioning of a power station. In the post-war period, it is advisable to have mobile monitoring and diagnostic systems. These should enable the rapid assessment of the technical condition of both primary and auxiliary equipment. The use of wireless technologies in the construction of control and diagnostic systems is particularly attractive. The structure of these systems depends on the equipment to be monitored and diagnosed.

There are modern technological solutions that have already become wireless communication standards and are used to exchange data between devices over a certain distance. The IEEE 802.11 (Wi-Fi) series of standards, the IEEE 802.15.1 (Bluetooth) standard, and solutions based on the 802.15.4 standard (ZigBee, WirelessHART, MiWi) are more widely used. The use of the LoRaWAN standard, which provides a long communication range but has limitations in terms of speed, offers great prospects. Such equipment is manufactured by ADVANTECH [2].

At the same time, the use of wireless channels in vibration diagnostics systems for power equipment creates additional cybersecurity risks, including unauthorised access to sensor nodes, interception or spoofing of diagnostic data, denial-of-service attacks, and manipulation of measurement results. Therefore, the design of such systems should include authentication of sensor nodes, protection of data transmission channels, network segmentation, access control, and mechanisms for detecting abnormal communication behaviour. These measures are particularly important for energy facilities that belong to critical infrastructure.

The Institute of Electrodynamics of the National Academy of Sciences of Ukraine is conducting research into the development of vibration diagnostic systems for electrical equipment, including wireless components [3]. A laboratory prototype of such a system has been developed (Fig. 1).

The wireless vibration diagnostics system comprises units responsible for measuring, converting, and transmitting data (hardware) and units that implement the system's software control, perform statistical processing of the measured

signals, and develop decision rules for determining the technical condition of the equipment being diagnosed (software).

The sensor unit is responsible for measuring, processing, and transmitting measured signals at individual components of electrical machines. When developing the laboratory prototype of the vibration diagnosis system, modular principles were applied to ensure that the system could be modified to meet the user's specific requirements.

When designing the components of the IMS system (information-measuring system) to account for the specific operational characteristics of the diagnostic target, a key step is to determine the type of wireless communication protocol and to develop an algorithm for the operation of the autonomous measurement transducer, which will take into account both the characteristics of the data transmission channel and the requirements for receiving and transmitting diagnostic information.

Figure 1 – Laboratory prototype of the wireless unit for the vibration diagnostics system for power equipment

The sensor unit is based on the ADXL202 sensor manufactured by Analog Devices and the Bluetooth data transmission protocol.

Physically, the sensor unit used in the laboratory prototype of the vibration diagnosis system comprises the following main components: two ADXL202 accelerometers; a PIC16LF873–041 microcontroller manufactured by Microchip Technology; an EYMF2CAMM–XX Bluetooth module manufactured by TAIYO YUDEN; and associated components that ensure the unit's operation.

The ease of use of sensors whose outputs provide a DCM signal is that such sensors can be connected directly to the microprocessor's counter input without the need for analogue-to-digital conversion or interface logic circuits, which simplifies the processing of the measured signal and increases the devices' battery life.

Using the developed IMS prototype, experimental studies were carried out on the vibration characteristics of the auxiliary motors at the Darnytsia Thermal Power Plant. Using the developed vibration module of the multi-level IMS diagnostic system, measurements and processing of vibration signals were carried out, which were recorded at the bearing assemblies and the rotating shaft of a DKRAI – 4519–4V (manufactured in Germany), with parameters P = 710 kW; U = 3000 V; I = 156 A; n = 1490 rpm.

In accordance with the international standard ISO 10816-3:1998 'Mechanical vibration – Evaluation of machine vibration by measurements on non-rotating parts – Part 3: Industrial machines with nominal power above 15 kW and nominal speeds between 120 r/min and 15,000 r/min when measured in situ (IDT)", which is in force in Ukraine, the DKRAI – 4519–4V electric machine belongs to Group 1 of the corresponding power classification. The sensor on the electric machine was also positioned in accordance with ISO 10816-3:1998.

The vibration signal was processed using the Bartlett window. Figure 2 shows a photograph of the performance test of a laboratory prototype of a wireless vibration diagnostics system at the Darnytsia Thermal Power Plant.

Figure 2 – Functionality testing of a laboratory prototype of a wireless vibration diagnostics system for power generation equipment at the Darnytsia CHP

The vibration signal measured at the moving component of the electrical machine under diagnosis is output from the sensor in analogue form.

A distinctive feature of this sensor unit is the high speed of the wireless channel, but the relatively low operational autonomy of the sensor unit without the use of energy-saving algorithms that take into account the operating characteristics of the object under diagnosis, and without the use of additional energy storage devices as a component of the wireless sensor unit.

The use of TE Connectivity's 8911 series sensors and ADVANTECH's WISE-2410 NB, which utilise the LoRaWAN wireless transmission channel, is also proposed.

Vibration signal processing algorithms, which form the basis of such systems' operation, are of great importance for the development of effective wireless vibration diagnostics systems [3–6].

1. Zaluzhnyi, V.F. (2026, March, 27). *Energy Intergrid: Resilience Architecture in the New Domain of Warfare, Proceedings of the International Scientific and Practical Conference «The Energy Front: The Sixth Theatre of Warfare» (Strategy for Defence, Management and Recovery)* (pp. 5–8). Kyiv, Ukraine. Retrieved May 12, 2026, from https://ipme.kiev.ua/konferencii/energy-front-2026/ [in Ukrainian].
2. ADVANTECH https://www.advantech.com/en-us/contact (Retrieved May 17, 2026).
3. Gyzhko, Yu., & Zvarych, V. (2024). Features of the design of equipment components taking into account the use of wireless communication units. *Technical Electrodynamics*, *5*, 94–98 [in Ukrainian]. https://doi.org/10.15407/techned2024.05.094.
4. Babak V.P., Babak S.V., Myslovych M.V., Zaporozhets A.O., Zvaritch V.M. Diagnostic Systems For Energy Equipments Part of the Studies in Systems, Decision and Control book series (SSDC, volume 281**)** - Erfurt: Springer Nature, (Switzerland), 2020. - 133 p. https://doi.org/10.1007/978-3-030-44443-3.
5. Zvaritch V., ”Some Singularities of Linear AR Processes Characterization in Applied Problems of Power Equipment and Power Systems Diagnosis”, In: Kyrylenko, O., Denysiuk, S., Strzelecki, R., Blinov, I., Zaitsev, I., Zaporozhets, A. (eds) Power Systems Research and Operation. Studies in Systems, Decision and Control, vol 512. Springer, Cham, 2024. DOI: 10.1007/978-3-031-44772-3_12.
6. Zaporozhets A., Babak V.,Zvaritch V., Kovtun S., Gyzhko Yu., Khaidurov V., Verpeta V. Integration of Physical and Probabilistic Measures in Stochastic Measurements of Manufacturing Processes, 2026, (accepted for publication in MDPI Metrology).

С.В. Калякін, І.В. Стародубцев

ПРАКТИЧНІ АСПЕКТИ ТЕХНІЧНОЇ ІДЕНТИФІКАЦІЇ ДЖЕРЕЛ СПАМ-РОЗСИЛОК ТА СОЦІОТЕХНІЧНИХ КІБЕРЗАГРОЗ

Актуальність теми дослідження зумовлена безпрецедентним зростанням кількості соціотехнічних кібератак в умовах глобальної цифровізації та ведення гібридної війни. Фішинг та спам-кампанії залишаються найпоширенішим вектором початкового компрометування як приватних осіб, так і об'єктів критичної інфраструктури. Оскільки зловмисники постійно вдосконалюють методи обходу автоматизованих систем захисту шляхом маніпуляцій з поштовими протоколами (зокрема, спуфінгу), виникає гостра потреба в розробці ефективних практичних алгоритмів глибокої технічної ідентифікації джерел таких загроз. Традиційні підходи до аналізу поштового трафіку втрачають свою ефективність, що вимагає впровадження новітніх інструментів атрибуції на рівні маршрутних метаданих.

Серед них фішинг і соціотехнічні атаки й далі посідають провідні позиції. За даними глобального звіту Verizon Data Breach Investigations Report за 2025 рік [1], людський фактор фігурує у 68% усіх успішних кібератак, а фішинг становить 57% серед інцидентів, пов’язаних із соціальною інженерією. На національному рівні ситуація також викликає серйозне занепокоєння: відповідно до офіційної статистики Урядової команди реагування на комп’ютерні надзвичайні події України (CERT-UA), у 2025 році загальна кількість оброблених кіберінцидентів зросла на 37,4%, тоді як кількість зафіксованих фішингових атак збільшилася вдвічі [2].

Однією з ключових проблем сучасного фішингу є те, що зловмисники дедалі вправніше використовують недоліки поштових протоколів для підміни адреси відправника, тобто спуфінгу. У результаті шкідливі повідомлення маскуються під офіційні листи відомих брендів, банків або державних установ. Їхнє візуальне оформлення та психологічні механізми впливу часто настільки добре продумані, що пересічному користувачеві вкрай складно відрізнити підроблений лист від справжнього. Саме тому сьогодні вже недостатньо обмежуватися поверхневим аналізом змісту повідомлення. Як свідчать сучасні дослідження, зокрема праці М. Ю. Кулікової [3], навіть передові гібридні системи виявлення цільового фішингу, що поєднують семантичний аналіз тексту за допомогою нейромереж (наприклад, моделі BERT) та автоматичну перевірку автентифікації доменів (SPF, DKIM, DMARC), мають певні обмеження. Зловмисники здатні обходити такі фільтри, використовуючи легітимні, але скомпрометовані корпоративні сервери або сервіси транзакційних розсилок, що робить автоматизований лінгвістичний чи технічний аналіз недостатнім для повної атрибуції атаки.

Натомість особливої ваги набуває глибоке технічне дослідження інцидентів на рівні службових метаданих. Лише детальний аналіз сирих поштових заголовків (raw headers) дає змогу обійти візуальні маніпуляції, відстежити реальні маршрути проходження трафіку та об'єктивно встановити інфраструктуру, з якої походить кіберзагроза.

Питання протидії соціотехнічним загрозам та розслідування кіберзлочинів перебувають у постійному фокусі вітчизняних науковців. Зокрема, загальні аспекти ідентифікації інформаційних злочинів, використання методів соціальної інженерії та кібертероризму ґрунтовно досліджувалися у працях С. В. Калякіна [4].

Водночас, незважаючи на вагомий внесок фахівців у формування теоретико-практичної бази кібербезпеки, вузькоспеціалізовані питання практичної атрибуції відправників спам-розсилок шляхом автоматизованого аналізу сирих поштових заголовків потребують додаткових прикладних досліджень.

Метою цього дослідження є практичне відстеження реальних джерел походження підозрілих електронних повідомлень на основі аналізу маршрутних метаданих, а також комплексна оцінка рівня технічної захищеності доменних зон від атак, пов'язаних із підміною відправника.

Для досягнення поставленої мети було застосовано комплексний підхід, який поєднує методи глибокого мережевого аналізу та автоматизацію розвідувальних процедур на основі відкритих джерел. З огляду на вимоги цифрової криміналістики, усі експериментальні дії з вилученими зразками небажаної пошти виконувалися в спеціально налаштованому ізольованому середовищі на базі операційної системи Kali Linux [5]. Такий підхід повністю усував ризик випадкового компрометування основної робочої станції під час взаємодії з потенційно небезпечними файлами.

Визначальним елементом методології та ключовою інновацією практичної частини дослідження стала розробка власного програмного сценарію мовою Python, призначеного для прискорення процесу атрибуції кіберзагроз. Запропонований алгоритм суттєво оптимізує рутинну роботу аналітика: він автоматично виконує парсинг сирих файлів формату EML, за допомогою регулярних виразів виокремлює реальну IPv4-адресу ініціатора розсилки з найнижчого службового поля Received та одразу формує системні виклики до мережевої утиліти whois [6]. Завдяки цьому в автоматичному режимі можна отримати первинні консолідовані відомості про інтернет-провайдера, власника апаратної інфраструктури та географічну юрисдикцію сервера-відправника, що створює надійну доказову основу для подальшого розслідування.

Результати проведеного експериментального дослідження дали змогу отримати низку критично важливих висновків щодо природи сучасних поштових атак. Передусім аналіз мережевої інфраструктури відправників

показав, що значна частина сучасного спаму та цілеспрямованого фішингу генерується не зі скомпрометованих персональних комп'ютерів чи традиційних ботнетів, а з використанням ресурсів легітимних хмарних платформ і комерційних сервісів транзакційних розсилок, зокрема Amazon AWS або Mailgun. Оскільки IP-адреси великих технологічних корпорацій за замовчуванням мають високий рівень довіри в глобальній мережі, традиційна практика блокування загроз виключно за IP-адресою або діапазоном підмереж сьогодні виявляється малоефективною та легко обходиться зловмисниками.

Ще одним, і фактично ключовим, результатом дослідження стало технічне підтвердження того, що фундаментальною передумовою безперешкодного електронного спуфінгу залишається неналежне налаштування криптографічних політик безпеки з боку власників корпоративних доменів. Експериментальна перевірка DNS-записів за допомогою утиліти dig [7] наочно показала, що комерційні компанії нерідко або повністю ігнорують впровадження протоколу DMARC, або залишають його в пасивному режимі моніторингу. Відсутність жорсткої політики автоматичного відхилення неавторизованого трафіку фактично змушує приймаючі сервери пропускати підроблені повідомлення, відкриваючи шахраям прямий доступ до поштових скриньок потенційних жертв під прикриттям авторитетних брендів.

Підсумовуючи отримані результати, варто наголосити, що ефективна протидія сучасним соціотехнічним загрозам вимагає суттєвого перегляду тактичних підходів до розслідування кіберінцидентів. Практична цінність цієї роботи полягає у формуванні дієвих рекомендацій для фахівців з інформаційної безпеки та аналітиків підрозділів кіберполіції. Насамперед існує нагальна потреба в суворій стандартизації процедури вилучення цифрових доказів на етапі первинного реагування на інциденти. Така процедура має безумовно передбачати вилучення та криптографічне хешування електронних повідомлень у вихідному форматі EML ще до будь-якої взаємодії слідчого з візуальним HTML-контентом. Саме це забезпечує юридичну цілісність маршрутних метаданих і збереження доказової бази.

Крім того, надзвичайно важливим превентивним заходом є впровадження практики регулярного автоматизованого аудиту DNS-записів об'єктів критичної інфраструктури, державних установ і великих комерційних організацій. Лише системний технічний контроль у поєднанні зі стимулюванням переходу до суворих політик автентифікації здатний суттєво зменшити ризики підміни доменних імен і, як наслідок, критично знизити загальний рівень успішності цілеспрямованих фішингових кампаній.

1. Verizon. Data Breach Investigations Report (DBIR). URL: https://www.verizon.com/business/resources/reports/dbir/ (Дата звернення: 15.03.2026).

2. Урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA): офіційний портал. URL: https://cert.gov.ua/ (Дата звернення: 24.03.2026).
3. Кулікова М. Ю. Розробка системи запобігання цільовому фішингу : кваліфікаційна робота бакалавра : спец. 125 Кібербезпека. Вінниця : Донецький національний університет імені Василя Стуса, 2025. 66 с. (Дата звернення: 20.03.2026).
4. Калякін С. В. Кіберпереслідування як інформаційний злочин // Актуальні питання протидії кіберзлочинності та торгівлі людьми : матеріали Всеукр. наук.-практ. конф. (м. Харків, 15 лист. 2017 р.). Харків : ХНУВС, 2017. С. 19–21. (Дата звернення: 20.03.2026).
5. Offensive Security. Kali Linux: Penetration Testing and Ethical Hacking Linux Distribution. URL: https://www.kali.org/ (Дата звернення: 20.03.2026).
6. Linux Programmer's Manual. WHOIS(1) - General Commands Manual. URL: https://linux.die.net/man/1/whois (Дата звернення: 21.03.2026).
7. Internet Systems Consortium (ISC). DIG(1) - BIND 9 Administrator Reference Manual. URL: https://bind9.readthedocs.io/en/latest/manpages.html (Дата звернення: 21.03.2026).

R. Vasylyshyn

LIMITATIONS OF ARTIFICIAL INTELLIGENCE USAGE IN THE NUCLEAR PLANTS' SECURITY

Artificial intelligence has opened new horizons for a holistic scientific approach, as it allows the analysis of large amounts of data from different sources in the shortest period of time. Modern scientists actively discuss the trend of creating computer simulations based on multifactor models.

This became possible due to several reasons. First, sensors appeared that are able to read signals from the environment over long distances. Second, the transition of data to a digital format helps to speed up their processing. Third, it became possible to better establish cause-and-effect relationships within the programmed model. Previously, geopolitical specialists were narrow-profile, had limited access to data, and the equipment for recording invasions was of lower quality [3].

The scientific work of I. Toton and J. Skouras emphasize that the most difficult stage of the defense of the nuclear facilities will be the development of an algorithm that represents the potential response of personnel to stressful situations according to requirements.

Human reaction to threats has to be researched in relation to personal factors. Including comparing data according to the political, cultural, and religious beliefs of the nation they represent. It is absolutely impossible to determine how valid predictive models are for rare events that did not occur. And untested models cannot be relied on.

It will likely be useful to first investigate simplified system models. The representativeness of the usefulness of predictions of the risk of failure in nuclear deterrence has not yet been established. After developing confidence in the ability of the models to qualitatively reflect reality, the developed methods should be used as a tool for analyzing the attack on security systems. Because the reliability of the program's responses will reflect the ability to rely on the analysis in the future [4].

One of the gaps in the nuclear security system is also the possibility of theft of equipment and technologies that support it. The human factor plays a key role in the security of the facility. The selection of highly qualified personnel capable of independently assessing the probability of damage according to calculations, finding inconsistencies in the data obtained, can save from a potential unintentional war.

Especially in conditions of intensive development and competition between countries. Physically, the structure of assessing the level of nuclear danger remains vulnerable to outside interference.

There are systems capable of deceiving existing radars, increasing the risk of false detection of attacks on nuclear objects.Technical errors due to inaccuracies in the coding of the data processing algorithm also should not be ignored.

A similar threat is the introduction of inappropriate information due to obsolescence. For the mentioned above reasons, S. M. Amadae and S. Evin believe that the nuclear security system should not be configured to the level of full automation and rely entirely on machine learning methods.

Scientists believe that existing technologies have not yet reached the level of development to function at a sufficient level without human intervention [1].

There is a clear understanding that predictive modeling requires training on a previous dataset. This fact creates an understanding that a nuclear deterrence program can be brought to an absolute. First, for a high level of efficiency, it is necessary to process a large amount of information. This statement proves that there is a significant limitation of practical data creation.

Although computer modeling helps to better identify potential nuclear safety problems, its capabilities are limited. According to international conventions, it is forbidden to carry out attacks on nuclear facilities. If other states carry out physical or hacker attacks on such structures, then these actions are completely illegal. It is strictly prohibited for disposal to the general public.

It is also impossible to reach information for foreign researchers to share the knowledge about committed attacks and identify potential weaknesses of security system. The presence of a powerful nuclear potential fades into the background compared to the diplomatic influence and activities of the intelligence systems of foreign states.

For this reason, the relationship between the ability of the system to isolate data during analysis and the stability of forecasts is difficult to determine. It is impossible to clearly establish whether adding technical details will necessarily lead to the transmission of reliable results. If with increasing accuracy and the amount of information entered, the predictive model produces more uncertain forecasts, then a quantitative assessment of the risk factors for errors in the structure of nuclear objects' security will be impossible to outline [2].

To conclude, computer simulation as a method used by artificial intelligence specialists helps to analyze multiple spheres of nuclear objects' risk. This can be a powerful tool for statistical assessment of information and potential threat probability. However, information about nuclear plants' security is limited by the individual policy of the country. Further limitations of the topic's research can be due to human interactions, technical misinterpretations, and physical threats. Well-prepared personnel of the nuclear facility are required to use artificial intelligence under strict control. Although many scientists do not consider the AI implementation without human intervention, the dynamic might change with the appearance of superintelligence in safety systems.

1. Amadae, S. M. & Avin, S. (2019) Autonomy and Machine Learning as Risk Factors at the Interface of Nuclear Weapons, Computers and People. *Vincent Boulanin, The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Euro-Atlantic Perspectives.* Stockholm: SIPRI. pp. 105-118. competition. Louisiana Tech Research Institute. Retrieved May 21, 2026, from https://ltri.org/wp-content/uploads/2020/12/Guide-to-Nuclear-Deterrence-in-the-Age-of-Great-Power-Competition.pdf.
2. Lowther, B. H. (2020) Guide to nuclear deterrence in the age of great-power.
3. Lustick, I.S.& Tetlock, P.E. (2021) The simulation manifesto: The limits of brute-force empiricism in geopolitical forecasting, *Future& Foresight Science,* 3 (2), 1-22.
4. Toton, E., Scouras, J. (2019) Nuclear deterrence as a complex system. National security report of Johns Hopkins applied physics laboratory, 20 p. Retrieved May 22, 2026, from https://apps.dtic.mil/sti/pdfs/AD1075533.pdf.

Д.С. Матушкін

КІБЕРСТІЙКІСТЬ ГІБРИДНИХ МІКРОМЕРЕЖ З ВІДНОВЛЮВАНОЮ ГЕНЕРАЦІЄЮ ТА СИСТЕМАМИ НАКОПИЧЕННЯ ЕНЕРГІЇ

Сучасні гібридні мікромережі поступово стають одним із ключових елементів розподіленої енергетики, оскільки дають змогу поєднувати локальну генерацію, накопичувачі енергії та інтелектуальні системи керування в єдину енергетичну структуру [1]. У таких системах електрична енергія вже не лише виробляється та споживається, а постійно перерозподіляється відповідно до стану генерації, навантаження, заряду акумуляторів, вартості енергії, технічних обмежень обладнання та команд системи керування. Саме тому гібридна мікромережа є не просто локальним енергетичним об'єктом, а складною кіберфізичною системою, у якій цифровий контур керування безпосередньо впливає на фізичні режими роботи обладнання.

Разом із тим гібридна мікромережа є не лише електротехнічною, а й кіберфізичною системою. Її функціонування значною мірою залежить від достовірності вимірювальних даних, коректності алгоритмів керування, надійності каналів зв'язку та захищеності програмно-апаратних засобів. Через це питання кібербезпеки для таких об'єктів не можна розглядати окремо від питань енергетичної надійності. Помилка або втручання в цифровий контур керування може мати цілком фізичні наслідки: порушення балансу потужності, некоректний режим заряджання накопичувача енергії, перевантаження інверторного обладнання, зниження якості електроенергії або втрата резервного електропостачання.

Типова гібридна мікромережа містить кілька взаємопов'язаних підсистем. До них належать підсистема генерації на основі відновлюваних джерел енергії, система накопичення енергії, блоки перетворення електроенергії, система керування енергопотоками (EMS), система керування батареєю (BMS), локальні контролери, засоби збору даних та інтерфейси диспетчеризації. Кожна з цих підсистем може бути потенційною точкою впливу. Наприклад, спотворення даних про напругу, струм, температуру або стан заряду акумулятора може призвести до неправильного вибору режиму роботи системи. На практиці це може проявлятися не як миттєва аварія, а як поступове зниження ефективності, прискорене старіння обладнання або накопичення режимних відхилень.

Центральне місце в роботі гібридної мікромережі займає EMS, яка приймає рішення щодо розподілу потужності між джерелами генерації, накопичувачем, мережею та навантаженням. Водночас BMS, відповідає за контроль напруги, струму, температури, стану заряду та допустимих режимів

роботи акумуляторів. Якщо мікромережа інтегрована із системою віддаленого моніторингу (SCADA), з'являється ще один рівень цифрової взаємодії, через який здійснюються збір даних, передавання команд, діагностика та диспетчеризація. Отже, EMS, BMS і SCADA формують критичний цифровий контур мікромережі, порушення роботи якого може мати не лише інформаційні, а й енергетичні наслідки [2, 3].

Особливо чутливим елементом гібридної мікромережі є система накопичення енергії. Акумулятори мають обмеження за напругою, струмом, температурою, глибиною розряду та швидкістю заряджання. Тому BMS має забезпечувати не лише енергетичну ефективність, а й безпечність режимів роботи. У разі несанкціонованої зміни параметрів заряджання або передавання некоректних команд між EMS і BMS можливе перевищення допустимих режимів, перегрів, зниження ресурсу акумулятора або аварійне відключення накопичувача. Потенційні кіберризики для основних елементів гібридної мікромережі та їх можливі енергетичні наслідки наведено в табл. 1.

Таблиця 1 – Потенційні кіберризики для гібридної мікромережі

Елемент мікромережі	Потенційний кіберризик	Можливий енергетичний наслідок
EMS	Несанкціонована зміна команд керування	Порушення балансу потужності
BMS	Підміна даних про SOC, напругу або температуру	Некоректне заряджання, перегрів, зниження ресурсу
SCADA / моніторинг	Спотворення або блокування даних	Ускладнення діагностики та реагування
Інверторне обладнання	Зміна параметрів роботи або команд відключення	Погіршення якості електроенергії, втрата живлення
Канали зв'язку	Затримка, втрата або підміна повідомлень	Перехід системи в неузгоджений режим

Окрему увагу доцільно приділяти прихованим або малопомітним впливам. У цьому випадку мікромережа не виходить з ладу миттєво, а продовжує функціонувати у зовні нормальному режимі. Проте її робота поступово відхиляється від оптимальної: знижується ефективність використання відновлюваної генерації, збільшується кількість циклів заряджання-розряджання акумулятора, зростають втрати в силових перетворювачах, погіршується ресурс обладнання або зменшується доступний резерв енергії. Саме такі сценарії є складними для виявлення, оскільки вони можуть виглядати як звичайна технічна нестабільність, похибка вимірювання або наслідок варіативності генерації.

Підвищення кіберстійкості гібридної мікромережі має базуватися не на одному окремому засобі захисту, а на багаторівневому підході, який може включати:

- контроль доступу до параметрів EMS, BMS та інверторного обладнання;
- сегментацію комунікаційної мережі;
- перевірку достовірності вимірювальних даних;
- виявлення аномалій у режимах роботи;
- резервні алгоритми керування та безпечні режими;
- журналювання подій для подальшого аналізу інцидентів [2, 3].

Особливе значення має порівняння цифрових команд із фізично можливими режимами системи. Наприклад, якщо команда на заряджання акумулятора не узгоджується з фактичною генерацією, температурою або станом заряду, така ситуація має розглядатися як потенційно небезпечна і переводити систему в обмежений безпечний режим.

Перспективним інструментом аналізу кіберстійкості гібридних мікромереж є цифровий двійник [4, 5]. Його використання дає змогу моделювати не лише нормальні, аварійні та перехідні режими, а й кіберфізичні збурення, пов'язані з підміною даних, затримками сигналів, втратою зв'язку або некоректними командами керування. У такому підході цифровий двійник може виконувати дві функції. Перша полягає у попередньому дослідженні вразливих режимів без ризику для реального обладнання. Друга полягає у формуванні еталонної поведінки системи, з якою можна порівнювати фактичні вимірювання для виявлення аномалій.

Таким чином, кіберстійкість гібридної мікромережі слід розглядати як складову її загальної енергетичної стійкості. Для таких систем недостатньо лише захищати канали зв'язку або обмежувати доступ до програмного забезпечення. Необхідно забезпечити узгодженість між цифровими командами, вимірювальними даними та фізичними режимами роботи обладнання. Найбільш критичними елементами є EMS, BMS, інверторне обладнання, канали обміну даними та системи моніторингу. Комплексний підхід, що поєднує контроль доступу, виявлення аномалій, резервні режими та цифрове моделювання, може стати основою для підвищення кіберстійкості гібридних мікромереж у сучасній розподіленій енергетиці.

1. Лещенко, П., Запорожець, А. (2025). Огляд архітектур кластерів мікромереж на базі розподілених джерел енергії. Системні дослідження в енергетиці, (2 (82), 13-28. https://doi.org/10.15407/srenergy2025.02.013.
2. 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.

3. Ayele, E. D., Gonzalez, J. F., & Teeuw, W. B. (2024). Enhancing Cybersecurity in Distributed Microgrids: A Review of Communication Protocols and Standards. Sensors, 24(3), 854. https://doi.org/10.3390/s24030854.
4. Abdelrahman, M. S., Kharchouf, I., Hussein, H. M., Esoofally, M., & Mohammed, O. A. (2024). Enhancing Cyber-Physical Resiliency of Microgrid Control under Denial-of-Service Attack with Digital Twins. Energies, 17(16), 3927. https://doi.org/10.3390/en17163927.
5. Matushkin, D., Zaporozhets, A. (2026). Models for Forecasting Solar Generation in the Microgrid. Smart Charging in Solar Microgrids. Lecture Notes in Electrical Engineering, vol 1518. Springer, Cham. https://doi.org/10.1007/978-3-032-12301-5_3.

О.С. Кушнір, Д.О. Рибачок

МЕРЕЖЕВИЙ АНАЛІЗ ЕНЕРГЕТИЧНИХ СИСТЕМ НА ОСНОВІ ДАНИХ ENTSO-E

Сучасні енергетичні системи Європи та України функціонують у середовищі високої невизначеності, що зумовлено зростанням частки відновлюваних джерел, збільшенням міждержавних перетоків, а також інтенсивністю загроз для критичної інфраструктури. У зазначених умовах ключовим стає кількісне оцінювання резильєнтності енергетики. Відповідно підходи до цифрової стійкості динамічних систем, зокрема роль структурованих електронних даних, можуть узгоджуватись з сучасними вимогами до обробки енергетичних потоків та забезпечення їхньої надійності [1].

Енергетичні мережі можуть бути описані як граф

$$G = (V, E, w),$$

де V – множина бідінгових зон, E – множина міждержавних інтерконекторів, а $w: E \to R_+$ задає ваги, що відображають середні або миттєві перетоки. Ступінь вершини визначається як:

$$k_i = \sum_{j \in V} a_{ij},$$

де a_{ij} – елемент матриці суміжності.

Міри центральності, зокрема посередницька

$$C_B(i) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}},$$

використовуються для виявлення критичних вузлів, відмова яких може спричинити каскадні збої. Для ринкового шару сформовано кореляційну мережу, де ваги ребер визначаються коефіцієнтом Пірсона:

$$\rho_{ij} = \frac{\sum_{t=1}^{T}(P_{i,t} - P_i)(P_{j,t} - P_j)}{\sqrt{\sum_{t=1}^{T}(P_{i,t} - P_i)^2}\sqrt{\sum_{t=1}^{T}(P_{j,t} - P_j)^2}}$$

Ребро може бути включено до мережі, якщо $\rho_{ij} > \tau$, де τ— параметр стійкості структури. Оптимальні значення τ визначаються за максимумом модулярності

$$Q = \frac{1}{2m}\sum_{i,j}\left(a_{ij} - \frac{k_i k_j}{2m}\right)\delta(c_i, c_j),$$

що дозволяє виділити стійкі ринкові спільноти (market coupling clusters).

Для оцінювання резильєнтності застосовано бутстреп-аналіз. Стабільність спільнот оцінюється індексом Жаккара:

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|},$$

де A - множина бідингових зон, що належать певній спільноті у базовій мережі, B - множина вершин, що належать відповідній спільноті у бутстреп-мережі або у наступному часовому вікні.

Середнє значення J по сотнях вибірок демонструє високу структурну стійкість ринку, а довірчі інтервали дозволяють кількісно оцінити чутливість до шуму та пропусків у даних. Додатково аналіз часових ковзних вікон $W_t = \{t - w + 1, \dots, t\}$ дозволяє оцінювати динамічну резильєнтність — здатність мережевої структури зберігати топологічні властивості у часі.

Потокова архітектура обробки даних, реалізована у системі EnergyNetDA [2,3], забезпечує відтворюваність та оперативність аналізу. Дані ENTSO-E [4] (перетоки, ціни, навантаження, генерація) обробляються у режимі near-real-time, що дозволяє виявляти аномалії, структурні збої та потенційні атаки на рівні даних. Потокова модель $D \xrightarrow{\Psi} D' \xrightarrow{\Phi} G \xrightarrow{A} R \xrightarrow{\Gamma} I$ забезпечує контроль параметрів на кожному етапі, що є критично важливим для кіберстійкості.

Отримані результати демонструють, що європейський ринок електроенергії має чітку кластерну структуру, стійку до випадкових збурень, а фізичний шар мережі містить вузли з високою посередницькою центральністю, які є критичними для запобігання каскадним відмовам. Для України, яка працює в синхронному режимі з ENTSO-E, такі методи дозволяють оцінювати стійкість ОЕС України, моделювати вплив атак на інфраструктуру та аналізувати стабільність ринкових взаємодій у період підвищених загроз.

Узагальнюючи, поєднання мережевих моделей, статистичних методів стабільності та потокової обробки великих даних формує сучасний інструментарій для оцінювання резильєнтності енергетичних систем. Це створює основу для підвищення кіберстійкості, оскільки дозволяє виявляти аномалії у структурі мережі, локалізувати критичні вузли, виявляти маніпуляції на ринку, вираховувати повільні та приховані атаки, моделювати сценарії відмов та підтримувати операторів у кризових ситуаціях.

1. Гавриленко С. О., Голоцуков Г. В., Голоцукова Т. Г., Кушнір О. С. Структуровані електронні документи – основа цифровізованої стійкості функціонування динамічних систем. II Науково-практична конференція «Резильєнтність динамічних систем», 2025. С. 86–90.
2. Рибачок Д. О., Кушнір О. С. Комп'ютерна програма «EnergyNetDA – система мережевого аналізу європейського ринку електроенергії "на добу наперед" на основі потокових даних ENTSO-E»: Свідоцтво про реєстрацію авторського права на твір № 145798 від 20 квітня 2026 р. Український національний офіс інтелектуальної власності та інновацій.
3. EnergyNetDA (веб-ресурс). Доступно: https://live.energyda.net/.
4. ENTSO-E Transparency Platform (офіційний веб-ресурс). Доступно: https://transparency.entsoe.eu/.

А.Р. Білоус

СИСТЕМА КОМПЛЕКСНОГО КІБЕРМОНІТОРИНГУ ТА АНАЛІЗУ АНОМАЛІЙ У СЕГМЕНТОВАНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ. Забезпечення кібербезпеки та підвищення рівня кіберстійкості об'єктів критичної інфраструктури енергетичного комплексу є стратегічним завданням для національної безпеки держави в умовах сучасних кіберзагроз. Традиційні підходи до захисту інформаційних та керуючих систем базуються на принципі глибокої ешелонованої оборони, що передбачає сувору ізоляцію технологічних мереж, апаратне розмежування сегментів за допомогою міжмережевих екранів промислового рівня (таких як Cisco ASA та Firepower) та організацію замкнених контурів VLAN. Проте, як свідчить світовий досвід інцидентів, повна ізоляція мережевого середовища не є абсолютною гарантією безпеки через існування прихованих векторів загроз: використання несанкціонованих знімних носіїв, компрометацію сервісних пристроїв підрядних організацій чи помилки конфігурації. У цих умовах виникає потреба у впровадженні комплексних систем безперервного проактивного моніторингу та аналізу аномалій, що функціонують у реальному часі, для забезпечення видимості процесів безпеки без порушення стабільності технологічного циклу.

Обмеження апаратних платформ та проблема втрати пакетів (Capture Loss). При спробі розгортання систем мережевого виявлення вторгнень (NIDS) та збору телеметрії (Network Security Monitoring - NSM) у розгалужених інфраструктурах працівники стикаються з серйозними архітектурними обмеженнями. Зокрема, у великих технологічних сегментах підприємства, що охоплюють тисячі кінцевих пристроїв, виникає необхідність агрегації та аналізу трафіку з декількох ізольованих мережевих сегментів. При дзеркалюванні трафіку за допомогою технологій SPAN/RSPAN на єдиний інтерфейс моніторингового сенсора початкового рівня та активації інструментів глибокого аналізу пакетів, таких як Zeek та Suricata фіксується стрімке зростання показника втрати пакетів (capture loss) — від 1.5% до 15% і більше. Такий рівень втрат є неприпустимим для об'єктів критичної інфраструктури, оскільки призводить до фрагментації мережевих сесій, пропуску сигнатур шкідливого програмного забезпечення та унеможливлює точний ретроспективний аналіз інцидентів аналітиками SOC.

Особливості маршрутизації та контролю багатоадресного (Multicast) трафіку. Іншим суттєвим викликом є забезпечення інформаційної безпеки специфічних технологічних потоків даних, зокрема багатоадресної розсилки, яка часто застосовується в системах оповіщення, синхронізації або передачі

телеметричних даних між робочими станціями та серверами. Маршрутизація мультикаст-трафіку через декілька рівнів міжмережевих екранів вимагає активації складних протоколів, таких як PIM Sparse Mode, та динамічного керування групами за допомогою IGMP. Налаштування списків контролю доступу ACL для багатоадресного трафіку в умовах ізольованих VLAN є нетривіальним завданням: занадто широкі дозволи створюють потенційні канали для несанкціонованого міжсегментного переміщення даних, тоді як надмірні обмеження блокують критично важливі технологічні сервіси. Системи моніторингу повинні мати можливість детального розбору таких протоколів без зниження продуктивності інтерфейсів.

Безпека інфраструктури моніторингу та міграція керуючих компонентів. Організація Центру реагування на кіберінциденти на базі відкритих рішень вимагає забезпечення безпеки самої платформи моніторингу. При перенесенні ключових компонентів системи, зокрема центрального менеджера до виділеного захищеного серверного приміщення з подальшою зміною IP-адресації виникає комплекс технічних завдань із реконфігурації доступів. Необхідно жорстко обмежити доступ до веб-інтерфейсів адміністрування за допомогою брандмауерів, дозволяючи підключення лише з фіксованих робочих місць аналітиків безпеки, і водночас зберегти безперебійний прийом зашифрованої телеметрії від віддалених сенсорів та агентів.

Пропонована архітектурна модель комбінованого кібермоніторингу. Для мінімізації апаратних навантажень та ліквідації сліпих зон пропонується впровадження гібридної архітектури, що поєднує хостовий (HIDS) та мережевий (NIDS) рівні захисту з урахуванням специфіки великих інфраструктур підприємства:

1. Впровадження хостового моніторингу на базі Wazuh: Розгортання легковажих агентів Wazuh на кінцевих точках дозволяє перенести значну частину аналітичного навантаження безпосередньо на хости. Агенти здійснюють моніторинг журналів подій операційних систем, контроль цілісності критичних файлів та виявлення локальних аномалій. При цьому обсяг даних, що передається мережею до центрального менеджера Wazuh, є мінімальним і складається з оптимізованих логів через зашифровані порти TCP, мінімізуючи навантаження на канали зв'язку;

2. Оптимізація мережевого рівня: Для повного усунення проблеми Capture Loss при зборі трафіку з багатьох паралельних сегментів мережі необхідно модернізувати апаратну складову сенсорів або оптимізувати розподіл системних ресурсів. На сенсорах рекомендується використовувати спеціалізовані мережеві карти з підтримкою апаратного кільцевого буфера та технології Receive Side Scaling для рівномірного розподілу черг обробки пакетів між ядрами центрального процесора. За наявності високих потоків даних виправданим є використання апаратних брокерів мережевих пакетів

NPB, які здійснюють попередню фільтрацію, дедуплікацію та балансування трафіку перед його подачею на аналітичні движки Zeek та Suricata;

3. Захист мультикаст-сегментів: Контроль багатоадресного трафіку реалізується за принципом Zero Trust. На міжмережевих екранах Cisco ASA та комутаторах налаштовуються строгі правила мультикаст-фільтрації, що обмежують адреси джерел та дозволені цільові групи, а паралельно в Suricata створюються кастомні сигнатури для виявлення аномальної активності або спроб сканування мережі через IGMP-запити.

Висновки. Створення ефективної системи виявлення кіберзагроз на об'єктах критичної інфраструктури потребує збалансованого поєднання інструментів хостового та мережевого аналізу. Використання відкритих платформ дозволяє побудувати масштабовану і гнучку систему моніторингу для великої кількості вузлів. Проте успішність її функціонування залежить від вирішення інженерних викликів: усунення втрати пакетів за допомогою апаратної оптимізації драйверів, а також жорсткого контролю мережевих потоків, включаючи складний багатоадресний трафік, на рівні міжмережевих екранів.

1. Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій: НП 306.2.237-2022. – К.: Державна інспекція ядерного регулювання України, 2022.
2. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р.
3. Порядок забезпечення кіберзахисту об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України № 518 від 19.06.2019 р.
4. Security Onion Solutions. Hardware Requirements and Performance Tuning. URL: https://docs.securityonion.net/en/2.4/hardware.html.
5. Wazuh Inc. Scalability and sizing guidelines for enterprise networks. URL: https://documentation.wazuh.com.

Б.А. Лаковський

ВПЛИВ ІНЕРТНОСТІ ОРГАНІЗАЦІЙНИХ ТА ТЕХНІЧНИХ ПІДХОДІВ НА ПІДТРИМАННЯ НАЛЕЖНОГО РІВНЯ КІБЕРБЕЗПЕКИ НА ДЕРЖАВНИХ ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Забезпечення кібербезпеки та кіберстійкості об’єктів критичної інфраструктури в умовах сучасного цифровізованого простору стає стратегічним завданням національної безпеки. Інтеграція технологічних процесів з корпоративними мережами створює нові вектори кіберзагроз, що вимагає переходу від статичних систем захисту до динамічного управління ризиками. Сучасна парадигма захисту державних об'єктів критичної інфраструктури базується на актуалізованих вимогах нормативних документів з технічного захисту інформації (НД ТЗІ), які в свою чергу опираються на передовимі міжнародні стандарти, зокрема сімейство NIST (фреймворк NIST CSF 2.0 та розширений каталог контролів безпеки NIST SP 800-53). Проте на практиці імплементація належного рівня кібербезпеки стикається з внутрішньою інертністю державних структур.

Вимоги НД ТЗІ та архітектура NIST CSF 2.0 передбачають безперервний моніторинг та оперативну адаптацію системи захисту. Проте ефективність протидії сучасним загрозам на державних ОКІ критично знижується через інертність. Організаційна інертність проявляється у тривалих бюрократичних процедурах погодження політик безпеки та бюджетів, небажання перегляду штатного розпису, сформованого десятиліттями тому, та приведення його до актуального стану. В свою чергу, технічна інертність визначається станом та актуальністю апаратного парку (комутаторів, міжмережевих екранів, ПК, серверів), фізичною деградацією обладнання внаслідок тривалої експлуатації та наявністю вимог до запасу ЗІП-у та безпосередньо його запас для його оперативної заміни.

На державних об'єктах ця проблема загострюється через фізичне та моральне зношення компонентів (наприклад, критичне вичерпання ресурсу перезапису enterprise-накопичувачів у масивах даних або термічна деградація елементної бази мережевих пристроїв), складність модернізації мережі за наявності застарілого обладнання, а також економії бюджету на необхідності формування відповідного запасу ЗІП. Процедури публічних закупівель комплектуючих, таких як накопичувачі стандарту NVMe формату U.2 для забезпечення відмовостійкості, можуть тривати місяцями. Це створює тривале вікно вразливості та відмови обладнання, особливо коли деградоване обладнання вже не здатне підтримувати необхідну продуктивність мережі та систем кіберзахисту.

Мета роботи. Запропонувати поверхневий аналітичний метод оцінки впливу організаційної та технічної інертності на реальний рівень кіберстійкості ОКІ, що дозволить обґрунтувати необхідність оптимізації процесів забезпечення та адаптації СУІБ.

Основний матеріал дослідження. Для формалізації впливу інертності на безпеку об'єкта пропонується розрахунок через коефіцієнт ефективної кіберстійкості. Згідно з підходом NIST, система має базовий рівень захищеності (закладений архітектурно), але реальна здатність протистояти атаці у конкретний момент часу знижується пропорційно до затримок у забезпеченні та реакції.

Ефективна кіберстійкість R_{eff} обчислюється як відношення базового рівня захищеності до сумарного фактора внутрішнього опору (інертності) системи:

$$R_{eff} = \frac{R_{base}}{1+L_{org}+L_{tech}}, \text{ де:}$$

R_{base} – базовий рівень захищеності, що забезпечується впровадженими контролями безпеки (наприклад, за NIST SP 800-53), виражений у відносних одиницях від 0 до 1;

L_{org} – індекс організаційної інертності (відображає затримки в управлінських рішеннях та бюрократичних процедурах), $I\_org \geq 0$;

L_{tech} – індекс технічної інертності (відображає рівень застарілості та фізичної деградації апаратного парку, дефіцит резервного обладнання у ЗІП та часові затримки на його закупівлю й інтеграцію), $L_{tech} \geq 0$.

Запропонована математична залежність демонструє: якщо інертність мінімізована ($I\_org \rightarrow 0$, $I\_tech \rightarrow 0$), система функціонує наближено до максимуму свого спроєктованого потенціалу. Збільшення часу на закупівлю апаратного забезпечення, ігнорування процесів деградації або тривала експлуатація legacy-систем неминуче знижують фактичний рівень безпеки. Результати розрахунків за цією моделлю для різних сценаріїв наведено в табл. 1.

Таблиця 1 – Падіння ефективної кіберстійкості (R_eff) залежно від інертності

Сценарій реагування та забезпечення	R_{base}	L_{org}	L_{tech}	R_{eff}
Еталонна архітектура (відповідно до NIST)	0,95	0,05	0,10	0,826
Типовий стан для державних ОКІ (затримки закупівель ЗІП)	0,95	0,40	0,45	0,513
Критичний стан (деградований парк, відсутність резерву)	0,95	0,60	0,80	0,395

Для візуалізації впливу інертності на деградацію захисних механізмів наведено структурну схему (рис. 1).

Рисунок 1 – Деградація базового рівня безпеки під впливом факторів інертності

Висновки. Наведений поверхневий аналіз свідчить, що впровадження контролів безпеки за стандартами НД ТЗІ та NIST не забезпечує достатнього рівня захисту державних об'єктів критичної інфраструктури без паралельного вирішення проблеми високої інертності. Своєчасне оновлення апаратного парку, врахування факторів фізичної деградації обладнання, оптимізація закупівель резервних складових до ЗІП та скорочення часу реакції на інциденти є необхідними умовами для підтримання фактичної кіберстійкості об'єктів енергетичного сектору.

1. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – На заміну ДСТУ 3008–95; чинний з 2017–07–01. https://lib.zsmu.edu.ua/upload/intext/dstu_3008_2015.pdf.
2. Національний інститут стандартів і технологій США (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology.
3. Загальне керівництво ENISA щодо критичної інфраструктури: European Union Agency for Cybersecurity (ENISA). (2023). *Good Practices for Cyber Resilience in the Energy Sector*. ENISA.

Н.М. Білоус

КІБЕРСТІЙКІСТЬ ІНТЕЛЕКТУАЛЬНИХ МІКРОМЕРЕЖ З РОЗПОДІЛЕНИМИ ДЖЕРЕЛАМИ ГЕНЕРАЦІЇ

Цифровізація сучасної енергетики та впровадження концепції Smart Grid сприяли активному розвитку інтелектуальних мікромереж (Microgrid), які поєднують розподілені джерела генерації, системи накопичення енергії, комунікаційні мережі та засоби автоматизованого керування в єдину кіберфізичну систему [1]. Такі мікромережі забезпечують гнучке управління потоками електроенергії, підвищення енергоефективності та можливість автономного функціонування в острівному режимі [2].

Інтеграція технологій Інтернету речей (IoT), SCADA-систем, інтелектуальних електронних пристроїв та цифрових каналів зв'язку суттєво розширює функціональні можливості мікромереж, однак одночасно підвищує їхню вразливість до кіберзагроз [3]. Порушення роботи інформаційної або комунікаційної інфраструктури може безпосередньо впливати на фізичні процеси генерації, розподілу та споживання електроенергії, що створює ризики для стабільності функціонування енергосистеми.

Проблема забезпечення кіберстійкості енергосистем набуває особливої актуальності в умовах зростання кількості атак на критичну інфраструктуру України. У зв'язку з цим особливої актуальності набуває проблема забезпечення кіберстійкості інтелектуальних мікромереж, тобто здатності системи зберігати керованість, базову функціональність та можливість відновлення в умовах кібератак або часткової компрометації її компонентів [1]. Для вирішення цієї проблеми необхідне застосування комплексних підходів, які поєднують сучасні методи мережевого захисту, відмовостійкого керування та інтелектуального аналізу даних.

Аналіз основних кіберзагроз у мікромережах показує, що активне використання Інтернету речей (IoT) та цифрових контролерів значно розширює поверхню для кібератак. Зловмисники цілеспрямовано шукають вразливості у системах SCADA та контролерах для впровадження шкідливого програмного забезпечення, що підтверджується відомими історичними атаками вірусів Stuxnet та BlackEnergy [4].

Однією з серйозних загроз є несанкціонований доступ до систем керування. Перехоплюючи бездротові або дротові канали зв'язку, хакери можуть отримати віддалений доступ до диспетчерських центрів і польових пристроїв [3].

Особливо небезпечним вектором атак є підміна даних сенсорів та ін'єкції хибних даних. У такому випадку зловмисники модифікують телеметричні дані від сенсорів, змушуючи контролери приймати неправильні рішення. Це може призводити до порушення режимів роботи мікромережі.

Суттєву небезпеку також становлять DDoS-атаки та порушення зв'язку. Подібні атаки перевантажують комунікаційну інфраструктуру великими обсягами трафіку, унаслідок чого системи керування стають недоступними. Навіть штучно створені мілісекундні затримки передачі даних можуть призвести до втрати управління динамічними процесами у мікромережі [5].

Успішні кіберфізичні маніпуляції порушують критичний баланс між генерацією та споживанням електроенергії. Це може викликати перевантаження компонентів, фізичне пошкодження обладнання та каскадні збої, які здатні призвести до масштабних блекаутів і створити загрозу для функціонування критичної інфраструктури.

Особливості інтелектуальних мікромереж полягають у переході до концепції Smart Grid, що перетворює сучасні мікромережі на гетерогенні кіберфізичні системи. Це досягається завдяки глибокому поєднанню обчислювальних, комунікаційних та фізичних підсистем в єдину інфраструктуру. Перехід до двонаправленого обміну даними та загальна цифровізація суттєво розширили можливості моніторингу, керування та захисту таких систем.

Окрему роль відіграють технології штучного інтелекту та машинного навчання, які застосовуються для прогнозування навантажень, оптимізації режимів роботи та виявлення інцидентів. Навчання моделей машинного навчання часто відбувається у хмарних середовищах, що забезпечує масштабованість обчислювальних ресурсів і можливість проведення складної аналітики в реальному часі [1].

Методи підвищення кіберстійкості базуються на комплексному підході до захисту інтелектуальних мікромереж, який охоплює як мережеву інфраструктуру, так і алгоритмічні та організаційні рівні. Одним із ключових підходів є багаторівневий захист мережі, що передбачає проєктування безпеки з урахуванням маршрутизації, сегментації та вибору протоколів. На практиці це реалізується через поділ архітектури на зони довіри, зокрема внутрішню мережу (LAN/OT), демілітаризовану зону (DMZ/Edge) та зовнішню мережу, що дозволяє ізолювати критичні процеси від потенційних зовнішніх загроз [1].

Важливу роль у забезпеченні безпеки відіграють механізми шифрування та автентифікації. Захист взаємодії між компонентами системи досягається шляхом застосування криптографічних методів як під час передавання, так і під час зберігання даних. Додатково використовуються інфраструктура відкритих ключів (PKI), системи управління доступом та концепція «нульової довіри», яка передбачає постійну перевірку всіх учасників мережевої взаємодії [1].

Окремим класом методів є системи виявлення вторгнень (IDS/IPS), які аналізують мережевий трафік та поведінкові патерни для виявлення аномалій. Проте класичні сигнатурні підходи мають обмежену ефективність

проти нових або складних атак, зокрема поліморфних загроз, що зумовлює необхідність їх модернізації та інтеграції з більш інтелектуальними підходами.

Сучасним напрямом підвищення кіберстійкості є застосування методів штучного інтелекту та машинного навчання для виявлення аномалій. Для аналізу телеметричних даних і мережевого трафіку можуть використовуватися моделі Isolation Forest, Autoencoder та рекурентні нейронні мережі LSTM, які здатні виявляти нетипові відхилення та приховані ін'єкції хибних даних (FDI) у реальному часі. Такі підходи дозволяють динамічно оцінювати рівень довіри до сенсорних даних і прогнозувати потенційні кіберзагрози на основі поведінкових аномалій [3].

Важливим елементом є також резервування та відмовостійке керування, яке забезпечує здатність системи зберігати базову функціональність у разі відмов або кібератак. У таких ситуаціях можливе автоматичне перемикання в деградований, але безпечний режим роботи, що підтримує стабільність мікромережі та запобігає каскадним відмовам і повному блекауту. Додаткову стійкість забезпечує використання хмарної інфраструктури та edge-вузлів, які підвищують рівень резервування та розподіленості обчислень [1].

Умови стрімкої цифровізації та впровадження концепції Smart Grid зумовлюють те, що кіберстійкість стає базовою та критично важливою вимогою для функціонування сучасних мікромереж. У таких системах традиційні підходи до кібербезпеки, орієнтовані переважно на захист периметра, виявляються недостатніми, оскільки сучасні кібератаки здатні реалізовуватися всередині інфраструктури та викликати каскадні збої, аж до фізичного пошкодження обладнання та масштабних блекаутів. У зв'язку з цим ключовим стає забезпечення здатності системи зберігати керованість, стабільність і базову функціональність навіть у разі часткової компрометації її компонентів, що є одним із ключових проявів кіберстійкості.

Дослідження показують, що перехід до інтелектуальних, багаторівневих підходів до захисту суттєво підвищує надійність роботи мікромереж із розподіленою генерацією. Поєднання сегментації мережі на зони довіри, відмовостійкого керування та механізмів динамічного оцінювання сенсорних даних дозволяє ефективно локалізовувати загрози й мінімізувати вплив скомпрометованих вузлів без необхідності їх повного відключення. Такі адаптивні гібридні рішення забезпечують підтримання стабільності системи навіть в умовах суттєвих втрат або компрометації каналів спостереження та керування, а також дозволяють мікромережам ефективно функціонувати як в інтегрованому, так і в острівному режимі.

Найбільш перспективним напрямом подальшого розвитку є глибока інтеграція технологій штучного інтелекту та прогнозної аналітики в системи кіберзахисту енергомереж. Використання моделей машинного навчання для виявлення аномалій у реальному часі дає змогу ідентифікувати складні, у

тому числі поліморфні, загрози та приховані ін’єкції даних, які залишаються невидимими для класичних сигнатурних методів. Це формує основу для переходу до автономних систем кіберзахисту, здатних працювати в замкненому циклі «оцінка — адаптація — реакція», що забезпечує швидке реагування на інциденти, ізоляцію загроз та ініціацію процесів самовідновлення без участі людини.

1. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Кібербезпека: освіта, наука, техніка, 2(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956.
2. Yaghoubi, E., Yaghoubi, E., Yusupov, Z., & Maghami, M. R. (2024). A real-time and online dynamic reconfiguration against cyber-attacks to enhance security and cost-efficiency in smart power microgrids using deep learning. Technologies, 12(10), 197. https://doi.org/10.3390/technologies12100197.
3. Rouhani, S. H., Su, C.-L., Mobayen, S., Razmjooy, N., & Elsisi, M. (2024). Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions. Energy, 309, 133081. https://doi.org/10.1016/j.energy.2024.133081.
4. Шиповський, В. (2024). Model for assessment of cyber resilience of information systems of critical infrastructure objects under the influence of hybrid cyber attacks using machine learning algorithms. Ukrainian Scientific Journal of Information Security, 30(2), 235–243. https://doi.org/10.18372/2225-5036.30.19234.
5. Syrmakesis, A. D., & Hatziargyriou, N. D. (2024). Cyber resilience methods for smart grids against false data injection attacks: Categorization, review and future directions. Frontiers in Smart Grids, 3. https://doi.org/10.3389/frsgr.2024.1397380.

В. Хаустова, Н. Трушкіна

КІБЕРРЕЗИЛЬЄНТНІСТЬ ЯК НОВА ПАРАДИГМА ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЗОВНІШНІХ ЗАГРОЗ

Дану публікацію підготовлено за рахунок грантової підтримки Національного фонду досліджень України в рамках реалізації проєкту «Розбудова резильєнтних розподілених енергетичних систем територіальних громад України» (реєстраційний № 2025.07/0056), який відібрано для виконання за конкурсом «Передова наука в Україні 2026-2028».

Сучасний етап розвитку національної економіки характеризується посиленням глобальної нестабільності, активізацією гібридних загроз, прискоренням цифрової трансформації та зростанням рівня залежності критичної енергетичної інфраструктури від інформаційно-комунікаційних технологій і цифрових систем управління. У цих умовах особливої актуальності набувають питання забезпечення стійкості енергетичних систем до кібератак, техногенних ризиків, воєнних дій, інформаційних загроз та інших деструктивних впливів зовнішнього середовища [1–2].

Для України дана проблематика має стратегічне значення, оскільки в умовах повномасштабної війни суттєво зростає рівень вразливості критично важливих об’єктів енергетичної інфраструктури [3-4]. Систематичні атаки на енергетичні об’єкти, пошкодження систем електропостачання, цифрових мереж диспетчеризації та телекомунікаційних систем підтверджують необхідність формування нових підходів до забезпечення енергетичної безпеки держави. У сучасних умовах надійність функціонування енергетичної інфраструктури визначається не лише технічним станом об’єктів, але й рівнем їх цифрової захищеності, адаптивності та здатності швидко відновлюватися після кризових ситуацій.

Критична енергетична інфраструктура забезпечує безперервність функціонування електроенергетичних систем, об’єктів теплопостачання, систем передачі та розподілу електроенергії, цифрових мереж управління, систем диспетчеризації та інших життєво важливих елементів енергетичного сектору. Водночас розвиток цифрових платформ, автоматизованих систем управління, інтелектуальних енергетичних мереж та сучасних інформаційних технологій формує нові виклики, які пов’язано зі зростанням масштабів кіберризиків і цифрової вразливості критичних об’єктів [4; 5]. У зв’язку з цим традиційні підходи до захисту інфраструктури, які орієнтовано переважно на фізичну безпеку та локальне реагування на інциденти, вже не забезпечують належного рівня стійкості енергетичних систем.

У сучасному науковому середовищі дедалі більшого поширення набуває концепція кіберрезильєнтності, яка розглядається як здатність критичної

інфраструктури протистояти кіберзагрозам, адаптуватися до кризових впливів, забезпечувати безперервність функціонування та швидке відновлення після деструктивних подій. На відміну від класичних підходів до кібербезпеки, концепція кіберрезильєнтності передбачає формування комплексної адаптивної системи управління ризиками [6], що інтегрує технологічні, організаційні, інформаційні, управлінські та безпекові складові. Таким чином, кіберрезильєнтність доцільно розглядати як нову парадигму забезпечення стійкості критичної енергетичної інфраструктури в умовах зростання зовнішніх загроз і цифрової трансформації енергетики.

Проведений бібліометричний аналіз наукових публікацій міжнародної наукометричної бази Scopus за 2005-2025 рр. засвідчив суттєве зростання наукового інтересу до проблематики резильєнтності критичної інфраструктури. Загальна кількість публікацій за пошуковими запитами «резильєнтність» і «критична інфраструктура» становила 7321 наукову працю, а середньорічний темп приросту публікацій перевищував 30 %. Отримані результати свідчать про поступову трансформацію сучасного наукового дискурсу від проблем фізичного захисту інфраструктури до досліджень цифрової стійкості, кібербезпеки, адаптивності та інтелектуалізації енергетичних систем.

Результати проведеного аналізу показали, що найбільш поширеними напрямами сучасних досліджень є управління ризиками, кібербезпека, інтелектуальні енергетичні мережі, штучний інтелект, цифрова трансформація, адаптивність інфраструктурних систем, управління кризовими ситуаціями та забезпечення стійкості міських систем [7; 8 та ін.]. Це підтверджує формування нової міждисциплінарної парадигми, у межах якої кіберрезильєнтність розглядається як ключова передумова забезпечення енергетичної безпеки держави, безперервності функціонування енергетичних систем та стійкого розвитку територій.

Особливого значення в сучасних умовах набуває забезпечення кіберрезильєнтності розподілених енергетичних систем територіальних громад. Розвиток локальної генерації, альтернативної енергетики, цифрових систем моніторингу, автоматизованих платформ управління та інтелектуальних мереж потребує впровадження нових механізмів управління стійкістю енергетичної інфраструктури. Такі механізми мають забезпечувати адаптивність, резервування, автономність функціонування, оперативне реагування на кризові ситуації та мінімізацію наслідків кібератак. У зв’язку з цим доцільним є виокремлення ключових складових забезпечення кіберрезильєнтності критичної енергетичної інфраструктури (*табл.*).

Як свідчать результати проведеного дослідження, кіберрезильєнтність доцільно розглядати як інтегровану систему забезпечення стійкості критичної енергетичної інфраструктури, яка поєднує механізми цифрової безпеки, адаптивного управління, прогнозування ризиків і кризового

реагування. Її впровадження сприятиме підвищенню рівня енергетичної безпеки держави, зниженню вразливості критичних об'єктів, забезпеченню безперервності функціонування енергетичних систем та формуванню адаптивної моделі інфраструктурного розвитку.

Таблиця 1 – Основні складові забезпечення кіберрезильєнтності критичної енергетичної інфраструктури

Складова	**Характеристика**	**Очікуваний результат**
Цифрова безпека	Захист інформаційних систем, цифрових платформ і каналів передачі даних	Зниження рівня кіберзагроз і цифрової вразливості
Адаптивність систем	Здатність до швидкого реагування на кризові впливи та зміни зовнішнього середовища	Підвищення стійкості функціонування енергетичних систем
Резервування ресурсів	Наявність альтернативних джерел енергозабезпечення та резервних каналів зв'язку	Забезпечення безперервності функціонування інфраструктури
Інтелектуальні системи управління	Використання цифрових технологій, автоматизації, аналітики даних і штучного інтелекту	Підвищення ефективності управління енергетичними системами
Управління ризиками	Ідентифікація, оцінювання та мінімізація ризиків і загроз	Зменшення рівня вразливості критичної інфраструктури
Кризове відновлення	Формування механізмів швидкого відновлення функціонування систем після кібератак і кризових ситуацій	Скорочення часу ліквідації наслідків криз

Джерело: складено авторами на основі [3-6].

Отже, в умовах цифрової трансформації економіки, зростання масштабів кіберзагроз та посилення зовнішніх безпекових викликів особливого значення набуває розроблення комплексних організаційно-економічних і технологічних механізмів забезпечення кіберрезильєнтності критичної енергетичної інфраструктури України.

Перспективи подальших досліджень полягають в обґрунтуванні методичних підходів до оцінювання рівня кіберрезильєнтності енергетичних систем і розробленні механізмів забезпечення стійкості розподілених енергетичних систем територіальних громад.

1. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance). *Official Journal of the European Union*. 2022. Dec. 27. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.
2. Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023 supplementing Directive (EU) 2022/2557 of the European Parliament and of the Council by establishing a list of essential services. *Official Journal of the European Union*. 2023. Oct. 30 (2023). URL: http://data.europa.eu/eli/reg_del/2023/2450/oj.
3. Хаустова В. Є., Трушкіна Н. В. Загрози розвитку критичної інфраструктури: сутність і класифікація. *Проблеми економіки*. 2025. № 3. С. 89-104. DOI: https://doi.org/10.32983/2222-0712-2025-3-89-104.
4. Kwilinski A., Trushkina N. Impact of Cyber Risks and Threats on the Critical Infrastructure Development: Visualization of Scientific Research. *Proceedings of the 12th International Conference on Applied Innovation in IT*. 2024. Vol. 12(2). P. 107–119. http://dx.doi.org/10.25673/118123.
5. Zaporozhets A., Khaustova V., Hubarieva I., Trushkina N. Digitization as a Modern Challenge for the Energy Systems' Transformation in the World. *Systems, Decision and Control in Energy VII. Studies in Systems, Decision and Control*. Berlin: Springer Science and Business Media Deutschland GmbH, 2025. Vol. 596. P. 3-31. DOI: https://doi.org/10.1007/978-3-031-90462-2_1.
6. Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Комплексний підхід до управління ризиками розвитку критичної інфраструктури регіонів в Україні в умовах зовнішніх загроз. *Інфраструктура ринку*. 2026. Вип. 88. С. 70-78. DOI: https://doi.org/10.32782/infrastruct88-11.
7. Aldrich D., Meyer M. Social Capital and Community Resilience. *American Behavioral Scientist*. 2015. Vol. 59. No. 2. P. 254-269. DOI: https://doi.org/10.1177/0002764214550299.
8. Ouyang M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliability Engineering and System Safety*. 2014. Vol. 121. P. 43–60. URL: https://doi.org/10.1016/j.ress.2013.06.040.

О.А. Добринчук, В.В. Лукашенко

ОГЛЯД СУЧАСНИХ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ

Вступ. У сучасних умовах цифрової трансформації енергетичний сектор зазнає суттєвих змін, пов'язаних із впровадженням smart grid, Industrial Internet of Things (IIoT), SCADA/ICS систем, хмарних платформ та технологій дистанційного управління. Водночас інтеграція інформаційних і операційних технологій (IT/OT convergence) значно розширює поверхню атаки та підвищує складність забезпечення кібербезпеки критичної інфраструктури. Особливої актуальності ця проблема набуває в умовах гібридних загроз, цілеспрямованих кібератак на енергетичні об'єкти та появи нових викликів, пов'язаних із застосуванням штучного інтелекту й перспективою квантових обчислень. У зв'язку з цим зростає потреба у розробленні комплексних підходів до забезпечення кіберстійкості енергетичних систем, які поєднують сучасні стандарти безпеки, механізми моніторингу, управління ризиками та перспективні криптографічні засоби захисту.

Основна частина дослідження. У сучасному цифровому середовищі захист критичної інфраструктури від кібератак став одним із головних пріоритетів національної безпеки, особливо в енергетичному секторі. У міру поширення цифровізації та розвитку гібридної війни енергетична інфраструктура дедалі частіше стає мішенню кіберзагроз, здатних порушити функціонування життєво важливих служб та дестабілізувати діяльність держави. Отже, забезпечення безпеки та стійкості енергетичних систем вимагає ефективних стратегій кібербезпеки та чіткого розуміння обмежень існуючих механізмів захисту. У цій статті представлено комплексний огляд літератури щодо підходів до кібербезпеки, що використовуються для захисту критичної енергетичної інфраструктури та систем «розумних» енергомереж від кібератак. У дослідженні [1] розглядаються загальноприйняті стратегії захисту, інтеграція технологій кібербезпеки в енергетичні системи та операційні виклики, пов'язані з їх впровадженням. Також аналізуються слабкі сторони та обмеження сучасних підходів до захисту, приділяючи особливу увагу таким питанням, як складність систем, еволюція методів атак та обмеження існуючих механізмів захисту. Загалом у статті підкреслюється, що розуміння недоліків сучасних засобів захисту кібербезпеки є необхідним для вдосконалення стратегій захисту, зміцнення стійкості енергетичної інфраструктури та підвищення національної безпеки в контексті сучасних цифрових та гібридних загроз.

Поява квантових комп'ютерів, здатних розшифровувати шифри (CRQC), становить серйозну загрозу для безпеки та криміналістичної цілісності систем промислового управління (ICS) та операційних технологій (OT) у

критичній інфраструктурі, зокрема на атомних електростанціях. Квантові атаки, включаючи кампанії «Збирай зараз, розшифровуй пізніше» (HNDL) з використанням таких алгоритмів, як алгоритм Шора, можуть порушити існуючі криптографічні засоби захисту, підірвати цифрові докази та сприяти складним саботажам. У статті [2] представлено криміналістично-орієнтовану структуру для досягнення квантової стійкості в середовищах з високими наслідками. У ній аналізуються квантові загрози в архітектурі Purdue та демонструється, як зловмисники можуть використовувати тривалі життєві цикли ОТ та криптографічні монокультури для атак на системи безпеки та створення криміналістичних викликів. Для зменшення цих ризиків у дослідженні пропонується поетапна стратегія переходу до постквантової криптографії (PQC), що включає гібридний обмін ключами, криптографічну різноманітність, безпечну синхронізацію часу та реалізації, стійкі до бокових каналів, що відповідають стандартам ISA/IEC 62443 та NIST. Загалом, у статті наголошується на нагальній потребі у засобах кібербезпеки, стійких до квантових загроз, для захисту операцій критичної інфраструктури та збереження цілісності цифрових криміналістичних доказів у майбутніх сценаріях квантових загроз.

Промислові системи управління (ICS), що забезпечують функціонування критичної інфраструктури, потребують структурованої оцінки ризиків у сфері кібербезпеки для встановлення надійних та обґрунтованих вимог безпеки для середовищ промислової автоматизації. З огляду на останні досягнення у сфері великих мовних моделей (LLM) зростає інтерес до того, чи можуть ці системи сприяти процесам оцінки ризиків на ранніх етапах відповідно до стандарту IEC 62443-3-2, а також до того, як результати їхньої роботи відрізняються залежно від моделі. У цій статті [3] представлено якісне порівняння «ШІ проти ШІ» артефактів оцінки ризиків за стандартом IEC 62443, згенерованих у контрольованих умовах однопрохідного проходження з використанням спільної моделі системи та стандартизованої структури завдань на основі стандарту IEC 62443-3-2. У дослідженні порівнюються результати моделей у трьох вимірах: еволюція моделей у межах одного сімейства LLM, порівняння передових моделей різних постачальників та порівняння моделей преміум-рівня з базовими передовими моделями. Оцінка зосереджується на структурі оцінки, архітектурній узгодженості та внутрішній узгодженості з принципами стандарту IEC 62443, а не на порівнянні із зовнішніми еталонними даними. Результати показують значні відмінності в тому, як моделі структурують сценарії загроз, визначають деталізацію зонування, призначають цільові рівні безпеки (SL-T) та враховують операційні припущення. Ці висновки висвітлюють як можливості, так і обмеження використання великих мовних моделей (LLM) як інструментів підтримки прийняття рішень на початкових етапах оцінки ризиків кібербезпеки об’єктів критичної інфраструктури.

Дослідження свідчить про те, що, хоча великі мовні моделі можуть сприяти структурованому аналізу та прискорювати процес документації, специфічні особливості моделей можуть впливати на якість та послідовність оцінки, що підкреслює незмінну важливість експертного нагляду у процесі планування безпеки об'єктів критичної інфраструктури.

У міру все більшої цифровізації промислових систем конвергенція інформаційних технологій (IT) та операційних технологій (OT) породила нові виклики у сфері кібербезпеки. Хоча IT-системи користуються перевагами відпрацьованих методів забезпечення безпеки, середовища OT, що керують критичною інфраструктурою, такою, як енергетичні, виробничі та транспортні системи, часто залишаються вразливими до кіберзагроз. Оскільки порушення роботи OT можуть спричинити операційні ризики та ризики для безпеки, забезпечення захисту цих систем стало головним пріоритетом. У цій статті [4] представлено стратегічний план дій для організацій, які розпочинають свою діяльність у сфері кібербезпеки OT. Починаючи з мінімального рівня безпеки, у ній окреслено впровадження стандарту ISO/IEC 27001 як основу для управління інформаційною безпекою. Далі у статті описано перехід до стандарту ISA/IEC 62443 – системи стандартів, спеціально розробленої для систем промислової автоматизації та управління. Цей перехід передбачає впровадження заходів захисту, специфічних для OT, таких як управління ризиками, сегментація мережі, зони безпеки та стратегії глибокого захисту. Крім того, у статті підкреслюється важливість постійного моніторингу, виявлення загроз, реагування на інциденти та навчання персоналу для забезпечення як безперебійності роботи, так і стійкості кібербезпеки. Загалом, дослідження надає практичні рекомендації та найкращі практики для організацій, які прагнуть забезпечити безпеку середовищ OT та захистити критичну інфраструктуру від постійно мінливих кіберзагроз.

Директива NIS2 встановлює більш суворі вимоги щодо кібербезпеки та повідомлення про інциденти для критично важливих суб'єктів, зокрема операторів енергетичного сектору. Однак багато організацій стикаються з труднощами у перетворенні цих юридичних зобов'язань на ефективні щоденні заходи безпеки, особливо в середовищах операційних технологій (OT), де можливості візуалізації та скоординованого реагування часто є обмеженими. У цій статті [5] розглядається, як SecureAI – інструмент виявлення та збагачення аномалій на основі штучного інтелекту в екосистемі розвідки кіберзагроз (CTI) – може сприяти дотриманню ключових вимог NIS2. Дослідження поєднує якісний кабінетний аналіз, порівняльне зіставлення функцій SecureAI зі статтями 20–26 NIS2 та сценарій, орієнтований на OT, на основі останніх моделей вторгнень. Аналіз показує, що SecureAI може виявляти аномальну активність у телеметрії мережі та хостів, збагачувати сповіщення контекстуальною інформацією про активи та

події, а також генерувати структуровані результати для підтримки прийняття рішень операторами. Інтегровані з інфраструктурою CTI, ці сповіщення можуть бути перетворені на об'єкти STIX/TAXII для звітності, документації та обміну інформацією. Модельований сценарій вторгнення, що включає несанкціонований віддалений доступ та підозрілу активність HMI-PLC, демонструє, як система підтримує виявлення аномалій, аналіз інцидентів та робочі процеси звітності. Загалом, це дослідження підкреслює потенціал інструментів CTI на основі штучного інтелекту для посилення заходів з кібербезпеки в сфері операційних технологій, а також сприяння практичній реалізації вимог щодо відповідності NIS2.

У статті [6] представлено порівняльний аналіз стандартів «Захисту критичної інфраструктури» Північноамериканської корпорації з надійності електропостачання (NERC-CIP) та концепції кібербезпеки Національного інституту стандартів і технологій (NIST). У дослідженні розглядаються їхні сильні та слабкі сторони, а також проблеми, пов'язані з впровадженням цих стандартів у сфері захисту систем критичної інфраструктури. Хоча NERC-CIP встановлює обов'язкові вимоги до кібербезпеки для магістральних електромереж, система NIST пропонує гнучкий та добровільний підхід до більш широкого управління ризиками кібербезпеки. У статті підкреслюється, як ці дві системи можуть доповнювати одна одну для підтримки розвитку стійкої та безпечної інфраструктури. У ній пропонується комплексна стратегія кібербезпеки, що поєднує визначення пріоритетів на основі ризиків, принципи глибокої оборони, постійний моніторинг та міжорганізаційну співпрацю. Крім того, у дослідженні наголошується, що лише дотримання нормативних вимог є недостатнім для протидії мінливим кіберзагрозам. Тому рекомендується впроваджувати передові методи виявлення загроз, архітектуру «нульової довіри» та навчання з питань кібербезпеки для подальшого зміцнення рівня безпеки організацій, що відповідають за критичну інфраструктуру. Загалом у статті показано, що поєднання структурованого підходу до дотримання вимог NERC-CIP з гнучким підходом до управління ризиками NIST може забезпечити більш ефективну та комплексну систему кібербезпеки для захисту критичної інфраструктури.

У дослідженні [7] розглядається дедалі актуальніша проблема забезпечення безпеки комунікацій SCADA, що передаються через оптоволоконні мережі з використанням оптичного заземлюючого проводу (OPGW) та повністю діелектричних самонесучих кабелів (ADSS) у рамках великих електроенергетичних систем США. Хоча оптоволоконні канали зв'язку забезпечують високу технічну ефективність, вони залишаються вразливими до кіберзагроз, фізичних та експлуатаційних загроз, які можуть вплинути на прозорість системи, цілісність команд та загальну стійкість. У дослідженні пропонується та емпірично оцінюється інженерна структура, що відповідає вимогам NERC CIP, призначена для підвищення безпеки та

стійкості комунікацій SCADA. У дослідженні розглядається вплив інженерних засобів безпеки, захисту каналів зв'язку, заходів контролю доступу, можливостей моніторингу та виявлення, а також відповідності стандартам NERC CIP на захист середовищ SCADA. Використовуючи кількісний поперечний дизайн, було зібрано дані від 220 фахівців, які працюють у сферах експлуатації комунальних мереж, кібербезпеки, інженерії SCADA та забезпечення відповідності вимогам. Статистичний аналіз продемонстрував високу надійність та значущі позитивні взаємозв'язки між усіма дослідженими факторами безпеки та стійкістю комунікацій SCADA. Серед оцінених змінних здатність до моніторингу та виявлення виявилася найсильнішим предиктором ефективності безпеки. Результати також показали, що середовища ADSS сприймаються як більш вразливі, ніж середовища OPGW, що підкреслює необхідність стратегій захисту, специфічних для конкретних засобів комунікації. Загалом, у дослідженні наголошується на важливості поєднання технічних засобів контролю, постійного моніторингу, управління доступом та дотримання нормативних вимог для підвищення стійкості критично важливих систем зв'язку комунальних підприємств та покращення захисту кібербезпеки в сучасних інфраструктурах SCADA.

Висновки. Проведений аналіз сучасних підходів до забезпечення кібербезпеки енергетичної критичної інфраструктури показав, що в умовах цифровізації та конвергенції IT/OT систем питання захисту енергетичних мереж, SCADA/ICS середовищ і smart grid набувають критичного значення для національної безпеки та стійкості держави. Дослідження засвідчили, що сучасні підходи до кіберзахисту базуються на поєднанні міжнародних стандартів (ISO/IEC 27001, ISA/IEC 62443, NIST, NERC CIP), механізмів моніторингу, оцінювання ризиків, сегментації мереж, концепції Zero Trust та засобів виявлення аномалій на основі штучного інтелекту. Водночас встановлено, що існуючі механізми захисту мають низку обмежень, пов'язаних зі складністю промислових систем, еволюцією кіберзагроз, недостатньою адаптацією до OT-середовищ, а також перспективними викликами, зумовленими розвитком квантових обчислень.

Окрему увагу приділено проблемам забезпечення криптографічної стійкості та необхідності переходу до post-quantum cryptography для захисту критичної інфраструктури від майбутніх квантових атак. Аналіз досліджень показав, що перспективними напрямами є інтеграція AI-driven cybersecurity, continuous monitoring, CTI-платформ, risk-oriented security frameworks та квантово-стійких криптографічних механізмів у системи управління критичною інфраструктурою. Отримані результати підтверджують необхідність комплексного підходу до забезпечення кіберстійкості енергетичних систем із поєднанням організаційних, технічних і криптографічних заходів захисту.

Перспективи подальших досліджень полягають у розробленні інтелектуальних методів виявлення кіберзагроз для SCADA/ICS середовищ на основі штучного інтелекту та машинного навчання, створенні адаптивних моделей оцінювання ризиків для критичної інфраструктури, а також у впровадженні квантово-стійких криптографічних механізмів у системи енергетичного сектору. Важливим напрямом є дослідження безпеки 5G/6G-орієнтованих енергетичних систем, захисту distributed energy resources та secure-by-design архітектур для smart grid. Крім того, актуальними залишаються питання інтеграції технологій кіберрозвідки (CTI), Zero Trust, Digital Twins і AI-driven monitoring у системи забезпечення кіберстійкості критичної інфраструктури в умовах сучасних гібридних загроз.

1. Kreso Phd, Inda. (2025). CYBERSECURITY IN THE ENERGY SECTOR: AN OVERVIEW OF DEFENSE STRATEGIES AND BEST PRACTICES. 130-148.
2. Baseri, Yaser & Waller, Edward. (2026). Quantum Attacks Targeting Nuclear Power Plants: Threat Analysis, Defense and Mitigation Strategies. 10.48550/arXiv.2602.21524.
3. Bernard, Andreas & Pfister, Mathias. (2026). AI-Driven Risk Assessment for Critical Infrastructure Based on IEC 62443 Using Large Language Models. 10.21203/rs.3.rs-9050939/v1.
4. Heinl, Michael & Pursche, Maximilian & Puch, Nikolai & Peters, Sebastian & Giehl, Alexander. (2023). From Standard to Practice: Towards ISA/IEC 62443-Conform Public Key Infrastructures. 10.1007/978-3-031-40923-3_15.
5. Siivola, Jani & Paronen, Rami & Tariq, Uzair & Pham, Quyet & Villegas, Warren & Tikanmäki, Ilkka & Rajamäki, Jyri. (2026). Exploring NIS2 Compliance in the Energy Sector Using AI-Driven Cyber Threat Intelligence. International Conference on Cyber Warfare and Security. 21. 714-717. 10.34190/iccws.21.1.4482.
6. Chatterjee, Suchismita. (2021). A Comparative Study between NERC-CIP and NIST Compliance-Defining the Critical Framework for Building Cyberrisk Free Infrastructure. ESP Journal of Engineering & Technology Advancements. 1. 273-281. 10.56472/25832646/JETA-V1I1P129.
7. Mosharraf, Abu. (2026). Securing SCADA Communications Over OPGW And ADSS Fiber In U.S. Bulk Electric Systems: A NERC CIP-Aligned Engineering Framework. American Journal of Advanced Technology and Engineering Solutions. 06. 416-459. 10.63125/hn42nw39.

