НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ВІДДІЛЕННЯ ЕНЕРГЕТИКИ
ТА ЕНЕРГЕТИЧНИХ ТЕХНОЛОГІЙ

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

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ЕНЕРГЕТИЧНИЙ ФРОНТ: ШОСТИЙ ТЕАТР ВОЄННИХ ДІЙ»
(стратегія захисту, управління та відновлення)

27 березня 2026 року

Київ – 2026

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Е-61

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 4 від 26 березня 2026 р.)

Е-61 **Енергетичний фронт:** шостий театр воєнних дій (стратегія захисту, управління та відновлення), Міжнародна науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 27 березня 2026 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2026. 154 с.

Е-61 **Energy front:** the sixth theater of military operations (defense, management and recovery strategy), The International Scientific and Practical Conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, March 27, 2026). Kyiv: PIMEE NAS of Ukraine, 2026. 154p.

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

**ВІДДІЛЕННЯ ЕНЕРГЕТИКИ
ТА ЕНЕРГЕТИЧНИХ ТЕХНОЛОГІЙ**

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

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ЕНЕРГЕТИЧНИЙ ФРОНТ: ШОСТИЙ ТЕАТР ВОЄННИХ ДІЙ»

(стратегія захисту, управління та відновлення)

27 березня 2026 року

Київ – 2026

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Відділення енергетики та енергетичних технологій НАН України
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

ПРОГРАМНИЙ КОМІТЕТ

Русанов Андрій Вікторович
академік НАН України, доктор технічних наук, професор, керівник Відділення Енергетики та Енергетичних Технологій Президії НАН України, голова програмного комітету

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

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

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

В.Ф. Залужний

ЕНЕРГЕТИЧНИЙ ІНТЕРГРІД: АРХІТЕКТУРА ЖИВУЧОСТІ У НОВОМУ ДОМЕНІ ВОЄННИХ ДІЙ

Розкриті особливості функціонування енергетичних систем в умовах ведення війни на виснаження.

Визначенні проблемні питання забезпечення живучості енергетичної систем та можливі шляхи їх вирішення.

Обговорюються питання впровадження нового підходу до трансформації існуючої енергетичної системи України та її Збройних Сил..

Ключові слова: війна на виснаження, енергія, енергетика, енергетичний інтергрід, живучість.

Вступ

У сьогоднішньому світі, захопленому дискусіями про дрони, штучний інтелект та футуристичні військові доктрини, поки стратегічні центри розробляють складні алгоритми ведення бойових дій у війнах майбутнього, ми ризикуємо пропустити головний урок сучасної війни – ***без енергії*** будь-яка технологічна система перетворюється на купу мертвого заліза.

Підтвердженням цього є російсько-українська війна у якій, в умовах недосягнення політичної мети війни з боку Росії та неприйняття капітуляції з боку України, Росія приходить до збільшення інтенсивності атак на енергетичні системи, які забезпечують інфраструктуру, транспортні вузли та інші ключові елементи державного управління і життєзабезпечення. За таких умов стратегія спрямована не стільки на захоплення територій, скільки на виснаження енергетичних ресурсів для досягнення противником своїх цілей.

Війна на виснаження в Україні – це насамперед війна проти економічних можливостей нашої держави. У такій війні саме енергетика визначає межу витривалості всієї нації та реалізацію потенційних спроможностей Сил безпеки та оборони України.

За таких умов енергосистема України стала повноцінним полем бою та виявила критичну ваду сучасних класичних індустріальних держав – надмірну централізацію життєво важливих енергетичних ресурсів, де традиційна концепція “об’єкта під захистом” більше не гарантує її стійкості. Сьогодні енергосистема – це не просто тилова інфраструктура, це новий театр воєнних дій, де старі методи централізованого захисту стали нашою головною вразливістю.

Настав час визнати: щоб вижити у війні на виснаження, нам потрібна не просто “ремонтна бригада”, а ***радикальна зміна самої генетики нашої енергетики*** як у державі, так і на полі бою. Єдиний шлях до перемоги у

довготривалій війні ресурсів – це перехід від вразливих “енергетичних фортець” до ***мережецентричної архітектури, здатної до самовідновлення***. Це не питання економічної доцільності, це питання національного виживання.

Основна частина

Війна на виснаження – це не лише дуель військових, це іспит на антикрихкість нашого життєзабезпечення. Ми звикли думати, що великі заводи та гігантські електростанції – це символи нашої міцності. Але в реаліях 2024-2026 років ці індустріальні титани перетворилися на ідеальні мішені, на зашморг, який ворог затягує на шиї цілої країни.

Сьогодні ми часто забуваємо про базову математику війни: жоден “розумний” алгоритм, жодна система РЕБ чи центр обробки даних не працюють без енергії. Якщо економіка – це кров сучасної війни, то ***енергетика – це її серцебиття***. Ми маємо нарешті визнати: енергосистема України, а згодом і всієї Європи та світу, перетворилася на повноцінний ***новий театр воєнних дій***.

Централізовані об’єкти (великі теплові електростанції, гідроелектростанції, атомні електростанції, лінії електропередач) перетворюються на “ахіллесову пяту” національної безпеки під час війни. Якщо ворог знищує кілька ключових вузлів, цілі регіони занурюються в темряву. Отже, енергетична безпека нерозривно пов’язана не тільки зі стійкістю економіки під час війни, а й стає частиною національної безпеки. За таких умов захист енергетичних об’єктів стає таким же важливим, як і захист територій.

Досвід 2024-2026 років переконливо свідчить, що сьогодні вирішення проблем захисту енергетичної системи, насамперед, пов’язана не зі збільшенням кількості сил та засобів ППО та швидкому впровадженні інноваційних рішень, а в тому, що існуюча система енергозабезпечення, вже не може існувати і захищатися у тому вигляді, у якому вона була створена в 50-х роках минулого століття. Імовірно, у таких умовах необхідно більше уваги приділити стратегії децентралізації енергетики як способу підвищення стійкості країни до будь-яких ударів.

За таких умов концепції централізованого захисту більше не працюють. Тому нам потрібна радикальна зміна парадигми. На зміну ієрархічним “енергетичним фортецям” має прийти ***Енергетичний Інтергрід*** – або те, що можна назвати **енергетичним інтернетом**.

Що це означає на практиці? Це перенесення логіки цифрових мереж на фізичний рівень розподілу ресурсів. Чому інтернет неможливо знищити одним ударом? Тому що в нього немає “серця”. Він складається з десятків тисяч автономних вузлів. Якщо один шлях заблоковано, пакет даних знайде інший.