Ю.М. Здоренко, М.О. Толочин

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ УПРАВЛІННЯ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ ХМАРНИХ ІНФРАСТРУКТУР ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Інформаційні системи об'єктів критичної інфраструктури, зокрема об'єктів енергетики, дедалі активніше ґрунтуються на використанні хмарних технологій для забезпечення виконання задач обробки даних, моніторингу та централізованого управління. Використання хмарних платформ забезпечує масштабованість, гнучкість та можливість швидкого розгортання інформаційних систем, однак одночасно створює нові виклики у сфері інформаційної безпеки та стійкості функціонування такої інфраструктури.

Особливої актуальності ці аспекти набувають в умовах нестабільного та динамічного навантаження на хмарні сервіси. Для об'єктів критичної інфраструктури навіть короткочасне перевантаження серверів або тимчасове зниження продуктивності можуть призводити до порушення роботи інформаційних систем, втрати доступності сервісів та в кінцевому результаті зниження рівня кіберстійкості [1]. У сучасних умовах значна частина державних цифрових сервісів України вже функціонує у хмарних середовищах, що додатково підкреслює необхідність забезпечення надійного та адаптивного управління обчислювальними ресурсами.

Традиційні методи розподілу ресурсів у хмарних інфраструктурах здебільшого базуються на використанні простих статистичних моделей з фіксованими пороговими значеннями. Такі підходи недостатньо ефективні у випадках різких змін навантаження, пікової активності та неповноти інформації про майбутній стан завантаженості системи. Крім того, статичні моделі не дозволяють враховувати складні взаємозв'язки між параметрами навантаження, мережевою активністю та станом окремих компонентів інфраструктури [2].

У зв'язку з цим перспективним напрямом досліджень є застосування інтелектуальних методів аналізу та прогнозування навантаження, здатних забезпечувати адаптацію до змін умов функціонування хмарної інфраструктури. Одним із таких підходів є використання моделей на основі нечіткої логіки, що дозволяє формалізувати експертні знання та приймати рішення в умовах невизначеності й неповноти даних. На відміну від традиційних методів, що базуються на жорстких порогових значеннях, нечіткі системи забезпечують більш гнучкий підхід до оцінювання стану обчислювальних ресурсів та дозволяють враховувати складний характер взаємодії між параметрами системи.

Нечіткі системи можуть одночасно враховувати множину параметрів функціонування інфраструктури, зокрема рівень використання CPU, оперативної пам'яті, мережевого трафіку, інтенсивність запитів, затримки передачі даних та швидкість зміни навантаження у часі. На основі множини нечітких правил система здатна оцінювати поточний стан інфраструктури та формувати рекомендації щодо перерозподілу ресурсів. Це особливо важливо для хмарних платформ, що забезпечують функціонування сервісів об'єктів критичної інфраструктури, де навіть короткочасне перевантаження може призвести до зниження показників доступності або повного порушення безперервності процесів.

Крім того, використання нечіткої логіки створює передумови для побудови адаптивних систем управління ресурсами, які можуть автоматично змінювати параметри функціонування відповідно до поточного стану елементів інфраструктури. Такий підхід дозволяє підвищити ефективність використання обчислювальних потужностей, зменшити енергоспоживання дата-центрів та забезпечити більш стабільну роботу хмарних сервісів в умовах нерівномірного навантаження. Додаткові можливості забезпечують нейро-нечіткі системи, зокрема моделі типу ANFIS (Adaptive Neuro-Fuzzy Inference System), які поєднують механізми нечіткої логіки та нейронних мереж [3]. Такі системи здатні автоматично адаптувати параметри моделі на основі аналізу попередніх даних та змін характеру навантаження. Це дозволяє підвищити точність прогнозування короткострокових сплесків навантаження та забезпечити більш ефективне управління обчислювальними ресурсами [4].

Одже, використання інтелектуальних методів прогнозування у хмарних інфраструктурах об'єктів критичної інфраструктури може забезпечити: своєчасне масштабування ресурсів; зменшення ризику перевантаження серверів; підвищення доступності сервісів; оптимізацію використання обчислювальних потужностей; підвищення стійкості інформаційних систем до кібератак [3].

Крім того, такі підходи можуть використовуватись як додатковий елемент забезпечення кіберстійкості хмарних інфраструктур. Аналіз аномальної поведінки навантаження дозволяє виявляти потенційні ознаки DDoS-атак, несанкціонованої активності тощо, що можуть впливати на стабільність функціонування інформаційних сервісів [5]. Зокрема, різкі короткочасні стрибки навантаження зафіксовані у мережевій підсистемі, системі зберігання даних тощо, можуть свідчити про спроби перевантаження серверів чи виконання зловмисних автоматизованих операцій. Використання методів нечіткої логіки дозволяє не лише фіксувати факт перевищення певних порогових значень, але й прогнозувати динаміку змін навантаження, враховуючи невизначеність та випадковий характер параметрів розподілених систем [4]. Це створює передумови для побудови адаптивних систем

моніторингу та реагування, здатних превентивно спрацьовувати у випадках потенційних загроз, автоматично перерозподіляти ресурси та підтримувати безперервність функціонування цифрових сервісів.

Таким чином, застосування методів нечіткої логіки та моделей прогнозування у системах управління хмарними інфраструктурами є перспективним напрямом підвищення ефективності, безпеки та кіберстійкості інформаційних систем об'єктів критичної інфраструктури в сучасних умовах.

1. Amahrouch, A., Saadi, Y., & El Kafhali, S. (2025). Optimizing energy efficiency in cloud data centers: A reinforcement learning-based virtual machine placement strategy. Network, 5(1), 1–18. https://doi.org/10.3390/network5010001.
2. Islam, S., Keung, J., Lee, K., & Liu, A. (2012). Empirical prediction models for adaptive resource provisioning in the cloud. Future Generation Computer Systems, 28(1), 155–162. https://doi.org/10.1016/j.future.2012.05.027.
3. Gill, S. S., & Buyya, R. (2021). Resource management in cloud computing: State of the art and future directions. Future Generation Computer Systems, 114, 97–120. https://doi.org/10.1016/j.future.2020.09.020.
4. Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., Tuli, S., Smirnova, D., Singh, M., Jain, U., Puthal, D., & Buyya, R. (2023). Transformative effects of artificial intelligence on cloud resource management. Future Generation Computer Systems, 140, 92–103. https://doi.org/10.1016/j.future.2022.10.015.
5. Mell, P., & Grance, T. (2020). The NIST definition of cloud computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145.

С.Ф. Гончар

КОМПЛЕКСНИЙ ПІДХІД ДО КІБЕРЗАХИСТУ ОБ'ЄКТІВ РОЗПОДІЛЕНОЇ ГЕНЕРАЦІЇ НА ОСНОВІ МОДЕЛЕЙ ZERO TRUST ТА ШТУЧНОГО ІНТЕЛЕКТУ

Сучасний стан енергосистеми України характеризується стратегічним курсом на децентралізацію. Станом на березень 2026 року в експлуатацію введено 465 одиниць обладнання розподіленої генерації загальною потужністю 651,5 МВт [1]. Попри підвищення фізичної стійкості, перехід до мікромереж та пристроїв Інтернету речей (IoT) кардинально розширює поверхню кібератак [2]. Традиційні периметрові моделі захисту SCADA-систем виявляються неефективними в умовах гетерогенного середовища [3]. Кожен новий вузол стає потенційною точкою входу для інжекції неправдивих даних (FDI) або DDoS-атак, що створює ризики для стабільності всієї енергосистеми.

Метою дослідження є визначення технологічних вразливостей децентралізованих енергосистем та обґрунтування комплексного підходу до їх захисту за допомогою архітектури Zero Trust, штучного інтелекту та блокчейн-технологій.

Трансформація архітектури безпеки супроводжується трьома критичними викликами: логічною децентралізацією точок входу, двонаправленістю інформаційних потоків та технологічною гетерогенністю обладнання. Для нейтралізації цих загроз запропоновано комплексну систему захисту:

- архітектура нульової довіри (Zero Trust Architecture) – базується на повній відсутності апріорної довіри до будь-якого вузла, мікросегментації мережі та безперервному аналізі контексту запитів. Алгоритм динамічної верифікації суб'єктів доступу представлено на рис. 1. Будь-який активний суб'єкт (пристрій або користувач) надсилає запит до Центру прийняття рішень (PDP). PDP, використовуючи ШІ, проводить автентифікацію та оцінку ризиків. У випадку успішної перевірки об'єкту надається тимчасовий доступ, інакше – запит відхиляється та фіксується системою SIEM;

- інтелектуальний кібер-фізичний моніторинг – використання штучного інтелекту (ШІ) для поведінкового аналізу забезпечує виявлення аномалій на ранніх стадіях із точністю до 96,5% [4]. Концептуальна модель кросдоменного моніторингу стану мікромережі зображена на рис. 2. Система паралельно здійснює цифровий моніторинг (аналіз мережевих логів і трафіку) та фізичний моніторинг (збір телеметрії: напруги, частоти, температури тощо). Центр кореляції проводить інтелектуальний аналіз відповідності дій цифрових команд реальним законам фізики, що дозволяє

виявляти приховані FDI-атаки та передавати рішення про стан безпеки до кінцевої системи SIEM;

- блокчейн-технології – інтеграція розподілених реєстрів забезпечує незмінність логів і команд керування, реалізує децентралізовану ідентифікацію пристроїв та автоматизує ізоляцію скомпрометованих вузлів через смарт-контракти.

Рисунок 1 – Алгоритм динамічної верифікації суб’єктів доступу в архітектурі Zero Trust для мікромереж

Для масштабування безпеки критично важливим є державне регулювання та уніфікація вимог НКРЕКП і стандартів [5]. Основними напрямами вдосконалення державної політики у цій сфері можуть бути:

- адаптація міжнародних стандартів: необхідним є впровадження в українське законодавство вимог, аналогічних стандартам NERC CIP. Ці стандарти чітко регламентують ідентифікацію критичних активів, контроль доступу та плани реагування на кіберінциденти;

- розробка галузевих вимог НКРЕКП**:** НКРЕКП має встановити обов'язкові технічні вимоги до кіберзахисту обладнання, що підключається до загальної мережі. Це стосується обов'язкового шифрування каналів зв'язку та підтримки протоколів безпечної автентифікації на рівні інверторів та SCADA-систем;

- створення єдиного координаційного центру: враховуючи гетерогенність систем, держава має забезпечити централізований моніторинг загроз та обмін інформацією про інциденти між власниками розподіленої генерації. Це дозволить масштабувати досвід відбиття атак з одного об'єкта на всю енергосистему в режимі реального часу;

- аудит та сертифікація: впровадження обов’язкового періодичного аудиту кібербезпеки для об’єктів розподіленої генерації потужністю понад певний поріг, що гарантуватиме дотримання встановлених стандартів протягом усього життєвого циклу обладнання.

Системне державне регулювання дозволить створити умови, за яких децентралізація енергетики посилюватиме національну безпеку

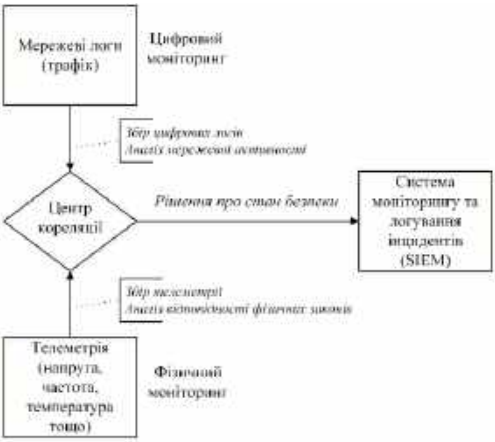


Рисунок 2 – Концептуальна модель крос-доменного моніторингу стану мікромережі

Таким чином, масштабування розподіленої генерації вимагає відмови від статичного захисту на користь динамічної екосистемної безпеки. Синтез моделі Zero Trust, алгоритмів ШІ та крос-доменного моніторингу дозволяє забезпечити цифрову стійкість критичної інфраструктури України навіть за умов компрометації окремих сегментів мережі.

1. Кулеба О. Комплексні плани стійкості регіонів та міст розроблені на основі реального досвіду цієї зими. Урядовий портал. 03.03.2026. URL: https://www.kmu.gov.ua/news/kompleksni-plany-stiikosti-rehioniv-ta-mist-rozrobleni-na-osnovi-realnoho-dosvidu-tsiiei-zymy-oleksii-kuleba?=print (дата звернення: 04.03.2026).
2. Decentralized energy security: Cybersecurity challenges and opportunities in distributed renewable energy / B. Pedro та ін. World Journal of Advanced Research and Reviews. 2025. С. 1256–1272.
3. Szczepaniuk, E.K.; Szczepaniuk, H. Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures. Energies 2025, 18, 5017.
4. Alshammari, A. Securing smart microgrids with a novel multi-layer cybersecurity framework for Industry 4.0 renewable energy systems. Discov Computing 28, 2025.
5. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання», Київ, 2014. – С. 92-95.

В.С. Волошин, О.В. Кленін

КІБЕРЗАХИСТ ДЕЦЕНТРАЛІЗОВАНОЇ ЕНЕРГЕТИКИ УКРАЇНИ: РОЛЬ І МОЖЛИВОСТІ *AI* У РОБОТІ РОЗПОДІЛЕНИХ ЕНЕРГОСИСТЕМ

Сучасна енергетика України на тлі бойових атак агресора на протязі чотирьох років зазнала суттєвих деформацій, які важко відновити і ще важче захистити у дійсному часі. Тому перехід від централізованої моделі до децентралізованої системи енергозабезпечення стає обґрунтованим, принаймні для декількох регіонів країни, які зазнали системних уражень. Якщо традиційна енергосистема базувалася на великих електростанціях і централізованому управлінні, то нова архітектура повинна включати мікромережі, розподілену генерацію (DER — Distributed Energy Resources), домашні сонячні електростанції, автономні системи накопичення енергії, інтелектуальні енергосистеми (smart grid), об'ємні IoT-пристрої та пірингові (peer-to-peer) енергетичні мережі [1, 2]. Така модель підвищує енергетичну стійкість держави у воєнний час, але одночасно різко збільшує небезпеку кібератак. Кожен smart meter, інвертор, контролер чи *IoT*-пристрій стає потенційною точкою проникнення для атакувальника. Саме тому система *AI* сьогодні розглядається не лише як інструмент автоматизації енергетики, а як ключовий елемент кіберзахисту децентралізованих енергосистем.

Треба визначитися з тим, що традиційна кібербезпека, яка будувалася як кіберзахист статичних мереж, централізованих архітектур з обмеженою кількістю вузлів, вже недостатня для активного захисту енергомереж держави.

В супротив, децентралізована енергетика може мати безліч *IoT*-вузлів з динамічною топологією та у реальному часі управління, високий рівень автономності. Людина фізично не здатна аналізувати такий потік подій у режимі реального часу. Це причина тому, що системи штучного інтелекту (*AI*) стають критично необхідними [3].

Децентралізована енергетика в такому сенсі — це система, у якій виробництво, зберігання та розподіл електроенергії відбувається через множину локальних вузлів, а не через один централізований центр. До таких систем належать: розумні мережі (*smart grid*), мікромережі типу microgrids, *DER*-системи, інтелектуальні інвертори, розподілені сховища та локальні мережі споживачів. У сучасній розподіленій моделі енергоспоживач одночасно може бути виробником енергії (prosumer). Це принципово змінює архітектуру управління мережею і збільшує її резистентність до ворожого враження.

Ми розглянемо найбільш типові кіберзагрози, притаманні децентралізованій енергетиці, які можна класифікувати наступним чином.

1.Атаки на *SCADA* (*Supervisory Control and Data Acquisition*) та *OT*-системи (*Operational Technology systems*). *SCADA*-диспетчери керують розподільчими підстанціями, мікромережами, локальними інверторами, підтримують балансування навантаження. У децентралізованій системі кількість *SCADA*-вузлів різко зростає, що збільшує кількість вразливостей.

2.Типові атаки на *SCADA*-systems включають стандартні False Data Injection Attack (*FDIA*), Spoofing, command injection, ransomware, *DDoS* - (*Distributed Denial of Service*) — «розподілена атака зі відмовою в обслуговуванні», кібератака, під час якої велика кількість пристроїв одночасно перевантажує сервер або мережу запитами, роблячи сервіс недоступним для користувачів.

3.Smart grid базується на масовому використанні *IoT*. Вразливості *IoT* у smart grid, може служити причиною виходу з використання розподілених енергетичних мереж. Це сенсори, розумні лічильники, периферійні пристрої та ін. обладнання та програмне забезпечення. Такі *IoT*-пристрої, як правило, мають слабку автентифікацію, частіші застаріли прошивки, відрізняються відсутністю шифрування або дефіцитом обчислювальних ресурсів для повноцінного захисту.

4.Потенційні атаки на distributed energy resources (*DER*) спрямовуються на сонячні станції, вітрові установки, батарейні системи, *EV* charging systems. Вихід зі строю систем *DER* може спричинити дестабілізацію несучої частоти, потенційне перевантаження мереж, каскадні відключення і локальні блекаути.

Тим не менш, роль *AI* у кіберзахисті децентралізованої енергетики має максимально зростати [1]. Machine Learning дозволяє виявляти аномалії захисту, оперативно аналізувати поведінку мережі за необмеженою кількістю параметрів, що недоступно для людини, виявляти нетипові патерни і прогнозувати бойові та кібернетичні атаки, автоматично реагувати на інциденти. *AI*-системи можуть навчатися на трафіку SCADA, поведінці DER, телеметрії smart grid та історичних атакових паралелях. Головні відмінності систем децентралізованої енергетики з використанням штучного інтелекту мають певні особливості, які притаманні нейронним мережам та системам з лінгвістичною екстраполяцією. А саме.

1. *AI*-powered intrusion detection systems (*AI IDS*) здатні заздалегідь виявляти zero-day атаки, аналізувати поведінкові відхилення, здійснювати профілактичні кореляції, працюючи у режимі реального часу. Дослідження 2025–2026 років показують, що системи з глибоким навчанням (hybrid deep learning) досягають точності понад 98% у виявленні *DDoS* та *FDIA*-атак у відмовах в обслуговуванні, перевантаженні обладнання, фальш-атаках та ін.

2. Системи (AI) дозволяють переходити від реактивного до прогнозного кіберзахисту. Вони здатні передбачати компрометацію вузлів, моделювати сценарії атак, оцінювати ризики cascading failures, прогнозувати поведінку

атакувальника. Це особливо важливо у воєнний час, коли кібератаки часто поєднуються з фізичними ударами по енергетиці.

3. Однією з ключових проблем smart grid є централізація даних. Системи *Federated Learning* забезпечує локальне навчання *AI*, обмежує передачу чутливих даних, чим суттєво зменшує ризик компрометації та підвищує резильєнтність системи. Для енергетики це критично, оскільки центральний дата-центр стає single point of failure, коли під час війни зв'язок може бути нестабільним а локальна автономність стає стратегічною перевагою.

4. Сучасні дослідження все частіше поєднують штучний інтелект з технологіями *blockchain* з використанням quantum-safe cryptography [4, 5]. Blockchain забезпечує незмінність журналів обліку, довіреність транзакцій та децентралізацію управління, що актуально для безпечної експлуатації розподілених енергетичних систем майбутнього України. В свою чергу, *AI* забезпечує адаптивний захист, інтелектуальне виявлення зовнішніх загроз, автоматизовані реакції на них. Разом вони створюють self-healing cybersecurity architecture для smart microgrids.

Як виклик традиційним воєнним технологіям, значення *AI* у воєнний час для енергетичної стійкості держави високе. Разом із системами *AI*, технології децентралізованої енергетики у воєнних умовах мають стратегічну перевагу за рахунок:

-відсутності єдиного центру ураження;

-швидкого локального відновлення;

-автономності регіонів;

-стійкості до блекаутів.

Системи *AI* підсилює ці можливості через:

-автономне балансування мережі;

-self-healing grid (самовідновлювальні мережі);

-автоматичне ізолювання заражених вузлів;

-adaptive rerouting energy flows (адаптивне перенаправлення енергетичних потоків).

У сучасних smart grids *AI* може:

-перерозподіляти навантаження;

-прогнозувати пошкодження;

-визначати критичні вузли;

-оптимізувати резервні джерела живлення.

Натомість існують певні проблеми, щодо використання *AI* у кібербезпеці розподіленої енергетики. Зокрема *AI* сам може становитися вразливою мішенню, яка в свою чергу, потребує фізичного та інформаційного захисту. На період бойових дій *AI*-системи можуть піддаватися збройним атакам, деформаціям даних, ухилення від моделей, оперативного маніпулювання. Компрометація *AI*-захисту може бути критичнішою за атаку на окремий вузол.

Потрібно розуміння, що енергетична інфраструктура це специфічна критична система. Тому оператор, як невід'ємна ланка управління, має розуміти зміст рішень, що приймає *AI*, зокрема, як модель визначила атаку і рівень достовірності її прогнозу. У цьому розрізі black-box AI створює серйозні ризики для критичної інфраструктури. Система *AI* завжди потребує великих баз даних, реалістичних послідовностей для можливих атак враження, якісної телеметрії. У інтелектуальних енергосистем часто існує фрагментація, особисті протоколи, затримки за впорядкованістю стандартизації, нестача відкритих datasets.

Перспективні напрями розвитку досліджень в галузі інтелектуальних локальних енергосистем включають актуалізацію *AI* для smart grid, створення умов для використання *AI*-driven *SOC* в енергетичних мережах, створення цифрових платформ для кібербезпеки та квантово-безпечних розумних мереж, автономності таких кіберсистем, інтелектуальних методів управління ризиками

Висновки.

1. Децентралізована енергетика радикально змінює підхід до енергетичної безпеки держави, а у поєднанні з *AI* створює стратегічну перевагу у довготривалому воєнному конфлікті зі збереженням умов енергетичної безпеки для населення. Вона знижує ефективність енергетичного шантажу, ускладнює проведення каскадних атак, підвищує автономність громад і регіонів, забезпечує гнучкість після руйнування інфраструктури, здатна сприяти швидшому відновленню держави.

2. Однак цифровізація та масове використання *IoT* створюють істотний рівень кіберризиків. Не зважаючи на це, AI повинна стати центральним елементом кіберзахисту нової децентралізованої енергетики, оскільки лише інтелектуальні системи здатні виконувати функції інтелектуального супроводу таких енергосистем.

3. У воєнний час поєднання децентралізації енергосистем з можливостями *AI* кібербезпеки та технологіями розподіленого керування типу *blockchain* формує основу енергетичної стійкості сучасної держави.

4. Для сучасної України розвиток децентралізованої та альтернативної енергетики є не альтернативою централізованій системі, а стратегічним напрямом формування нової моделі національної безпеки. У майбутньому перевагу матимуть не найбільші енергосистеми, а найбільш адаптивні, автономні та кіберстійкі. Саме поєднання distributed energy, *AI*-driven *cybersecurity* та *cyber resilience* формує основу енергетичної безпеки держави у XXI столітті.

1. Achaal B., Adda M., Berger M. Study of Smart Grid Cyber-Security, Examining Architectures, Communication Networks, Cyber-Attacks, Countermeasure Techniques, and Challenges, Springer Nature, Cham, 2024, pp. 1–38. DOI 10.1186/s42400-023-00200-w.

2. Chen J., Yan J., Kemmeugne A. Cybersecurity of Distributed Energy Resource Systems in the Smart Grid: A Survey, Elsevier, Amsterdam, Applied Energy, Vol. 383, 2025, pp. 125364–125390. DOI 10.1016/j.apenergy.2025.125364.
3. Integrated Blockchain and Federated Learning for the Cybersecurity of Distributed Energy Resources, Elsevier, Amsterdam, 2025, International Journal of Electrical Power & Energy Systems, Vol. 173, pp. 111286–111340. DOI 10.1016/j.ijepes.2025.111286.
4. Manoj N., Aneesh K. A., Malvoni M. Distributed Energy Resources and the Application of AI, IoT, and Blockchain in Smart Grids, MDPI, Basel, Energies, Vol. 13(21), 2020, pp. 5739–5768. DOI 10.3390/en13215739.
5. Ahmad J., Rizwan M., Ali S. F. Cybersecurity in Smart Microgrids Using Blockchain-Federated Learning and Quantum-Safe Approaches: A Comprehensive Review, Elsevier, Amsterdam, 2025, Applied Energy, Vol. 393, pp. 126118–126170. DOI 10.1016/j.apenergy.2025.126118.

В.С. Волошин, О.В. Кленін

КІБЕРБЕЗПЕКА РОЗПОДІЛЕНИХ ЕНЕРГОСИСТЕМ УКРАЇНИ: ЕНТРОПІЙНО-ТОПОЛОГІЧНИЙ ПІДХІД

Сучасна енергетика України у тій її частині, яка позиціонується, як децентралізована, є надзвичайно складною системою, у якій одночасно взаємодіють енергетичні потоки, цифрові мережі, *AI*-системи *SCADA* (*Supervisory Control and Data Acquisition*) - диспетчерське керування та збір даних, *IoT, DER* (*Distributed Energy Resources*) - розподілені енергетичні ресурси), smart grids - інтелектуальні мережі, *blockchain*-технології та системи накопичення енергії. Це показано, в супротив класичній централізованій енергетиці, для якої існує ієрархічна структура, що включає велику електростанцію, центральний диспетчерський пункт, лінійну систему управління та розподілу енергії між споживачами.

У структурі децентралізованої моделі ситуація принципово інша. Вона передбачає появу тисяч автономних вузлів, кожен з них має особистий цифровий інтерфейс. Вузли постійно змінюють свій стан, а система функціонує у реальному часі. Це означає, що енергетика перетворюється на суцільну кіберфізичну систему (*Cyber-Physical System*), де співіснують: фізична енергетика, цифрове управління, *AI*-аналітика, мережеві взаємодії, тобто все, що утворює єдину складну динамічну структуру [1].

В такій конфігурації ефективність класичної кібербезпеки стає вже недостатньою. Вона працювала для статичних мереж з невеликою кількістю вузлів, мала передбачувану архітектуру, систему централізованого моніторингу. У суперечь цьому пропонуються інтелектуальні мережі (smart grids), які складаються з десятків тисяч *IoT*-вузлів з динамічною топологією і нелінійними зв'язками, високошвидкісним обміном телеметрією та автономністю окремих *DER* [2]. Така конфігурація більш не потребує від людини аналізувати увесь енергетичний трафік, прогнозувати всі можливі сценарії будь-яких зовнішніх атак, локалізувати cascading failures у реальному часі. Тому така система переходить у режим високої інформаційної складності. Саме це і є причиною застосування методів ентропійно-топологічного аналізу з використанням *AI-driven cybersecurity*.

Основна ідея ентропійно-топологічного аналізу описана в роботі [3]. Методика поєднує напрями – топологію, термодинаміку та *AI*-аналіз, як адаптивне управління ризиками. Топологічне уявлення енергосистеми описується гіперграфом

$$G = (V, E), \tag{1}$$

де: V — множина вузлів; E — множина зв'язків між вузлами.

Фундаментальним моментом в дослідженні є те, що сукупна енергетика більш не розглядається, як «чиста електростанція-користувачі». Вона

уявляється, як мережа великої кількості взаємодіючих об'єктів. Вузлами V являються: smart meters, *AI IDS* (*Artificial Intelligence Intrusion Detection System)* - система виявлення вторгнень на основі штучного інтелекту, *DER, SCADA*-контроль, *blockchain* моделі, *microgrids*, інверторні *AI*-модулі.

Зв'язки в графовій моделі описують: енергетичні потоки; наведення команд; телеметрію; *AI*-синхронізацію; *blockchain* консенсуси. Топологія в моделі дозволяє визначити рівень критичності вузлів, можливі каскадні збої та області найбільшого ефекту від атаки, напрями поширення можливого кіберзараження.

Ентропійний опис системи базується на ентропії Шеннона

$$H = -\sum p_i log_2 p_i \tag{2}$$

і визначає рівень хаосу, невизначеність стану системи, деградацію керованості, інформаційну нестабільність.

Якщо система стабільна то вузли працюють прогнозовано, навантаження збалансовані, а система *AI* контролює трафік. На це показує низькі значення ентропії окремих вузлів $H_i(t)$. Якщо починається фізична або кібернетична атака, з'являються аномальні пакети для окремих вузлів системи, в моделі це супроводжується помилковими командами, перевантаженням, втратою синхронізації. На це показує зростання ентропії системи.

Для окремого вузла така локальна ентропія

$$H_i(t) = -\sum p_{i,j} log_2 p_{ij}(t) \tag{3}$$

означає, що *AI* аналізує характер зміни поведінки $i-$го вузла по певному $j-$му фактору, виникнення аномалії або нетипові трафіки, виявляє присутність спроб компрометації.

Розглянемо динаміку деградації системи. Критичний інформаційний режим описується відношенням

$$\frac{dH}{dt} > H_{crit}, \tag{4}$$

тобто швидкість росту хаосу в системі вища ніж критично заданий поріг. Фізично це означає, що виникнення та зростання хаосу швидше за можливості стабілізації. Це показує на те, що мережа втрачає синхронізацію, *DER* перестають балансувати систему, починаються каскадні збої.

Критичність вузла з позиції його топологічної вразливості запишемо, як

$$C_D(v) = \deg(v) \tag{5}$$

де ознака $deg\ (v)$ показує на кількість зв'язків вузла. Якщо вузол має багато зв'язків, це означає, що через нього проходять ключові потоки і він є «центром» системи. Наслідком є компрометація такого вузла, що проявляється у виникненні каскадних збоїв, поширенні атак по всій мережі, і, як слідство - збільшується ентропія системи. У цій моделі *AI* виступає, як ентропійний стабілізатор.

Динаміка системи описується рівнянням

$$\frac{dH}{dt} = A(t) - AI(t) \tag{6}$$

Тут: *A(t)* — інтенсивність атак; *AI(t)* — ефективність *AI*-захисту.

У такій системі *AI* фактично грає роль «викачувального насосу», виконуючи функції аномальної детекції, адаптивного перенаправлення команд і потоків, самовідновлення, прогнозування хаотичних режимів роботи системи та локальної ізоляції системи. Якщо для конкретного часу $AI(t) > A(t)$, це означає, що система стабілізується. Якщо виникає умова $AI(t) < A(t)$, починається нелінійне зростання ентропії, що в свою чергу показує на руйнування smart grid и каскадні вимкнення.

Модель *blockchain*, як механізм стабілізації, призваний мінімізувати ентропію журналів урахувань

$$H_{ledger} \to min \tag{7}$$

тим самим унеможливлює фальсифікацію, стабілізує довіру в системі, забезпечує незмінність подій. Це особливо важливо для smart contracts у системі управління *blockchain*, координацію протоколів *DER*, чим забезпечує стійкість енергетичної системи у воєнний час.

Для інтегральної оцінки рівня кіберстійкості децентралізованої енергетичної системи зі штучним інтелектом запропонуємо емпіричний інтегральний показник кіберстійкості у вигляді

$$R = \frac{AI(t) \cdot D}{H \cdot C} \tag{8}$$

який напряму показує на ефективність *AI*-захисту, рівень децентралізації (*D*) і обернено пропорційний ентропії системи (*H*) та її топологічній критичності (*C)*.

Формула показує на те, що кіберстійкість розподіленої енергетичної системи зростає якщо в її складі закладено ефективний *AI*, а система сильно децентралізована. І, навпаки, показник знижується, якщо хаос росте, в системі існують критичні вузли.

Можна аналітично довести переваги кіберзахисту децентралізованої енергетики у порівнянні зі централізованою системою енрегозабезпечення.

Для централізованої системи характерним є низький рівень децентралізації: $D_c \ll D_d$ і висока топологічна критичність $C_c \gg C_d$ оскільки існують центральні вузли (SCADA, диспетчер, магістральні підстанції).Тоді

$$R_c = \frac{AI_c(t) \cdot D_c}{H_c \cdot C_c} \tag{9}$$

а для децентралізованої системи, відповідно,

$$R_d = \frac{AI_d(t) \cdot D_d}{H_d \cdot C_d} \tag{10}$$

Як умова переваги децентралізованої системи, необхідно довести що $R_d \gg R_c$, або

$$\frac{AI_d}{AI_c} > \frac{H_d}{H_c} \cdot \frac{C_d}{C_c} \cdot \frac{D_c}{D_d} \tag{11}$$

Це є фундаментальна умова для фіксації переваги децентралізованої кіберфізичної енергосистеми. Її фізичний зміст викладається наступним чином. Система розподіленої енергетики буде кіберстійкішою, якщо:

1. *AI*-захист масштабується швидше, ніж росте ентропія.
2. Децентралізація зменшує критичність вузлів.
3. Кількість автономних *DER* компенсує локальні компрометації.
4. Атака не здатна викликати глобальний каскадний колапс.

У централізованій системі $C_c \to max$, бо існують точки single point of failure.

У децентралізованій системі $C_d \to min$ через розподіл функцій між DER. Отже, для цього варіанту R_d зростає, навіть якщо ентропія мережі більша.

Для такої системи кібервпливів характерні нелінійні залежності як для термодинамічної системи. Це можна побачити на прикладі нелінійності ентропії. У реальних smart grids, як правило, зовнішні атаки підсилюють одна одну, існуючі каскадні відмови породжують нові і, в цілому, деградація є нелінійною. Тому рівняння (6) має більш визначений вигляд

$$\frac{dH}{dt} = A(t)^{\alpha} - AI(t)^{\beta} \qquad (12)$$

де $\alpha > 1$ – нелінійне зростання хаосу, а β>1 - проказує на ефект самоадаптації *AI*.

Можна показати на критичний фазовий перехід, коли $A(t) \approx AI(t)$. Тут система перебуває біля точки біфуркації (AI_{crit}). Невелике збільшення атак викликає $H(t) \to \infty$, тобто, втрату синхронізації, каскадні blackout, fragmentation collapse.

Відмінності у системі розподіленого управління пов'язані з нелінійністю топології. Зокрема, у централізованій мережі топологічна критичність, це C~N, де N — кількість залежних вузлів. А у децентралізованій мережі $C \sim logN$, тобто ріст складності не приводить до пропорційного росту вразливості. Це принципово важливо.

І наприкінці, покажемо на існування *AI*-ефекту насичення. Він пов'язаний із умовами великої кількості атак, коли $AI(t) \to AI_{crit}$, тобто *AI* має межу продуктивності. Тоді система входить у режим: $AI(t) > AI_{crit}$ і починається ентропійний вибух.

Зробимо аргументований аналіз подібної моделі на прикладі двох систем: централізованого та децентралізованого енергозабезпечення певного об'єму енергозабезпечення (табл. 1.), що приходиться на енергетичну одиницю системи. Такі параметри узгоджені з теорією складних мереж, з кіберфізичними системами, з ентропією Шеннона, з resilience engineering та distributed systems theory.

Таблиця 1 – Початкові дані для розрахунків рівнів кібернетичної безпеки для енергетичних систем, які прийняті до порівняння

Параметр	Обрані значення параметрів			
	Для централізованої системи, («c»)		Для децентралізованої системи («d»)	
	«c»	Обгрунтування	«d»	Обгрунтування
AI	40	AI_c має обмежений масштаб адаптації, рішення в одному SCADA, обмежена кількість точок моніторингу, швидкість локальної реакції менша	75	AI_d масштабується, працює паралельно, локалі-зує атаки до їх поширення, приймає автономні рішення і аналізує локальні аномалії, самонавчається
D	1	Одна диспетчерська вертикаль, як центр координації, структура магістральна, слабко розподілена, наявність single point of failure.	8	Велика кількість DER, автономність microgrids, локальні системи балансування, peer-to-peer координація, blockchain-взаємодії.
H	12	Максимально обмежена кількість вузлів, телеметрії, маршрутів, станів та нелінійних взаємодій впливають на складність системи	20	Велика кількість вузлів, телеметрії, маршрутів, станів та нелінійних взаємодій впливають на складність системи (формула Шеннона)*
C	15	Центральні вузли мають величезний degree, SCADA є вузлом надвисокої зв'язності, а компро-метація центру руйнує мережу ($C_d(v) = \deg(v) \to max$)	4	Функції розподілені, відсутність єдиного центру, локальні вузли автономні, атаки ізолюються локально. Це є головною перевагою smart grid.
R	0,222	Одночасно низький D, високий C, слабка масштабованість AI. Тому в цілому $R_c \ll 1$	7,5	Одночасно високий D, низький C, сильний AI. Тому в цілому $R_d \gg 1$

*- децентралізована система може мати більшу ентропію, але бути стійкішою. Тут стійкість визначається не лише хаосом, а локалізацією пошкоджень відсутністю глобального центру відмов, топологією.

Типова інтерпретація результатів. Запрограмований результат $R_d \gg R_c$ показує, що централізована система перебуває у критичній зоні, а децентралізована — у стабільному режимі.

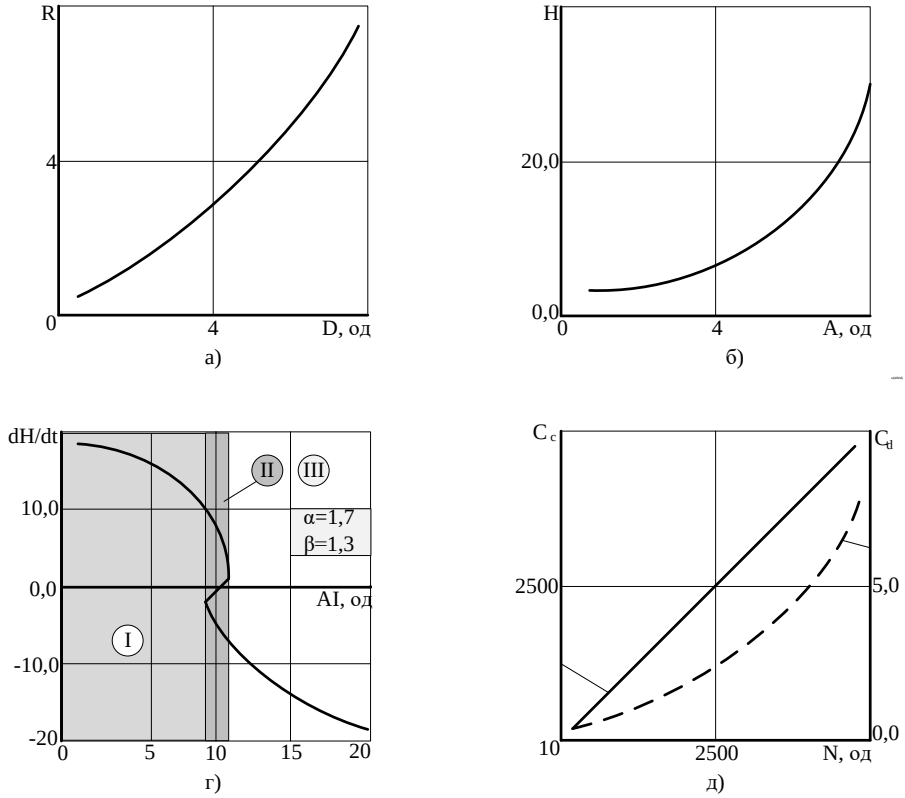


Рисунок 1 ─ Термодинамічні показники ефективності засобів квбернетичного захисту для різних видів енергетичних систем. Тут а) - залежність стійкості від рівня децентралізації енергетичної системи; б)- залежність ентропії системи від інтенсивності атак; в) – вплив AI на рівень стабілізації енергетичної системи (I-ентропійний вибух; II-критична фаза і точка біфуркації, атракція моделі; III – стабільна фаза); г)-вразливість централізованої та децентралізованої енергосистем.

Аналіз графіка (рис. 1, а) показує, що при малих *D* система нестійка, а після певного порогу *R>1*, мережа входить у режим резильєнтності. При цьому децентралізація працює як механізм придушення каскадних аварій. Як ентропія системи відображає інтенсивність кібернетичних атак, показано на

рис 1, б. Залежність $H(A)$ існує як нелінійна. Це означає, що після певного рівня атак система деградує лавіноподібно, при цьому класичний кіберзахист не встигає реагувати на атаки до системи, і для стабілізації системи необхідний predictive *AI*.

І, наприкінці, як впливає присутність *AI* на стабільність системи енергопостачання (рис. 1, в). Графік показує, що при обраних межових параметрах ($\alpha = 1{,}7, \beta = 1{,}3$) у моделі (12) відбувається фазовий перехід $\frac{dH}{dt} < 0$. Режим I – це хаос у контролі, коли система входить у runaway entropy і виникає fragmentation collapse. Режим II – показує на критичну межу між стабільністю та хаосом, коли $AI \to AI_{crit} = A^{\alpha/\beta}$. Він показує на надчутливість при різкому зростанні флуктуацій. Виникає режим bifurcation instability. Режим III – показує на стабільність системи відносно будь-яких збурень, ентропія затухає, система поводиться у фазовому просторі, як один стабільний атрактор (*H, A, AI*). Рівняння (12) фактично описує модель теорії катастроф [4] у динаміці типових точок. Після проходження критичної точки невелика зміна параметра $\Delta A \ll 1$ викликає $\Delta H \gg 1$. Тому ця система вже не лінійна, вона має критичні режими з фазовими переходами та нелінійною деградацією. Важливо, що до критичної точки AI_{crit} *DER* у системі управління компенсуються термодинамічні навантаження і *AI* локалізує атаки. Тому microgrids синхронізовані. А після критичної точки *AI* перевантажується, знижується синхронізація за рахунок нестабільної флуктуації, каскадних збоїв та фрагментації.

Це показує на зменшення хаотичних змін у системі при можливих атаках, *AI* переходить у режим активного придушення ентропії і система самостабілізується.

Підсумковим стає співставний аналіз вразливості централізованої та децентралізованої енергетичних систем (рис. 1, г). Це один з найважливіших результатів, який надає інформацію про суттєвість кіберзахисту для енергостистем в Україні. У централізованій системі $C \propto N$, тобто масштабування збільшує вразливість. І навпаки, для smart grid - $C \propto logN$, тому система може масштабуватись, топологічна стійкість у будь-якій конфігурації не руйнується, а мережа не має глобального центру відмови.

Загальний висновок

1. Проведений ентропійно-топологічний аналіз показує, що децентралізована енергетика принципово стійкіша за термодинамічними умовами. Головна перевага smart grid відноситься не в меншій ентропії, а у зменшенні топологічної критичності, здатності до локалізації атак, автономності DER та AI-керованій адаптації.

5. У воєнних умовах майбутня енергетика України повинна розглядатися як *AI*-керована децентралізована кіберфізична система, у якій топологія визначає стійкість, ентропія визначає рівень деградації, *AI* виступає як механізм стабілізації, а технологія *blockchain* забезпечує резильєнтність

мережі. Саме така архітектура повинна формувати основу енергетичної безпеки держави у XXI столітті.

1. Kumar N. M., Chand A. A., Malvoni M. at all. Distributed Energy Resources and the Application of AI, IoT, and Blockchain in Smart Grids. Journal: Energies, Vol. 13, № 21, Basel, 2020. pp. 1–42. DOI 10.3390/en13215739.
2. Li Z., Shahidehpour M., Liu X. Cyber-secure decentralized energy management for IoT-enabled active distribution networks. Journal of Modern Power Systems and Clean Energy, Vol. 6, 2018. pp. 900–917 DOI 10.1007/s40565-018-0425-1.
3. Волошин В. С., Ткаленко І. А. Метод аналізу полікомпонентних складних систем нга основі багатовимірних матриць суміжності та ентропійних відношень між компонентами системи. KPI Science News. Системний аналіз та наука про дані. №1, 2026. С. 32-41. DOI 10.20535/kpisn.2026.1.350050.
4. Poston T., Steward I. Catastrophe Theory and Its Applications Dov.er Publications. New York, 1998. 512 p.

П.С. Шпилюр, Н.П. Іваненко

МОДЕЛЮВАННЯ РЕЗИЛЬЄНТНОСТІ ФОТОЕЛЕКТРИЧНИХ СИСТЕМ ІЗ ВИКОРИСТАННЯМ АКТИВНОГО ОХОЛОДЖЕННЯ ТА BESS

У сучасних умовах розвитку розподіленої генерації та підвищення вимог до стійкості енергетичних систем особливого значення набуває забезпечення ефективного та надійного функціонування фотоелектричних систем. Для України ця проблема є особливо актуальною в умовах необхідності підвищення енергетичної резильєнтності, розвитку локальних енергетичних вузлів та зростання ролі автономних джерел енергопостачання.

Одним із ключових факторів, що впливають на ефективність роботи сонячних електростанцій, є температурний режим фотоелектричних модулів. Підвищення температури модулів призводить до зниження їх ефективності, втрат генерації та прискорення деградаційних процесів. Водночас системи накопичення енергії (BESS) дозволяють підвищити стійкість локальних енергетичних систем за рахунок резервування енергопостачання, накопичення надлишкової генерації та згладжування нерівномірності виробництва електроенергії.

У роботі запропоновано регіонально-адаптивну модель функціонування фотоелектричних систем, яка базується на комплексному врахуванні кліматичних умов, температурного режиму фотоелектричних модулів, процесів деградації та режимів роботи систем накопичення енергії. Основною особливістю запропонованого підходу є перехід від локального оцінювання миттєвої генерації до системного аналізу життєвого циклу фотоелектричної системи з урахуванням її ефективності, ресурсу та стійкості функціонування.

Модель побудована на основі трьох взаємопов’язаних контурів: фізичного, ресурсного та енергетико-економічного.

Фізичний контур описує процеси перетворення сонячної енергії в електричну та вплив погодних факторів на роботу фотоелектричних модулів. У межах цього контуру враховуються температура навколишнього середовища, інтенсивність сонячної радіації, швидкість вітру, хмарність та інші кліматичні параметри, які визначають температурний режим модулів і рівень втрат генерації. Також у фізичному контурі враховуються параметри систем активного охолодження та особливості різних типів фотоелектричних модулів і матеріалів фотоелектричних елементів.

Ресурсний контур орієнтований на оцінювання довгострокового впливу температурних навантажень на технічний стан фотоелектричних модулів. У цьому контурі враховуються процеси накопичення термічного навантаження, кількість циклів перегріву, тривалість роботи при підвищених температурах

та особливості деградації різних типів фотоелектричних елементів. Такий підхід дозволяє оцінювати не лише поточну ефективність роботи СЕС, а й прогнозувати зміну характеристик системи протягом усього життєвого циклу.

Енергетико-економічний контур описує взаємодію фотоелектричної генерації, систем активного охолодження та BESS. У межах цього контуру аналізуються режими накопичення та використання електроенергії, рівень автономності локальної енергосистеми, стабільність енергопостачання, а також економічні показники функціонування системи. Системи накопичення енергії розглядаються як важливий елемент забезпечення енергетичної резильєнтності, який дозволяє підвищити стійкість роботи фотоелектричних систем в умовах змінної генерації та нестабільних режимів роботи енергосистеми.

Загальну структуру запропонованої моделі наведено на рис. 1.

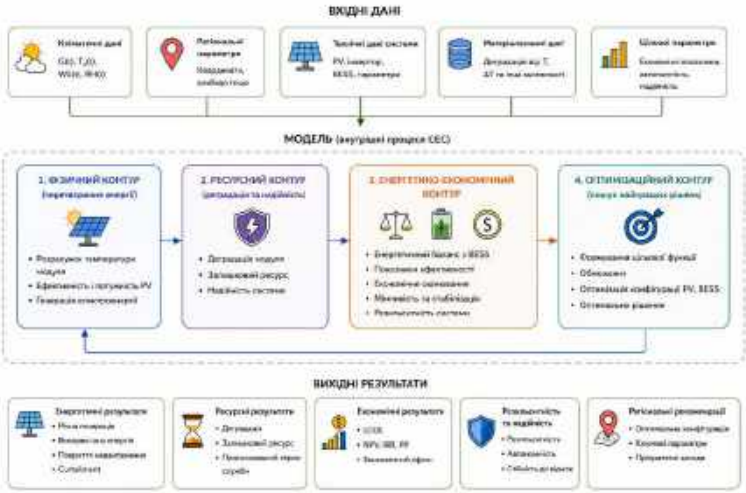


Рисунок 1 – Структура регіонально-адаптивної моделі функціонування фотоелектричної системи

Важливою особливістю запропонованого підходу є використання погодинних кліматичних даних для різних регіонів України. Для формування часових рядів погодних параметрів передбачається використання відкритих міжнародних баз кліматичних даних, зокрема PVGIS, NASA POWER, ERA5 та Meteostat, які містять інформацію щодо сонячної радіації, температури повітря, швидкості вітру, хмарності та інших метеорологічних показників. Це

дозволяє враховувати регіональні особливості функціонування СЕС та оцінювати вплив різних кліматичних режимів на ефективність і ресурс фотоелектричних систем.

На даному етапі дослідження основна увага приділяється реалізації фізичного контуру моделі, який є базовим для подальшого формування ресурсного та енергетико-економічного контурів. У межах поточного етапу здійснюється формування погодинних часових рядів кліматичних параметрів для різних регіонів України на основі відкритих міжнародних баз даних PVGIS, NASA POWER, ERA5 та Meteostat. Використання погодинних кліматичних даних дозволяє перейти від спрощених усереднених оцінок до динамічного моделювання режимів роботи фотоелектричних систем у реальних умовах експлуатації.

На основі сформованих часових рядів виконується аналіз регіональних особливостей температурних режимів та інсоляції для різних областей України. Особлива увага приділяється оцінюванню тривалості періодів перегріву фотоелектричних модулів, сезонній нерівномірності генерації та впливу кліматичних факторів на втрати потужності. Паралельно здійснюється систематизація технічних характеристик різних типів фотоелектричних модулів і матеріалів фотоелектричних елементів, зокрема їх температурних коефіцієнтів, номінальних робочих температур та особливостей деградації в умовах тривалого термічного навантаження.

У межах фізичного контуру також реалізується блок моделювання температурного режиму фотоелектричних модулів з урахуванням параметрів активного охолодження. Досліджується вплив інтенсивності охолодження на температуру модулів, величину температурних втрат генерації та потенційне підвищення ефективності роботи СЕС у різних кліматичних умовах. Окремо аналізується енергоспоживання систем активного охолодження та його вплив на загальний енергетичний баланс системи.

Крім того, на поточному етапі проводиться порівняльний аналіз різних регіонів України за рівнем кліматичного навантаження на фотоелектричні системи. Передбачається формування регіональних профілів функціонування СЕС, які враховуватимуть температурні режими, рівень сонячної радіації, сезонність генерації та потенційну доцільність застосування активного охолодження. Отримані результати будуть використані як основа для подальшої реалізації ресурсного контуру моделі, пов’язаного з оцінюванням деградації модулів, а також енергетико-економічного контуру, у межах якого планується моделювання роботи BESS та оптимізація режимів функціонування фотоелектричних систем.

1. Шпилюр П.С., Іваненко Н.П. Методи підвищення ефективності та продовження терміну служби фотоелектричних систем // Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.

2025. Том 36 (75). № 3. С. 193–198. URL: https://www.tech.vernadskyjournals.in.ua/journals/2025/3_2025/part_1/27.pdf.
2. Jordan D.C., Kurtz S.R. Photovoltaic degradation rates — An analytical review // Progress in Photovoltaics: Research and Applications. 2013. Vol. 21(1). P. 12–29. DOI: 10.1002/pip.1182.
3. Skoplaki E., Palyvos J.A. On the temperature dependence of photovoltaic module electrical performance: A review of efficiency/power correlations // Solar Energy. 2009. Vol. 83(5). P. 614–624. DOI: 10.1016/j.solener.2008.10.008.
4. Yang Y., Bremner S., Menictas C., Kay M. Battery energy storage system size determination in renewable energy systems: A review // Renewable and Sustainable Energy Reviews. 2018. Vol. 91. P. 109–125. DOI: 10.1016/j.rser.2018.03.047.

УДК 004.056.5

Г.І. Рибачок

ОЦІНЮВАННЯ ДОПУСТИМОСТІ АЛЬТЕРНАТИВ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Кіберінциденти у секторі безпеки і оборони та на об'єктах критичної інфраструктури дедалі частіше мають не лише технічний, а й управлінський зміст. Для органів військового управління Збройних Сил України важливо встановити не тільки тип інциденту чи факт порушення конфіденційності, цілісності або доступності інформації, а й те, як подія впливає на управлінський цикл, обмін даними, координацію підпорядкованих елементів і здатність виконувати завдання в обмежений час. Для енергетичної критичної інфраструктури ця логіка є особливо значущою, оскільки порушення інформаційних систем або каналів керування може швидко вплинути на безперервність критичних процесів.

Міжнародні стандарти й рекомендації визначають загальну рамку управління кіберінцидентами: підготовку, виявлення, аналіз, реагування, відновлення та післяінцидентне вдосконалення [2–5]. Законодавство України формує правові засади забезпечення кібербезпеки та взаємодії суб'єктів реагування [1]. Водночас ці документи не розв'язують повною мірою завдання вибору конкретної альтернативи дій у військово-управлінському контексті. Після оцінювання інциденту суб'єкт управління має отримати не загальну вказівку на потребу реагування, а впорядковану множину дій, з якої вилучено варіанти, що є неприйнятними за наявних умов.

Метою тез є обґрунтування методичних засад оцінювання допустимості альтернатив реагування на кіберінциденти в системі підтримки прийняття рішень органів військового управління Збройних Сил України з урахуванням особливостей інформаційних систем критичної енергетичної інфраструктури.

Альтернатива реагування розглядається як можливий варіант дій щодо нейтралізації кіберінциденту, сформований з урахуванням результату оцінювання інциденту, початкового управлінського стану, вимог до ефективності реагування, допустимого залишкового ризику та профілю умов реагування. Базова множина альтернатив не повинна одразу ототожнюватися з рекомендованим рішенням. Вона є початковим простором можливих дій, який потребує перевірки на допустимість і здійсненність.

У загальному вигляді перевірку доцільно подати як формування множини допустимих альтернатив:

$$A_i feas = \{a_{ij} \in \mathcal{A}_i^0 \mid Feas_i(a_{ij}, \Pi_i, E_i req, Risk_i adm) = 1\},$$

де a_{ij} — j-та альтернатива реагування для і-го кіберінциденту; $\mathcal{A}_i^0$ — базова множина альтернатив; Π_i — профіль умов реагування; вимоги до ефективності реагування визначають очікуваний результат нейтралізації; допустимий залишковий ризик задає межу прийнятності наслідків; предикат Feas визначає допустимість і здійсненність альтернативи. Якщо значення предиката дорівнює 1, альтернатива може бути передана на критеріальне оцінювання.

До основних груп умов допустимості належать повноважна й процедурна допустимість, часова здійсненність, ресурсна забезпеченість, режимно-безпекова сумісність, ризикова прийнятність та управлінська придатність. Повноважна умова не допускає варіантів, що виходять за межі компетенції суб'єкта рішення або порушують порядок ескалації. Часова умова відсікає дії, які не забезпечують досягнення потрібного рівня нейтралізації в наявних часових межах. Ресурсна умова перевіряє наявність сил, засобів, фахівців і доступу до необхідних даних. Режимно-безпекова умова враховує обмеження щодо інформації, режимів роботи систем і недопущення вторинних ризиків. Ризикова умова пов'язує альтернативу з допустимим залишковим ризиком. Управлінська придатність показує, чи не погіршує дія керованість, інформаційний обмін або виконання завдань більше, ніж сам інцидент.

Для енергетичної критичної інфраструктури такий підхід дає можливість відокремити технічно можливі дії від управлінсько прийнятних. Наприклад, локалізація інциденту може бути технічно швидкою, але неприйнятною, якщо вона зупиняє критичний процес, потребує неузгодженого втручання або створює надмірний залишковий ризик. Саме тому оцінювання допустимості має передувати критеріальному вибору рекомендованої альтернативи.

Якщо після перевірки множина допустимих альтернатив є порожньою, інформаційна технологія не повинна імітувати наявність готового рішення. У такому випадку результатом має бути висновок про відсутність допустимих альтернатив у наявному профілі умов реагування з пропозицією уточнення даних, перегляду ресурсних меж, формування комбінованих варіантів або ескалації рішення.

Отже, оцінювання допустимості альтернатив є необхідною проміжною ланкою між формуванням базового простору дій і вибором рекомендованого рішення щодо нейтралізації кіберінциденту. Його використання підвищує відтворюваність підготовки управлінського рішення, забезпечує пояснюваність відбору альтернатив і зберігає принципову межу: інформаційна технологія формує обґрунтовану рекомендацію, а остаточне рішення залишається за уповноваженим суб'єктом військового управління.

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 19.05.2026).
2. ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process. Geneva : International Organization for Standardization, 2023. URL: https://www.iso.org/standard/78973.html (дата звернення: 19.05.2026).
3. ISO/IEC 27035-2:2023. Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. Geneva : International Organization for Standardization, 2023. URL: https://www.iso.org/standard/78974.html (дата звернення: 19.05.2026).
4. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3. Gaithersburg : National Institute of Standards and Technology, 2025. URL: https://doi.org/10.6028/NIST.SP.800-61r3 (дата звернення: 19.05.2026).
5. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/NIST.CSWP.29 (дата звернення: 19.05.2026).

УДК 004.8:004.056:620.9

О.О. Верголяс

ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЧИННИК СОЦІОІНЖЕНЕРНИХ ЗАГРОЗ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Кібербезпека енергетики сьогодні вже не зводиться до захисту серверів, корпоративних мереж чи автоматизованих систем управління технологічними процесами. Об'єкти критичної енергетичної інфраструктури працюють у середовищі, де технічна атака часто супроводжується інформаційним тиском на людей, які приймають або виконують рішення. Уразливими стають не лише програмні засоби, а й диспетчерські служби, чергові зміни, управлінські ланки, підрядники та канали службової комунікації.

Закон України «Про критичну інфраструктуру» пов'язує захист таких об'єктів із своєчасним виявленням, запобіганням і нейтралізацією загроз, а також із мінімізацією наслідків у разі їх реалізації [1]. Для енергетичного сектору це означає, що кіберзахист має враховувати не тільки індикатори компрометації чи технічний стан системи. Не менш важливими є поведінка персоналу, достовірність управлінських повідомлень і стійкість процедур, за якими ухвалюються рішення під час інциденту.

Генеративний штучний інтелект помітно змінює саме цей людський і комунікаційний рівень загрози. Він дає змогу швидко створювати переконливі фішингові листи, фальшиві службові повідомлення, голосові звернення, відеофрагменти, псевдоінструкції та профілі посадових осіб. Для енергетики небезпека полягає не лише в тому, що такий контент може виглядати правдоподібно. Небезпека в тому, що він може з'явитися саме в момент нестачі часу, аварійної ситуації або паралельного кіберінциденту, коли перевірка повідомлень ускладнена.

Соціоінженерні загрози, посилені генеративним ШІ, мають кілька практичних проявів. По-перше, повідомлення можна стилістично підлаштувати під конкретну групу: операторів, технічних спеціалістів, адміністративний персонал або керівників зміни. По-друге, одна й та сама легенда може швидко набувати десятків варіантів, через що її важче виявити за типовими ознаками шаблонного фішингу. По-третє, текст, голос, зображення й відео можуть використовуватися разом, створюючи для адресата відчуття підтвердження з кількох джерел. По-четверте, маніпулятивний контент може супроводжувати реальний інцидент: поширювати хибні інструкції, сіяти недовіру до офіційних каналів або перевантажувати чергові служби зайвими зверненнями.

Тому соціоінженерну атаку на енергетичний об’єкт варто розглядати не як окремий епізод фішингу, а як можливий елемент комбінованого кіберінциденту. Компрометація облікового запису може поєднуватися з deepfake-повідомленням від імені керівника, підробленим службовим листуванням, неправдивою інформацією про стан об’єкта або створенням фальшивого каналу зв’язку для персоналу. У такій ситуації реагування не може бути лише технічним. Потрібні також організаційні й когнітивні заходи, спрямовані на перевірку джерела повідомлення та недопущення помилкової дії.

У воєнних умовах важливим стає не тільки факт спроби проникнення в інформаційну систему, а й управлінський ефект, якого прагне противник. Соціоінженерний вплив може бути спрямований на затримку реагування, провокування неправильного рішення, розрив довіри до офіційних каналів зв’язку або дезорганізацію персоналу під час реального чи імітованого інциденту. Через це в системах кіберзахисту енергетичної інфраструктури доцільно фіксувати не лише технічні ознаки атаки, а й ознаки її інформаційно-психологічного супроводу.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає загальну нормативну рамку кібербезпеки, а Загальні вимоги з кіберзахисту об’єктів критичної інфраструктури встановлюють організаційні та технічні підходи до їх захисту [2; 3]. Проте поширення генеративного ШІ потребує додаткової уваги до тих процедур, які раніше могли вважатися допоміжними: перевірки автентичності управлінських повідомлень, захисту службових каналів, навчання персоналу розпізнаванню синтетичного контенту та опису дій у разі появи фальшивих інструкцій або повідомлень.

Міжнародні підходи до управління кіберризиками також дають підстави для такого розширеного бачення. NIST Cybersecurity Framework 2.0 розглядає управління кіберризиками через функції govern, identify, protect, detect, respond і recover [4]. NIST SP 800-61r3 пов’язує реагування на інциденти з ширшою системою управління кіберризиками [5]. Для об’єктів енергетичної критичної інфраструктури це означає, що реагування має охоплювати не тільки локалізацію технічної загрози, а й комунікаційні ризики, поведінку персоналу та здатність організації не допустити рішення, нав’язаного маніпулятивним контентом.

Практично це може передбачати багатоканальну верифікацію критичних команд, обмеження неофіційних месенджерів для службових рішень, тренування персоналу щодо deepfake, голосових імітацій і персоналізованого фішингу, швидке спростування фальшивих повідомлень, а також фіксацію соціоінженерних ознак у журналах інцидентів. Окремо слід аналізувати, яку саме дію або помилку намагався спровокувати противник. Без такого аналізу технічна атрибуція атаки залишає поза увагою її управлінську мету.

ENISA Threat Landscape 2025 звертає увагу на соціоінженерні, дезінформаційні та пов'язані зі штучним інтелектом загрози [6]. Для енергетичної критичної інфраструктури це є підставою розглядати людський фактор не як слабку периферійну ланку, а як повноцінний елемент кіберстійкості. Захищеність технічних систем має поєднуватися зі здатністю персоналу та органів управління діяти правильно в умовах інформаційного шуму, браку часу й психологічного тиску.

Отже, генеративний штучний інтелект доцільно розглядати як окремий чинник ризику для кібербезпеки енергетики. Він впливає не тільки на технічний контур захисту, а й на комунікацію, поведінку персоналу та процес прийняття рішень. Для об'єктів критичної енергетичної інфраструктури ефективне реагування на кіберінциденти має включати не лише виявлення й нейтралізацію технічної загрози, а й захист управлінського рішення від соціоінженерного та інформаційно-психологічного впливу.

1. Верховна Рада України. (2021). *Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX*. https://zakon.rada.gov.ua/go/1882-20.
2. Верховна Рада України. (2017). *Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII*. https://zakon.rada.gov.ua/go/2163-19.
3. Кабінет Міністрів України. (2019). *Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури: Постанова від 19.06.2019 № 518*. https://zakon.rada.gov.ua/go/518-2019-%D0%BF.
4. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
5. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61r3). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf .
6. European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

С.Б. Бурченко, І.І. Сватовський

АНАЛІЗ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ОПЕРАЦІЙНИХ ТЕХНОЛОГІЙ ТА ПРОМИСЛОВИХ СИСТЕМ КЕРУВАННЯ

Стрімкий розвиток технологій штучного інтелекту (AI) та їх масове впровадження у промислові середовища визначають нову парадигму безпеки операційних технологій (OT). За даними Rockwell Automation у 2024–2025 роках кількість кіберінцидентів у сфері промислових систем керування (ICS) та OT зросла на 87%, причому значна частина атак демонструє ознаки AI-assisted автоматизації: поліморфна поведінка malware, адаптивне ухилення від виявлення, скорочення часу від розвідки до виконання attack payload [1]. Водночас лише 10% ICS/OT середовищ впровадили AI-інструменти захисту [1], що свідчить про критичний структурний дисбаланс між можливостями атакуючих та захисників. При цьому ринок AI в OT Security прогнозується на рівні $14 млрд до 2033 року [2], що свідчить про масштабне технологічне зрушення. Також змінюється регуляторний ландшафт: EU AI Act вперше вводить обов'язкові вимоги до high-risk AI у критичній інфраструктурі, а CISA опублікувала спеціальні настанови щодо безпечної інтеграції AI в OT-середовища [3,6]. Отже актуальним є питання систематизації аналізу впливу Industrial AI на кібербезпеку OT/ICS для оцінки нових векторів загроз та обґрунтування рекомендацій щодо безпечного його впровадження.

Industrial AI як феномен кібербезпеки принципово відрізняється від AI в сфері IT своїм безпосереднім зв'язком з фізичними процесами. Компрометація AI-системи в інформаційному середовищі можуть привести до витоку та порушенні конфіденційності даних, а компрометація Industrial AI може призвести до порушення процесів управління критичної інфраструктури та аварій на небезпечних виробництвах. Це визначає принципово інший підхід до оцінки ризиків та проектування систем захисту. Генеративний AI та великі мовні моделі (LLM) кардинально знизили бар'єр для атак на промислові системи. Аналіз інцидентів 2024 року [4] дозволяє виокремити чотири ключові напрямки застосування AI атакуючими: 1. Автоматизована генерація ICS exploit: 2. Поліморфне malware для OT; 3. AI-orchestrated kill chains - автоматизовані багатоетапні атаки без участі оператора-людини; 4. Цільова соціальна інженерія. Попри загрози, AI є найперспективнішою технологією для фундаментального покращення OT-безпеки, вирішуючи проблеми, що традиційні підходи не здатні подолати: 1. Behavioral anomaly detection: ML-моделі будують поведінковий профіль технічних систем і пристроїв, виявляючи тонкі відхилення та аномальні зміни; 2. Protocol-semantic analysis: AI аналізує семантику OT-протоколів на контекстному рівні - виявляє не просто аномальний трафік, а аномальну

команду в контексті технологічного процесу; 3. Predmaintenance-Security Fusion: єдина модель AI одночасно застосовується для моніторингу і технологічних процесів і для мережевого трафіку OT, атаки через кореляцію фізичних аномалій із кіберподіями; 4. Automated incident response: AI-playbooks реагують на Tier 1–2 загрози за секунди при збереженні обов'язкового Human-in-the-Loop (HITL, «людина в циклі») для відповідальних операцій.

Впровадження AI в промислові системи супроводжується появою векторів атак, які були принципово відсутні в традиційному OT-середовищі. Проведена систематизація цих векторів на основі аналізу актуальних джерел [1-5] представлена нижче і є необхідною умовою для розробки адекватних засобів захисту: 1. Prompt Injection через OT-дані - найбільш специфічним для Industrial AI вектором є indirect prompt injection через дані промислових систем. Ефективність поточних засобів виявлення prompt injection в OT-контексті оцінюється на рівні 22% [2], що свідчить про критичну вразливість у захисті; 2. Adversarial Machine Learning проти OT-IDS - сучасні OT-орієнтовані системи виявлення вторгнень (Claroty, Dragos Platform, Nozomi Networks) базуються на алгоритмах машинного навчання (ML) і до них можуть бути проведені атаки типу Low-and-slow baseline poisoning (маніпулювання профілем поведінки шляхом відтворення шкідливих дій із невеликою амплітудою відхилень), GAN-generated industrial traffic та Targeted model evasion (мінімальні модифікації шкідливого трафіку, достатні для обходу ML-моделі); 3. Атаки на Digital Twin – симуляція атак або ін'єкція хибних даних у цифрові двійники промислових систем; 4. Multi-Agent System Cascade Failures - у промислових середовищах із декількома взаємодіючими AI-агентами компрометація одного може каскадно впливати на рішення всіх агентів. На основі аналізу відкритих даних оцінок ефективності платформ OT-безпеки [2,4,5] сформовано порівняльну матрицю ефективності AI-enhanced та традиційних засобів виявлення:

Таблиця 1 – Порівняльна ефективність AI-based та rule-based OT-IDS

Тип загрози	**AI-Based IDS (%))**	**Rule-Based IDS (%)**	**Покращення**
Anomalous setpoint зміни в OT	**91**	34	**+167%**
Unknown/Zero-day атаки	**85**	0	**+85 п.п.**
Lateral movement у OT-мережі	**78**	42	**+86%**

Low-and-slow APT кампанії	**72**	18	**+300%**
Supply chain compromise	**45**	22	**+105%**
Adversarial evasion атаки	**38**	55	**−31%**
Prompt injection у AI-агентів	**22**	Н/З	**Н/З**

Наведені дані свідчать про суттєву перевагу AI-based підходу для виявлення невідомих та складних загроз, однак виявляють критичну загрозу: prompt injection у industrial AI-агентів характеризується ефективністю виявлення лише 22%, що є незадовільним для промислового середовища з прямим зв'язком з управлінням фізичними процесами. Цей результат підкреслює необхідність розробки спеціалізованих методів захисту від prompt injection в OT-контексті.

Однак автоматизація робочих процесів може давати збій під впливом багатьох факторів. Машинне навчання з функцією HITL дозволяє людям контролювати та вносити визначальний внесок у робочі процеси штучного інтелекту [7]. Підхід HITL дозволяє забезпечити точність, надійність та етичність прийняття рішень. Деякі правила щодо штучного інтелекту вимагають певних рівнів високоризикової безпеки для HITL [6]. Наприклад, стаття 14 Закону ЄС про штучний інтелект вимагає, щоб системи штучного інтелекту високого ризику повинні бути розроблені та розроблені таким чином, зокрема з використанням відповідних інструментів інтерфейсу людина-машина, щоб фізичні особи могли ефективно контролювати їх протягом періоду їх використання. Тому при впровадженні безпечного Industrial AI фундаментальним принципом повинно бути збереження людського контролю над потенційно небезпечними діями. Пропонується при цьому використовувати трирівневу модель HITL:

Для покращення безпеки HITL рекомендується в майбутньому розробляти моделі загроз, які виявлятимуть вразливості в системах HITL [7], що виникають внаслідок втручання людини, а також пропонуватимуть контрзаходи для різних контекстів ризику.

Таблиця 2 – Трирівнева модель Human-in-the-Loop для Industrial AI

Tier	Тип дій	Режим виконання	Безпека
Tier 1 (AUTO)	Алерти, логування, оновлення dashboard, threat score recalculation	Повна автоматизація без підтвердження. Швидкість: мілісекунди.	Низький фізичний ризик
Tier 2 (ASSIST)	Ізоляція мережевого сегмента, блокування з'єднання, сповіщення SOC	Автовиконання + обов'язкове сповіщення оператора + rollback протягом 60 с.	Середній ризик, зворотній зв’язок
Tier 3 (MANUAL)	Зміна setpoint, зупинка обладнання, модифікація Safety System, PLC firmware update	Тільки оператор. AI рекомендує, але не виконує. Фізична двофакторна авторизація.	Критичний – рішення тільки за людиною

Таким чином, можна зробити висновок про те, що Industrial AI наразі змінив співвідношення сил між атакуючими та захисниками: AI-enhanced атакуючим протистоїть переважно rule-based захист. Prompt injection через OT-дані, adversarial ML проти OT-IDS та атаки на Digital Twin є принципово новими векторами атак на критичні технічні системи без наявності аналогів у традиційній OT-безпеці. Ефективність поточних засобів захисту проти prompt injection (22%) є критично недостатньою. Технологічна ефективність AI-захисту може визначатись коректністю Governance-рішень та застосування Human-in-the-Loop архітектури, що є необхідними та критичними вимогами для впровадження безпечного Industrial AI.

1. State of Smart Manufacturing Report. Rockwell Automation Inc., 2025. https://www.rockwellautomation.com/en-us/capabilities/digital-transformation/state-of-smart-manufacturing.html.
2. Artificial Intelligence (AI) in Operational Technology (OT) Cybersecurity Market Report, 2026–2033. Grand View Research, 2025. https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market.

3. Guidance for Artificial Intelligence in Operational Technology Environments. U.S. Cybersecurity and Infrastructure Security Agency, December 2024. https://industrialcyber.co/download/secure-integration-of-ai-in-ot-principles-and-guidance-for-critical-infrastructure-cisa/.
4. 2026 OT Cybersecurity Threat Landscape Analysis Report. https://shieldworkz.com/reports/ot-cybersecurity-threat-landscape-analysis-report-2026.
5. OT Cybersecurity Year in Review 2024. Dragos, Inc., 2025. https://www.dragos.com/resources/press-release/dragos-ot-cybersecurity-year-in-review-reports-rise-in-geopolitically-driven-attacks-ransomware-and-threat-groups.
6. Regulation (EU) 2024/1689 of the European Parliament — AI Act. Official Journal of the European Union, July 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
7. Human-in-the-Loop Artificial Intelligence: A Systematic Review of Concepts, Methods, and Applications. Entropy 2026, 28(4). https://doi.org/10.3390/e28040377.

В.М. Мацука

УПРАВЛІННЯ КІБЕРРИЗИКАМИ В SMART GRID ТА ЦИФРОВИХ ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

Сучасний енергетичний сектор активно впроваджує цифрові технології, автоматизовані системи управління та мережі Smart Grid. Це підвищує ефективність енергосистем, оптимізує споживання ресурсів і покращує якість енергопостачання, але водночас створює нові кіберризики для критичної інфраструктури. Проблема кібербезпеки особливо актуальна в умовах гібридних загроз і кібератак на енергетичний сектор. Оскільки енергетика є основою функціонування держави та економіки, забезпечення її кіберзахисту стає одним із ключових напрямів державної безпеки [1].

Управління кіберризиками в Smart Grid передбачає комплекс заходів, спрямованих на виявлення, оцінку, мінімізацію та контроль кіберзагроз. Ефективна система управління ризиками повинна поєднувати організаційні, технічні, технологічні та управлінські рішення.

Smart Grid – це інтелектуальна енергетична мережа, яка використовує сучасні цифрові технології для автоматизованого управління процесами генерації, передачі, розподілу та споживання електроенергії. Основною особливістю Smart Grid є двосторонній обмін інформацією між усіма учасниками енергетичної системи.

До структури Smart Grid входять: автоматизовані системи диспетчерського управління (SCADA); інтелектуальні лічильники; цифрові підстанції; IoT-пристрої; сенсори моніторингу; хмарні сервіси; системи аналізу великих даних [2].

Використання цифрових технологій дозволяє здійснювати оперативний контроль за станом енергомережі, прогнозувати навантаження, зменшувати втрати електроенергії та підвищувати енергоефективність. Однак інтеграція великої кількості цифрових компонентів одночасно збільшує кількість потенційних вразливостей.

Сучасні енергетичні мережі фактично перетворюються на кіберфізичні системи, де порушення роботи інформаційної інфраструктури може спричинити фізичні наслідки: аварії, знеструмлення об’єктів або пошкодження обладнання [3].

Кіберризики в інтелектуальних енергетичних мережах є багаторівневими та складними. Найпоширенішими загрозами є: несанкціонований доступ до систем управління; атаки на SCADA-системи; DDoS-атаки; зараження шкідливим програмним забезпеченням; компрометація IoT-пристроїв; фішингові атаки; перехоплення каналів передачі даних; внутрішні загрози з боку персоналу.

Особливо небезпечними є атаки на операційні технології (OT), оскільки вони безпосередньо впливають на функціонування енергетичного обладнання. Порушення роботи диспетчерських систем може призвести до масштабних аварій та економічних збитків.

Зростання кількості підключених пристроїв у Smart Grid збільшує поверхню атак. Багато IoT-пристроїв мають низький рівень захисту, що робить їх потенційною точкою проникнення до енергетичної мережі.

Одним із найвідоміших прикладів кібератак на критичну інфраструктуру стала атака на українські енергетичні компанії у грудні 2015 року. Унаслідок втручання хакерів було тимчасово відключено електропостачання для сотень тисяч споживачів.

Зловмисники отримали доступ до корпоративних мереж через фішингові листи та шкідливе програмне забезпечення BlackEnergy. Після проникнення в систему вони змогли дистанційно керувати SCADA-системами та вимикати електропідстанції.

Цей випадок продемонстрував: критичну важливість сегментації мереж; необхідність багатофакторної автентифікації; потребу у постійному моніторингу кіберзагроз; важливість підготовки персоналу до кіберінцидентів.

У 2016 році було зафіксовано ще одну масштабну атаку на українську енергетичну інфраструктуру із застосуванням шкідливого програмного забезпечення Industroyer (CrashOverride). Особливістю цього вірусу була його здатність взаємодіяти з промисловими протоколами управління енергетичними системами.

Програма автоматично виконувала команди відключення енергетичного обладнання, що свідчить про високий рівень підготовки кіберзлочинців.

Після інциденту енергетичні компанії почали активніше впроваджувати: SOC-центри; системи виявлення вторгнень; резервне копіювання; процедури реагування на кіберінциденти.

У 2021 році кібератака на компанію Colonial Pipeline стала однією з найрезонансніших у світі. Внаслідок ransomware-атаки було тимчасово зупинено найбільший паливний трубопровід США [4].

Хоча атака була спрямована переважно на IT-інфраструктуру компанії, керівництво ухвалило рішення тимчасово припинити роботу операційних систем для уникнення подальших ризиків.

Цей кейс підтвердив: взаємозалежність IT- та OT-систем; необхідність резервування критичних даних; важливість планів безперервності бізнесу; значення кризового менеджменту в умовах кібератак.

Управління кіберризиками є безперервним процесом, спрямованим на забезпечення кіберстійкості енергетичної інфраструктури. Основними етапами цього процесу є:

На першому етапі визначаються критичні активи системи та потенційні джерела загроз. Особлива увага приділяється SCADA-системам, каналам зв'язку, серверному обладнанню та системам диспетчеризації.

Оцінка ризиків передбачає визначення ймовірності реалізації кіберзагроз та масштабу можливих наслідків. Для цього застосовуються міжнародні стандарти ISO/IEC 27001, ISO/IEC 27005 та NIST Cybersecurity Framework.

До основних заходів мінімізації ризиків належать: сегментація мережі; шифрування даних; контроль доступу; багатофакторна автентифікація; регулярне оновлення програмного забезпечення; резервне копіювання; використання IDS/IPS-систем.

Системи моніторингу забезпечують виявлення аномалій та оперативне реагування на кіберінциденти. Для цього використовуються SOC-центри та SIEM-платформи, які здійснюють аналіз подій безпеки в режимі реального часу.

Ефективність кіберзахисту залежить не лише від технічних рішень, але й від якості управління. Організаційна складова включає: розроблення політики кібербезпеки; розподіл відповідальності; проведення аудиту безпеки; навчання персоналу; створення планів реагування на інциденти; управління безперервністю діяльності [5].

Людський фактор залишається одним із головних джерел кіберризиків, тому регулярне навчання працівників є важливою умовою забезпечення кіберстійкості.

Крім того, важливого значення набуває формування культури кібербезпеки на підприємствах енергетичного сектору.

Серед сучасних технологій захисту Smart Grid можна виділити: системи SIEM; IDS/IPS; Zero Trust Architecture; технології штучного інтелекту; блокчейн; системи резервування даних; засоби криптографічного захисту.

Особливо перспективним є використання штучного інтелекту для автоматичного виявлення аномальної активності в енергетичних мережах. AI-системи здатні аналізувати великі обсяги даних та прогнозувати потенційні загрози.

Концепція Zero Trust передбачає перевірку кожного користувача та пристрою незалежно від місця їхнього підключення, що значно зменшує ризик несанкціонованого доступу.

Подальший розвиток Smart Grid супроводжуватиметься збільшенням кількості цифрових компонентів, IoT-пристроїв та хмарних сервісів. Це вимагатиме створення адаптивних систем кіберзахисту, здатних оперативно реагувати на нові загрози.

Одним із ключових напрямів розвитку є впровадження концепції кіберстійкості (Cyber Resilience), яка передбачає не лише захист від атак, але

й здатність швидко відновлювати функціонування системи після інциденту [6].

Для України питання кібербезпеки енергетики має стратегічне значення, оскільки стабільне функціонування енергосистеми безпосередньо впливає на національну безпеку та економічну стабільність держави.