Енергетичний Інтергрід – це побудова мережі, де кожна громада, кожен промисловий кластер і кожен оборонний об’єкт стають автономними

вузлами. Це архітектура "***мережецентричної стійкості***", де генерація розсіяна, а система здатна до самовідновлення. У такому форматі енергія, як і інформація, знаходить обхідні шляхи, роблячи стратегію масованих ракетних ударів економічно безглуздою для агресора.

Ми маємо перейти до принципу ***енергетичної стільниковості***. Система повинна складатися з тисяч автономних енергетичних "клітин", здатних підтримувати життя всього організму, навіть коли центральні магістралі перебиті. Це не питання екології чи тарифів – це питання національної безпеки та нашої спроможності тримати удар у довгій війні ресурсів.

Світ навколо нас стрімко змінюється, а старі міжнародні інститути та договори дедалі частіше нагадують ***бутафорську броню***. Вона створює ілюзію захисту на папері, але миттєво пробивається реальною агресією. В епоху глобальних загроз справжню безпеку дає не дипломатична риторика, а технологічна антикрихкість.

Побудова ***Енергетичного Інтергріду*** – це наш шлях до того, щоб зробити енергетику "мережевим щитом" держави. Ми повинні проявити волю і почати цю трансформацію вже зараз. Тільки математична точність, децентралізація та технологічна перевага дозволять нам не просто вижити в темряві, а вийти з неї переможцями.

Важливо зазначити, що в умовах системних викликів та цілеспрямованих атак на об'єкти енергетичної системи, впровадження ***Енергетичного Інтергріду*** стає не просто технічним рішенням, а фундаментальною складовою національної безпеки. Перехід до мережецентричної моделі енергозабезпечення дозволяє створити гнучку систему, яка зберігає працездатність навіть за умови пошкодження окремих її сегментів.

Для цивільного сектору та держави локальні джерела енергії наближають виробництво до споживача. Це мінімізує втрати при транспортуванні та дозволяє громадам самостійно забезпечувати роботу підприємств, лікарень, водоканалів, систем опалення тощо. Економічний ефект досягається через, живучість, оптимізацію витрат та поступову відмову від дорогого імпорту енергоносіїв завдяки підвищенню енергоефективності на місцях.

Для Збройних Сил розподілена генерація забезпечує стратегічну, оперативну та тактичну автономність. Впровадження мобільних та стаціонарних локальних систем енергоживлення безпосередньо в зоні бойових дій, військових містечках, логістичних центрах та ремонтних базах гарантує:

безперервність управління – стабільну роботу системи управління;

живучість – розосередження енергооб'єктів робить їх менш вразливими для розвідки та засобів ураження противника;

оперативність – швидке розгортання енергомодулів у польових умовах для підтримки технологічного озброєння.

Таким чином, ***Енергетичного Інтергріду*** перетворює енергосистему на "***цифровий хребет***", де кожен окремий вузол підсилює загальну стійкість країни. Це шлях до створення енергетичного фронту та тилу, здатних витримати будь-які навантаження та забезпечити надійну підтримку сил оборони.

Висновки

1. Енергетичний простір став новим доменом воєнних дій, а стійкість енергетики визначає результат протистояння. Перехід від централізованої мережі енергозабезпечення України та її Збройних Сил до сучасної мережецентричної системи – це не тільки її трансформація, а й здатність виживати, а й значить перемагати.

2. Забезпечення стійкості та адаптивності енергозабезпечення сил і засобів Збройних Сил України вимагають оперативного впровадження резильєнтних енергетичних систем військового призначення, пошуку нестандартних інноваційних рішень для автономізації енергозабезпечення військ від тактичного до стратегічного рівнів управління.

3. Побудова Енергетичного інтергріду це шлях до того, щоб зробити енергетику "мережевим щитом" держави. Ми повинні проявити волю і почати цю трансформацію вже зараз. Тільки математична точність, децентралізація та технологічна перевага дозволять нам не просто вижити в темряві, а вийти з неї переможцями.

4. Енергетичний інтергрід – це шлях до створення таких енергетичного фронту та тилу, які здатні витримати будь-які навантаження та забезпечити надійну підтримку Сил безпеки і оборони України.

5. Збереження та захист енергетичної інфраструктури мають спиратися на реальні, а не на очікувані та неконтрольовані спроможності. Формула виживання проста: продовжувати боротись, укріплювати економіку та зберігати єдність.

1. Залужний В. Ф. Нова природа війни змінила сутність основ глобальної безпеки: український досвід і майбутній світовий порядок. Українська правда. 2025. 25 квітня. URL: https://www.pravda.com.ua/columns/2025/04/25/7509135/

2. Залужний В. Ф. Технологічна війна на виснаження та як у ній перемогти. Українська правда. 2025. 13 липня. URL: https://www.pravda.com.ua/articles/2025/07/13/7521484/.

3. Залужний В Ф. Роль інновацій як основи стратегії стійкого опору у позбавленні росії можливості нав'язувати свої умови через війну. Дзеркало тижня. 2025. 24 вересня. URL: https://zn.ua/ukr/war/rol-innovatsij-jak-osnovi-stratehiji-stijkoho-oporu-u-pozbavlenni-rosiji-mozhlivosti-navjazuvati-svoji-umovi-cherez-vijnu.html.

4. Залужний В. Ф. Російська дипломатія як інструмент системного впливу у війні проти України. Українська правда. 2025. 10 листопада. URL: https://www.pravda.com.ua.

5. Залужний В. Ф. Політика і війна. Реальність проти очікування. LIGA.net. 2025. 29 листопада. URL: https://www.pravda.com.ua/news/2025/11/29/8009595/.

6. Залужний В. Ф. Чотири роки повномасштабного вторгнення: головні висновки війни. Українська правда. 2026. 23 лютого. URL: https://www.pravda.com.ua/columns/2026/02/23/8022301/.

7. Залужний В. Ф. Забезпечення живучості розподілених автоматизованих систем організаційного управління силами та засобами: енергетична складова. XLIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України : матер. конф. (Київ, 14 травня 2025 р.). Київ, 2025. С. 42–45.

8. Залужний В. Ф. Забезпечення енергетичної резильєнтності морських портів України в сучасних умовах ведення збройної боротьби. Резильєнтність динамічних систем : матер. ІІ наук.-практ. конф. (Київ, 12 червня 2025 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2025. С. 5–9.

9. Когут Ю. І. Енергетичні війни та політики безпеки об’єктів ядерної енергетики : практ. посіб. Київ : Консалтингова компанія “СІДКОН”; ВД “ДАКОР”, 2023. 352 с.

10. Когут Ю. І. Енергетичні війни як загроза національній безпеці держав Євросоюзу : практ. посіб. Київ : Консалтингова компанія “СІДКОН”; ВД “ДАКОР”, 2023. 364 с.