Управління кіберризиками в Smart Grid та цифрових енергетичних мережах є одним із ключових напрямів забезпечення безпеки критичної інфраструктури. Активна цифровізація енергетичного сектору створює нові можливості для підвищення ефективності енергосистем, але водночас збільшує кількість потенційних кіберзагроз.

Практичні кейси кібератак на енергетичну інфраструктуру України та інших держав демонструють необхідність комплексного підходу до кіберзахисту. Ефективна система управління кіберризиками повинна поєднувати сучасні технології захисту, ефективний менеджмент, підготовку персоналу та міжнародні стандарти інформаційної безпеки.

Забезпечення кіберстійкості Smart Grid є необхідною умовою стабільного функціонування енергетики та гарантування енергетичної безпеки держави в умовах сучасних кіберзагроз.

1. Медвідь, В. Ю., Дячков, Д. В., Галич, О. А., Калініченко, О. В., & Лесюк, В. С. (Ред.). (2026). Вплив воєнного стану та політика повоєнного відновлення України: національні стратегії, регіональна безпека та стійкість громад [Колективна монографія]. ПП «Астрая». https://repository.mu.edu.ua/jspui/handle/123456789/10696.
2. Костюк, Ю. В., Складанний, П. М., Рзаєва, С. Л., Самойленко, Ю. О., & Коршун, Н. В. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Кібербезпека: освіта, наука, техніка, 2(30), 125–156.
3. Стойка, А. В., Верительник, С. М., & Мацука, В. М. (2025). Діджиталізація управління проєктами і вплив на світову економіку та інвестиції. Вчені записки, 39(2), 45–58. http://doi.org/10.33111/vz_kneu.39.25.02.04.026.032.
4. Cherep, A. V., Dashko, I. M., Ohrenych, Yu. O., Cherep, O. H., & Helman, V. M. (Eds.). (2025). European experience in the use of digital technologies in the economy [Collective monograph]. Baltija Publishing. European Experience Monograph. https://dspace.znu.edu.ua/xmlui/bitstream/handle/12345/26563/0063121.pdf?sequence=3#page=193.
5. Cherep, A. V., Dashko, I. M., Ohrenych, Yu. O., & Cherep, O. H. (Eds.). (2024). Theoretical and methodological foundations for the use of digital technologies in Ukraine through the implementation of EU experience [Collective monograph]. Publisher of FOP Mokshanov V.V. Digital Technologies in Ukraine Monograph https://dspace.znu.edu.ua/xmlui/handle/12345/24080.
6. Information Technology Laboratory. Computer Security Resource Center. (2014). Guidelines for Smart Grid Cybersecurity https://csrc.nist.gov/pubs/ir/7628/r1/final.

O.M. Dzhyhun

FORMATION OF THE OBJECTIVE FUNCTION IN PROBLEMS OF OPTIMIZING THE MODES OF THE ELECTRIC POWER SYSTEM

One of the main tasks of energy system management is to optimize load distribution between the power plants within the system based on the criterion of minimum fuel costs (or, more generally, the price per kilowatt-hour of generated electricity). Local control tasks for established modes, which are addressed by dispatch services at various levels of management of the energy system as a whole and its individual components, are considered in three aspects.

- territorial (from individual power plants to the system as a whole);
- temporary (from ensuring the daily load schedule to long-term planning for 5-10 years);
- situational (normal, deficit, emergency, etc. modes).

An electric power system is defined as a system designed to generate and transmit electricity to consumers via a transmission network to end-users. To create a practical and functional power system, the main components and characteristics of the power system have been developed: These components include hardware such as high-voltage power lines, underground cables, high-voltage transformers, nuclear, hydroelectric, or hydrothermal power plants, compensators, and so on. Electricity can be supplied in the form of direct or alternating current; however, at the beginning of the 20th century, alternating current was identified as the more economical and technically feasible solution. An electrical power system where the sources are alternating current is predominantly dynamic in nature, meaning that the current and the quantities dependent on it, such as voltage and the electrical power itself, vary over time [1].

In total, many subtasks of controlling the functioning of the electric power system (EPS) form a complex (both in the energy and mathematical sense) single multi-stage task of comprehensive optimization.

In this case, the complexity of the mathematical formulation of the final problem (determining the composition of generating capacities that ensures a minimum of costs for the production of energy to cover the load schedule) and the accuracy of its solution are determined by the type of functional dependencies that approximate the characteristics of individual units and the overall characteristics of power plants.

Formation of the objective function in the problems of optimizing the modes of the electric power system:

The main indicators used to evaluate the efficiency of EPS are the following:

- fuel consumption per kilowatt-hour of energy produced by power plants;
- electricity consumption for own needs of power plants;

- power losses in networks.

Modern approaches to solving the problem of optimizing the operating mode of a power system are based on the use of characteristics of relative increases in generating units [1−3].

The characteristics of relative increments are built on the basis of the dependences of the nominal fuel consumption (Q) on the load (P) obtained during the tests of the generating unit, the consumption characteristic ($Q=f(P)$) is defined as the dependence of the relative increment $q=dQ/dP$ on the load P.
In this case, the cost characteristic is a dependence

$$Q=Q_0+qP, \tag{1}$$

where Q_0 is the hourly consumption of conventional fuel at idle speed of the generating unit.

If the relative increase q does not depend on the load P, then the flow characteristic is linear; otherwise, it is nonlinear.

Based on dependence (1), the mathematical formulation of the problem of optimal loading of power plants in the energy system as a problem of mathematical programming can be formulated in the form: minimize the objective function

$$\Sigma \ \Sigma \ q_{ij}(P_{ij})P_{ij} \rightarrow \min, \tag{2}$$

$$(j=1, T)\ (i=1, k)$$

where k is the number of power plants in the energy system; T is the number of periods of operation of the energy system during which the load mode is optimized, P_{ij} is the load of the i-th power plant in the j-th period; q_{ij} is the value of the relative increase in the i-th power plant corresponding to the load in the j-th period under constraints of the type:

$$q_{ij}=f_i(P_{ij}); \tag{3}$$

$$P_i\min < P_{ij} < P_i\max . \tag{4}$$

Depending on the type of functions and variables included in (2)-(4), the problem of finding a favorable operating mode for a power system is defined as a linear, nonlinear, holistic or dynamic programming problem.

For specific types of characteristics of relative increases in power plants, various types of approximation by analytical functions must be investigated and target functions must be formed using them.

1. Gornshtein V.M,. Miroshnichenko B.P, Ponomarev A.V. Methods for Optimizing Power System Modes, etc. (edited by V.M. Gornshtein). – M.: Energy, 1981, 336 p.
2. Лесько В. О., Кулик В. В., Нетребський В. В. Оптимізація режимів електроенергетичних систем.− Вінниця, 2020, 138 с. https://pdf.lib.vntu.edu.ua/books/2024/Lesko_2020_138.pdf

3. Rainer Bacher Power system models, objectives and constraints in optimal power flow calculations/ Optimization in Planning and Operation of Electric Power Systems. Swiss Federal Institute of Technology (ETH) CH-8092 Zurich, Switzerland, Physica-Verlag (Springer), Heidelberg, May 93, pp. 217-264. https://link.springer.com/chapter/10.1007/978-3-662-12646-2_8.

Т.Т. Бондарук

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ РАННЬОГО ВИЯВЛЕННЯ ДЕГРАДАЦІЇ ВЕБСЕРВІСІВ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Сучасні об’єкти критичної енергетичної інфраструктури значною мірою залежать від вебсервісів, які забезпечують моніторинг, передавання даних і окремі функції телекерування. На практиці вебсервіс не завжди переходить від стабільного стану до повної відмови миттєво. Частіше цьому передує фаза деградації, коли поступово погіршуються окремі метрики: зростає час відповіді, збільшується споживання пам’яті, накопичується черга запитів або підвищується частота помилок.

На відміну від різких збоїв, такі процеси складніше виявляти традиційними пороговими механізмами, оскільки значення метрик певний час можуть залишатися близькими до допустимих меж. Al-Hawawreh та ін. [1] зазначають, що період між початком деградації та фактичною відмовою може створювати додаткові ризики для критичної інфраструктури. Тому раннє виявлення деградації має практичне значення, оскільки дає системі моніторингу більше часу для реагування до настання критичного стану.

Alkhaleel [2] у систематичному огляді підкреслює, що попри активне використання методів машинного навчання для захисту критичної інфраструктури, у багатьох роботах основна увага приділяється точності класифікації, тоді як час реакції системи аналізується менш детально. У зв’язку з цим доцільно порівнювати методи виявлення не лише за якістю класифікації, а й за тим, наскільки рано вони фіксують ознаки деградації.

Постановка задачі

Мета роботи – порівняти три класи методів виявлення аномалій за їхньою здатністю фіксувати деградацію вебсервісів до переходу системи у критичний стан. Об’єктом дослідження є часові ряди чотирьох телеметричних метрик: часу відповіді (latency), споживання пам’яті (memory), розміру черги (queue size) та частоти помилок (error rate).

Методи порівнюються за F1-score, precision, recall та умовним часом раннього виявлення (Lead). Показник Lead у цій роботі трактується як час випередження відносно заздалегідь визначеної контрольної точки переходу до критичного стану. Водночас цей показник не розглядається окремо від precision, оскільки надто раннє спрацювання може бути пов’язане не лише з кращою чутливістю, а й із ризиком хибних спрацювань.

Методи дослідження

У роботі порівнюються три підходи різної природи. Z-score використовується як статистичний критерій нормалізованого відхилення від

базової лінії стабільної зони. Алгоритм машинного навчання Isolation Forest визначає аномалії за глибиною ізоляції точки в ансамблі випадкових дерев; його застосування для аналізу вебсерверних журналів розглянуто, зокрема, у роботі [3]. Moving Average використовується як сигнальний метод: він згладжує локальне вікно спостережень і дає змогу виявляти трендові відхилення від базового стану, що може бути корисним для повільних деградаційних процесів [4].

Для зменшення кількості випадкових спрацювань застосовано правило K-of-N: деградація фіксується лише тоді, коли $k = 3$ з $N = 5$ послідовних значень перевищують заданий поріг. Таке правило використано як компроміс між стійкістю до шумових сплесків і здатністю реагувати на реальну зміну стану системи. Усі моделі навчаються лише на стабільній зоні, тобто на перших 100 точках із 500. Це зменшує ризик завищення результатів через потрапляння даних деградації до навчальної вибірки.

Експериментальна частина

Для перевірки методів сформовано чотири синтетичні сценарії деградації по 500 часових точок із кроком 10 с. Такий обсяг вибрано як компроміс між стабільністю оцінювання та простотою модельного стенда. Кожен сценарій має тризонну структуру: стабільна зона (0–100), зона розвитку деградації (100–250) та зона критичного стану або відмови (250–500, мітка = 1).

Умовний час раннього виявлення розраховується відносно контрольної точки 250, що відповідає моменту $t = 2500$ с. В цій роботі оцінюється не реальний фізичний початок зміни розподілу, а випередження відносно наперед заданої межі критичного стану. Це є важливим обмеженням синтетичного маркування, яке потрібно враховувати під час інтерпретації результатів.

Сценарії охоплюють такі типи деградації: memory leak – лінійне накопичення пам’яті та зростання латентності; latency growth – прискорене збільшення часу відповіді; queue overload – нелінійне переповнення черги; gradual drift – слабкий дрейф на тлі шуму ($\sigma = 30$ у. о.), що моделює складний для виявлення тип деградації.

Зведені результати порівняння наведено в таблиці 1.

Таблиця 1 – Порівняльні результати методів виявлення деградації

Сценарій	Метод	F1	Precision	Recall	Lead, с
Memory leak	Z-score	0,790	0,653	1,000	1310
Memory leak	Isolation Forest	0,787	0,649	1,000	1310

Memory leak	Moving Average	0,864	0,760	1,000	970
Latency growth	Z-score	0,778	0,636	1,000	1440
Latency growth	Isolation Forest	0,770	0,627	1,000	1410
Latency growth	Moving Average	0,845	0,731	1,000	2130
Queue overload	Z-score	0,774	0,631	1,000	1460
Queue overload	Isolation Forest	0,770	0,627	1,000	1440
Queue overload	Moving Average	0,840	0,725	1,000	2250
Gradual drift	Z-score	0,759	0,666	0,884	1470
Gradual drift	Isolation Forest	0,736	0,653	0,844	1470
Gradual drift	Moving Average	0,907	0,880	0,936	2450

Обговорення результатів

У межах проведеного модельного експерименту Moving Average показав найвищі значення F1-score у більшості сценаріїв. Найпомітнішою його перевага є у сценарії gradual drift, де F1 = 0,907, precision = 0,880, а recall = 0,936. Ймовірно, це пов’язано з тим, що згладжування краще накопичує слабкий, але тривалий сигнал деградації, який складно зафіксувати простими пороговими правилами.

Водночас результати не означають, що Moving Average є універсально найкращим методом. У сценарії memory leak він виявляє деградацію пізніше, ніж Z-score: Lead становить 970 с проти 1310 с. Це свідчить про компроміс між точністю та швидкістю реагування: вікно згладжування може підсилювати повільний сигнал, але водночас затримувати реакцію на ранні зміни.

Z-score та Isolation Forest у більшості сценаріїв демонструють близькі значення F1-score. У межах цього експерименту Isolation Forest не показав помітної переваги над простішим статистичним підходом. Це можна пояснити малою розмірністю вектора ознак, який містить лише чотири

метрики, а також синтетичним характером сценаріїв. Подібну закономірність узагальнено в роботі Mehedi та Azam [4], де зазначено, що складні ML-методи повніше розкривають потенціал на високо розмірних даних.

У сценарії gradual drift recall статистичних методів знижується до 0,844–0,884. Це означає, що за слабкого сигналу на тлі шуму частина деградаційних точок не фіксується. Саме цей сценарій добре показує практичну межу простих порогових підходів і пояснює, чому в системах моніторингу доцільно поєднувати методи різної природи.

З практичної точки зору отримані результати свідчать, що під час побудови систем раннього виявлення деградації важливо оцінювати не лише факт правильної класифікації, а й момент спрацювання методу відносно наближення критичного стану. Метод із вищим F1-score не завжди забезпечує найшвидшу реакцію, тому вибір підходу має залежати від характеру деградації та допустимого рівня хибних спрацювань.

Обмеження дослідження полягає в тому, що експеримент виконано на синтетичних часових рядах. Такі дані дають змогу контрольовано порівняти методи, однак спрощують реальні деградаційні процеси: не враховують сезонність, міжсервісні залежності, нерівномірність навантаження та можливі кореляції між компонентами інфраструктури. Тому отримані результати слід розглядати як модельну оцінку, яка потребує подальшої перевірки на реальних телеметричних даних.

Висновки

У роботі проведено порівняльний аналіз трьох методів виявлення деградації вебсервісів: статистичного Z-score, алгоритму машинного навчання Isolation Forest та сигнального методу Moving Average. Порівняння виконано за F1-score, precision, recall та умовним часом раннього виявлення відносно контрольної точки критичного стану.

За результатами модельного експерименту Moving Average забезпечив найвищі значення F1-score у більшості сценаріїв, особливо для gradual drift. Z-score показав конкурентні результати та в окремих випадках забезпечив швидшу реакцію. Isolation Forest у межах заданої малої розмірності ознак не продемонстрував помітної переваги над Z-score.

Отримані результати підтверджують, що для раннього виявлення деградації вебсервісів немає одного універсального методу. Доцільним є поєднання статистичних, сигнальних і ML-підходів, оскільки вони по-різному реагують на різкі зміни, поступовий дрейф і шумові коливання телеметричних метрик.

1. Al-Hawawreh, M., Baig, Z., & Zeadally, S. (2024). AI for critical infrastructure security: Concepts, challenges, and future directions. *IEEE Internet of Things Magazine*, *7*(4), 136–142. https://doi.org/10.1109/IOTM.001.2300181.

2. Alkhaleel, B. A. (2024). Machine learning applications in the resilience of interdependent critical infrastructure systems: A systematic literature review. *International Journal of Critical Infrastructure Protection*, *44*, 100646. https://doi.org/10.1016/j.ijcip.2023.100646.
3. Benova, L., & Hudec, L. (2024). Comprehensive analysis and evaluation of anomalous user activity in web server logs. *Sensors*, *24*(3), 746. https://doi.org/10.3390/s24030746.
4. Mehedi, Md., & Azam, S. (2024). A comprehensive investigation of anomaly detection methods in deep learning and machine learning: 2019–2023. *IET Information Security*, 8821891. https://doi.org/10.1049/2024/8821891.
5. Jadidi, Z., Pal, S., Hussain, M., & Nguyen, K. (2023). Correlation-based anomaly detection in industrial control systems. *Sensors*, *23*(3), 1561. https://doi.org/10.3390/s23031561.

О.В. Коломійцев, В.В. Пустоваров, О.Ю. Слободяник

УДОСКОНАЛЕНИЙ МЕТОД ГЛИБИННОГО НАВЧАННЯ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ТИПОВИХ ШАБЛОНІВ У PQ-ДАНИХ ПОКАЗНИКІВ ЯКОСТІ ЕЛЕКТРОЕНЕРГІЇ

Показники якості електроенергії (ПКЕ) – це сукупність параметрів, що визначають відповідність характеристик струму встановленим нормам (згідно з ДСТУ EN 50160). Відхилення цих показників від норми призводить до збоїв або пошкодження побутової та промислової техніки. До основних показників якості електричної енергії можливо віднести наступні: відхилення напруги і частоти, коефіцієнт нелінійних спотворень (гармоніки), розмах змін напруги (коливання напруги); провали, перенапруги та імпульси напруги, а також несиметрія напруг (у трифазних мережах).

Автоматизоване виявлення типових шаблонів у PQ-даних (Power Quality – показники якості електроенергії) – це процес моніторингу та аналізу електричних сигналів за допомогою алгоритмів машинного навчання (ML) та штучного інтелекту (AI). Такий підхід дозволяє точно виявляти відхилення, прогнозувати аварії та оптимізувати роботу мереж.

Використання методів глибинного навчання (Deep Learning) для аналізу PQ-даних є основним напрямком для сучасних інтелектуальних енергомереж. Такий підхід дозволяє автоматизувати виявлення аномалій та класифікацію типових збоїв. Залежно від типу даних та необхідного результату застосовують наступні архітектури нейронних мереж для PQ-даних:

– згорткові нейронні мережі (CNN) – аналізують графічні зображення сигналів (часові діаграми напруги/струму) або двовимірні спектрограми, отримані за перетворенням Фур'є або вейвлет-перетворення (CWT). Вони автоматично виділяють геометричні та текстурні шаблони;

– рекурентні мережі (LSTM/GRU) – використовуються для роботи з послідовностями у часовому вимірюванні (Time-series). Вони чудово розпізнають перехідні процеси та довготривалі зміни;

– гібридні моделі (CNN-LSTM) – поєднують просторовий аналіз згорткових шарів та здатність LSTM запам'ятовувати контекст у часі. За тким підходом забезпечується висока точність у виявленні багатокомпонентних збоїв;

– автоенкодери (Autoencoders) – застосовуються для навчання без вчителя (Unsupervised Learning). Вони вивчають нормальну форму синусоїди, що дозволяє мережі автоматично виявляти будь-які відхилення або шуми.

До основних етапів автоматизованої обробки даних можливо віднести наступні:

– збір даних – використання інтелектуальних лічильників та реєстраторів, які фіксують параметри (згідно зі стандартом IEC 61000-4-30);

– попередня обробка – очищення від шуму, нормалізація даних та часове виділення (Windowing) – розбиття безперервного сигналу на окремі вікна, що містять подію;

– виділення ознак (Feature Extraction) – замість ручного інжинірингу ознак, застосовуються математичні перетворення (STFT та DWT), які переводять 1D-сигнал у форму, придатну для обробки штучним інтелектом;

– класифікація – робота самої моделі глибинного навчання, яка маркує подію (на приклад, провал, перенапруга, імпульс, мерехтіння або гармоніки).

Удосконалено метод глибинного навчання для автоматизованого виявлення типових шаблонів у PQ-даних показників якості електроенергії. Метод складається з двох основних компонентів:

– багатошарового автоенкодера для зменшення розмірності даних та вилучення найважливіших ознак;

– алгоритму кластеризації *k*-середніх (*k*-means) для групування схожих ознак у кластери, які відповідають різним шаблонам поведінки параметрів якості електроенергії .

Метод дозволяє об’єднати можливості автоматичного навчання ознак глибинними нейронними мережами із силою простих некерованих алгоритмів кластеризації для інтелектуального аналізу PQ-даних. Він працює за наступними послідовними етапами:

– попередня обробка та формування добових послідовностей із вихідного довготривалого ряду PQ-даних;

– глибинне автоенкодерне кодування, яке перетворює кожну добову послідовність на набір основних ознак;

– кластеризація отриманих ознак методою *k*-середніх для виділення груп схожих днів та візуалізація простору ознак та перевірка утворених кластерів у нижчій розмірності (наприклад, методом t-SNE);

– декодування (відновлення) представницьких добових сигналів для кожного кластера за допомогою декодера автоенкодера;

– емпіричний аналіз та експертна інтерпретація отриманих шаблонів з метою встановлення їх фізичної природи.

Таким чином, удосконалений метод працює без вчителя – після тренування автоенкодера результати кластеризації автоматично виділяють типові шаблони, які надалі підлягають експертному тлумаченню.

1. Коломійцев О.В., Слободяник О.Ю., Комаров В.О., Катунін А.М., Рикун В.Г., Кібальник В.М., Слободенюк Ю.В., Василець Д.О., Сапон В.І., Камишинський О.М., Хабоша С.М., Кувшинова О.С. Аналіз даних показників якості електроенергії в умовах цифровізації енергосистем. *ГРААЛЬ НАУКИ*: *міжнар. наук. журнал*. – Вінниця: ГО «Європейська наукова платформа»; НУ «Інститут науково-технічної інтеграції та співпраці», 2026. – No 68. – С. 1046-1062. https://doi.org/10.36074/grail-of-science.15.05.2026.

М.Л. Дранік

ВПЛИВ КІБЕРАТАК НА ПРОФІЛЬ ЕЛЕКТРОСПОЖИВАННЯ МІКРОМЕРЕЖ З ВДЕ У ЛІКАРНЯХ ТА НАСЛІДКИ ДЛЯ ПРОГНОЗУВАННЯ ПОПИТУ НА ЕЛЕКТРОЕНЕРГІЮ

1. Вступ

Інтеграція мікромереж на базі відновлюваних джерел енергії у закладах охорони здоров'я розглядається як один із пріоритетних напрямів підвищення енергетичної автономності та стійкості критичної соціальної інфраструктури. Водночас цифровізація таких систем, що передбачає використання інверторів, локальних контролерів, систем диспетчеризації, засобів віддаленого моніторингу та обміну даними, формує додаткові кіберфізичні вразливості, за яких порушення інформаційного контуру здатні трансформуватися у відхилення режимів електроспоживання. За матеріалами ENISA, у європейському секторі охорони здоров'я ransomware (програмне забезпечення-вимагач) становив 54% зафіксованих кіберзагроз, а серед найбільш уражених суб'єктів домінували саме надавачі медичних послуг і лікарні. Це свідчить про те, що кібербезпека лікарняних енергетичних систем є важливою не лише з точки зору інформаційного захисту, а й у контексті забезпечення енергетичної безпеки та надійності функціонування соціальної інфраструктури [1, 2, 3, 4].

2. Мета і завдання дослідження

Метою дослідження є обґрунтування впливу кібератак на профіль електроспоживання мікромереж з ВДЕ у лікарнях та визначення наслідків цього впливу для прогнозування попиту на електроенергію на різних ієрархічних рівнях. Для досягнення цієї мети поставлено такі завдання: проаналізувати характерні типи кібератак на мікромережі; визначити механізми зміни фактичного та виміряного профілю навантаження внаслідок атак; встановити, яким чином такі зміни впливають на якість прогнозування попиту; обґрунтувати доцільність урахування кіберзагроз у сценарному та багаторівневому моделюванні енергоспоживання закладів соціальної інфраструктури [5, 6].

3. Основні результати

Встановлено, що кібератаки на мікромережі з ВДЕ можуть змінювати профіль електроспоживання лікарні трьома основними способами.

По-перше, втручання в роботу інверторів, контролерів і систем диспетчеризації здатне призводити до часткової або повної втрати внеску локальної генерації та накопичувачів енергії, внаслідок чого зростає відбір потужності із зовнішньої мережі у години, коли навантаження мало б покриватися за рахунок ВДЕ [7, 8].

По-друге, порушення алгоритмів керування може викликати додаткові піки, провали та коливання навантаження через розбалансування режимів мікромережі [7, 8].

По-третє, атаки на цілісність вимірювальних даних створюють спотворене інформаційне уявлення про електроспоживання навіть за відносно незмінного фізичного режиму роботи об'єкта [7, 8].

Показано, що такі спотворення мають важливі наслідки для прогнозування попиту на електроенергію. Якщо історичні часові ряди навантаження містять аномалії, викликані кібератаками або хибною телеметрією, моделі прогнозування інтерпретують їх як нові закономірності функціонування закладу, що призводить до зміщення оцінок тренду, сезонності та пікових навантажень. На рівні окремого закладу це означає зниження точності прогнозу, а в умовах багаторівневого моделювання такі похибки агрегуються на регіональному та національному рівнях. Таким чином, кібератаки слід розглядати не лише як загрозу безперервності електропостачання, але і як фактор викривлення прогнозного попиту на електроенергію [6, 9].

Додатково встановлено, що проблема має виражений економічний вимір. У дослідженні, проведеному на матеріалах публічної системи охорони здоров'я Португалії, у 2017–2022 роках було ідентифіковано шість кіберінцидентів у державних лікарнях, а оцінений економічний ефект одного інциденту становив від 115 882,96 до 2 317 659,11 євро залежно від масштабу порушення діяльності та частки уражених ресурсів. Це підтверджує, що ігнорування кіберризиків у процесі впровадження цифрових енергетичних рішень у лікарнях може призводити не лише до технічних, а й до суттєвих фінансових втрат [7].

4. Висновки та перспективи подальших досліджень

Отже, кібератаки на мікромережі з ВДЕ у лікарнях можуть змінювати як фактичний, так і виміряний профіль електроспоживання, що безпосередньо впливає на достовірність прогнозування попиту на електроенергію. Урахування цього фактора є необхідним для побудови адекватних моделей прогнозування на рівні закладу, регіону та країни, особливо в умовах зростання частки децентралізованої генерації у соціальній інфраструктурі. Перспективи подальших досліджень пов'язані з розробленням сценарних і робастних моделей прогнозування, які дозволятимуть формалізувати вплив різних типів кібератак на енергоспоживання лікарняних мікромереж та враховувати кіберстійкість як окремий параметр енергетичного планування [1, 6, 7].

1. Zhang, Z., Turnbull, B., Kermanshahi, S. K., Pota, H., Damiani, E., Yeun, C. Y., & Hu, J. (2025). A survey on resilient microgrid system from cybersecurity perspective. *Applied Soft Computing Journal*, *175*, Article 113088. https://doi.org/10.1016/j.asoc.2025.113088.
2. European Commission. (2025, January 14). *Bolstering the cybersecurity of the healthcare sector*. https://commission.europa.eu/news-and-media/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en.
3. European Commission. (2025, January 14). *European action plan on the cybersecurity of hospitals and healthcare providers*. https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en.
4. European Union Agency for Cybersecurity. (2023). *ENISA threat landscape: Health sector*. ENISA. https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf.
5. Rouhani, Seyed Hossein & Su, Chun-Lien & Mobayen, Saleh & Razmjooy, Navid & Elsisi, Mahmoud, 2024. "Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions," Energy, Elsevier, vol. 309(C). DOI: 10.1016/j.energy.2024.133081.
6. Arash Moradzadeh, Mostafa Mohammadpourfard, Charalambos Konstantinou, Istemihan Genc, Taesic Kim, Behnam Mohammadi-Ivatloo, Electric load forecasting under False Data Injection Attacks using deep learning, Energy Reports, Volume 8, 2022, Pages 9933-9945, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2022.08.004.
7. Portela, D., Nogueira-Leite, D., Almeida, R., & Cruz-Correia, R. (2023). Economic Impact of a Hospital Cyberattack in a National Health System: Descriptive Case Study. JMIR formative research, 7, e41738. https://doi.org/10.2196/41738.
8. Martine Chlela, Geza Joos, and Marthe Kassouf. 2016. Impact of cyber-attacks on islanded microgrid operation. In Proceedings of the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems (RSES '16). Association for Computing Machinery, New York, NY, USA, Article 1, 1–5. https://doi.org/10.1145/2939940.2939943.
9. Yize Chen, Yushi Tan, Ling Zhang and Baosen Zhang «Vulnerabilities of Power System Operations to Load Forecasting Data Injection Attacks», https://ar5iv.labs.arxiv.org/html/1906.04926.

М.В. Зеліско, З.Л. Рибчак, О.А. Басистюк

МЕТОДИ МОНІТОРИНГУ ТА ПРОГНОЗУВАННЯ ЕНЕРГОСПОЖИВАННЯ НА ОСНОВІ МУЛЬТИСЕНСОРНИХ ДАВАЧІВ ІНФОРМАЦІЇ

Сучасна Об'єднана енергосистема (ОЕС) [1] України є однією з найбільших і найскладніших кіберфізичних систем Європи. Умови її функціонування суттєво ускладнилися після історичної синхронізації з континентальною мережею ENTSO-E [2] у березні 2022 року, що висунуло жорсткі вимоги до дотримання балансових зобов'язань та операційної безпеки згідно з європейськими регламентами.

Відповідно до Закону України «Про ринок електричної енергії», НЕК «Укренерго» як системний оператор зобов'язаний забезпечувати суворий баланс між попитом і пропозицією в режимі реального часу, підтримуючи стабільність частоти та напруги. Успішне виконання цього завдання безпосередньо залежить від якості прогнозування навантаження та точності формування диспетчерських графіків [3].

Проте сьогодні традиційні математичні моделі прогнозування стикаються із комплексом критичних ускладнень, таких як нестаціонарність процесів, а саме сезонності, піків споживання, особливостей споживання при запровадженні обмежень системним оператором або введенні обмежень на споживання. Окремим чинником є чутливість споживання до температурних коливань (опалення взимку та кондиціонування влітку) [4].

За таких умов класичних історичних даних енергоспоживання вже недостатньо для точного балансування системи. Виникає гостра потреба у впровадженні методів моніторингу та прогнозування на основі мультисенсорних давачів інформації.

Ключова наукова цінність даного дослідження, полягає у науковому обгрунтуванні доцільності інтеграції мультисенсорних систем в єдиний аналітичний простір не лише погодинні дані про фактичне споживання, а й різнорідні зовнішні чинники (динамічні метеорологічні параметри, телеметричні дані стану мережі, регіональні індикатори навантаження).

Це забезпечує оперативний моніторинг і побудову гнучких, адаптивних моделей прогнозування на горизонтах 24 години, 7 та 30 діб, що є критично важливим для забезпечення живучості та енергетичної безпеки України в кризових умовах.

На основі проведеного аналізу предметної області сформульовано задачу моніторингу та прогнозування енергоспоживання в ОЕС України з використанням мультисенсорних давачів інформації та методів інтелектуального аналізу даних. Для дослідження використано погодинні часові ряди фактичного споживання електроенергії, метеорологічні

параметри, календарні ознаки та індикатор воєнного стану, що дозволило врахувати як сезонні, так і кризові фактори впливу на енергосистему. У межах роботи виконано порівняльний аналіз кількох моделей прогнозування на трьох аналітичних сегментах даних - загальному, довоєнному та воєнному із використанням метрик MAE та RMSE для оцінювання точності прогнозів.

Отримані результати підтвердили ефективність сегментованого підходу до навчання моделей та доцільність поєднання класичних статистичних методів із адаптивними алгоритмами прогнозування для роботи в умовах нестабільності енергетичної інфраструктури. Практичним результатом дослідження став програмний застосунок, який автоматизує повний цикл обробки даних від збору та зберігання інформації у реляційній базі даних до побудови прогнозів і візуалізації показників якості моделей та може бути використаний як система підтримки прийняття рішень у сфері енергетичного моніторингу й управління енергоспоживанням.

$$MAE = \frac{1}{n}\sum_{i=1}^{n} | y_i - \hat{y}_i| \tag{1}$$

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

Для візуалізації послідовності етапів обробки даних та взаємодії між учасниками процесу було розроблено відповідну модель у нотації BPMN. Узагальнену схему моніторингу та прогнозування енергоспоживання на основі мультисенсорних давачів, яка відображає логіку проходження інформаційних потоків від моменту збору даних до отримання фінального результату, наведено на рис. 1.

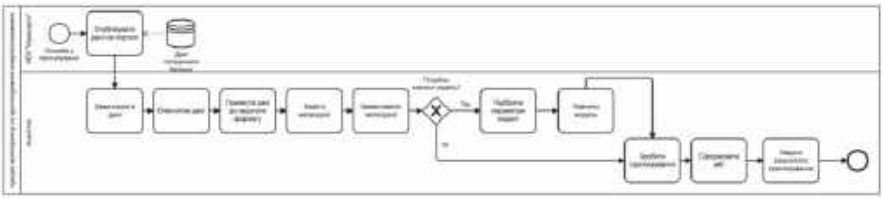


Рисунок 1 – Схема моніторингу та прогнозування енергоспоживання на основі мультисенсорних давачів

Аналіз отриманих результатів дає змогу простежити низку характерних тенденцій. Зокрема, модель Linear Regression показує найменші значення MAPE у сегменті pre_war: 1,33% для горизонту прогнозування 24 години, 1,54% для 7 днів та 1,11% для 30 днів. Це свідчить про відносно стабільний і

лінійний характер енергоспоживання у довоєнний період. У сегменті post_war рівень похибки дещо зростає, що може бути пов’язано зі збільшенням нестабільності та зміною структури споживання електроенергії.

Таблиця 1 – Результати порівняльного аналізу моделей прогнозування енергоспоживання на основі мультисенсорних давачів у різних часових проміжках

Модель	Часовий горизонт	Сегмент	MAE
Linear Regression	24h	All	9 212,57
Linear Regression	7d	Pre_war	5 171,90
Linear Regression	30d	Post_war	6 341,53
ARIMA	24h	All	8 087,20
ARIMA	30d	Pre_war	47 556,80
ARIMA	24h	Post_war	5 006,39
Prophet	30d	All	55 626,06

У результаті проведеного дослідження методів моніторингу та прогнозування енергоспоживання на основі мультисенсорних давачів інформації встановлено, що найбільш ефективними для задач оперативного аналізу енергосистем є лінійні моделі прогнозування, які забезпечують високу точність та стабільність результатів навіть в умовах значної динаміки навантажень. Показано, що класичні моделі часових рядів типу ARIMA демонструють прийнятну ефективність лише для короткострокових прогнозів, тоді як їх точність суттєво погіршується на середньострокових горизонтах у періоди структурних змін. Водночас моделі, орієнтовані на історичну сезонність, виявили низьку адаптивність до кризових та форс-мажорних умов функціонування енергетичної інфраструктури. Доведено доцільність сегментації даних за характером режимів роботи системи, що дозволяє підвищити точність прогнозування шляхом навчання моделей на однорідних наборах даних. Отримані результати підтверджують ефективність використання мультисенсорних систем збору даних у поєднанні з адаптивними алгоритмами аналізу для побудови інтелектуальних систем підтримки прийняття рішень у сфері енергомоніторингу та прогнозування енергоспоживання.

1. Міністерство енергетики України. (2019). Про ринок електричної енергії (Закон України № 2019-VIII). Верховна Рада України. Закон України «Про ринок електричної енергії».
2. ENTSO-E. (2026). European Network of Transmission System Operators for Electricity. Retrieved May 25, 2026, from https://www.entsoe.eu/.
3. Rakhimzhanova, A., Zhakiyev, N., & Nugumanova, A. (2026). Short-Term Hydropower Generation Forecasting for Operational Planning and Early Energy Procurement: Multi-Model Evidence from Kazakhstan. Energies, 19(11), 2520. https://doi.org/10.3390/en19112520.
4. Wang, Y., Wang, Z., Wang, P., & Sang, Y. (2026). Development of Experimental System for a Novel Piston Gravity Energy-Storage System. Energies, 19(11), 2543. https://doi.org/10.3390/en19112543.

В.С. Комарніцький, С.В. Калякін

ОПТИМІЗАЦІЯ МЕТОДІВ ДЕТЕКЦІЇ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ ЗАСТОСУВАННЯ ТЕХНІК ОБФУСКАЦІЇ ТА УХИЛЕННЯ

Зростання складності шкідливого ПЗ (ШПЗ) у 2024–2025 роках зумовлене рекордною кількістю нових вразливостей понад 21 500 CVE лише за перше півріччя 2025 року, що створює близько 133 векторів атак щодня [1]. В Україні, за даними CERT-UA, кількість інцидентів зросла на 37,4%, де шкідливий код залишається ключовим фактором загрози [2]. Глобальні масштаби розповсюдження ШПЗ призводять до колосальних економічних збитків, які до кінця 2025 року можуть сягнути 10,5 трильйонів доларів США. За таких умов, коли середня вартість витоку даних становить 4,44 мільйона доларів [3], удосконалення методів аналізу стає критичною потребою для забезпечення кібербезпеки.

Метою дослідження є оптимізація процесу виявлення новітніх кіберзагроз шляхом визначення меж ефективності статичного та динамічного аналізу та обґрунтування їхньої синергії для подолання технік обфускації та ухилення від детекції (anti-VM/anti-debugging).

Дослідження H. Zhang [4] та B. Pargi [5] підтверджують ефективність гібридних систем, що використовують машинного навчання для аналізу статичних (ентропія, заголовки) та динамічних (API-виклики) ознак ШПЗ. Праці П. Г. Регіди [6] акцентують на впровадженні розподілених систем для виявлення поліморфних загроз. Проте розробленим підходам бракує адаптивності до новітніх технік anti-VM та anti-debugging, а також актуальних наборів даних (datasets) періоду 2025–2026 років для аналізу еволюціонуючого коду.

Необхідність оптимізації засобів детекції шкідливого ПЗ зумовлена стрімким зростанням збитків від прихованих кібератак, спрямованих на несанкціоноване перехоплення конфіденційних даних та клавіатурного вводу. У матеріалах наукової публікації Калякіна С.В., Загорецької Є.Р. [7] наголошується, що однією з ключових проблем кібербезпеки в Україні є потреба у розробці та практичній апробації методів оцінки ефективності засобів захисту інформації.

Сучасні розробники шкідливого програмного забезпечення масово відмовляються від простих статичних сигнатур на користь багатопотокових специфічних тригерів ухилення від детекції (зокрема, інтелектуальних технік anti-VM та anti-debugging). Існуючі автоматизовані моделі часто демонструють високий рівень хибнонегативних спрацьовувань (False Negative), оскільки розраховані на роботу зі застарілими наборами даних

(datasets), які не відображають поведінкові патерни ШПЗ останнього покоління.

У межах практичного етапу дослідження було реалізовано двоетапну процедуру аналізу сучасного шкідливого програмного забезпечення з метою верифікації його прихованих функцій та оцінки меж ефективності застосованого інструментарію. Як тестовий об'єкт використовувався верифікований зразок ШПЗ із відкритих репозиторіїв.

На першому етапі за допомогою статичних інструментів досліджувалася архітектура файлу без його активації, а на другому — об'єкт переводився в активний стан у пам'яті всередині ізольованого середовища для подолання тригерів ухилення. Емпіричні результати фіксації технічних параметрів та поведінкових патернів досліджуваного зразка деталізовано та систематизовано у табл. 1.2.

Таблиця 1.2 — Інструментальні результати статичного та динамічного аналізу ШПЗ

Етап дослідження та інструмент	**Об'єкт та показники моніторингу**	**Зафіксована активність та технічні параметри зразка**	**Науково-практичний висновок (Ознаки детекції та протидії)**
Статичний: Detect It Easy, PE-bear	Заголовки файлу, сигнатури, таблиця імпорту (IAT)	Визначено архітектуру PE. Виявлено високу ентропію окремих секцій файлу (7.5 - 7.9), реальний імпорт DLL прихований.	Аномалія: Висока ентропія свідчить про глибоку обфускацію коду з метою приховування сигнатур від антивірусів. Статичний аналіз обмежений через пакувальники.
Динамічний: Any.Run, ProcMon	Процес у пам'яті, системні виклики, мережева активність	Фіксація створення дочірніх процесів, модифікація ключів реєстру (автозавантаження). HTTP/DNS-запити до командного сервера (C2).	Поведінковий патерн: ШПЗ намагалося виконати техніки anti-VM/anti-debugging. Після імітації дій користувача захист подолано і зафіксовано алгоритм закріплення в ОС та IoC.

Для розв'язання проблеми хибнонегативних спрацьовувань та обходу захисних механізмів на основі отриманих емпіричних даних було розроблено правила взаємодоповнюваності методів. Схему оптимізації процесу дослідження кіберзагроз завдяки синергетичному ефекту поєднання структурного та поведінкового аналізу наведено у табл. 1.3.

Таблиця 1.3 — Матриця оптимізації детекції на основі синергії методів

Маркер аномалії (Статика)	**Обмеження методу (Проблема)**	**Рішення через динамічний підхід**	**Підсумковий синергетичний результат дослідження**
Аномальна ентропія секцій файлу (>7.5).	Класичні антивіруси видають False Negative (пропуск загрози) через обфускацію та пакування.	Інтерактивний запуск в Any.Run дозволяє упакованому коду саморозпакуватися в оперативній пам'яті.	Отримано повний зліпок поведінки та логіки ШПЗ в обхід будь-яких статичних крипторів.
Прихована таблиця імпорту (IAT).	Неможливо сигнатурно визначити, які функції (мережеві, файлові) викликає програма.	Локальний моніторинг ProcMon перехоплює реальні API-виклики під час виконання операцій в ОС.	Ідентифіковано конкретні механізми модифікації реєстру для забезпечення персистентності ШПЗ.
Наявність потенційних anti-VM тригерів.	Програма розпізнає автоматичну пісочницю і завершує роботу, приховуючи деструктивні функції.	Інтерактивна підміна поведінкових факторів та емуляція дій користувача в середовищі Any.Run.	Спровоковано активацію прихованих функцій ШПЗ, що дозволило перехопити IP-адреси командного сервера.

Результати комплексного компаративного аналізу меж ефективності методів продемонстрували, що ізольоване використання статичного або динамічного підходу за умов сучасної архітектури ШПЗ призводить до критичного підвищення ризиків False Negative спрацьовувань. Практична цінність роботи полягає у формуванні стійких правил кореляції (синергії методів), де первинні статичні маркери утиліти PE-bear (зокрема, критичний

рівень ентропії коду) виступають індикаторами для адаптивного налаштування динамічного середовища та інтерактивного обходу anti-debugging і anti-VM тригерів у пісочниці Any.Run. Майбутні етапи дослідження будуть спрямовані на автоматизацію побудованої гібридної моделі детекції із залученням інструментів штучного інтелекту для деобфускації в реальному часі.

1. Vulnerabilities Statistics 2025: Record CVE Surge. DeepStrike. URL: https://deepstrike.io/blog/vulnerability-statistics-2025 (дата звернення: 26.03.2026).
2. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: які були атаки - Юридична Газета. Юридична газета – онлайн версія. URL: https://yur-gazeta.com/golovna/certua-u-2025-roci-opracyuvala-mayzhe-6000-kiberincidentiv-yaki-buli-ataki.html (дата звернення: 26.03.2026).
3. $213 Billion Cybersecurity Spending in 2025. Hype or Hoax? - XenTegra. XenTegra. URL: https://xentegra.com/resources/213-billion-cybersecurity-spending-in-2025-hype-or-hoax/ (дата звернення: 26.03.2026).
4. Government-Led Digital Governance and the Digital Divide Among Cities: Implications for Sustainable Digital Transformation in China / C. Zhang et al. Sustainability. 2025. Vol. 17, no. 23. P. 10700. URL: https://doi.org/10.3390/su172310700 (дата звернення: 26.03.2026).
5. Bhavik Pargi, Dr. Sheshang Degadwala, Malini Joshi. Hybrid Malware Analysis using Static and Dynamic Techniques with Machine Learning. International Journal of Scientific Research in Science, Engineering and Technology. 2026. Vol. 13, no. 1. P. 22–27. URL: https://doi.org/10.32628/ijsrset2613101 (дата звернення: 26.03.2026).
6. Концепція застосування розподілених систем для аналізу поліморфних вірусів / П. Регіда, О. Бармак, А. Каштальян, Е. Манзюк // Вісник Хмельницького національного університету. Технічні науки. - 2024. - № 1. - С. 38-43.
7. Загорецька, Є. Р. Проблема захисту інформації в Україні / Загорецька Єлизавета Романівна, Калякін Сергій Володимирович // Застосування інформаційних технологій у діяльності правоохоронних органів: матеріали круглого столу (м. Харків, 14 груд. 2021 р.) / МВС України, Харк. нац. ун-т внутр. справ., Каф. кібербезпеки та DATA-технологій. – Харків: ХНУВС, 2021. – С. 55-57.

А.М. Катунін, О.В. Коломійцев, В.В. Пустоваров

УДОСКОНАЛЕНИЙ СПОСІБ ЗАХИСТУ НАЗЕМНИХ ОБ'ЄКТІВ ВІД ЗАСОБІВ ПОВІТРЯНОГО НАПАДУ ПРОТИВНИКА, ОСНАЩЕНИХ ЛАЗЕРНИМИ СИСТЕМАМИ НАВЕДЕННЯ

Захист наземних об'єктів (зразків озброєння та військової техніки) від засобів повітряного нападу (ЗПН) противника, оснащених лазерними системами наведення (керовані авіабомби, ракети, безпілотні літальні апарати (БпЛА) тощо) досягається комбінацією пасивних і активних заходів, які спрямовані на зрив підсвічування цілі, створення перешкод для головки самонаведення (ГСН) або фізичного знищення носія. Основні способи захисту поділяються на наступні категорії: пасивний захист (маскування та дезорієнтація) – аерозольні та димові завіси, поглинаючі покриття, хибні цілі та відбивачі, а також оптичні пастки; радіоелектронна боротьба та системи попередження – системи попередження про опромінення та пригнічення каналів управління (БпЛА), а також активний захист та фізичне знищення – системи активного захисту та вогневе ураження.

Протидія оптико-електронним системам (ОЕС) наведення, зокрема лазерним системам (ЛС), боєприпасів є основним елементом захисту військових та цивільних об'єктів. При цьому, результатами протидії можуть бути як ураження складових систем наведення, так і навмисне викривлення оптичної інформації, яка реєструється сенсорами ОЕС наведення.

На даний час існує декілька відомих способів захисту наземних об'єктів, які передбачають застосування димових піротехнічних засобів для постановки димових завіс, а також дифракційно відбивних покриттів для формування на підстильної поверхні світлових плям – оптичних перешкод для головок самонаведения ракет [1; 2]. Дані способи захисту об'єктів від ЗПН противника, оснащених ЛС наведення, мають відповідні недоліки, а саме: залежність ефективності димових завіс від частоти випромінювання лазерної станції підсвічування цілей, а також складність технічної реалізації способів захисту, що передбачають використання дифракційно відбивних покриттів.

Таким чином, актуальним завданням є розробка пропозицій щодо удосконалення способів захисту наземних об'єктів від ЗПН противника, оснащених ЛС наведення для одночасного забезпечення зниження оптичної помітності об'єктів та придушення ЛС наведення ЗПН противника.

Одним зі шляхів вирішення даного завдання є одночасне використання димових піротехнічних засобів та світлоповертальних елементів. Отже, удосконалений спосіб захисту наземних об'єктів від ЗПН противника, оснащених ЛС наведення, має базуватися на використанні димових піротехнічних засобів для формування димових завіс та застосуванні світлоповертальних елементів для створення об'ємної області оптичних перешкод в полі зору ЛС наведення ЗПН противника.

Формування димових завіс забезпечує зниження оптичної помітності наземних об’єктів, а створення об'ємної області оптичних перешкод в полі зору ЛС наведення – придушення систем наведення ЗПН противника.

Об'ємна область оптичних перешкод створюється застосуванням світлоповертальних елементів, які відбивають (повертають) падаюче оптичне випромінювання в напрямах, близьких до напряму підсвічування елементів та характеризуються високим значенням коефіцієнту світлоповернення.

Високе значення коефіцієнту світлоповернення має місце при умовах, коли кут підсвічування поверхні елементу складає -30º…+30º для неметалізованих світлоповертальних елементів та -45º…+45º – для металізованих світлоповертальних елементів, що визначає більшу ефективність застосування металізованих світлоповертальних елементів.

Робота удосконаленого способу захисту наземних об’єктів від ЗПН противника, оснащених ЛС наведення здійснюється за наступними етапами. При виявленні лазерної станції підсвічування та ЗПН противника, оснащеного ЛС наведення, визначають напрями на лазерну станцію підсвічування та ЗПН противника. На основі отриманих даних здійснюють застосування димових піротехнічних засобів для зниження оптичної помітності наземного об’єкту шляхом створення димової завіси в напрямках виявлених лазерної станції підсвічування та ЗПН противника. Зниження оптичної помітності об’єкту відбувається за рахунок ослаблення лазерного випромінювання в димової завісі. Одночасно з цим відбувається застосування (відстріл) світлоповертальних елементів у напрямку лазерної станції підсвічування для створення об'ємної області оптичних перешкод в полі зору ЛС наведення ЗПН противника таким чином, щоб центр об'ємної області оптичних перешкод знаходився на осі, яка з’єднує наземний об’єкт, що захищається, та лазерну станцію підсвічування. Світлоповертальні елементи, що створюють об'ємну область оптичних перешкод, відбивають (повертають) лазерне випромінювання підсвічування в напрямі, який є близьким до напряму підсвічування, а значить, до напряму на ЗПН противника, оснащеного ЛС наведення, що призводить до придушення системи наведення. У залежності від параметрів світлоповертальних елементів, щільності в повітрі світлоповертальних елементів та відстані між областю оптичних перешкод та ЛС наведення ЗПН противника можливо досягнення короткочасного або довготривалого придушення системи наведення.

1. Патент на корисну модель №147508, Україна, МПК G08B 25/00 G02B 27/44. Спосіб індивідуального захисту зразків бронетанкової техніки від ракет, оснащених напівактивними лазерними системами наведення / А.М. Катунін, О.В. Кулаков, С.В. Рудаков та ін. – № u2021 000 27; заяв. 04.01.2021; опубл. 12.05.2021; Бюл. №19. – 4 с.
2. Маскування військ та об’єктів. Захист від високоточної зброї: навч. посіб. / В.В. Пугач, В.П. Чепурний, А.І. Куртов та ін. Харків: ВІОІ НЮУ ім. Ярослава Мудрого, 2022. – 116 с.

УДК 621.31:004.056.5

П.О. Сідлярчук

АПАРАТНО-ВКОРІНЕНА ВЕРИФІКАЦІЯ ВИРОБНИЦТВА ВІДНОВЛЮВАНОЇ ЕЛЕКТРОЕНЕРГІЇ ЯК ЗАСІБ ПРОТИДІЇ ШАХРАЙСТВУ В ОБЛІКУ ЗЕЛЕНОЇ ЕНЕРГІЇ ТА ШАР КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У роботі розглянуто архітектуру системи, що криптографічно захищає первинні дані виробництва відновлюваної електроенергії від маніпуляцій з боку будь-якого учасника ринку — власника генеруючого об'єкта, продавця гарантій походження, покупця або оператора реєстру. Запропоноване рішення спрямоване на викорінення системного шахрайства в обліку зеленої електроенергії: завищення обсягів виробництва, подвійного продажу сертифікатів, видачі гарантій походження за неіснуючою генерацією. Архітектура базується на принципі нейтральності даних: показники лічильників підписуються приватним ключем, що зберігається в апаратно захищеному модулі і не підлягає експорту, після чого записуються у незмінний розподілений реєстр і доступні для незалежної верифікації будь-яким зацікавленим учасником без необхідності довіри до самого оператора системи. Реалізовано п'ятишаровий захисний контур, що включає захищені сенсорні пристрої, сервіс агрегації, докази з нульовим розголошенням, розумні контракти на сумісних з Ethereum мережах та шар публічної верифікації. Подано результати незалежних аудитів безпеки: статичний аналіз Slither (0 знахідок високого та середнього ризику), символьне виконання Mythril (0 легітимних вразливостей), тестування на основі властивостей з випадковими даними Echidna (понад 100 мільйонів викликів без порушення інваріантів), 91,88% покриття коду модульними тестами. Розглянуто співвідношення архітектури з регуляторними вимогами Європейського Союзу: Директивою RED III та Механізмом коригування вуглецевих кордонів CBAM. Сформульовано перспективні напрями впровадження для українського енергетичного сектору в контексті післявоєнного відновлення та європейської інтеграції.

Ключові слова: кібербезпека енергетики, протидія шахрайству в енергетиці, верифікація виробництва електроенергії, апаратно-вкорінене засвідчення, криптографічний захист обліку, докази з нульовим розголошенням, критична інфраструктура, відновлювана електроенергетика, Директива RED III, Механізм CBAM.

1. Постановка проблеми: системне шахрайство в обліку відновлюваної електроенергії

Світовий ринок гарантій походження зеленої електроенергії оцінюється в понад 10 мільярдів доларів США щорічно і продовжує зростати. Зі збільшенням обсягів цього ринку пропорційно зростають і можливості для шахрайства, що набувають системного характеру в усьому ланцюжку обліку відновлюваної генерації.

Основні джерела ризиків можна звести до чотирьох категорій:

— маніпуляція показниками лічильників з боку власника генеруючого об'єкта з метою завищення обсягів виробництва та отримання неправомірних доходів від продажу гарантій;

— подвійний продаж однієї одиниці гарантії походження різним покупцям через прогалини в міжкордонних реєстрах та відсутність єдиного джерела істини;

— створення фантомних показників, що не мають фізичного підкріплення реальною генерацією, через компрометацію або несправності первинних систем обліку;

— видача сертифікатів зеленої електроенергії за фактично відсутньою або тепловою генерацією через корупційну змову операторів реєстру з виробниками.

Поточна архітектура довіри в енергетичному обліку базується на припущенні чесності всіх ланок ланцюга — виробника, оператора реєстру, аудитора, контрагента. Це припущення вже неодноразово виявлялося безпідставним. Журналістські розслідування 2022—2025 років у країнах Європейського Союзу зафіксували численні випадки видачі гарантій походження за неіснуючою генерацією, перепродажу одного й того ж сертифікату декільком покупцям, маніпуляції часовою прив'язкою для отримання преміальної ціни на ринку погодинних гарантій.

Кореневою причиною цих явищ є концентрація довіри у двох-трьох вузлах ланцюга обліку. Поки існує технічна можливість впливу на первинний показник з боку будь-кого з учасників ринку — власника генерації, продавця, покупця або оператора реєстру — система залишається схильною до шахрайства, незалежно від кількості зовнішніх аудитів та формальних процедур.

Регуляторні зрушення Європейського Союзу — Директива RED III щодо обов'язковості погодинних гарантій походження з 2026 року та Механізм коригування вуглецевих кордонів CBAM — переводять проблему з категорії «індустріальна незручність» у категорію «юридична неможливість дотримання» для платформ, які базуються виключно на програмному обліку без апаратного засвідчення джерела даних.

Український енергетичний сектор, що обирає вектор європейської інтеграції, неминуче зіткнеться з потребою відповідності цим вимогам. У

контексті післявоєнного відновлення енергетичної інфраструктури України виникає рідкісна можливість впровадити рішення «з чистого аркуша», уникаючи помилок усталених, але вразливих систем обліку, успадкованих від доцифрової епохи.

2. Принцип нейтральності даних: захист від впливу учасників ринку

Запропонована архітектура побудована на принципі, який кардинально відрізняє її від існуючих систем обліку: первинні дані виробництва криптографічно захищені від моменту їх формування і не можуть бути змінені жодним учасником ринку.

Ця нейтральність забезпечується трьома взаємодоповнюючими механізмами:

— Підпис показників приватним ключем, який зберігається в апаратно захищеному модулі лічильника. Власник генеруючого об'єкта не має фізичного доступу до приватного ключа, оскільки ключ генерується безпосередньо всередині захищеної мікросхеми під час виготовлення пристрою і не може бути експортований жодним відомим способом, не пов'язаним з фізичним руйнуванням мікросхеми.

— Запис підписаних показників у незмінний розподілений реєстр через розумні контракти, які виключають можливість зміни вже опублікованих даних навіть з боку оператора самої системи. Будь-яка спроба ретроактивної модифікації записів технічно неможлива.

— Незалежна крос-валідація показників через метеорологічні дані з трьох публічних джерел, що унеможливлює симуляцію генерації у періоди фактичної відсутності первинного енергоносія (сонячного, вітрового тощо). Кожен заявлений обсяг виробництва зіставляється з погодними умовами на момент генерації.

Внаслідок цього жоден учасник ринку не має технічної можливості повпливати на первинний показник після його формування:

— власник генерації, вмотивований до завищення показників задля збільшення доходів від продажу гарантій походження, не може модифікувати дані після виходу сигналу із захищеного модуля;

— продавець гарантій походження, вмотивований до подвійного продажу однієї одиниці, не може створити дублюючий запис у незмінному реєстрі;

— покупець, вмотивований до фіктивного зарахування зелених сертифікатів задля задоволення регуляторних вимог чи покращення іміджу, не може приймати у власність сертифікати без публічно верифікованого фізичного підкріплення;

— оператор реєстру, навіть за наявності корупційних інтересів або зовнішнього тиску, не має технічних повноважень модифікувати чи приховувати записи.

Це не покращення існуючої моделі довіри. Це її структурна заміна: довіра до людських ланок замінюється довірою до математичних властивостей криптографії та фізичних властивостей захищеної апаратури.

3. Архітектурне рішення: п'ятишаровий захисний контур

Запропоновано п'ятишарову архітектуру апаратно-вкоріненої верифікації, кожен шар якої адресує конкретний клас загроз.

3.1. Шар периферійних пристроїв із захищеними апаратними елементами.

Сенсорні пристрої побудовано на основі мікроконтролера ESP32 з інтегрованим захищеним елементом ATECC608B, сертифікованим за стандартом FIPS 140-2 Level 2. Приватний криптографічний ключ генерується безпосередньо в захищеному елементі під час провадження пристрою і не може бути експортований. Підпис лічильникових показників відбувається в точці генерації за алгоритмом ECDSA на еліптичній кривій P-256. Корпус пристрою сертифіковано за стандартом IP67 з вбудованими сенсорами виявлення несанкціонованого розкриття.

3.2. Шар агрегації подій.

Прийом підписаних пакетів від периферійних пристроїв, верифікація підписів, крос-валідація з трьома незалежними джерелами метеорологічних даних, агрегація показників у відповідні часові епохи. Сервіс реалізовано на мові TypeScript у середовищі Node.js зі зберіганням часових рядів у базі даних PostgreSQL із розширенням TimescaleDB.

3.3. Шар криптографічних доказів з нульовим розголошенням.

Задіяно схеми Noir з валідатором Honk, що дозволяють підтверджувати факт правомірної генерації без розголошення комерційно чутливих показників, таких як точна локація, миттєва потужність або часовий профіль роботи. Поточна продуктивність становить близько 11 секунд на генерацію доказу для однієї епохи.

3.4. Шар розумних контрактів на сумісних з Ethereum мережах.

Контракти Verifier V3, DeviceRegistry, P256VerifierAdapter, HonkVerifier розгорнуто на тестовій мережі Ethereum Sepolia. Архітектура використовує паттерн оновлюваного проксі UUPS із контролем доступу та можливістю заморозки контрактів у разі інциденту безпеки.

3.5. Шар публічної верифікації та моніторингу.

Індексування подій розподіленого реєстру через підграфи The Graph з публічною інформаційною панеллю. Будь-який зацікавлений учасник — регулятор, аудитор, контрагент, журналіст-розслідувач — може незалежно

верифікувати агреговані показники без необхідності довіри до самого оператора системи. Публічна інформаційна панель з реальними даними тестового запуску доступна за посиланням: https://sidliarchukpetro.github.io/infraveritas-energy/dashboard.html.

4. Кіберстійкість: захист від типових векторів атак

Архітектура спрямована на нейтралізацію наступних класів атак.

4.1. Маніпуляція показниками лічильника.

Будь-яка зміна показників після виходу сигналу із захищеного елемента призводить до недійсного підпису. Без приватного ключа, що зберігається в непідробному модулі, створити правильний підпис для модифікованих даних неможливо.

4.2. Атаки повторного відтворення.

Кожен підпис містить часовий маркер епохи та унікальний ідентифікатор сесії. Спроба повторного використання раніше валідного підпису відхиляється на рівні агрегатора як дублікат.

4.3. Компрометація центрального серверу агрегатора.

Скомпрометований сервер агрегатора не може створити фальшиві дані: підпис генерується на периферійному пристрої та переходить далі без можливості модифікації. Найгірший сценарій атаки на агрегатор — відмова в обслуговуванні, але не фальсифікація даних.

4.4. Симуляційні атаки.

Спроба згенерувати фальшивий профіль сонячної генерації на хмарний день виявляється через крос-валідацію з трьома незалежними метеорологічними джерелами. Невідповідність між заявленою генерацією та фактичною погодою фіксується системою як аномалія, що потребує додаткового розслідування.

4.5. Компрометація приватного ключа.

Ключ ATECC608B є нерозголошуваним: апаратний дизайн виключає експорт ключа з мікросхеми відомими способами. Атака на криптографічний матеріал потребує фізичного доступу до пристрою та спеціалізованого обладнання вартістю, що значно перевищує економічну цінність потенційного шахрайства.

5. Результати валідації безпеки

Реалізація системи пройшла комплексний попередній аудит безпеки у чотирьох незалежних інструментах.

5.1. Статичний аналіз — Slither 0.11.5.

Перевірено 94 окремих детектори властивостей безпеки. Знахідок високого або середнього ризику не виявлено. Зафіксовано 3 інформаційні зауваження, кожне з яких задокументовано як свідоме архітектурне рішення.

5.2. Символьне виконання — Mythril 0.24.8.

Виконано валідацію шляхів виконання байт-коду в семи контрактах. Виявлено 2 потенційні точки, обидві встановлено як хибнопозитивні спрацювання, спричинені використанням шаблонів OpenZeppelin Security.

5.3. Тестування на основі властивостей з випадковими даними — Echidna 2.3.2.

Виконано 100 256 174 транзакцій з тестуванням п’яти інваріантів безпеки. Порушень не виявлено. Цикл тестування зайняв 17 годин 16 хвилин неперервної роботи.

5.4. Покриття модульними тестами — Foundry 1.7.1.

Досягнуто 91,88% покриття на рівні операторів. Реалізовано 100 модульних тестів та 2 додаткові інваріантні тести.

Розгортання на тестовій мережі Ethereum Sepolia підтвердило працездатність повного циклу обробки з 14 травня 2026 року. Час від відправки сигналу з периферійного пристрою до підтвердження транзакції в мережі становить близько 27 секунд. Вихідний код проекту відкрито доступний за посиланням: https://github.com/sidliarchukpetro/infraveritas-energy.

6. Висновки та перспективи

Розглянута архітектура демонструє практичну можливість впровадження апаратно-вкоріненої верифікації як засобу системної протидії шахрайству в обліку відновлюваної електроенергії та одночасно шару кіберстійкості для критичної енергетичної інфраструктури. Ключові висновки:

1. Технічна здійсненність підтверджена. Працююча реалізація на Ethereum Sepolia з валідованим контуром безпеки демонструє, що архітектура не є концепцією, а функціональною системою.

2. Структурна нейтральність забезпечена. Жоден учасник ринку — власник генерації, продавець, покупець, оператор реєстру — не має технічної можливості повпливати на первинні показники виробництва після їх криптографічного засвідчення. Це усуває кореневу причину системного шахрайства в обліку зеленої електроенергії.

3. Регуляторні драйвери очевидні. Директива RED III та Механізм CBAM створюють об’єктивну потребу в верифікації, яка виходить за межі можливостей виключно програмних рішень.

4. Український вектор європейської інтеграції відкриває рідкісне вікно. Післявоєнне відновлення енергетичної інфраструктури України з можливістю проектування «з чистого аркуша» створює унікальний шанс для впровадження найкращих практик кіберзахисту з самого початку, без необхідності болісної міграції з усталених, але вразливих систем.

Перспективні напрями подальшої роботи: розгортання промислового пілотного проекту на трьох об'єктах відновлюваної генерації в Україні (сонячна, мала вітрова та мала гідрогенерація) загальною потужністю не менше 500 кВт; сертифікація відповідності українським нормативам кібербезпеки критичної інфраструктури; координація з Європейською мережею операторів передачі електроенергії (ENTSO-E) та національним оператором передачі для інтеграції в загальноєвропейський облік; розробка стандарту IPAS (Infrastructure Physical Asset Standard) як відкритого стандарту фізичної верифікації об'єктів інфраструктури.

Технічна документація проекту та архітектурні специфікації захищено в рамках попередньої патентної заявки USPTO № 63/876,031 від 12 вересня 2025 року.

Додаткові посилання

— Публічна інформаційна панель з реальними даними тестового запуску:
https://sidliarchukpetro.github.io/infraveritas-energy/dashboard.html
— Вихідний код проекту (відкритий доступ):
https://github.com/sidliarchukpetro/infraveritas-energy
— Корпоративний сайт проекту: https://infraveritas.pro

1. Європейський Парламент. Директива (ЄС) 2023/2413 щодо просування використання енергії з відновлюваних джерел (RED III). 2023.
2. Європейська Комісія. Регламент (ЄС) 2023/956 щодо встановлення механізму коригування вуглецевих кордонів (CBAM). 2023.
3. NIST. FIPS Publication 140-2: Вимоги безпеки до криптографічних модулів. 2001.
4. Microchip Technology. Захищений криптографічний пристрій ATECC608B. Технічна документація, 2024.
5. Aztec Labs. Noir: доменно-специфічна мова для доказів з нульовим розголошенням. Технічна специфікація, 2024.
6. Energy Web Foundation. Технічна документація EW-DOS та Energy Web X. 2024.
7. OpenZeppelin. Методологія аудиту безпеки розумних контрактів. 2024.
8. The Graph Foundation. Документація протоколу індексації підграфів. 2024.
9. ERC-3643 Association. Стандарт T-REX щодо прав на дозволені токени. 2024.
10. Granular Energy. Погодинні гарантії походження: архітектура та стандарти. Дослідницька стаття, 2024.
11. Сідлярчук П. О. Стандарт фізичної верифікації об'єктів інфраструктури IPAS v1.0. Попередня патентна заявка USPTO № 63/876,031. 2025.

В.В. Шкарупило, В.О. Артемчук

КОНЦЕПЦІЯ ВАРІЮВАННЯ РІВНЯ АТОМАРНОСТІ ФОРМАЛІЗОВАНИХ ПОДАНЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПРИ ПРОЄКТУВАННІ

Роботу виконано у напрямі розвинення теоретичних засад формалізації складових концепції резилієнтності електроенергетичних систем (ЕЕС).

Представлена концепція базується на припущенні, згідно якого резилієнтність ЕЕС опрацьовується вже на ранніх етапах процесу розроблення означених систем. У якості такого охоплюється етап проєктування – етап, на якому визначається архітектурна складова (АС) цільової системи. Формалізація при цьому розглядається як механізм забезпечення уніфікованості у частині подання і інтерпретації АС при проєктуванні, а також як засіб уможливлення автоматизації процесу контролю несуперечливості формалізованих подань АС – формальних специфікацій (ФС).

З-поміж визначальних чинників у контексті синтезу ФС – застосування належного засобу формалізації. У якості останнього залучається перевірений часом математично строгий модульний формалізм TLA+ темпоральної логіки дій TLA (Temporal Logic of Actions) лауреата премії Тюрінга Л. Лемпорта (Leslie Lamport) [1].

Розроблене рішення базується на оперуванні формалізованими поданнями концепції дії (Action) логіки TLA [2]. Відповідні конструкції залучаються при формуванні більш комплексних темпоральних формул на основі виразних засобів TLA+ [3]. Такий підхід інтерпретується як крок у напрямі забезпечення уніфікованості ФС. Для групування складових ФС за показником їх комплексності проводиться стратифікація: виокремлюються три ієрархічні рівні, при цьому формалізовані подання концепції дії залучаються у якості елементів середньої страти [4].

На нижньому ієрархічному рівні розробники оперують базовими конструкціями, що безпосередньо визначають рівень атомарності результуючої трирівневої ФС. У частині концептуального навантаження відповідні формалізовані подання є імплікаціями, модифікованими темпоральним оператором часового зсуву «Next» [5]. Кожна така конструкція є поданням збереження або модифікації значення відповідної змінної станів системи переходів, що будується і опрацьовується у процесі формальної верифікації поширеним методом перевірки на моделі TLC (TLA Checker). Означені формалізовані подання, у свою чергу, сполучаються у формі кон'юнкцій. Останні при цьому є елементами середньої (другої) страти – поданнями згаданих вище «дій». Продовжуючи рух індуктивним шляхом, формуються елементи верхнього (третього) ієрархічного рівня – як кон'юнкції на основі формалізованих подань дій.

Центральна ідея в основі представленої концепції полягає в оперуванні елементами верхнього (третього) ієрархічного рівня: за рахунок залучення коефіцієнту, значення якого визначає кількість елементів верхньої страти, які опрацьовуються у процесі TLC-верифікації. Значення коефіцієнту визначається розробником з урахуванням попереднього досвіду, комплексності ФС, а також обчислювальних обмежень наявної обчислювальної системи. Значення коефіцієнту задає результуючий рівень атомарності ФС.

Отримані результати обчислювального експерименту надають підстави припустити, що слідування представленій концепції на практиці дозволить стримувати небажаний ефект експоненційного зростання простору станів систем переходів, що будуються і опрацьовуються у процесі формальної верифікації поширеним методом TLC [6].

Автори висловлюють подяку Національному фонду досліджень України за грантову підтримку, завдяки якій було виконано дане дослідження в рамках проєкту 2025.07/0204 «Паралельні методи та алгоритми розв'язування задач змішаного цілочисельного лінійного програмування для планування розвитку структурно мінливих і резильєнтних електроенергетичних систем України».

1. Lamport, L. (2026). *A science of concurrent programs*. Cambridge University Press. https://doi.org/10.1017/9781009719841.
2. Lamport, L. (2002). *Specifying systems: the TLA+ language and tools for hardware and software engineers* (1st edition). Addison-Wesley Longman Publishing Co., Inc.
3. 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/.
4. Shkarupylo, V., Shkarupylo, V., Dusheba, V., Kudermetov, R., & Polska, O. (2025). On variation of formal specification abstraction level through operation with TLA+ concepts. *2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 929–932). IEEE. https://doi.org/10.1109/IDAACS68557.2025.11322075.
5. Shkarupylo, V., Alsayaydeh, J. A. J., Tomičić, I., Chemeris, A., & Dusheba, V. (2021). A technique for checking the adequacy of formal model. *ARPN Journal of Engineering and Applied Sciences*, 16(16), 1707–1719. http://www.arpnjournals.org/jeas/research_papers/rp_2021/jeas_0821_8670.pdf.
6. Shkarupylo, V., Artemchuk, V., Chemerys, O., Alsayaydeh, J. A. J., & Kulinich, O. (2026). Hierarchical concept of formal specifications' abstraction level amendment in energy scenarios. In: Bazilo, C., Bondarenko, M., Faure, E., Antonyuk, V., Dzierwa, A., Usyk, L. (Eds.) *Sensors, Devices and Systems. SDaS 2025. Lecture Notes in Electrical Engineering* (pp. 172–181), vol. 1570. Springer, Cham. https://doi.org/10.1007/978-3-032-18415-3_18.

А.В. Бойченко, В.Р. Сенченко

ЗАСТОСУВАННЯ СИМВОЛОГІЇ NATO ДЛЯ ВІЗУАЛЬНОГО АНАЛІЗУ КІБЕРБЕЗПЕКИ

В умовах постійного зростання обсягів кіберзагроз особливої актуальності набуває вдосконалення методів аналізу інформаційної безпеки. Кіберпростір критичних інфраструктур характеризується складністю і динамічністю що ускладнює його захист [1].

З огляду на дефіцит часу на вироблення рішень, традиційні методи представлення даних кібербезпеки не завжди дозволяють оперативно виявити приховані закономірності та аномалії. Впровадження інструментів візуальної аналітики забезпечує швидке розпізнавання критичних станів керованої системи, знижуючи рівень когнітивного навантаження фахівців [2,3].

Водночас, в ситуації взаємодії фахівців з різних галузей, важливим моментом є використання єдиної симвології – уніфікованого набору правил графічного відображення елементів та їх поведінки [4].

У 2025 році NATO опублікувала оновлену версію стандарту NATO Joint Military Symbology (APP-06(E)(2)) [5], що містить розділ Cyberspace Symbols, який, подібно до MIL-STD-2525E[6], присвячений уніфікації символіки для кіберпростору. Цей розділ вводить стандартизовані позначення для кібероб'єктів (сервери, мережі, дані), кіберзагроз (DDoS, шкідливе ПЗ), кібероперацій (наступальні, оборонні) та засобів захисту (брандмауери, системи виявлення вторгнень). Використання стандарту сприяє формування єдиного інформаційного простору, у якому фахівці з кібербезпеки та аналітики можуть ефективно співпрацювати з військовими та однозначно інтерпретувати кіберінциденти.

Стандарт спирається на доктрину JP 3-12 Cyberspace Operations [7], яка визначає кіберпростір як середовище, що складається з трьох взаємопов'язаних рівнів.

Рівень Physical Network охоплює фізичну інфраструктуру кіберпростору. До нього належать сервери, маршрутизатори, комутатори, канали зв'язку, дата-центри, супутникові вузли, SCADA-компоненти та засоби телекомунікації.

Рівень Logical Network описує логічну структуру взаємодії систем незалежно від їх фізичного розташування. До нього входять IP-мережі, домени, VLAN, сервіси, протоколи, VPN, маршрути доступу та політики взаємодії між сегментами.

Рівень Cyber-Persona охоплює цифрові сутності, пов'язані з діяльністю користувачів і процесів. До нього належать облікові записи, цифрові ідентичності, групи доступу, оператори, бот-мережі, сесії та адміністративні ролі.

Візуалізація об’єтів кіберпростору, представлена на рис. 1, дозволяє інтегрувати сутності кіберпростору з географічними мапами, що забезпечує можливість планування кібероперацій. Деякі підрозділи знаходяться у областях невизначеності (на мапі відображено червоними овалами) що означає що відоме лише їх приблизне розташування.

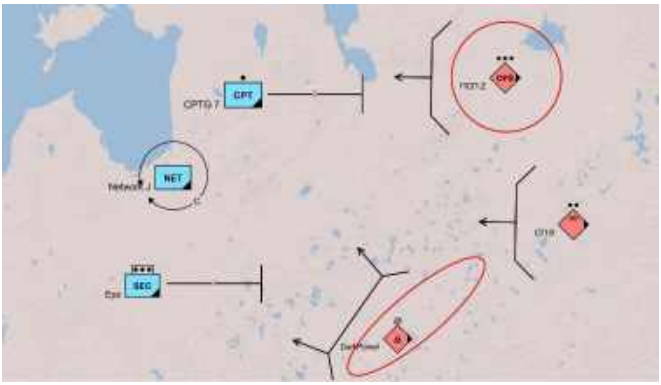


Рисунок 1 – Приклад поєднання симвології кіберпростору з мапою

Візуалізація об'єктів кіберпростору без прив'язки до геопросторових мап, як це показано на рис. 2, зосереджується на відображенні логічної архітектури мережі, зв'язків між об’єктами та сегментації. Це дозволяє розглядати операції та загрози в кібердомені незалежно від фізичного розташування активів.

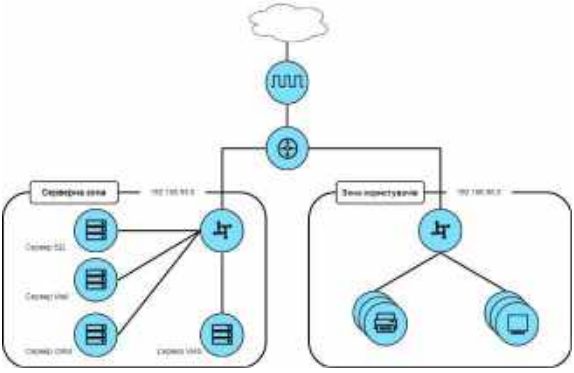


Рисунок 2 – Приклад використання симвології кіберпростору без відображення геопросторових даних

Використання моделі дозволяє поєднувати різні типи даних у межах аналітичного середовища. Наприклад, компрометація облікового запису на рівні Cyber-Persona може бути пов'язана з маршрутом на рівні Logical Network та з конкретним сервером на рівні Physical Network.

Модель може бути розширена додатковими рівнями: Entity-persona, який розглядає живих людей і Geographical – з прив'язкою до просторових координат [8].

Для впровадження симвології NATO до системи візуальної аналітики кібербезпеки критичних інфрасткуктур пропонуємо наступну методику.

1. Визначення цілей візуальної аналітики кібербезпеки.
2. Визначення логічних доменів кіберпростору інфраструктури.
3. Інтегрування стандартів симвології до існуючі засобів візуалізації.
4. Нормалізація даних для відображення кіберпростору.
5. Налаштування правил динамічного відображення атак.
6. Впровадження правил доступу та рівнів деталізації інформації.
7. Валідування ефективності відображення оперативної картини.
8. Оцінювання ефективності та коригування правил візуалізації.

Реалізація представленої методики дозволить побудувати уніфікувану технологію візуальної аналітики кібербезпеки для критичних інфраструктур. Це дозволить зробить вироблення стратегічних та оперативних рішень точнішими, швидшими та стійкішими до викликів сучасного кіберсередовища.

1. Boychenko A.V., Senchenko V.R. An approach to development of cyberattack scenarios for digital substations. Cybersecurity of energy, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine. May 29, 2024. Kyiv: PIMEE NAS of Ukraine, 2024. p. 4 – 6.
2. Додонов, О. Г., Бойченко, А. В. Методи візуалізації та візуальної аналітики в інформаційних системах організаційного управління // Математичні машини і системи. 2025. Т. 4, 20-32.
3. Бойченко, А. В., & Сенченко, В. Р. (2023). Підхід до моделювання геопросторових каскадних ефектів критичних інфраструктур. Інформаційні технології та безпека. 56(7). – с. 35-40.
4. Kim, K., Youn, J., Yoon, S., Kang, J., Kim, K., & Shin, D. (2023). Study on cyber common operational picture framework for cyber situational awareness. Applied Sciences, 13(4), 2331.
5. NATO Joint Military Symbology (APP-06(E)(2)). NATO Standardization Office. https://nso.nato.int/cad804f5-0215-44dc-821c-7b27831db180.
6. Department of defense interface standard joint military symbology, MIL-STD-2525E, 2 March 2025. quicksearch.dla.mil/ImageRedirector.aspx?token=5795656.114934.
7. Joint publication 3-12, Cyberspace Operations, 8 June 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
8. Zhang, L., Wang, G., You, X., Liu, Z., Ma, L., Tian, J., & Su, M. (2023). Research on the cyberspace map and its conceptual model. ISPRS International Journal of Geo-Information, 12(9), 353.

D.I. Bakhtiiarov, A.V. Leleko, S.V. Sova

METHODS OF INTELLIGENT SECURITY AND PROTECTION OF TELECOMMUNICATION DATA

Processing information in real time generated by means of latest telecommunication technologies (5G/6G networks, IoT, and UAS sensor networks) as well as by increasing number of devices requires fast processing and secure information exchange. Thus, the traditional security approach is not sufficient and has to be changed from the typical signature detection by an Intrusion Detection System (IDS) to intelligent security methods by using Machine Learning (ML) and Deep Learning (DL).

The main goal of this work is to review the last intelligent security methods and to design a conceptual model of a hybrid anomaly detection system for traffic of telecommunication networks, which is able to work in real time and to be able to detect the last cyberattacks.

In recent years, many researchers have tried to implement the various methods of the artificial intelligence for the traffic analysis. The analysis of the recent publications in the area of the cybersecurity for the traffic classification has revealed that the majority of the known methods of the machine learning (such as SVM, Random Forests, Naive Bayes, etc.) for the traffic classification taking into account the pre-extracted statistical characteristics of the traffic have high accuracy for the various applications. The accuracy of the classification and the speed of the processing of the traffic can be improved by using various features taking into account both the characteristics of the packets and the characteristics of the connections as well as by various methods of the preprocessing etc. All the above-mentioned approaches, however, require a lot of effort for the selection and the processing of the appropriate features and require a lot of expertise in order to obtain the appropriate results. Thus, these approaches are not very suitable for the processing.