11. Когут Ю. І. Гібридна війна нового типу як загроза національній безпеці держав / за ред. А. С. Довгополого. Київ : Консалтингова компанія “СІДКОН”; ВД “ДАКОР”, 2024. 348 с.

12. Мохор В. В., Коробейніков Ф. О. Стійкість і резильєнтність у безпековому домені. Реєстрація, зберігання і обробка даних. 2024. Т. 26, № 1. С. 113–120.

S.Ye. Saukh

SOCIETAL LIFE SPACE AND ENERGY IN PERIODS OF PEACE, WAR, AND RECOVERY

The theatre of war, in the words of Carl von Clausewitz, is "the space over which war prevails." Russia's war against Ukraine is total, as it has long extended beyond the five theatres of military operations defined by military science—land, sea, air, space, and cyberspace. The war has engulfed virtually every sphere of Ukrainian society. Broad societal resistance has led to the emergence of multiple "fronts."

The term front, originally used in military science to describe areas of armed confrontation, has been metaphorically extended to different spheres of social life. Expressions such as gas front, water front, transport front, energy front, economic front, food front, medical front, psychological front, information front, technological front, cultural front, scientific front, and political front first appeared in the media space. Today, journalists, government officials, activists, volunteers, and experts actively use these terms to draw the attention of the public, businesses, foreign media, and partner governments to the diverse areas of struggle for the survival of Ukrainian society.

The driver of Russia's aggressive policy is systematic, large-scale attacks on Ukraine's societal space. As a result, the resilience of Ukrainians' life space is gradually eroded, even though it has been sustained until now by resistance across the clusters of the aforementioned fronts.

The proliferation of fronts demonstrates how war spreads into different spheres of social life—from infrastructure to psychology, from economics to information. If the theatre of war is the operational space of the armed forces under centralized military-political command, then the fronts of social life are sustained by society itself and by the diverse actions of political institutions, ministries, executive agencies, military-civil administrations, volunteer groups, and civic organizations. These actions cannot be functionally centralized, since societal space has a complex organizational form.

The need to study social transformations during peace, war, and recovery requires the development of a model of societal life space.

Societal Life Space (SLS) is a multidimensional systemic construct encompassing all key spheres of modern society's functioning: physical, infrastructural, economic, political, social, scientific-technological, informational-psychological, cultural, and others. It is not only a physical space but also an institutional, symbolic, and logical structure within which society operates, adapts to challenges, and formulates strategies for continuity and development.

The SLS model represents this multidimensional space as a limited set of key dimensions, necessary and sufficient for systemic analysis of social change. The model allows researchers to:

- Examine the logic of societal transformations in periods of peace, war, and recovery.
- Assess the resilience of society.
- Identify cascading effects between dimensions.
- Detect early warning signs of systemic collapse.
- Develop strategic scenarios for societal development.

In the context of Russia's total war against Ukraine, the SLS model is an essential tool for studying societal transformations. It reveals how changes in one sphere (e.g., energy) trigger chain reactions in others (economy, security, psychology), and how society transitions from a logic of development in peacetime to survival in wartime and regeneration in recovery.

Definition and Operationalization of SLS Dimensions. The proposed SLS model consists of **15 dimensions**. Each dimension is defined by its role in societal systems and its significance during peace, war, and recovery.

Detailed Description of SLS Model Dimensions. This description provides a comprehensive overview of the dimensions within the Societal Life Space (SLS) model, focusing on their role in satisfying necessity and sufficiency demands for systemic resilience.

1. Physical Dimension
2. Infrastructure Dimension
3. Economic Dimension
4. Social Dimension
5. Cultural Dimension
6. Psychological Dimension
7. Informational Dimension
8. Cybernetic Dimension
9. Technological Dimension
10. Scientific Dimension
11. Political Dimension
12. Security Dimension
13. Geopolitical Dimension
14. Strategic Dimension
15. Integrated Political-Strategic *(*Integrated Pol-Str*)* Dimension

Each dimension of the SLS model is necessary for systemic resilience, but only together are they sufficient to meet the demands of sustainability. The interplay between necessity and sufficiency highlights the importance of integration: no single dimension can secure resilience alone, but their combined strength ensures adaptability, stability, and long-term survival. Thus, we have:

- 75 indicators = 15 dimensions × 5 key indicators.
- Each dimension has its own key indicators reflecting its state in periods of peace, war, and recovery.

This indicator system provides the empirical foundation for cross-impact analysis and scenario modeling.

The calculation of the resilience vector $\boldsymbol{R}$ of the SLS model for each of its spatial dimensions requires excessive effort in searching for large volumes of data and their error-free processing. Modern artificial intelligence tools provide effective execution of such work.

For the generalized assessment of the resilience of the SLS for each annual time period $\mathbf{t}$, we will use the absolute norm of the vector function $\mathbf{R}(\mathbf{t})$:

$$R_{SLS}(t) = \|W\mathbf{R}(t)\|_1 = \sum_{i=1}^{i=15} |R_i(t)| .$$

Using this norm, generalized indicators of the resilience of the SLS of NATO, the EU, Ukraine, and the Russian Federation were obtained.

Cross-impact methodology. Cross-impact analysis is used to model the interdependencies among all 15 dimensions of SLS model. The method evaluates how changes in one dimension influence others, producing a 15×15 matrix of impact strengths.

The idea of cross-impact matrices has existed for decades in futures studies and systems analysis (e.g., Godet's "cross-impact analysis" in the 1970s). Traditionally, these matrices are used to map systemic interdependencies in one state of a system (usually "baseline" or "future scenarios").

Normalized Weighted Systemic Resilience (NWSR-) Matrices is a methodological innovation for analyzing SLS development. The NWSR-Matrices framework consists of three distinct cross-impact matrices – W_{peace}, W_{war} and $W_{recovery}$ – each normalized and weighted to reflect systemic resilience under different conditions. While cross-impact matrices have been employed in futures studies and systemic analysis since the 1970s, they have traditionally been applied to single scenarios or baseline conditions. The innovation presented here lies in the explicit differentiation of systemic behavior across three historical and developmental phases – peacetime equilibrium, wartime mobilization, and post-war reconstruction – and in the normalization of values to allow comparative resilience measurement. By structuring these matrices side-by-side, the NWSR-Matrices enable comparative systemic analysis, revealing how interconnections shift from distributed balance (peace), to centralized survival (war), to reconstruction and modernization (recovery). To the best of my knowledge, this is the first application of cross-impact methodology to a tri-matrix model of national systemic resilience, specifically tailored to Ukraine's SLS. This contribution extends classical systemic analysis by embedding temporal and situational dynamics into a normalized matrix structure, offering a new tool for both academic research and policy design.

A new methodological category – the NWSR-Matrices – that can be applied not only to Ukraine's SLS but potentially to other nations or systems facing crisis and recovery cycles.

The NWSR-Matrices term strengthens researches:

- "Normalized" emphasizes that values are scaled consistently across matrices, enabling direct comparison.
- "Weighted" highlights that systemic impacts are not equal — some domains exert stronger influence than others.
- "Systemic Resilience" situates the matrices in resilience theory, making them relevant to both futures studies and national security/strategic research.
- "Matrices" ties the innovation back to the established cross-impact methodology, but clearly marks it as an extension.

The NWSR-Matrices – W_{peace}, W_{war} and $W_{recovery}$ – structure:

- "Rows → Source Dimension". Each row represents a "domain that exerts influence". For example, the "Economic" row shows how the economy affects infrastructure, social cohesion, politics, etc. It's the "cause" side of the relationship.
- "Columns → Target Dimension". Each column represents a "domain being influenced". For example, the "Security" column shows how security is impacted by physical, economic, informational, and other domains. It's the "effect" side of the relationship.
- "Cell values (0.0-1.0)". A higher value (closer to 1.0) means "stronger systemic impact". A lower value (closer to 0.0) means "weaker systemic impact".
- "Diagonal entries (always 1.00)". Each domain fully reinforces itself – this is a baseline assumption in cross-impact matrices.
- "Rows tell us who is driving change". They show the "outward influence" of a domain.
- "Columns tell us who is receiving change". They show the "inward vulnerability or dependency" of a domain.
- "Comparing rows vs. columns" helps identify:
- "Drivers" (high row averages).
- "Receivers" (high column averages).
- "Balanced nodes" (similar row and column strength).

Together, the NWSR-Matrices map how Ukraine's systemic dimensions interact in peace, war, and recovery.

SLS of Ukraine in the phase transitions «Peace→War» and «War→Recovery».

- The phase transition from «Peace→War» is accompanied by a transformation of the distributed balance of interconnections among all SLS dimensions and the formation of concentrated resilience in the interconnections between the Security, Political, Cybernetic, and Information dimensions, with efforts directed toward ensuring the survival of the SLS in its other dimensions, particularly Infrastructure.
- The phase transition from 'War→Recovery' is accompanied by a reconstruction of the balance of interconnections among all SLS

dimensions, where Infrastructure and Economy once again take precedence.

The consequences of the phase transitions «Peace→War» and «War→Recovery» for Ukraine's SLS dimensions are reflected as graphs of average values and standard deviations of cross-impact indices. These graphs reveal transformational changes in the characteristics of the cross-impact indices, as a result of which Ukraine's post-war SLS dimensions appear more balanced and interconnected than during the pre-war peaceful period.

Strategic Consequences of Transformations in Ukraine's SLS

1. Policy Target Points:
   - In peacetime, it is necessary to maintain a distributed balance and prevent excessive centralization.
   - During war, investments must be directed toward security, cyber defense, and informational resilience.
   - In the recovery period, priority should be given to infrastructural, economic, and scientific modernization, as well as external partnerships.
2. Systemic Fragility:
   - During war, the Infrastructure and Economic domains are particularly vulnerable. These domains attract special societal attention through metaphorical expressions such as gas front, water front, transport front, energy front, economic front, food front, medical front, and others, emphasizing the need to concentrate efforts on their protection.
   - In recovery, the Political and Security domains should not dominate excessively, in order to enable modernization.
3. Pathways to Resilience:
   - The Social, Informational, and Cybernetic domains act as shock absorbers during wartime.
   - Infrastructure and Economy serve as engines of growth during recovery.

The analysis of transformations in Ukraine's SLS during the phase transitions «Peace → War» and «War → Recovery» makes it possible to formulate **strategies for the development of Energy**, as a component of the Infrastructure domain, across periods of peace, war, and recovery, each pursued through different policy directions.

In peacetime, a scenario of maximizing societal well-being is implemented

- **Goal:** Energy development is aimed at maximizing societal welfare by ensuring prosperity, stability, and sustainability.
- **Policy drivers:**
  1. Safe, accessible, and diversified energy supply.
  2. Investment in renewable energy sources and low-carbon technologies to reduce ecological risks.
  3. Long-term planning for energy efficiency in industry, transport, and housing.

- **Infrastructure requirements:**
    1. Expansion of smart grids and digital management systems.
    2. Electrification of transport and modernization of industrial systems.
    3. Implementation of reserve mechanisms in energy networks to absorb shocks.

During wartime, a survival and continuity scenario for the management system is implemented.

- **Goal**: Energy development shifts toward survival and continuity of functioning, with energy regarded both as a vulnerability and as a weapon.
- **Policy drivers**:
    1. Centralized management of energy assets and rationing.
    2. Prioritization of military logistics and emergency power systems.
    3. Strategic prevention of energy supplies to adversaries (blockades, sabotage).
- **Infrastructure requirements**:
    1. Strengthening of networks and fuel supply chains to protect against attack.
    2. Reserving energy equipment and ensuring rapid repair capabilities.
    3. Repurposing civilian energy systems for defense needs.

During the recovery period, a scenario of restoration and transformation of Energy is implemented.

- **Goal**: Energy development becomes a catalyst for regeneration (social activity), stimulating recovery, independence, and transformation of the SLS.
- **Policy drivers**:
    1. A strategic push toward energy independence and resilience.
    2. Incentives for green recovery and the adoption of resilience technologies.
    3. Integration of energy policy with economic recovery and decarbonization goals.
- **Infrastructure requirements**:
    1. Reconstruction through the deployment of renewable energy sources, decentralized microgrids, and adaptive energy clusters.
    2. Expansion of resilient energy systems to support industrial and social recovery.
    3. Energy innovations as the foundation for renewed geopolitical positioning and long-term sustainability.

In addition, with the help of NWSR-*M*atrices it is possible to form vector of shock impacts accompanied by cascading effects in the SLS, or to reproduce vectors of drivers of the SLS development.

Conclusions. This study introduced and applied the **Societal Life Space (SLS) model** to analyze Ukraine's systemic resilience across the phases of **peace, war, and recovery**. By operationalizing 15 dimensions through 75 indicators, the model provided a comprehensive framework for assessing resilience, interdependencies, and vulnerabilities.

The methodological innovation of the **Normalized Weighted Systemic Resilience (NWSR-) Matrices** extended classical cross-impact analysis by embedding temporal and situational dynamics into a tri-matrix structure. This allowed comparative measurement of resilience across equilibrium, mobilization, and reconstruction phases, revealing how systemic interconnections shift under stress and recovery.

Overall, the SLS model and NWSR-Matrices provide a robust analytical tool for understanding societal transformations under extreme conditions. They offer both **academic value**—advancing resilience theory and systemic analysis—and **policy relevance**—guiding strategic priorities for Ukraine and potentially other nations facing cycles of crisis and recovery.