In addition to using Machine Learning for Network Traffic Analysis, recent research has been focusing on applying Deep Learning techniques for detecting hidden patterns and anomalies within various types of network traffic, including multimedia and encrypted network traffic. The approach of Deep Packet Inspection (DPI) combined with Deep Neural Networks (DNNs) has been a recent area of interest in the field of network security and intrusion detection.

On the other hand, there are many types of threats that are of a time-distributed nature. Such threats cannot be found by analyzing a single sample, but by monitoring a sequence of network events occurred in time. To address such threats, there are intelligent methods that utilize Recurrent Neural Networks (RNNs) to model time-distributed information. Representative RNNs include Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRUs).

The work presented in this paper is based on the numerous sources reviewed in order to develop and analyze intelligent security methods. A new conceptual model for an intelligent, real-time, hybrid system for detection of unknown attacks in modern telecommunication systems is introduced and analyzed. A new approach for the real-time detection of unknown attacks in traffic of modern telecommunication is presented in the work. The approach includes a data processing pipeline, where the traffic is first collected, then processed by a set of preprocessing functions to produce two sets of features, spatial and temporal features of the traffic data. In the next stage of the processing, the two sets of features are processed in parallel, the spatial features are processed by a 1D-CNN to detect local anomalies in packets, the temporal features are processed by a number of LSTM layers to detect anomalies in time sequences of data.

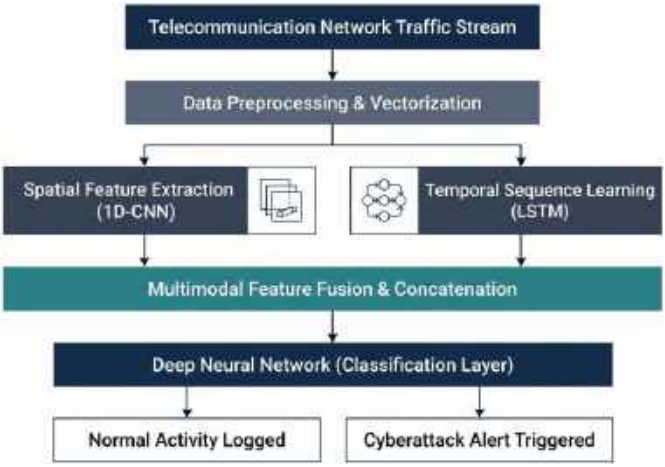


Figure 1 – Conceptual architecture of a hybrid intrusion detection system for telecommunication data

The proposed hybrid neural network model of sequential structure for classification and training all model components in a sequence, is optimized for the cross-entropy type objective function to minimize the errors in anomaly detection. In order to recognize the anomalies (attacks) of interest, the model computes the probabilistic characteristics of individual network packets as well as of their aggregates – data flows. The output of the fully connected layer of the neural network, after going through the respective activation function, are the values, which are then processed in order to classify the analyzed traffic into the normal traffic and the traffic of various types of cyberattacks in a binary form (normal/attack) or in multi-class form (different attacks). The weights of the model are updated through backpropagation in the framework of the respective iterative learning cycles, while the model is trained in a sequence.

We have also investigated the Quantization and Pruning of deep neural networks in order to decrease the size of model that is run on edge of network (e.g. on edge router or on gateway of IoT) and to improve the processing speed of packets (inference) without loss of detection quality.

The results of the testing of the proposed solution on a number of standard network datasets (such as NSL-KDD and CIC-IDS2018) demonstrated the possibility of the increase of the detection accuracy of the various types of cyberattacks to 98–99 % as well as the number of false alarms to a single one per day, on average, while using the proposed multimodal solution for the spatial (via CNN) and temporal (via LSTM) feature extraction from a variety of traffic flows of heterogeneous nature to "see around the corner" of the traditional solutions that are unable to detect such attacks.

In summary, intelligent protection and ensuring of security of telecommunications data today is a very complex task that goes beyond the framework of traditional static solutions for protection of information. Intelligent protection of telecommunications data can be realized by means of deep learning and implementation of hybrid neural networks, which are the core of adaptive systems for detection of intrusions in telecommunications and information space. Intelligent systems for real-time processing of information flow on the basis of hybrid neural networks allow to realize efficient, sustainable and highly efficient recognition of different types of attacks with immediate response to newly emerging threats, thus, to provide reliability and security of modern telecommunications infrastructure.

1. Kotyk, B., Bakhtiiarov D., et al. (2025). Neural network approach to 5G digital modulation recognition. CEUR Workshop Proceedings, 3925, 82-92.
2. T. Ma, J. Bao, H. Yang, X. Zhao, Q. Zhang and W. Lv, "Network Anomaly Behavior Detection and Security Protection based on Clustering Algorithm," 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), Bidar, India, 2025, pp. 1-6.
3. M. Agrawal, P. Tiwari, N. Tripathi, N. K. Pandey, A. K. Mishra and A. Dumka, "A Novel Data Protection Technique to Prevent Data Compromise and Privacy Preservation," 2024 International Conference on Communication, Computing and Energy Efficient Technologies (I3CEET), Gautam Buddha Nagar, India, 2024, pp. 471-476.
4. Y. Liu, "Design of Network Information Security System Based on Artificial Intelligence Algorithms," 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-5.
5. D. A. Jadhav, J. G. Thatipudi, V. Thakur, N. Y, K. M. Lakshmi and S. Sharma, "Enhanced Privacy and Security Maintenance to Preserve BigData using Cipher Policy," 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 218-224.
6. H. B. Gangadharaswamy et al., "An Efficient and Intelligent IoT-Based Security Model for Enhanced Protection Using Motion Detection and Cloud Storage Optimization," 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2024, pp. 1-6.

V.V. Telnykh, D.I. Bakhtiiarov, V.V. Antonov

AI METHODS FOR INTRUSION AND ANOMALY ACTIVITY DETECTION

Modern telecommunications as well as infocommunication services and systems have drastically grown and as a result, their complexity have also increased. Large-scale implementation of Internet of Things (IoT) as well as deployment of 5G/6G communication systems, as well as use of cloud computing and big data processing in information processing have increased number of potential points of impact greatly, and therefore, are subject to attacks by cybercriminals. Current threats and attacks are mostly of automated type and include large number of newly developed polymorphic threats that in each implementation have a different signature, and thus cannot be detected by traditional perimeter security solutions (based on set of rules as well as on signature-based). In addition, large part of modern threats are so-called zero-day threats as well as so-called Advanced Persistent Threats (APTs), and due to their complex nature, cannot be detected by existing IDS solutions based on Intrusion Detection Systems (IDS).

To tackle today's advanced cyber threats with the help of Artificial Intelligence (AI) new approaches and architectures have to be developed in order to increase the detection rate of cyber threats. Most existing approaches for an Intrusion Detection System (IDS) are based on machine learning (ML) and use supervised learning in order to detect attacks within a network. The most common used supervised learning approaches are for example Random Forests, Support Vector Machines and also deep neural networks. These systems are able to detect attacks within a network with a high detection rate, but they also have some severe disadvantages. For example supervised learning approaches need a huge amount of labeled data in order to train the model. In real world networks it is nearly impossible to get this amount of labeled data in time, in order to train the model and to use it for detection in the network. Also supervised learning approaches do not have any prior knowledge about new attack patterns, because of that they are not able to detect them. The main trend in modern information security systems is to use unsupervised learning and generative AI for the detection of unknown attacks. The objective of the current study is to design and to investigate a two-tier distributed intelligent system for intrusion detection, which is based on the synergy of autoencoders and GANs.

One example of a neural network is the Deep Autoencoder. A Deep Autoencoder is a special kind of neural network that is trained and wants to reproduce its input as closely as possible after it has gone through the neural network. A Deep Autoencoder consists of two mirrored layers. The first layer is called the Encoder and the second layer is called the Decoder. The Encoder and the Decoder are composed of multiple fully connected layers. The weights of the layers are learned during the training process of the Autoencoder. The network feature space of network traffic (e.g. packet size, time between packets, flags of packet headers, etc.) is mapped into a much lower-dimensional feature space by the Encoder, also known as a bottleneck. The Decoder tries to map this low-dimensional representation back to the original high-dimensional input space where the network traffic originated. A Deep Autoencoder can be trained in an unsupervised manner. After it has been trained on a sufficient amount of examples of normal network traffic for a certain enterprise network, the Autoencoder can be deployed to monitor a network for potential threats. During the inference process, all packets (or even entire sessions) that pass through the Autoencoder are reconstructed by the output of the Decoder (the reconstructed input). If a packet (or even entire sessions) cannot be reconstructed correctly by the output of the Decoder, a large increase in the reconstruction error will occur. If the large increase in the error is above a dynamically calculated threshold, then the packet (or even entire sessions) of network traffic under scrutiny is flagged as an anomaly that needs to be further analyzed in detail for potential threats to the network.

The Autoencoder has a few key advantages, the first being that the system does not require a large amount of labeled data. In fact, it can be trained on “clean” data, which is data typical of a network and gathered from said network. Since a human is not required to label the data, this is a huge advantage in itself. The other advantage is that the Autoencoder can automatically learn the complex, non-linear relationships between the features of network traffic. In essence, the Autoencoder can automatically learn the typical behavior of a network and then detect and report any deviations from typical behavior. The training process of an Autoencoder involves a decoder that tries to recreate the input to the encoder (i.e. the original input) from the latent space which is the output of the encoder. This process results in a reconstructed error which indicates how well the decoder was able to recreate the original input. The reconstructed error for each input can then be used as an indicator of normal or anomalous behavior. Sessions that have a large reconstructed error for their traffic flow would be reported as anomalies and would then be subject to further analysis.

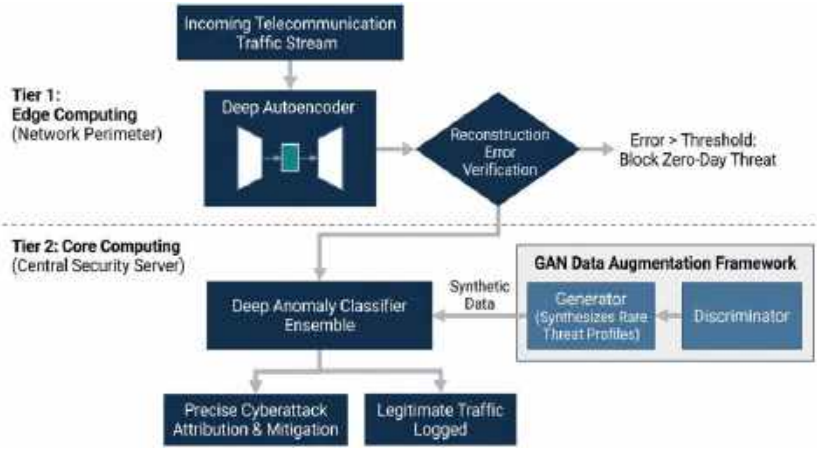


Figure 1 – Two-tier intelligent intrusion detection architecture based on autoencoders and GANs

The second challenge facing Applied Network Traffic Analysis (ANT) is the so-called "catastrophic class-imbalance problem". Stated briefly, normal traffic (corresponding to network activity by users behaving normally) accounts for more than 99.9% of all network traffic while misuse and malicious activity (herein referred to as attacks) account for a very small number of events, and correspond to a few categories of threats: User-to-Root (U2R) attacks (in which a user executes misuse of functionality in order to escalate that user's privileges to that of a super-user), and Remote-to-Local (R2L) attacks (in which an outside user launches a bid to access local resources on a computer). The number of events generated by these types of threats are a very small fraction of all events generated by normal users. Because of this, typical machine learning models are completely unable to recognize Minority Class threats (U2R and R2L attacks) because they are optimized to recognize the Majority Class (normal traffic) correctly. In general, Majority Class instances are treated as if they were the only instances of that class type by the machine learning model. In the field of machine learning, the failure to recognize Minority Class instances correctly is commonly referred to as.

The Generation of Synthetic Data for the Anomaly Detection in Networks with the Usage of Generative Adversarial Networks is dealing with the severe class imbalance in network traffic. In network traffic, a large amount of data belongs to normal behavior and a very small amount of data belongs to attacks and anomalies. Because of this class imbalance, the accuracy of the classification is heavily biased towards normal behavior. A huge amount of data has to be classified correctly in order to get a correct classification of the minority class, whereas only very few samples of these data points have to be classified correctly in order to get a bad classification of the minority class. This is why the accuracy of the classification is

biased towards normal behavior and therefore the network intrusion detection system is not able to detect attacks and anomalies. To deal with the class imbalance, we use Generative Adversarial Networks, which are able to generate synthetic data, that represents attacks and anomalies, in order to balance the classes in the network traffic data. The use of Generative Adversarial Networks for the anomaly detection in networks leads to a severe increase in the F1-score of rare attacks and therefore to a severe decrease in the False Positive Rate. The detection of attacks and anomalies with the usage of Generative Adversarial Networks for the data augmentation is completely automated and therefore very efficient and robust.

The proposed system consists of two tiers of a system. In the first tier, of the system edge computing is performed. The edge computing is done on various network devices i.e. routers, switches and also on IoT gateways. In the edge computing pruned autoencoders are used for the purpose of detection and filtering of obvious attacks and also for handling DDoS attacks in real time. Traffic that contains anomalies which have large but not critical reconstruction errors by the edge autoencoders are forwarded to the second tier of the system. In the second tier of the system, a deep neural network classifier is used for processing the traffic. This system of network traffic analysis does a thorough analysis of the traffic and it is able to identify the type of cyberattack that is being launched. This deep neural network is trained by using a large dataset of normal and abnormal traffic that was created by using GANs. The system is able to identify a variety of attacks including SQL injection, cross-site scripting and port scanning to name a few.

The proposed system can be also effectively evaluated on current networks traffic data-sets like UNSW-NB15 and CIC-IDS-2018 etc. and achieves 96% detection rate of zero-day attacks by using the edge-based deep autoencoder for early detection and filtration. Furthermore, the GAN-based data augmentation significantly increases F1-score of rare threats of classes U2R and R2L by 23% to 27% on the already good supervised learning of supervised approaches, while keeping the False Positive Rate (FPR) at very low values.

Supervised learning methods for the security of telecommunications are ineffective, due to a high level of threat dynamics and the complexities of data labeling. A two-tier intelligent system of network security, based on unsupervised learning for the detection of anomalies at the edge of the network and that is combined with GANs for overcoming class imbalance in supervised learning for the detection of known and novel threats, can effectively and in real-time ensure the security and protection of critical information infrastructure.

1. D. Bakhtiiarov, B. Chumachenko, O. Lavrynenko, O. Kryvonosenko and B. Kotyk, "Development of a Microwave Communication System for Unmanned Aerial Vehicles," 2025 IEEE 8th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC), Kyiv, Ukraine, 2025, pp. 1-6.

2. G. Devadharshini, S. Aadhish and R. Vanitha, "AI-Driven Detection of Malicious Network Intrusions Using Decision Tree Algorithm," 2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT), Kollam, India, 2025, pp. 1029-1033.
3. M. R. Bayesh and M. S. Hossain, "An Automated Network Intrusion Detection and Identification System by Synergizing AI Techniques," 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2024, pp. 203-206.
4. M. A. Ameen, D. Basak, L. S. F. Lin and B. Das, "Intrusion Detection Using AI and ML in Cybersecurity," 2026 9th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2026, pp. 1-6.
5. S. Madhan and S. BrinthaRajakumari, "Hybrid Intrusion Detection Framework for IoT Applications Enhancing Cybersecurity with AI-Driven Threat Mitigation," 2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2025, pp. 1-8.
6. N. Jain, J. Hawari, P. Jha, H. N. Vishwas and M. Jain, "An Optimized Intrusion Detection Model Using ML and Explainable AI," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6.

С.Є. Саух

КЛАСТЕРНА МОДЕЛЬ РЕЖИМІВ НАВАНТАЖЕННЯ ГІБРИДНИХ ЕНЕРГОСИСТЕМ ЛІКАРЕНЬ

У сучасному контексті військових конфліктів та зростаючих вимог до енергетичної автономності об'єктів критичної інфраструктури особливої актуальності набуває дослідження стійкості гібридних енергосистем лікарень (ГЕСЛ) України. Запровадження графіків аварійних відключень (черги 1–6) у воєнний час створює нові виклики для забезпечення безперервності критичних функцій медичних закладів, адже лікарні повинні адаптуватися до нерівномірного та непередбачуваного режиму роботи зовнішніх мереж.

Медичні заклади є найбільш енергозатратними серед комунальних підприємств, що обумовлено цілодобовим функціонуванням, використанням критичного обладнання (ШВЛ, операційні, реанімації, діагностичні центри) та дотриманням жорстких кліматичних стандартів. Лікарні належать до І категорії (особливої) надійності електропостачання, що означає обов'язкове забезпечення двома незалежними джерелами живлення та резервними автономними установками (ДБН В.2.5 23:2010; ДБН В.2.2 10:2017).

Оцінювання стійкості ГЕСЛ в умовах миру та війни

У публікаціях аналізується стійкість енергозабезпечення лікарень переважно у мирних умовах — стихійних лих, пандемій чи техногенних аварій. Основний акцент робиться на забезпеченні резервного живлення протягом 24–72 годин, інтеграції відновлюваних джерел енергії та підвищенні енергоефективності.

Однак ці підходи мають суттєві обмеження для умов війни, адже:

- не враховують багатоденні відключення (1–2 тижні і більше),
- не моделюють систематичні атаки на енергетичну інфраструктуру,
- не інтегрують гібридні системи (генератори, СЕС, акумулятори) у єдину модель,
- не враховують нестабільність логістики постачання палива.

Таким чином, сучасні дослідження створюють корисну базу, але є непридатними для українського контексту воєнного часу, де лікарні стикаються з періодичними графіками відключень та потребою у багатоденній автономності. У дослідженнях специфічні обмеження виключно мирного часу моделюються через 50% поріг критичного навантаження ГЕСЛ, розрахований на основі даних аудиту та досліджень стійкості.

Виклики для ГЕСЛ у воєнних умовах

В умовах воєнного стану в Україні лікарні стикаються з іншими викликами:

нерівномірність та непередбачуваність мережевого електропостачання;

необхідність адаптації до різних сценаріїв тривалості перебоїв;

підвищені вимоги до резервування палива та управління навантаженням.

Тому оцінка стійкості систем енергозабезпечення медичних закладів України є стратегічною необхідністю. Вона гарантує, що гібридні енергетичні системи лікарень здатні надійно постачати електроенергію навіть за найнесприятливіших умов, включно з воєнним станом, забезпечуючи адаптивність у ситуаціях війни та можливої ізоляції.

Методологічні підходи

Адекватну оцінку стійкості ГЕСЛ можна отримати, аналізуючи відношення обсягу енергії, не поставленої лікарні, до обсягу попиту. Точність визначення цього показника забезпечується використанням **моделей режимів навантаження ГЕСЛ**.

Інженерія стійкості формує методологічну основу для кількісної оцінки здатності автономних гібридних енергосистем до задоволення попиту. Стійкість ГЕСЛ стає критичним показником, адже безперебійне енергопостачання безпосередньо визначає функціонування медичних закладів. Застосування показників інженерії стійкості у сценарному моделюванні екстремальних температур, перевантажень та логістичних обмежень дозволяє оцінювати ГЕСЛ не лише за ефективністю, але й за їхньою здатністю витримувати складні умови функціонування та адаптуватися до них.

Особливої актуальності набуває дослідження стійкості ГЕСЛ в умовах запровадження **шести різних черг відключення споживачів**. Такі режими створюють додаткові виклики для забезпечення безперервності критичних функцій медичних закладів, що потребує застосування високоточних кластерних моделей ГЕСЛ для оцінки їх адаптивності до нерівномірних та непередбачуваних режимів роботи розподільчих мереж.

Кластерні моделі енергосистем

Найбільш широко використовуваними спеціалізованими інструментами для моделювання гібридних енергетичних систем є REopt, HOMER Pro, SAM, RETScreen, PVsyst, PVsol, iHOGA та Genewable. Для оцінки стійкості військових та цивільних автономних гібридних енергетичних систем найбільш актуальними залишаються REopt та HOMER Pro, тоді як інші інструменти можуть доповнювати аналіз у вужчих сферах, таких як моделювання фотоелектричних систем, економічна оцінка, попередня оцінка доцільності та подібні напрями.

Важливо зазначити, що REopt використовує комерційний високопродуктивний розв’язувач IBM ILOG CPLEX як основний механізм

оптимізації для вирішення задач цілочисельного лінійного та квадратичного програмування (MILP та MIQP). HOMER Pro, натомість, застосовує власний алгоритм оптимізації, заснований на методах перерахування та евристичних підходах. Основна перевага REopt полягає у високій точності рішень та можливості моделювати гібридні енергетичні системи протягом великих часових горизонтів з високою роздільною здатністю (наприклад, п'ятихвилинні інтервали), що є критично важливим для аналізу стійкості систем у динамічних умовах.

Для дослідження стійкості електроенергетичних систем були розроблені кластерні моделі режимів їх навантаження [11]. Запропоновані моделі також використовують розв'язувач IBM ILOG CPLEX, але відрізняються від добре відомих моделей режимів навантаження [25–28] тим, що включають балансові рівняння кількісного складу доступних для використання енергоблоків та описують режими навантаження не окремих енергоблоків, а кластерів однакових енергоблоків. Це дозволяє суттєво зменшити розмірність задач прогнозування, а самі задачі формулювати на періодах тривалістю до одного року з погодинною деталізацією, зберігаючи при цьому адекватність моделі до реальних умов навантаження електроенергетичних систем.

У сучасному контексті воєнного стану в Україні особливої актуальності набуває дослідження стійкості ГЕСЛ з урахуванням запровадження шести різних черг – графіків відключення споживачів. Такі режими створюють додаткові виклики для забезпечення безперервності виконання медичними закладами властивих їм критичних функцій , що потребує використання високоточних інструментів моделювання їх енергосистем та кластерних підходів для оцінки адаптивності таких систем до нерівномірних та непередбачуваних режимів роботи зовнішніх мереж.

Розроблена кластерна модель гібридних енергосистем лікарень забезпечує проведення обчислювальних експериментів для визначення рівня стійкості енергосистеми у сценарних умовах війни. До таких умов належать:

- запровадження різних черг відключення лікарень від розподільчих електричних мереж;
- зниження на 15% коефіцієнтів ефективності акумуляторних батарей у режимах заряджання та розряджання через екстремальні температури та відсутність систем охолодження/підігріву;
- підвищення на 20% обсягу споживання електроенергії;
- запровадження логістичних обмежень на постачання дизельного палива.

Обчислювальні експерименти підтвердили спроможність моделі визначати рівень резильєнтності ГЕСЛ за різних сценарних припущень, що

дозволяє оцінювати придатність енергосистеми до забезпечення безперервної роботи лікарні в умовах війни.

Результати дослідження показали необхідність розробки алгоритмів управління ГЕСЛ, які забезпечують високу ефективність у керуванні режимами навантаження дизельних генераторів, систем зберігання енергії та сонячних електростанцій. Це особливо важливо в умовах воєнного стану та періодичного запровадження графіків відключення лікарень від розподільчих мереж.

Таким чином, кластерна модель ГЕСЛ є не лише інструментом для кількісної оцінки стійкості, але й методологічною основою для розробки практичних рішень щодо управління енергетичною інфраструктурою медичних закладів у кризових умовах. Її застосування дозволяє формувати рекомендації для підвищення автономності та адаптивності лікарень, що має стратегічне значення для забезпечення безперервності медичної допомоги в Україні.

Дослідження проводилося в рамках проєкту № 2025.07/0204 *«Паралельні методи та алгоритми розв'язання задач змішаного цілочисельного лінійного програмування для планування розвитку структурно мінливих та резильєнтних електроенергетичних систем України»****, що фінансується Національним фондом досліджень України (НФДУ).***

О.С. Потенко

ДОСЛІДЖЕННЯ ВІДМІННОСТЕЙ МІЖ БАЗОВИМ ТА ГАЛУЗЕВИМ ПРОФІЛЯМИ БЕЗПЕКИ В КОНТЕКСТІ ЗАХИСТУ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Енергетична галузь України належить до критичної інфраструктури держави, функціонування якої безпосередньо впливає на енергетичну безпеку, економічну стабільність та безперервність життєво важливих процесів. В умовах зростання кількості кібератак на об'єкти енергетики особливого значення набуває питання формування ефективної системи кіберзахисту інформаційно-комунікаційних систем енергетичної галузі.

Сучасний підхід до побудови системи захисту інформації в Україні базується на використанні профілів безпеки, визначених нормативними документами системи технічного захисту інформації, зокрема НД ТЗІ 3.6-006-24 та НД ТЗІ 2.3-025-24 [1].

У 2025 році Адміністрація Держспецзв'язку України затвердила базові профілі безпеки, що визначають мінімальні вимоги до захисту інформації в інформаційних та інформаційно-комунікаційних системах. Наказом № 409 від 30.06.2025 затверджено профіль для систем, де обробляється відкрита або конфіденційна інформація, а наказом № 419 від 02.07.2025 — профіль для систем зі службовою інформацією, який передбачає підвищені вимоги до захисту. Для систем, що обробляють державну таємницю («Таємно» та «Цілком таємно»), також розроблено окремі профілі, які не є публічними [2].

Проект наказу Міністерства енергетики України «Про затвердження профілів безпеки системи для паливно-енергетичного комплексу України»(ПЕК) було оприлюднено для громадського обговорення 7 листопада 2025. Проектом запропоновано Галузевий профіль безпеки системи, у якій обробляється відкрита або конфіденційна інформація для ПЕК України, а також Галузевий профіль безпеки системи, де обробляється службова інформація для паливно-енергетичного комплексу України [3].

Базовий профіль безпеки визначає мінімально необхідний набір заходів захисту для інформаційних систем, тоді як галузевий профіль враховує специфіку функціонування окремої галузі та встановлює додаткові або посилені вимоги до безпеки.

У зв'язку з цим актуальним є порівняння базового профілю безпеки та галузевого профілю безпеки системи для енергетичної галузі України. Таке порівняння дозволяє визначити відмінності між універсальними та галузево-орієнтованими вимогами, оцінити рівень посилення заходів захисту для об'єктів енергетичної інфраструктури, а також виявити додаткові механізми забезпечення кіберстійкості для систем класу SCADA/ICS та інших технологічних мереж.

Отже, порівняльний аналіз базового та галузевого профілів безпеки є необхідним етапом формування цільового профілю безпеки для інформаційно-комунікаційних систем енергетичної галузі України, а також важливим інструментом підвищення рівня захищеності критичної енергетичної інфраструктури.

Для наочного порівняння базового та галузевого профілів безпеки доцільно використати графічні методи візуалізації даних. Це дозволяє спростити аналіз вимог безпеки та визначити напрями посилення захисту інформаційно-комунікаційних систем енергетичної галузі.

Для аналізу використано Radar Chart, що дозволяє зіставляти вимоги за категоріями захисту, а також Heatmap, яка відображає ступінь критичності та інтенсивність вимог безпеки.

Для порівняння візьмемо Базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація, затверджений наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409 та Галузевий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація для ПЕК України.

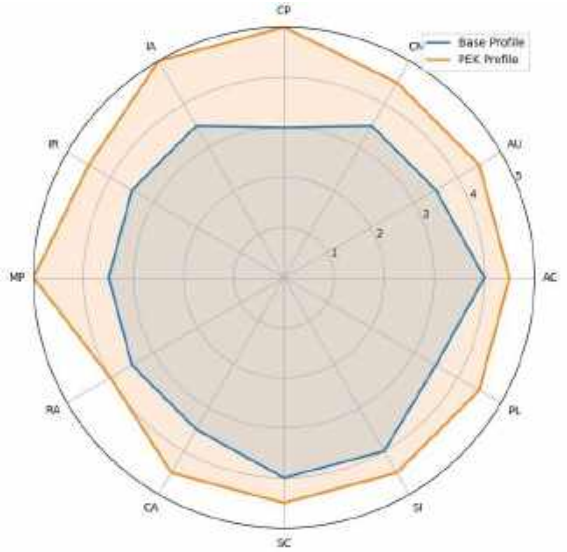


Рисунок 1 – Порівняння рівнів вимог до окремих категорій захисту

Radar-Chart (рис. 1) показує, що галузевий профіль ПЕК містить більш жорсткі вимоги до реалізації заходів безпеки практично за всіма напрямами. Найбільше підсилення спостерігається у сферах автентифікації, аудиту, захисту мобільних пристроїв та забезпечення безперервності роботи. Це свідчить про орієнтацію профілю ПЕК на захист критичної інфраструктури та підвищення кіберстійкості систем.

Рисунок 2 – Підсилення вимог у галузевому профілі

Heatmap (рис 2.) демонструє нерівномірне підсилення вимог у галузевому профілі. Найбільшу увагу приділено багатофакторній автентифікації, безперервності функціонування, захисту мобільних пристроїв, аудиту та конфігураційному управлінню. Це пояснюється необхідністю мінімізації ризиків кібератак та забезпечення стабільної роботи об'єктів ПЕК.

Отримані результати дозволяють зробити висновок, що галузевий профіль ПЕК відповідає більш високому рівню зрілості системи кібербезпеки та забезпечує значно вищий рівень захищеності інформаційних і технологічних процесів порівняно з базовим профілем. Його впровадження є обґрунтованим з огляду на підвищену критичність об'єктів паливно-енергетичного комплексу та потенційно значні наслідки реалізації кіберзагроз для економічної та національної безпеки держави.

1. Потенко О. С., Комаров М. Ю., Артемчук В. О., Зубок В. Ю., Гончар С. Ф. Порівняльний аналіз нових українських та міжнародних стандартів інформаційної безпеки // Електронне моделювання. 2025. Т. 47, № 5. С. 56–74. DOI: 10.15407/emodel.47.05.056.
2. Державна служба спеціального зв’язку та захисту інформації України.Базові профілі безпеки URL: https://cip.gov.ua/ua/news/bazovi-profili-bezpeki.
3. Проєкт наказу Міністерства енергетики України «Про затвердження профілів безпеки системи для паливно-енергетичного комплексу України» URL: https://www.mev.gov.ua/rehulyatornyy-akt/povidomlennya-pro-oprylyudnennya-proyektu-nakazu-ministerstva-enerhetyky-34.

О.В. Немикіна, І.П. Бабанін, Д.С. Чорнокнижний

КІБЕРЗАХИСТ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ В ЕНЕРГЕТИЦІ: ЗАГРОЗИ ТА МЕТОДИ ПРОТИДІЇ

Автоматизовані системи управління технологічними процесами є основою функціонування сучасної енергетичної інфраструктури. Вони забезпечують диспетчеризацію підстанцій, управління генерацією та розподілом електроенергії, моніторинг параметрів мережі в режимі реального часу. Зростаюча інтеграція промислових систем із корпоративними мережами та мережею Інтернет кардинально розширила поверхню кібератак, перетворивши системи управління на одну з найбільш вразливих складових критичної інфраструктури.

Промислові системи управління суттєво відрізняються від корпоративних інформаційно-технологічних систем за своїми пріоритетами безпеки. В класичній інформаційній безпеці ключовими цілями є забезпечення конфіденційності, цілісності та доступності даних. В системах управління технологічними процесами на першому місці стоїть безперервність технологічного процесу та фізична безпека обладнання. Характерними рисами промислових систем, що ускладнюють їх захист, є: тривалий строк служби обладнання (десятки років), застарілі протоколи зв’язку без вбудованих механізмів аутентифікації (Modbus, DNP3), а також географічна розподіленість об’єктів.

Спектр загроз для енергетичних систем управління є широким і постійно еволюціонує. Серед найбільш небезпечних: цільове шкідливе програмне забезпечення для промислових систем — Stuxnet (2010), BlackEnergy (2015), Industroyer (2016), TRITON (2017); атаки через ланцюжок постачань, що передбачають компрометацію обладнання або програмного забезпечення ще до його встановлення на об’єкті; фішинг та соціальна інженерія; атаки типу «відмова в обслуговуванні» на мережеву інфраструктуру.

Основою архітектури промислових мереж є ієрархічна модель (Purdue Reference Architecture), яка описує розподіл мережі на рівні від польових пристроїв до корпоративних систем. Модель передбачає чітке розмежування між операційними та інформаційними технологіями, яке реалізується через промислову демілітаризовану зону. Дотримання цієї архітектури є фундаментальним принципом захисту: за жодних обставин прямий маршрут від мережі Інтернет до програмованих логічних контролерів є неприпустимим.

Ефективний захист будується на принципі глибокої ешелонованої оборони, що передбачає застосування кількох незалежних рівнів захисних засобів. Жорстке розмежування мереж із застосуванням промислових міжмережевих екранів є першим рівнем захисту. Критично важливим є впровадження систем глибокої інспекції пакетів, які розуміють специфіку промислових протоколів: IEC 61850, IEC 60870-5-104, DNP3, Modbus TCP. Такі системи здатні виявляти аномальні команди навіть при використанні легітимних облікових даних. Системи виявлення вторгнень для промислового середовища використовують виключно пасивне прослуховування трафіку, оскільки активне сканування може спричинити відмову застарілих контролерів.

Концепція нульової довіри є відповіддю на реалію, за якої периметровий захист більше не є ефективним. Усі підключення до систем управління повинні здійснюватися через захищені шлюзи з обов'язковою багатофакторною автентифікацією та повним записом сесій. Технічні засоби захисту не можуть бути ефективними без відповідних організаційних заходів: розробки планів реагування на кіберінциденти, регулярних навчань персоналу, аудиту ланцюжка постачань.

Висновки

Кіберзахист систем управління технологічними процесами в енергетиці є комплексним завданням, що виходить за межі класичної інформаційної безпеки. Ефективний захист досягається лише шляхом поєднання технічних засобів (мережева сегментація, пасивний моніторинг аномалій, глибока інспекція промислових протоколів, концепція нульової довіри) з організаційними заходами (навчання персоналу, плани реагування, аудит постачальників) та методологічною базою відповідно до стандартів IEC 62443. В умовах сучасних реалій України, де енергетична інфраструктура функціонує під постійним комбінованим тиском, впровадження описаних заходів є питанням державної безпеки та стійкості критичної інфраструктури.

1. EC 62443: Industrial Automation and Control Systems Security. International Electrotechnical Commission, 2018–2023.
2. MITRE ATT&CK for ICS [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/matrices/ics/.
3. Директива NIS2 Європейського Парламенту та Ради (ЄС) 2022/2555 від 14 грудня 2022 року. – Офіційний журнал ЄС, 2022.
4. Немикіна О.В. Поновлювальні та альтернативні джерела енергії: навчальний посібник. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 187 с.
5. Caso D., Galloway B. Industrial Network Security: Securing Critical Infrastructure Networks. Syngress, 2021. – 460 p.

О.А. Владимирський, І.А. Владимирський, Д.М. Семенюк

ДОСЛІДЖЕННЯ АКУСТИЧНИХ ВЛАСТИВОСТЕЙ ТРУБОПРОВОДІВ ВЕЛИКИХ ДІАМЕТРІВ

Актуальність досліджень акустичних властивостей сталевих трубопроводів великих діаметрів, наприклад 820 мм, викликана, з одного боку, підвищеною потребою в їхньому діагностуванні внаслідок значного загальним зносу, зокрема міських магістральних трубопроводів теплових мереж, а з іншого боку - складною структурою реєстрованих при діагностуванні акустичних сигналів. Таке ускладнення хвильової структури сигналу є відомим і відбувається у випадках, коли довжина хвилі наближається до діаметру провідника і навіть стає меншою. За відомими формулами Д.Й. Кортевега і М.Є. Жуковського [1], швидкість хвиль гідравлічного удару для трубопроводу діаметром 820 мм з типовою товщиною стінки 9 мм. при температурі 20°С, тиску 4 Атм. у прісній воді становить: C_0=1067 м/с. Це означає, що у звичайному робочому діапазоні частот течешукачів 100-5000 Гц вже на частоті f =1500 Гц довжина хвилі є меншою ніж діаметр трубопроводу і становить: $\lambda = C_0 / f$ = 711 мм. Тому кількість та параметри збуджених, домінуючих за потужністю акустичних хвиль, що реєструє діагностичний прилад, потребують додаткових досліджень та врахування під час діагностування вказаних трубопроводів.

Необхідні для цього дослідження розпочато на ділянці сталевого технологічного трубопроводу діаметром 820 мм. довжиною 146 м. з прокладкою у прохідному каналі. Трубопровід є технологічним, заповненим водою під тиском 4,5 Атм. У травні поточного 2026 року проведено низку випробувань. Випробування містили вимірювання трьох типів: акустичні низькочастотні дистанційні, ультразвукові точкові для визначення фактичної товщини стінки та вимірювання електричного потенціалу у контрольних місцях трубопроводу з метою перевірки на присутність анодних зон.

Відомо, що на трубопроводі домінуючою є внутрішня корозія, рис.1а. Основну увагу у випробуваннях зосереджено на акустичних низькочастотних вимірюваннях, бо саме вони здатні забезпечити витребувану дистанційність діагностування. Для цього застосовувались прилади розробки ІПМЕ ім. Г.Є. Пухова НАН України: параметричний кореляційний течешукач К-10.5М3 і апаратно-програмний комплекс (АПК) «РАСТР-2В». У всіх випробуваннях відбувалось кероване за частотою та рівнем штучне вібраційне збудження стінки трубопроводу за допомогою акустичних випромінювачів. Для визначення хвильової структури відгуків проводилась їхня реєстрація на різних відстанях від випромінювача. Для підвищення хвильової розподільчої здатності застосовувались акустичні вимірювання трьох типів:

- багатоточкові синхронні вимірювання за параметричним кореляційним методом [2-5];
- вимірювання шляхом синхронної реєстрації не тільки нормальних, а ще й повздовжних та крутильних коливань стінки трубопроводу (тобто за напрямками координатних осей x,y,z);
- паралельно-послідовна реєстрація відгуків за допомогою сітки датчиків за принципами антенної решітки.

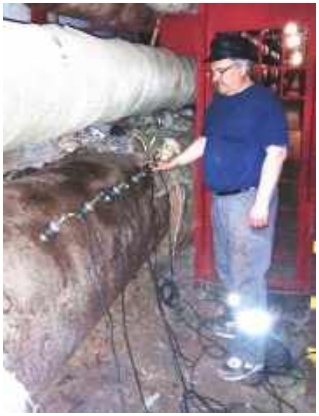
На рис.1 і 2 представлені відповідні фото.

Кожний тип вимірювань призначений для відповідного способу обробки сигналів.

а)

б)

в)



г)

д)

Рисунок 1 – Вид трубопроводу з внутрішньою корозією (а), вимірювання вібрації стінки трубопроводу трьох координатне (б), модельованою сіткою датчиків (в), та лінійною антеною з датчиків (г), вид двох реєстраторів, праворуч, підключених до датчиків на трубі, ліворуч (д).

Перші результати досліджень показали, що на фоні основної за площою, доволі товстої стінки трубопроводу товщиною 8,2…10,2 мм присутні місця

значного стоншення стінки, причому ці місця відповідають анодним рівням електричного потенціалу, рис.2в. Обробка та дослідження зареєстрованих масивів акустичних відгуків трубопроводу продовжується.

а)

б)

в)

Рисунок 2 – Вид реєстратора з генератором зондувальних сигналів, ліворуч, підключених до акустичного випромінювача та датчиків на трубі, праворуч (а), показання товщиноміра у точці трубопроводу з нормальною товщиною 9 мм (б) і поруч, у місці зі стоншенням до 1.2 мм (в) внаслідок внутрішньої корозії.

Дослідження виконується за бюджетною темою «ПАРАМЕТРИК» і за тематикою сумісних робіт з ДНТЦ ЯРБ.

1. В.Т. Гринченко, Г.Л. Комиссарова Особенности формирования волновых полей в заполненных жидкостью цилиндрах из жестких и мягких материалов. Акустичний вісник. 2012. Том 15, N 3. С. 3 – 21.

URL: https://nasplib.isofts.kiev.ua/server/api/core/bitstreams/ff061820-af6d-4614-9be1-8ce186f09125/content.

2. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання.* 2021. Т. 43, № 3. С. 3—16.
URL: https://doi.org/10.15407/emodel.43.03.003.
3. Патент на корисну модель № 144444; G01M 3/24, G01M 3/18, F17D 5/02. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат витоків трубопроводів. Публікація відомостей 25.09.2020, Бюл. №18. URL: https://sis.nipo.gov.ua/uk/search/detail/1456109/.
4. Патент на корисну модель №149956. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат пошкоджень трубопроводів. Публікація відомостей 15.12.2021р, Бюл. №50.
URL: https://sis.nipo.gov.ua/uk/search/detail/1668449/.
5. Патент на корисну модель №160421. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення фактичного значення швидкості поширення акустичних хвиль гідравлічного удару по трубопроводу. Публікація відомостей 10.09.2025р, Бюл. №37.
URL: https://sis.nipo.gov.ua/uk/search/detail/1875550.

С.Я. Гільгурт

РЕКОНФІГУРОВНІ ЗАСОБИ ПРИСКОРЕННЯ СИГНАТУРНОГО ВИЯВЛЕННЯ КІБЕРАТАК НА ЦИФРОВІ ПІДСТАНЦІЇ

Цифровізація електроенергетичних об'єктів та впровадження цифрових підстанцій відповідно до комплексу стандартів МЕК 61850 створюють нові можливості для автоматизації керування енергосистемами, але одночасно суттєво підвищують їх вразливість до кібератак [1]. Особливої актуальності проблема набуває в умовах воєнного стану, коли енергетична інфраструктура є одним із пріоритетних об'єктів кібернетичного впливу. Одним із найефективніших механізмів протидії мережевим атакам залишаються сигнатурні мережеві системи виявлення вторгнень (МСВВ), здатні здійснювати глибокий аналіз мережевого трафіку та виявляти відомі шаблони шкідливої активності.

Особливістю цифрових підстанцій є використання спеціалізованих протоколів MMS, GOOSE та Sampled Values, а також жорсткі вимоги до затримок передавання повідомлень і гарантованого часу реакції систем автоматики. Тому програмні МСВВ, побудовані на базі універсальних процесорів, не завжди забезпечують необхідний рівень продуктивності при аналізі мережевого трафіку в режимі реального часу. У ході досліджень було розглянуто сучасні підходи до побудови сигнатурних МСВВ на базі регулярних виразів та скінченних автоматів. Встановлено, що традиційні програмні реалізації глибокої інспекції пакетів стикаються зі значним падінням продуктивності у зв’язку зі збільшенням кількості сигнатур та складності правил аналізу. Для сучасних наборів правил МСВВ характерна наявність тисяч сигнатур, значна частина яких містить оператори повторення, альтернативи та символьні класи. Це призводить до різкого збільшення кількості станів автоматів та зростання навантаження на центральний процесор [2].

Для усунення зазначених обмежень досліджено можливість перенесення операції множинного розпізнавання сигнатур до реконфігуровних апаратних засобів на базі ПЛІС типу FPGA. На відміну від програмних реалізацій, реконфігуровні засоби дозволяють виконувати аналіз множини сигнатур паралельно на апаратному рівні, забезпечуючи детерміновану продуктивність незалежно від навантаження. Особливий інтерес для задач кіберзахисту цифрових підстанцій становлять архітектури, побудовані на основі недетермінованих скінченних автоматів (NFA), які природним чином відображають структуру регулярних виразів та добре пристосовані до апаратної реалізації [2-4].

У роботі проаналізовано модифікований алгоритм Домьолкі–Бейза-Ятса–Гоннета (Extended Shift-And), що використовує бітово-паралельне подання станів NFA. Перевагою цього підходу є можливість реалізації

великої кількості переходів за один такт FPGA шляхом використання операцій зсуву та логічної обробки бітових масок. Дослідження показали, що застосування каскадованих модулів розпізнавання дозволяє усунути обмеження на кількість станів автоматів та підтримувати складні сигнатури з великою кількістю повторень і вкладених конструкцій. Крім того, використання блокової пам'яті FPGA для зберігання таблиць переходів дозволяє значно зменшити апаратні витрати порівняно з традиційними реалізаціями [3].

На підставі проведених досліджень сформовано концепцію апаратного прискорення виявлення вторгнень для цифрових підстанцій. Запропонований підхід передбачає багаторівневу структуру захисту. На нижньому рівні виконуються високошвидкісна фільтрація трафіку та сигнатурний аналіз мережевих пакетів із використанням регулярних виразів. На верхньому рівні здійснюється кореляція подій та аналіз специфічних для МЕК 61850 ознак атак на протоколи MMS, GOOSE та SV. Використання FPGA дозволяє перенести найбільш ресурсоємні операції зіставлення шаблонів до апаратного рівня, залишаючи центральному процесору лише функції прийняття рішень та управління.

Отримані результати дозволили розвинути методичні засади побудови сигнатурних систем виявлення вторгнень для цифрових підстанцій на базі регулярних виразів і реконфігуровних обчислювальних засобів. Запропоновані підходи забезпечують поєднання високої швидкодії, масштабованості та можливості оперативного оновлення сигнатур атак, що є необхідною умовою захисту сучасних цифровізованих об'єктів енергетики. Практичне впровадження таких рішень сприятиме підвищенню кіберстійкості цифрових підстанцій та зміцненню безпеки енергетичної інфраструктури України в цілому.

1. Гільгурт С.Я. (2025) Підвищення резильєнтності реконфігуровних сигнатурних систем технічного захисту інформації шляхом використання регулярних виразів. У *Резильєнтність динамічних систем: Матеріали II науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України* (с. 83-85). ІПМЕ ім. Г.Є. Пухова НАН України.
2. Nam, J., Na, S. H., Shin, S., & Park, T. (2022). Reconfigurable regular expression matching architecture for real-time pattern update and payload inspection. *Journal of Network and Computer Applications*, 103507. https://doi.org/10.1016/j.jnca.2022.103507.
3. 2. Kim J., Park J. (2018) FPGA-based memory efficient shift-and algorithm for regular expression matching. *Lecture Notes in Computer Science. 14th International Symposium on Applied Reconfigurable Computing* (p. 132-141), 10824. https://doi.org/10.1007/978-3-319-78890-6_11.
4. Zhang, C., Tang, X., & Peng, Y. (2024). Enhancing regular expression processing through field-programmable gate array-based multi-character non-deterministic finite automata. *Electronics*, 13(9), 1635. https://doi.org/10.3390/electronics13091635.

С.В. Сушко

СУЧАСНІ ЗАСОБИ МОНІТОРИНГУ ПАРАМЕТРІВ ЕНЕРГОМЕРЕЖІ

Способи віддаленого моніторингу різноманітних об’єктів, включаючи моніторинг параметрів енергомережі, досліджуються тривалий час [1-5]. Загалом, це велика задача, оскільки для повної реалізації моніторингу параметрів енергомережі зокрема або керування «розумним будинком» загалом потрібно:

- Створення програмного коду для пристроїв і серверної частини;
- Використання наявних протоколів передачі даних або створення нових;
- Створення пристроїв під різноманітні задачі;
- Створення графічної оболонки для відображення отриманих даних.

Наразі існує декілька існуючих систем «розумного будинку», що можуть використовуватись для задач моніторингу параметрів енергомережі. Розглянемо систему Tuya Smart [6]. Вона задовольняє усім вимогам, що перераховані вище та забезпечує інтеграцію багатьох пристроїв, використовуючи мережі передачі даних WI-FI або Zigbee.

Після додавання пристрою, в залежності від параметрів пристроїв, доступна інформація щодо напруги, струму споживання, потужності, історії споживання потужності з графіками по годинам, дням, місяцям. Приклад отриманих даних для пристрою наведено на рис. 1.

Рисунок 1 – Приклад загального інтерфейсу пристрою вимірювання параметрів енергомережі та історичний графік вимірів потужності споживання по дням

Після тривалого використання автором, головні функції та сервіси Tuya Smart підтверджено.

Переваги системи Tuya Smart:

1. Наявність на ринку великої кількості різноманітних пристроїв під будь-які потреби: моніторинг параметрів енергомереж, контроль параметрів стану довкілля, домашня автоматизація та інші;
2. Легка інтеграція нових пристроїв;
3. Невисока ціна для більшості пристроїв ($5-$20);
4. Наявність застосунку для Android та IOS.

Недоліки системи Tuya Smart:

1. Система використовує хмарне зберігання даних;
2. Протоколи передачі даних не афішуються, незрозуміла криптостійкість переданих даних;
3. Відсутність української мови серед наявних мов інтерфейсу.

Висновок: використання системи «розумного будинку» Tuya Smart забезпечує зручну і наочну взаємодію з великою кількістю пристроїв від багатьох виробників. Водночас, зберігання і оброблення даних на хмарних серверах становить загрозу стосовно захищеності переданих даних і можливості дистанційного втручання зловмисників. Існують способи розгортання серверу локально, проте такі рішення вимагають специфічних знань і компетенцій.

1. Singh, K. J. , Kapoor, D. S. . (2017) Create your own internet of things: a survey of iotplatforms. IEEE Consumer Electronics Magazine, 6: 57-68.
2. Melloul, L. , Fox, O. . (2001) Towards zero-code service composition. Proceedings of 8thWorkshop on Hot Topic in Operating Systems, 0172.
3. Kuang, X. H. , & Huo, H. B. . (2014) A design of WiFi wireless transmission module based onMCU. Applied Mechanics & Materials, 442: 367-371.
4. Nguyen, K. T. , Laurent, M. , & Oualha, N. . (2015) Survey on secure communication protocols for the internet of things. Ad Hoc Networks, 32: 17-31.
5. Talesra, K., Nagaraja, G. S.. (2021) Low-code platform for application development. International Journal of Applied Engineering Research, 16:346-351 *(PDF) Design and implementation of intelligent dimming switch based on "Tuya Cloud"*.https://www.researchgate.net/publication/384139099_Design_and_implementation_of_intelligent_dimming_switch_based_on_Tuya_Cloud.
6. Tuya Developer Documentation https://developer.tuya.com/en/overview

О.А. Владимирський, І.А. Владимирський, Д.М. Семенюк

АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ДЛЯ ДІАГНОСТУВАННЯ ТРУБОПРОВОДІВ

Для оперативного пошуку витоків в Україні застосовуються найсучасніші прилади від провідних виробників. Проте умови пошуку витоків є ширшими ніж діагностичні можливості існуючих приладів. Різниця між цими умовами та можливостями призводить до зайвих розтинів підземних трубопроводів, додаткових втрат часу та ресурсів під час ремонтів мереж, затримкам у відновленні тепло- та водопостачання споживачів. До типових ускладнень призводять: розгалуженість підземних мереж у сукупності зі зносом запірної арматури, суттєве корозійне потоншення стінок трубопроводів, різноманітність акустичних завад, мале відношення сигнал-завада і т.і.. Необхідність більш повного врахування цих особливостей задля точного інструментального визначення витоків у наявних складних умовах стало причиною створення апаратно-програмного комплексу (АПК) «РАСТР-2В» .

АПК «РАСТР-2В» (рис.1) [1, 2, 3] являє собою низькочастотну систему акустичного зондування трубопроводу та пошуку витоків. АПК є модернізованим варіантом системи акустичного моніторингу трубопроводів «РАСТР-1» розробки ІПМЕ ім. Г.Є. Пухова НАН України. Система реалізує вдосконалений та доповнений новими функціями, поширений кореляційний метод визначення координат витоків на підземних ділянках трубопроводів.

АПК призначений для пошуку витоків у важких для діагностування трубопроводів умовах, виконує функції базової системи для випробування та застосування “нестандартних” рішень завдяки спрямованій на це, гнучкій за схемою застосування апаратній структурі та можливостей програмування її функцій. Основними функціями АПК є наступні:

- проведення пошуку витоків кореляційним методом в умовах потужних радіо завад без використання якісного задіозв’язку шляхом застосування реєстраторів акустичних сигналів трубопроводів, які встановлюються біля місць реєстрації сигналів;
- проведення пошуку витоків в умовах послаблених сигналів від витоку та, як наслідок цього, малого відношенні сигнал-завада, завдяки використанню параметричної узгодженої, просторово-частотної селекції корисних сигналів та їхніх кореляційних функцій [1];
- врахування та усунення впливу на точність визначення координат витоків інтерференційних спотворень, що виникають під час реєстрації акустичних сигналів трубопроводів зі складною структурою [1];
- проведення пошуку витоків в умовах потужних зовнішніх акустичних завад, якщо їхнє тимчасове відключення є неможливим;

Рисунок 1 – Складові АПК «РАСТР-2В»: реєструючи станції «А», «В» і «С» (а), реєструюча станція з підключеними датчиками ВДМ-6 (б); три різновиди акустичних випромінювачів з магнітними кріпленнями з супер магнітів (в,г); генератор зондувальних сигналів трубопроводів з підключеними акустичними випромінювачами (д); кейс з датчиками ВДМ-6 (е)

- уточнення фактичної швидкості поширення інформативних акустичних хвиль по трубопроводу з врахуванням його корозійного зносу та дисперсії акустичних хвиль;
- проведення акустичного тестування трубопроводу для з'ясування умов та можливостей його подальшого якісного діагностування акустичними

методами, для з'ясування причини можливих утруднень з визначення витоку та виконання відповідних дій.

Склад та призначення складових АПК наведено у табл. 1. Основні технічні характеристики представлено у табл.2.

Таблиця 1 – Склад АПК «РАСТР-2В»

Назва складової АПК	Призначення
Станція реєстрації (3шт)	Реєстрація акустичних сигналів трубопроводів та їх накопичування у вигляді файлів для наступної обробки [3].
Вібродатчик ВДМ-6 з магнітним тримачем (7шт)	Перетворення вібрації стінки трубопроводу у електричний сигнал для його подальшої реєстрації станцією.
Генератор синхросигналу	Радіо синхронізація одночасного запису сигналів у реєструючи станції.
Генератор зондувальних сигналів	Формування електричних сигналів з завданими параметрами для акустичного зондування трубопроводу
Акустичний випромінювач (7шт)	Перетворення електричних зондувальних сигналів у акустичні та їх передача у стінку трубопроводу
Мобільний ПК зі спеціальним програмним забезпеченням	Цифрова фільтрація даних, обчислення ВКФ сигналів, їхніх параметрів, проведення параметричного аналізу ВКФ та визначення найбільш вірогідної координати витоку [2].
Комплект електричних сигнальних кабелів	Передача сигналів між складовими АПК.
Термо-акучтичний течешукач А-10Т3	Допоміжний засіб з пошуку витоків.

Ефективність АПК «РАСТР-2В» доведено при пошуку витоків у міських системах тепло- та водопостачання м. Києва.

Робота виконана за сприянням фонду НФДУ 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень системи тепло- та водопостачання з урахуванням зношення та мілітарних впливів».

Таблиця 2 – Основні характеристики АПК «РАСТР-2В»

Складова АПК	Характеристики
Станція реєстрації акустичних сигналів трубопроводів	• Кількість каналів реєстрації сигналів – 3; • частота дискретизації сигналів – 25кГц; • частотний діапазон сигналів – 10Гц-12кГц; • динамічний діапазон сигналів – 120дБ
Вібродатчик ВДМ-6 з магнітним тримачем	• Тип: п'єзокерамічний акселерометр; • чутливість – 10мВ×М/с^2; • убудоване підсилення – 0Дб і 40дБ. • частотний діапазон – 10Гц-12кГц.
Випромінювач радіо синхронізації	• Дальність дії - 1 км.
Генератор зондувальних сигналів трубопроводів	• Потужність – до 100Вт; • кількість рівнів регулювання за потужністю – 10; • тривалість генерованих сигналів хвилин: 1…11; • кількість видів зондувальних сигналів – 9.
Акустичний випромінювач зондувальних сигналів	• тип 1: потужність 50 Вт опір 8 Ом – 2 шт; • тип 2: потужність 25 Вт опір 4 Ом – 4 шт; • тип 3: потужність 100 Вт опір 4 Ом – 1 шт; • частотний діапазон 10 Гц - 18кГц.

1. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання.* 2021. Т. 43, № 3. С. 3—16.
   URL: https://doi.org/10.15407/emodel.43.03.003.
2. О.А. Владимирський, І.А. Владимирський. Комп'ютерна програма "Режим параметричного аналізу кореляційних функцій "Аналізатор-2В" системи виявлення витоків підземних трубопроводів "РАСТР-2В". Свідоцтво про реєстрацію авторського права на службовий твір № 141405 від 03.12.2025р. ІПМЕ ім. Г.Є. Пухова НАН України. Публ. 31.01.2026, бюл. № 97.
   URL: https://sis.nipo.gov.ua/uk/search/detail/1897653/.
3. Владимирський О.А, Владимирський І.А., Артемчук В.О. Комп'ютерна програма «Багатоканальний реєстратор «Вібрологгер - 3.02» системи виявлення витоків підземних трубопроводів «РАСТР-2В». Свідоцтво про реєстрацію авторського права на службовий твір № 132954 від 03.02.2025р. ІПМЕ ім. Г.Е.Пухова НАН України. Публ. 31.03.2025, бюл. № 87.
   URL: https://sis.nipo.gov.ua/uk/search/detail/1848332/.

В.В. Мохор, О.В. Цуркан, Р.П. Герасимов, В.П. Яшенков, Т.М. Клименко

АНАЛІЗ УНІФІКОВАНОЇ МОДЕЛІ ОПОСЕРЕДКУВАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Один з негативних аспектів використання штучного інтелекту є орієнтованість на порушування властивостей інформації [1, 2]. Об'єктом такого впливання насамперед виокремлюється людина (зокрема, працівник організації). Маніпулювання нею реалізується використанням відповідних моделей генеративного штучного інтелекту, наприклад [2]: WormGPT, FraudGPT, VirusGPT, PoisonGPT. Попри наявність даних екземплярів, їх застосування зі зловмисною метою притаманне й типовим рішенням GPT, DeepSeek, Gemini, LLaMA. Завдяки цьому можливе моделювання вірогідних сценаріїв взаємодіяння соціального інженера та працівника організації. Це призводить до виникання нових векторів атак [1–4]. Тому аналізування уніфікованої моделі опосередкування соціальної інженерії на основі штучного інтелекту актуальне.

Уніфіковану модель опосередкування соціальної інженерії на основі штучного інтелекту запропоновано в [5]. Її розробляння зосереджене на подоланні обмежень застосування відомих рішень. Отриманим аналізом демонструється зосередженість на екземплярах моделей генеративного штучного інтелекту та об'єктах маніпулювання. У даному випадку операційними обмеженнями вказується на відсутність пояснень реалізування атак соціальної інженерії. Тож для їх подолання у [4] запропоновано відображення можливостей генеративного штучного інтелекту на етапах життєвого циклу в поєднанні з прийняттям рішень. Наступними встановленими обмеженнями є відсутність кількісного оцінювання дій з боку соціального інженера. Вони усуваються урахуванням змін впливу генеративного штучного інтелекту на процес прийняття рішень (наприклад, «атакувати», «не атакувати»). До того ж соціальний інженер відображається як раціональний економічний агент. У такий спосіб унеможливлюється його інтерпретування через пасивну сутність. Загалом подолання виокремлених обмежень виконано інтегруванням представлень трьох вимірів – реалізм, персоналізування, автоматизування. До того ж кількісним оцінюванням їхнього впливання на поведінку соціального інженера.

Відповідно до [5] уніфікована модель опосередкування соціальної інженерії на основі штучного інтелекту (англ. Unified Model of AI-Mediated Social Engineering) визначається кортежем

$$M = (S, A, P, R, \gamma),$$

де S – множина вірогідних станів соціального інженера стосовно працівника організації, наприклад: довірений;

A – множина дій соціального інженера, наприклад: обманути;

P – імовірність переходу соціального інженера до стану s' зі стану s після дії a;

R – винагорода переходу соціального інженера до стану s' зі стану s після дії a;

γ – коефіцієнт дисконтування, яким відображається перевага поточних винагород соціального інжереренера порівняно з майбутніми.

Взаємодіяння між даними складниками обумовлюється метою соціального інженера. Зокрема його прагненням максимізувати очікувану кумулятивну винагороду внаслідок вчинених дій [5]. Її велична, $V^*(S)$, визначається рівнянням оптимальності Беллмана

$$V^*(s) = \max_{a \in A} \sum_{s' \in S} P(s,a,s')[R(s,a,s') + \gamma V^*(s')].$$

Використання даного виразу зводиться до знаходження очікуваної корисності виконання дії для усіх вірогідних результатів і, як наслідок, обирання серед них оптимальної. Це дозволяє встановлювати поріг прийняття рішень з огляду на діяльність соціального інженера.

Отже, використання уніфікованої моделі опосередкування соціальної інженерії на основі штучного інтелекту орієнтоване на подолання обмежень асоційованих з діями соціального інженера. Основний акцент робиться на корисності дій з його боку та обиранні серед них оптимальної. Це досягнуто інтегруванням представлень трьох вимірів – реалізму, персоналізування, автоматизування. Проте поза увагою залишено вразливості, наприклад, працівника організації які та як використовує соціальний інженер у межах кожних з виокремлених станів і дій.

1. Мохор В. В., Цуркан О. В., Герасимов Р. П., Клименко Т. М., Яшенков В. П. Соціоінженерний аспект використання генеративного штучного інтелекту. *Кібербезпека енергетики* : матеріали (Київ, 29 травня 2024 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2024. С. 114–115.
2. Мохор В. В., Цуркан О. В., Герасимов Р. П., Яшенков В. П., Клименко Т. М., Павловська В. І. Аналіз використання великих мовних моделей в атаках соціальної інженерії. *Штучний інтелект і безпека* : матеріали (Київ, 04 грудня 2025 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2025. С. 178–179.
3. Webb J., Abri F., Akther S. Synthetic Social Engineering Scenario Generation Using LLMs for Awareness-Based Attack Resilience. *IEEE Access*. 2025. Vol. 13. P. 174831–174856. DOI: https://doi.org/10.1109/ACCESS.2025.3614550.
4. Yu T., Yang Y., Zhou Z., Xu J., Li S., Guan T., Wang K., Bi T. *PhySE : A Psychological Framework for Real-Time AR-LLM Social Engineering Attacks*. Computer Science. Artificial Intelligence. 2026. arXiv : 2604.23148. DOI: https://doi.org/10.48550/arXiv.2604.23148.
5. Gonzaga K., Serra S., Gomes M., Malta S. AI-Powered Social Engineering : Emerging Attack Vectors, Vulnerabilities, and Multi-Layered Defense Strategies. *Computers*. 2026. Vol. *15, No.* 2. P. 1–35. DOI: https://doi.org/10.3390/computers15020128.

А.В. Ковилін

КОМПЛЕКСНЕ ЕКСПЕРИМЕНТАЛЬНЕ ОЦІНЮВАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ВІДОМИХ ТА НЕВІДОМИХ КІБЕРАТАК У ЦИФРОВИХ ПІДСТАНЦІЯХ

Цифровізація енергетичної інфраструктури супроводжується активним впровадженням промислових комунікаційних протоколів, автоматизованих систем керування, віддаленого моніторингу та інтеграції технологічних об'єктів із корпоративними інформаційними системами. Такі процеси підвищують ефективність експлуатації електроенергетичних об'єктів, однак водночас розширюють кількість контурів для кібератак і формують нові ризики для стабільності та безпеки енергосистем [1]. Особливої уваги потребують цифрові підстанції, у яких інформаційні потоки використовуються для передавання телеметрії, керуючих команд, повідомлень про стан обладнання та інших критично важливих даних. Одним із протоколів, що застосовується для телемеханіки, віддаленого моніторингу та керування, є IEC 60870-5-104 [4].

Порушення доступності, цілісності або достовірності такого трафіку може негативно впливати на функціонування систем керування та процеси прийняття рішень оператором. Одним із перспективних напрямів підвищення кіберстійкості цифрових підстанцій є використання систем виявлення вторгнень.

У сучасних дослідженнях значна увага приділяється застосуванню методів машинного навчання для аналізу мережевого трафіку, виявлення аномалій та класифікації шкідливої активності у промислових системах керування [5], [6]. Водночас значна частина експериментальних досліджень обмежується сценарієм, у якому всі типи атак, наявні у тестовій вибірці, також представлені у навчальних даних. Такий підхід може призводити до надмірно оптимістичної оцінки якості моделей, оскільки у практичних умовах експлуатації система може зіткнутися з новими, модифікованими або раніше невідомими атаками [7], [8]. У зв'язку з цим актуальною є задача комплексного оцінювання моделей машинного навчання не лише у стандартному сценарії відомих атак, але й у сценаріях невідомих атак, нестачі розмічених даних, нерівномірного розподілу класів, перенесення ознак між різними атаками та зміни порогів прийняття рішення. Саме тому метою роботи є комплексне експериментальне оцінювання моделей машинного навчання для виявлення відомих та невідомих кібератак у трафіку цифрових підстанцій.

Для експериментального дослідження використано processed IEC104 частину набору даних SANDI-2024, призначену для навчання та оцінювання методів виявлення вторгнень у середовищі цифрових підстанцій [2], [3].

Вибір цього набору даних зумовлений його предметною орієнтацією на енергетичну інфраструктуру, наявністю нормального трафіку та декількох типів атак, що дозволяє формувати різні сценарії експериментального оцінювання.

У дослідженні розглянуто такі класи трафіку: нормальний трафік, DoS attack, flood attack, fuzzy attack, IEC104 starvation attack, MITM attack, NTP DDoS attack та port scan attack.

У стандартному сценарії, коли всі типи атак були представлені у навчальній вибірці, supervised-моделі продемонстрували дуже високу якість виявлення. Це свідчить, що за наявності прикладів відомих атак моделі машинного навчання здатні ефективно розпізнавати шкідливий трафік у даних цифрової підстанції. Водночас такий сценарій слід розглядати як базовий та оптимістичний, оскільки він не відображає умови появи нових або раніше невідомих атак.

Попри те що узагальнення результатів показало, що стандартний сценарій оцінювання відомих атак демонструє майже ідеальну якість supervised-моделей необхідно перевірити чи є він достатнім для висновку про їхню стійкість до нових загроз. Саме тому в роботі були використані додаткові сценарії експериментального оцінювання: leave-one-attack-out, leave-attack-group-out, anomaly-based detection, few-shot adaptation, rare-attack training stress, cross-attack transfer та threshold tuning.

Сценарії leave-one-attack-out та leave-attack-group-out виявили залежність якості виявлення від типу невідомої атаки, причому найбільш складною для моделей стала NTP DDoS. Anomaly-based підходи забезпечили високу чутливість до атак, але супроводжувалися підвищеним рівнем хибних спрацювань. Few-shot adaptation підтвердила практичну доцільність донавчання моделей після появи перших прикладів нової атаки, а rare-attack training stress показав потенційну стійкість ансамблевих моделей до дефіциту розмічених даних. Cross-attack transfer засвідчив нерівномірність перенесення ознак між різними атаками, а threshold tuning показав необхідність налаштування порогів прийняття рішення з урахуванням допустимого рівня хибних спрацювань та критичності енергетичного об’єкта.

Висновок. У роботі проведено комплексне експериментальне оцінювання моделей машинного навчання для виявлення відомих та невідомих кібератак у трафіку цифрових підстанцій. На відміну від стандартного benchmark-підходу, дослідження охоплює кілька сценаріїв: виявлення відомих атак, leave-one-attack-out, leave-attack-group-out, anomaly-based detection, few-shot adaptation, rare-attack training stress, cross-attack transfer та threshold tuning. Результати показали, що supervised-моделі

забезпечують високу якість виявлення відомих атак, однак їхня ефективність може знижуватися у випадку окремих невідомих атак, зокрема NTP DDoS. Anomaly-based підходи можуть підвищувати чутливість до потенційно нових загроз, але потребують контролю рівня хибних спрацювань. Few-shot adaptation підтверджує доцільність донавчання моделей після появи перших прикладів нової атаки, а cross-attack transfer показав, що перенесення ознак між різними атаками є нерівномірним. Аналіз порогів прийняття рішення засвідчив, що налаштування threshold може суттєво впливати на баланс між Recall та False Positive Rate. Отримані результати обґрунтовують доцільність комбінованого підходу до побудови компонентів IDS для цифрових підстанцій з використанням моделей машинного навчання, у якому supervised-моделі, anomaly-based detection, few-shot adaptation та калібрування порогів використовуються як взаємодоповнювальні елементи.

1. Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to operational technology (OT) security (NIST Special Publication No. 800-82 Rev. 3). National Institute of Standards and Technology. doi: 10.6028/NIST.SP.800-82r3.
2. 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, 111153. doi: 10.1016/j.dib.2024.111153.
3. Gutiérrez Mlot, E. D., Saldana, J., Rodríguez, R. J., Kotsiuba, I., & Gañán, C. (2025). Dataset to train intrusion detection systems based on machine learning models for electrical substations [Data set]. Zenodo. doi: 10.5281/zenodo.15487636.
4. International Electrotechnical Commission. (2006). IEC 60870-5-104:2006: Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles. International Electrotechnical Commission.
5. Umer, M. A., Junejo, K. N., Jilani, M. T., & Mathur, A. P. (2022). Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. International Journal of Critical Infrastructure Protection, 38, 100516. doi: 10.1016/j.ijcip.2022.100516.
6. Gauthama Raman, M. R., Ahmed, C. M., & Mathur, A. (2021). Machine learning for intrusion detection in industrial control systems: Challenges and lessons from experimental evaluation. Cybersecurity, 4, Article 27. doi: 10.1186/s42400-021-00095-5.
7. Zoppi, T., Ceccarelli, A., Puccetti, T., & Bondavalli, A. (2023). Which algorithm can detect unknown attacks? Comparison of supervised, unsupervised and meta-learning algorithms for intrusion detection. Computers & Security, 127, 103107. doi: 10.1016/j.cose.2023.103107.
8. Sarhan, M., Layeghy, S., Gallagher, M., & Portmann, M. (2023). From zero-shot machine learning to zero-day attack detection. International Journal of Information Security, 22, 947–959. doi: 10.1007/s10207-023-00676-0.

Я.Ю. Дорогий, В.С. Ракович, В.В. Цуркан

КОНЦЕПТУАЛЬНІ РІВНІ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кібербезпека об'єктів критичної інфраструктури обумовлюється узгодженістю з міжнародними, регіональними та національними нормативними документами [1–6]. Перш за все це пов'язується з прагненнями України до європейського та євроатлантичного інтегрування. Крім того, кібербезпека об'єктів критичної інфраструктури забезпечується розробляннням відповідної національної системи [1]. В межах діяльностей її складників передбачається взаємодіяння з відповідними міжнародними структурами. Тож урахування найкращих світових практик доповнюється необхідністю гармонізування вітчизняного законодавства з нормативними документами міжнародної організації зі стандартизації [2–4], Європейського союзу [5], Національного інституту стандартів і технологій [6]. Тому формулювання концептуальних рівнів повідомляння про події кібербезпеки об'єктів критичної інфраструктури актуальне.

Міжнародний рівень визначається на основі серії нормативних документів ISO/IEC 27035 [3], а також [4]. При цьому поводження з інцидентами є одним з ключових організаційних заходів обробляння неприйнятних ризиків. Він реалізується при розробляннні систем управління інформаційною безпекою [2]. У межах даного рівня об'єкт критичної інфраструктури інтерпретується як організація. Цим обумовлюється необхідність упроваджування механізму своєчасного повідомляння працівниками або відповідальної особи, або підрозділу кіберзахисту про події кібербезпеки встановленими каналами [1, 3]. Насамперед стосовно вірогідних або порушень властивостей інформації, або збоїв відповідних заходів і засобів. Тож подія кібербезпеки інтерпретується як один з визначальних об'єктів інциденту. З огляду на дескриптивне представлення потоку подій ініціюється отриманням інформації про неї [1]. За результатами виявляння і звітування подія кібербезпеки оцінюється. Як наслідок, приймається рішення стосовно її належності до інциденту.

Регіональний рівень визначається настановами директиви NIS 2 і насамперед узгоджується з прагненням України до європейського інтегрування [5]. Вони стосуються перш за все інформаційної інфраструктури (наприклад, мережевих та інформаційних систем). На регіональному рівні ключовим поняттям залишається «Інцидент», а також послідовність і дієвість поводження з повідомленнями про нього. Це спонукає до запроваджування «єдиного вікна» – механізму автоматичного та прямого звітування перед зацікавленими сторонами [5]. Його використанням передбачено врахування угод нерозголошення інформації за протоколом TLP. Таким підходом передбачається гармонізування шаблонів повідомлень про інциденти кібербезпеки. При цьому їх врегулювання покладається на групи реагування на інциденти комп'ютерної безпеки/комп'ютерні надзвичайні ситуації (CSIRT/CERT). Дане завдання виконується обробляннням великих обсягів інформації про вразливості, загрози, ризики.

Національний рівень визначається настановами директиви NIST SP 800-61:Rev. 3 і, за аналогією з регіональним, насамперед узгоджується з прагненням України до євроатлантичного інтегрування [6]. Основна увага зосереджується на несприятливих подіях кібербезпеки інформаційних систем. І, водночас, на реалізуванні єдиного підходу як при внутрішньому, так і при зовнішньому обміні інформацією між організаціями [6]. При цьому реагування на інциденти розглядається як критично важливий складник процесу управління ризиками. Його впроваджування ґрунтується на шести функціях фреймворку кібербезпеки CSF 2.0. Так [6], реалізування функції ідентифікування (англ. Identify) передбачає усвідомлювання потенційних несприятливих подій. З огляду на це вживаються відповідні заходи забезпечування кібербезпеки (англ. Protect). Виокремлені дії виконуються відповідно до встановлених стратегії і політики управління ризиками (англ. Govern). Тоді як реагування на інциденти починається у межах функції виявляння (англ. Detect).

Отже, концептуальні рівні повідомляння про події кібербезпеки об'єктів критичної інфраструктури формулюються з урахуванням, по-перше, прагнення України до європейського та євроатлантичного інтегрування. По-друге, необхідності взаємодіяння з відповідними міжнародними системам. Як наслідок, сформульовано міжнародний, регіональний і національній рівні повідомляння про події кібербезпеки об'єктів критичної інфраструктури. Характерною особливістю міжнародного рівня є зосередженість на події, встановленні ознак її належності до інциденту. Для обробляння події кібербезпеки передбачається розробляння і впроваджування в організації механізму повідомляння. Тоді як у межах двох інших рівнів основна увага зосереджується на діяльності стосовно поводження з інцидентами.

1. Цуркан В., Ракович В. Механізм повідомляння про події кібербезпеки об'єктів критичної інфраструктури. *Кібербезпека : освіта, наука, техніка*. 2026. Том 4, № 32. P. 1002–1014. DOI: https://doi.org/10.28925/2663-4023.2026.32.1200.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-09-23]. URL: https://www.iso.org/standard/27001 (accessed on: 25.05.2026).
3. ISO/IEC 27035-1:2023. Information technology. Information security incident management. Part 1: Principles and process. [Valid from 2023-02-13]. URL: https://www.iso.org/standard/78973.html (accessed on: 25.05.2026).
4. ISO/IEC/IEEE FDIS 23612:2025. Software and systems engineering. Incident management. [Valid from 2025-11-18]. Geneva, 2025. 41 p.
5. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) : Директива європейського парламенту і ради (ЄС) 2022/2555 від 14.12.2022. URL:https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 25.05.2026).
6. NIST SP 800-61:2025 (Rev. 3). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. [Valid from 2025-04-03]. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (accessed on: 25.05.2026).

О.А. Чемерис

УЧАСТЬ УКРАЇНСЬКИХ ОРГАНІЗАЦІЇ В КОНКУРСАХ ПРОГРАМИ HORIZON EUROPE ЗА НАПРЯМОМ КІБЕРБЕЗПЕКА

У рамках програми "Горизонт Європа" кібербезпека є частиною кластера, що охоплює цивільну безпеку суспільства. Європейська комісія фінансує дослідницькі та інноваційні проєкти, які стосуються управління кризовими ситуаціями, боротьби з тероризмом, а також забезпечення зовнішньої та прикордонної безпеки. У рамках цього кластера акцентується на зміцненні європейської стійкості до кіберзагроз і сприянні розвитку передових технологій у сфері безпеки. Єврокомісія вважає, що кібербезпека є критично важливою для забезпечення стабільності та безпеки в цифровому середовищі, а також сприяє розвитку економіки і технологічного прогресу в Європейському Союзі. Вона впроваджує нові ініціативи для зміцнення кібернетичної безпеки в країнах-членах. Програма «Горизонт Європа» є одним з механізмів для створення і впровадження інноваційних розробок в даній сфері.

Великі можливості програма надає для науковців та практиків в сфері кібербезпеки. Табл. 1 демонструє основні показники конкурсів щодо напряму кібербезпеки.

Таблиця 1 – Загальні показники конкурсів з кібербезпеки

	2023	2024	2025	2026	2027
Число конкурсів, шт.	3	2	6	3	4
Загальний бюджет млн. євро	58,7	60,4	90,55	56,2	71,8
Кількість проєктів переможців, шт.	10	10	16	11-14	15-18

Результати конкурсу продемонстровано на статистиці Єврокомісії, яка надається Національним контактним пунктам після оголошення переможців конкурсу. Проте це ще не остаточний результат, бо може бути додано додаткові проєкти при наявності фінансування. Для цього формується резервний список, з якого до списку переможців додають проєкти, що мають

потенціал. На рис. 1 представлено кількість учасників проєктів, які було позитивно оцінено і кількість учасників в проєктах, що виграли конкурс.

По результатам основної оцінки проєктів 9 українських команд брали участь в проєктах, які були високо оцінені. Тим не менш, жоден цей проєкт не було включено до Main List. тобто списку, який фінансується. Проте, один проєкт, в якому брали участь дві організації з України було включено до резервного списку. На щастя, при пересмотрі результатів цей проєкт було включено до списку проєктів на фінансування. Таким чином, до списку переможців увійшли Національний координаційний центр кібербезпеки та Київський авіаційний інститут. Особливістю їх участі є статус асоційованих членів консорціуму, що не дає їм фінансування, проте надає право брати участь у всіх заходах консорціуму.

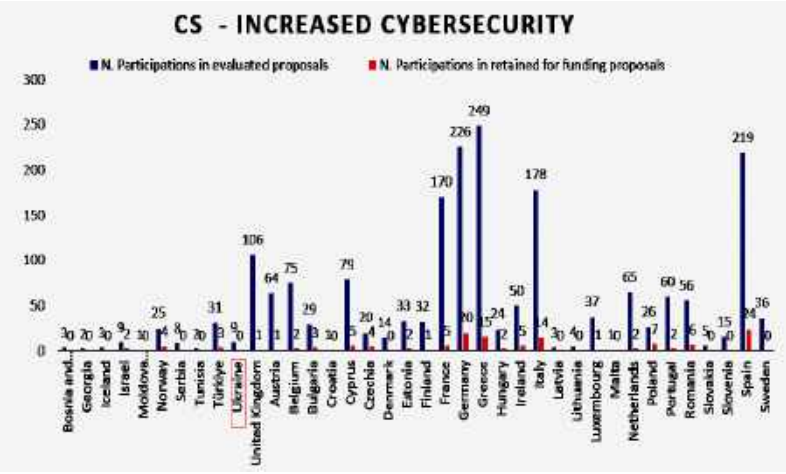


Рисунок 1 – Результати конкурсів за напрямом кібербезпека з розподіленням по країнам – учасницям

В 2026 році в конкурсах напряму з кібербезпеки перемогли два проєкта, в яких беруть участь три українські команди. Таблиця 1 показує, що на 2026-2027 рр. заплановано досить велика кількість проєктів, що увійдуть до списку переможців, і шанси отримати грант є досить великими. Не впустіть свій шанс стати переможцем такої престижної програми, як Горизонт Європа, отримати досвід європейської співпраці в галузі кібербезпеки, розширити свій обрій та впровадити інноваційні розробки в життя.

1. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Press release, Dec 16, 2020. Brussels, Джерело: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (20.05.2026).

ЗМІСТ

МАТЕРІАЛИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»
03 червня 2026 року

Відповідальні за випуск:
О.В. Цуркан, Т.М. Клименко

Місце проведення: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України; м. Київ, вул. Генерала Наумова, 15.

З питаннями щодо конференції звертатися:

ІПМЕ ім. Г.Є. Пухова НАН України, вул. Генерала Наумова, 15,
кім. 303, Цуркан Оксана Володимирівна, тел. 424-91-62,
068-014-57-22, e-mail: otsurkan24@gmail.com

Інститут проблем моделювання в енергетиці
ім. Г. Є. Пухова НАН України,
вул. Генерала Наумова, 15, Київ, 03164, Україна,
тел.: +38 044 424 91 62, факс: +38 044 424 10 63
веб сайт: https://ipme.kiev.ua/