The research was conducted within the framework of project No. 2025.07/0204*, «Parallel Methods and Algorithms for Solving Mixed-Integer Linear Programming Problems in the Planning of Structurally Flexible and Resilient Power Systems Development in Ukraine»* ***funded by the National Research Foundation of Ukraine (NRFU).***

Р.В. Грищук, О.М. Грищук

ВОЄННА НАУКА НА ЗЛАМІ КЛАСИЧНОЇ ПАРАДИГМИ: ОКРЕМА ДУМКА ПРО «ЕНЕРГЕТИЧНИЙ ФРОНТ» ЯК ШОСТИЙ ТЕАТР ВОЄННИХ ДІЙ

Актуальність. Виборюючи своє законне право на існування на сучасній геополітичній карті світу, Україна як активний гравець на міжнародній арені вимушено здійснила технологічний стрибок у розвитку озброєнь і військової техніки. Це спричинило неминучі зміни у формах ведення воєнних дій та способах застосування військ (сил). У результаті виникла потреба чергового критичного переосмислення усталених класичних засад теорії війни Клаузевіца [1], які визначають традиційні, але не враховують нові домени ведення сучасних і, що особливо важливо, війн майбутнього.

Поточний стан справ. Історична ретроспектива показує, що розвиток *космічних технологій* в другій половині XX століття призвів до розгортання в космосі орбітальних угруповань для ведення *"зоряних війн"*. Це стало підґрунтям для включення космічного простору до вже існуючих на той час доменів збройної боротьби. На початку XXI століття *інформаційно-комунікаційні технології* охопили практично всі без винятку сфери суспільного життя та систему державного управління. У другому десятилітті двохтисячних років, після *"кібервійн"* російської федерації проти Естонії та Грузії [2], світова спільнота визнала кіберпростір п'ятим доменом збройної боротьби. Таким чином, станом на сьогодні суходіл, море, повітря, космос й кіберпростір де-факто та де-юре [3] є основою загальновизнаної класичної воєнної парадигми.

Нові домени збройного протиборства. Останнім часом в науковому середовищі формуються концептуальні засади щодо віднесення до існуючих театрів воєнних дій (ТВД) ще одного – так званого "енергетичного фронту". Така думка підтверджується конкретними фактами. Зокрема, досвід російсько-української війни в зимовий період 2025/2026 р. показує, що агресор окрім серед іншого вбачає досягнення своїх цілей шляхом зниження енергетичного потенціалу України з використанням конвенційних засобів. Іншим прикладом є конфлікт, що зароджується на Близькому Сході між США та Ізраїлем з одного боку та Іраном з іншого. Цілком зрозуміло, що він також має "енергетичне" підґрунтя, навіть попри офіційно анонсовану мету операції "Епічна лють".

Дискусійні питання. Попри наведені аргументи на користь "енергетичного фронту", існує й інша думка. Вона не збігається з думкою про те, що "енергетичний фронт" – це новий ТВД, а тим паче шостий домен збройної боротьби. Таке твердження ґрунтується на положеннях воєнної науки. Відомо, що відхилення від загальноприйнятої аксіоматики може призвести до руйнації системи знань, накопиченої роками. Йдеться про закони

та закономірності розвитку збройної боротьби, питання оборонного менеджменту, підготовку держави до оборони та застосування збройних сил, їх всебічного забезпечення тощо.

Основна проблема на наш погляд полягає в антагонізмі ідей, які породжують протиріччя на стику між "цивільною" та воєнною наукою. Воєнна наука чи то в англосаксонській, чи в прусській, чи то в пострадянській наукових школах чітко та однозначно оперує такими категоріями та співвідношеннями між ними, як ТВД, фронт, домен, операційний простір, операційне середовище тощо. Це не означає, що воєнна наука не повинна розвиватися з появою нових технологій та війн нового покоління. Такі категорії можуть уточнюватися, можуть з'являтися нові поняття тощо. Однак їх загальноприйнята сутність не повинна підмінюватися та підлаштовуватися під конкретний історичний тренд. Спробуємо це аргументувати.

По-перше, скориставшись загальноприйнятою у західній військовій науковій спільноті головною ідеєю удосконаленої теорії кілець полковника Уордена [4], яка залишається актуальною, можна стверджувати: "енергетичний фронт" – це не новий ТВД, а один із центрів тяжіння у другому стратегічному кільці. Конвенційний або не конвенційний вплив на нього за принципом "ефекту доміно" здатний спричинити стратегічний параліч всіх інших критичних інфраструктур держави. Причинно-наслідковий зв'язок цього явища, зокрема в енергетичному секторі Індії, ґрунтовно розкрито у [2].

По-друге. У вузькому сенсі фізична безпека "енергетичного фронту" як критичної галузі будь-якої розвиненої держави світу є ознакою її економічної стабільності. У глобальному вимірі "енергетичний фронт" перш за все виступає рушієм міжнародних відносин.

По-третє, у воєнному сенсі "енергетичний фронт" не передбачає розгортання у ньому угруповань військ (сил) для ведення збройної боротьби. Виходячи з цього він також не може розглядатися як новий ТВД.

Таким чином, "енергетичний фронт" є складовою операційного середовища та виступає одним із центрів тяжіння в межах операційного простору. Він одночасно входить до складу одного або кількох ТВД у доменах де ведуться воєнні дії, проте сам по собі не формує окремого театру воєнних дій.

Висновки. Отже, дискусію щодо віднесення "енергетичного фронту" до шостого ТВД не можна вважати завершеною. Лише після узгодження дефініційного апарату, уникнувши концептуальної плутанини, можна повернутися до її обговорення та знайти коректне вирішення піднятої проблеми.

1. Clausewitz, C. (1984). *On War*. Princeton University Press.

2. Грищук, Р. В., & Даник, Ю. Г. (2016). *Основи кібернетичної безпеки: монографія*. Житомир: ЖНАЕУ.

3. NATO. (2016, July 9). *Warsaw Summit Communiqué*. Warsaw: NATO.

4. Warden, J. A., III. (1995). The enemy as a system. *Airpower J., 9* (Spr.), 43–55.

Ф.О. Коробейніков

ЕНЕРГЕТИКА ЯК ТЕАТР ВОЄННИХ ДІЙ: ЛОГІКО-СИСТЕМНИЙ АНАЛІЗ

Останніми роками у стратегічному та безпековому дискурсі дедалі частіше використовується метафора «енергетичного фронту». Масштабні атаки на енергетичну інфраструктуру стали характерною рисою сучасних конфліктів - від систематичних ударів по енергосистемі України під час російсько-української війни до загострення протистояння навколо енергетичної інфраструктури та морських енергетичних маршрутів на Близькому Сході. Зокрема, нещодавня ескалація напруження між США та Іраном знову продемонструвала, що енергетичні системи дедалі частіше розглядаються як стратегічна ціль у сучасному протиборстві. У цьому контексті дедалі частіше висловлюється теза про можливість трактувати енергетику як «шостий театр воєнних дій».

Разом з тим така інтерпретація потребує додаткового теоретичного уточнення. У класичній військовій теорії поняття «театр воєнних дій» використовується для позначення географічно визначеного простору, в межах якого розгортаються та ведуться військові операції. У сучасних концепціях багатодоменних операцій (*multi-domain operations*) для опису середовищ, у яких здійснюється військове протиборство і можна досягти переваги, дедалі частіше використовується поняття операційного домену [1, 2].

У методологічному сенсі ці категорії виконують подібну аналітичну функцію: вони позначають середовище, в межах якого можуть розгортатися сили, здійснюватися маневр та реалізовуватися специфічні способи ведення бойових дій. Саме в цьому аналітичному значенні у даній роботі поняття «театр воєнних дій» розглядається як функціонально еквівалентне поняттю операційного домену.

У сучасній військовій доктрині зазвичай виокремлюють п’ять основних доменів протиборства: *суходіл*, *море*, *повітря*, *космос* та *кіберпростір*. Водночас у новітніх стратегічних дослідженнях дедалі частіше пропонується виділяти *когнітивний домен*, пов’язаний зі сферою формування сприйняття, рішень і стратегічного наміру [3, 4].

З огляду на це вже на рівні формальної логіки виникає очевидна проблема: якщо когнітивний вимір розглядається як шостий домен сучасного протиборства, то енергетика, навіть у разі визнання її окремим операційним середовищем, могла б претендувати лише на статус *сьомого домену*, але не шостого.

Але, енергетична система, попри її критичне значення для функціонування держави та збройних сил, має іншу онтологічну природу:

вона виступає передусім об'єктом стратегічного впливу, розташованим у різних доменах, а не самостійним операційним середовищем.

Метою цієї роботи є логіко-системний аналіз структури сучасного протиборства, який дозволяє показати, що енергетика не може розглядатися як окремий театр воєнних дій. Використовуючи формалізовану модель взаємодії доменів та цільових систем і спираючись на базові закони математичної логіки [5], можна продемонструвати, що будь-який вплив на енергетичну систему може бути описаний як проєкція дій, що здійснюються з уже існуючих доменів протиборства.

Для формалізації цієї проблеми введемо аксіоматичну модель доменної структури сучасного протиборства.

Визначимо множину операційних доменів

$$D = \{d_1, d_2, d_3, d_4, d_5, d_6\}$$

де:

d_1, d_2, d_3 - фізичні середовища протиборства (суходіл, море, повітря);
d_4 - космічний домен;
d_5 - кіберпростір;
d_6 - когнітивний домен.

У концепції *multi-domain operations* домен визначається як операційне середовище, у якому можливі розгортання сил, маневр та здійснення впливу на противника. Іншими словами, домен має операційну суб'єктність: з нього може здійснюватися стратегічний вплив.

Формалізуємо впливу на енергетичну систему, позначивши енергетичну систему як множину її можливих станів

$$E = \{e_1, e_2, \dots, e_n\}$$

і введемо функцію стратегічного впливу

$$f : \mathcal{P}(D) \to E$$

Ця функція описує зміну стану енергетичної системи внаслідок дій, що здійснюються в одному або кількох доменах.

Слід зазначити, що у строгішій формалізації функція впливу повинна визначатися не на множині доменів, а на множині конкретних дій, що здійснюються в межах цих доменів. Стан енергетичної системи залежить не від самого факту належності до певного домену, а від конкретних операцій, які в ньому виконуються. Наприклад, суходільний домен сам по собі не породжує впливу; вплив виникає через конкретні дії, такі як удар по

інфраструктурі, захоплення об'єктів або саботаж. У цьому сенсі домен визначає простір можливих дій, які можуть бути реалізовані в його межах. Водночас для цілей даного дослідження, спрямованого на логічний аналіз структури протиборства, доцільно використати спрощену модель, у якій функція впливу задається безпосередньо на множині доменів.

Якщо будь-який стан енергетичної системи може бути досягнутий через вплив із множини доменів D , то виконується умова

$$\forall e \in E, \exists \delta \subseteq D : f(\delta) = e$$

де:

- e - конкретний стан енергетичної системи;
- E - множина можливих станів енергетичної системи (наприклад, нормальна робота мережі, пошкодження підстанції, порушення режимів роботи мережі тощо);
- D - множина операційних доменів сучасного протиборства;
- $\delta \subseteq D$ - деяка комбінація доменів, у межах яких здійснюється вплив;
- $f(\delta)$ - результат впливу, що виникає внаслідок дій у цих доменах;

символ $\forall$ *означає - «для будь-якого»;* $\exists$ *означає «існує);* $\in$ *означає «належить до множини»;* $\subseteq$ *означає «є підмножиною»* [6].

Таким чином, для будь-якого можливого стану енергетичної системи існує певна комбінація дій, здійснених у наявних доменах протиборства, яка може породити цей стан.

Це означає, що будь-які зміни в енергетичній системі (від фізичного руйнування інфраструктури до порушення режимів роботи мережі) можуть бути пояснені впливами, що здійснюються в межах уже існуючих доменів.

Інакше кажучи, енергетична система не виступає самостійним середовищем ведення бойових дій, а є об'єктом, на який проєктуються впливи з різних доменів протиборства.

Наприклад:

- кінетичний вплив (d_{1-4}) - фізичне руйнування інфраструктури;
- кібервплив (d_5) - атаки на SCADA або дата-центри;
- когнітивний вплив (d_6) - дезінформація операторів, провакування панічної поведінки споживачів.

Тобто, у системній онтології *домени виступають джерелами впливу*, тоді як *енергетична система є об'єктом цього впливу*.

Введемо відношення впливу

$$R \subseteq D \times E$$

де $(d, e) \in R$ означає зміну стану енергетичної системи під впливом дій у домені d.

Таким чином, домени впливають на енергетичну систему. Однак енергетична система не є операційним середовищем, у межах якого формується власний клас військових операцій.

Для верифікації отриманих висновків використаємо метод *reductio ad absurdum* (доведення від супротивного) [7]. Припустимо, що енергетика є окремим доменом.

$$E = d_7$$

Тоді, згідно з принципом онтологічної незалежності, повинен існувати принаймні один стан системи, який не є результатом проєкції сил із наявних доменів $d_1, \dots d_6$

$$\exists e \in E: \nexists \delta \subseteq D : f(\delta) = e.$$

Однак будь-який вплив на енергетичну систему завжди зводиться, наприклад, або до фізичного замикання (d_1), або до програмної помилки (d_5), або до помилки оператора (d_6). Тобто редукується до одного з уже існуючих доменів: фізичного, кібернетичного або когнітивного.

І оскільки $E = \varphi(d_1, \dots d_6)$ - тобто стан енергетичної системи є функцією впливів із наявних доменів, виникає логічна суперечність: система не може бути одночасно автономним джерелом операцій (доменом) і повністю залежною функцією від дій у інших доменах. Згідно з законом усунення суперечності, початкове припущення про те, що енергетика є доменом, є хибним.

Резумуючи ми можемо зробити висновок - енергетика не може розглядатися як окремий домен оскільки:

- вона є об’єктом впливу, а не операційним середовищем;
- її стан повністю визначається впливами з уже існуючих доменів;
- вона не має операційної суб’єктності, необхідної для статусу домену.

Отже, якщо енергетика не є операційним доменом, постає ключове аналітичне питання: яку роль вона відіграє у структурі сучасного багатодоменного протиборства?

З позицій теорії складних соціотехнічних систем [8] енергетика не є окремим операційним середовищем, а виступає критичною інфраструктурною основою, що забезпечує функціонування інших елементів державної та військової системи. Вона формує фізичний та ресурсний шар, який підтримує роботу економіки, транспорту, зв'язку, військової логістики та систем управління. Саме в силу своєї «об'єктності» та жорсткої фізичної зв'язності, енергетика виступає ідеальним провідником для ризиків високого ступеня впливу (*HILP*), оскільки збій в одному вузлі спричиняє каскадні ефекти, що поширюються на всі фізичні домени.

У структурі сучасного багатодоменного протиборства домени виконують різні функції. Фізичні, кібернетичний та космічний домени забезпечують можливість здійснення безпосередніх операцій, тоді як когнітивний домен формує стратегічний намір (*intent*), у межах якого приймаються рішення та визначаються способи застосування сили (у цьому сенсі введення когнітивного домену як шостого дозволяє замкнути повний контур управління протиборством: від формування наміру до його операційної реалізації).

Енергетична система займає у цій структурі принципово інше місце. Вона не є середовищем, у межах якого розгортаються військові операції, а виступає ресурсною основою та об'єктом стратегічного впливу. Класичне визначення театру воєнних дій передбачає простір, у межах якого можливе розгортання сил, маневр та безпосереднє ведення бойових дій. У межах енергетичної системи такі дії здійснюватися не можуть. Війська можуть контролювати лише окремі фізичні об'єкти інфраструктури: електростанції, підстанції або мережеві вузли, що фактично належать до суходільного домену. І тоді як у військовій справі маневр спрямований на зміну оперативної ситуації, зміни в енергетичній системі жорстко обмежені фізичними константами та топологією мережі. Маневр в енергетиці - це технічний перерозподіл навантаження, а не військово-стратегічна дія

Крім того, енергетична система функціонує відповідно до жорстко визначених фізичних законів: електродинаміки, механіки, тощо. Ці закони визначають межі її функціонування незалежно від стратегічних намірів акторів. Військова стратегія може використовувати домени для впливу на енергетичну систему, але не змінює фундаментальних принципів її роботи.

Таким чином, у логіці багатодоменного протиборства енергетика повинна розглядатися не як окремий театр або домен війни, а як об'єкт (операнд) - цільове середовище (*target environment*) [9] або критична інфраструктура [10], на яку проєктуються впливи з різних доменів.

Проте сучасні конфлікти дедалі чіткіше демонструють формування особливого класу дій, який можна описати як ***інфраструктурну війну***. Йдеться про системні операції, спрямовані на *некомбатантів* та глибокий тил: штучні блекаути, позбавлення цивільного населення водопостачання, опалення та каналізації, руйнування ланцюгів постачання палива й

продовольства, а також спроби обвалу національної економіки. Хоча такі дії часто переходять у сіру зону міжнародного права та порушують Женевські конвенції, вони поступово стають окремим класом воєнних операцій, метою яких є ***стратегічна децивілізація*** противника - примусове зниження його соціотехнічного рівня до стану примітивного виживання. Логіка агресора в таких операціях базується на припущенні, що вплив на критичну інфраструктуру прямо конвертується у злам волі в когнітивному домені. Однак результати таких конфліктів свідчать про зворотне.

Спроба *вимкнути цивілізацію* ігнорує фундаментальні когнітивні та еволюційно-психологічні механізми. Позбавлення доступу до благ сучасності не дезорганізує соціум, а ініціює атавістичний резонанс - регресію психіки до архаїчних інстинктів, що мільйони років допомагали людству виживати як виду. На зміну складним соціополітичним міркуванням, рефлексії і гуманістичним ідеям приходять жорсткі механізми реактивної агресії, зниження емпатії, ненависті до усього чужого та безкомпромісного захисту своєї групи. У когнітивному вимірі противника замість очікуваної апатії виникає екзистенціальна лють. Одним із можливих наслідків стають процеси радикалізації цивільного населення, що у крайніх формах можуть проявлятися у зростанні підтримки або участі у терористичних атаках та інших асиметричних формах насильства. Це робить війну значно кривавішою, некерованішою та позбавляє її будь-яких раціональних меж.

Таким чином, у логіці багатодоменного протиборства енергетика повинна розглядатися не як окремий театр або домен війни, а саме як критична інфраструктура.

Будь-які спроби використати її як інструмент децивілізації є не лише воєнним злочином, а й грубою стратегічною помилкою: вони не ламають волю до опору, а лише переводять конфлікт у стан атавістичної безкомпромісності, де ціна перемоги стає неприйнятною для обох сторін.

1. U.S. Army Training and Doctrine Command. (2018). The U.S. Army in multi-domain operations 2028 (TRADOC Pamphlet 525-3-1). https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

2. Department of the Army. (2022). Operations (Field Manual No. 3-0). https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.

3. Cole, A., Le Guyader, H., (2020). Cognitive : a 6th Domain of Operations. Norfolk (VA, USA) : Innovation Hub, NATO ACT Edition.

4. Claverie, B., & Du Cluzel, F. (2021). «The Cognitive Warfare Concept». (NATO Innovation Hub).

5. Copi, I. M., Cohen, C., & McMahon, K. (2016). Introduction to logic (14th ed.). Routledge. https://doi.org/10.4324/9781315510897.

6. Kuratowski, K., & Mostowski, A. (1976). Set theory: With an introduction to descriptive set theory (2nd ed.). North-Holland Publishing Company.

7. Tarski, A. (1994). Introduction to logic and to the methodology of deductive sciences (4th ed.). Oxford University Press.

8. Korobeynikov, F., & Mokhor, V. (2026). Adaptive security: strategic principles for complex socio-technical systems. Royal Society Open Science, 13(1). https://doi.org/10.1098/rsos.251481.

9. Joint Chiefs of Staff. (2013). Joint targeting (Joint Publication 3-60). U.S. Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/21-F-0520_JP_3-60_9-28-2018.pdf.

10. Cybersecurity and Infrastructure Security Agency (CISA). (2024). Energy sector. U.S. Department of Homeland Security. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/energy.

І.Р. Гладченко, П.В. Шиманюк

MICROGRIDS ЯК ДЕЦЕНТРАЛІЗОВАНІ ЕНЕРГЕТИЧНІ СИСТЕМИ ДЛЯ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ СТІЙКОСТІ ГРОМАД В УМОВАХ ВОЄННИХ ЗАГРОЗ

Вступ. В умовах сучасних воєнних загроз енергетична інфраструктура стає одним із ключових об’єктів атак. Пошкодження електростанцій, підстанцій або магістральних електромереж може призвести до значних порушень електропостачання на великих територіях. Традиційна централізована модель електропостачання характеризується високою залежністю споживачів від великих генеруючих об'єктів та магістральних мереж [1]. У разі пошкодження ключових вузлів системи відновлення електропостачання може потребувати значного часу. Одним із перспективних напрямів підвищення енергетичної стійкості є розвиток децентралізованих енергетичних систем, що базуються на використанні локальних джерел генерації [2], [3].

Метою роботи є обґрунтування доцільності використання локальних енергетичних систем типу microgrid для підвищення енергетичної стійкості територіальних громад та формування практичного підходу до організації microgrid для забезпечення електропостачання критичної інфраструктури.

Структура локальної енергетичної системи громади. Microgrid являє собою локальну електроенергетичну систему, що включає: джерела розосередженої генерації; установки зберігання енергії; систему керування енергетичними потоками; споживачів електроенергії [4-6]. Інвертори відновлюваних джерел енергії можуть використовуватися не лише для перетворення електроенергії, але й для керування режимами мережі, зокрема регулювання потоків реактивної потужності та стабілізації напруги [7]. На рисунку 1 наведено типову структуру Microgrid громади [8].

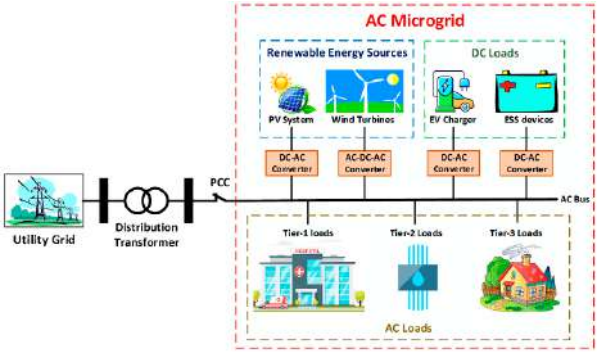


Рисунок 1. – Типова структура Microgrid громади

Практична модель microgrid для громади. Одним із підходів до підвищення енергетичної автономності громади є формування локальної microgrid для забезпечення електропостачання критичної інфраструктури.

До таких об'єктів належать:

- заклади охорони здоров'я;
- системи водопостачання;
- насосні станції;
- центри управління громадою;
- об'єкти зв'язку.

У разі пошкодження централізованої енергосистеми microgrid може перейти в **острівний режим** роботи [4], [9].

Принцип керування локальною енергосистемою може базуватися на пріоритетному використанні джерел енергії:

1. Відновлювані джерела енергії
2. Система накопичення енергії
3. Локальна резервна генерація
4. Центральна енергосистема

Такий підхід дозволяє максимально використовувати локальні ресурси та забезпечувати електропостачання критичних споживачів.

Порівняння класичної та гібридної структури microgrid. У більшості існуючих систем microgrid використовується традиційна AC-архітектура, у якій усі джерела генерації та споживачі підключені до спільної змінної шини (AC Bus) [10]. Така структура є сумісною з існуючою енергосистемою та дозволяє легко інтегрувати microgrid до централізованої мережі.

Однак значна частина сучасних джерел енергії та споживачів фактично працює у постійному струмі, таких як: акумуляторні системи накопичення енергії; зарядні станції електромобілів; електронне обладнання та телекомунікаційні системи [11], [12].

У традиційній AC-мікромережі такі елементи підключаються через інвертори та випрямлячі, що призводить до додаткових перетворень енергії та втрат [13].

Коефіцієнт корисної дії таких перетворювачів, що має вихідну потужність P_{out} та вхідну потужність P_{in} , визначається як [14]:

$$\eta = \frac{P_{out}}{P_{in}} \tag{2}$$

Втрати потужності у перетворювачі

$$P_{loss} = P_{in} - P_{out} \tag{3}$$

можна пов'язати з вихідною потужністю таким співвідношенням

$$Q = \frac{P_{out}}{P_{loss}} = \frac{\eta}{1-\eta} \quad (4)$$

Рівняння (4) зображено на рис. 2 Величина $Q=P_{out}/P_{loss}$ є фундаментальною характеристикою якості перетворювача електроенергії.

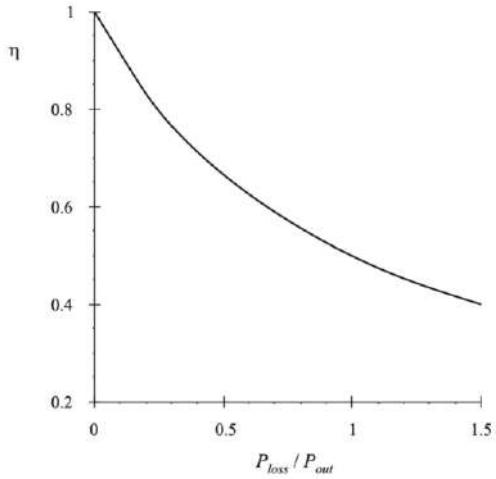


Рисунок 2. – Залежність втрат потужності в перетворювачі від коефіцієнта корисної дії

Альтернативним підходом є використання гібридної AC/DC microgrid (рис. 3), у якій одночасно використовуються дві енергетичні шини: AC-шина для традиційних електричних мереж і навантажень; DC-шина для джерел та споживачів постійного струму [9], [15].

У такій системі фотоелектричні системи та акумулятори підключаються безпосередньо до DC-шини, традиційні споживачі працюють від AC-шини, між шинами використовується двонаправлений AC/DC перетворювач.

Це особливо актуально на тлі стрімкого зростання електрифікації транспорту та збільшення частки DC-навантажень у сучасних енергосистемах [11], [12]. Електромобілі використовують акумуляторні батареї постійного струму, а швидкі зарядні станції фактично працюють із DC-енергією. Не останнє значення також має і зростання цін на пальне, що пов’язано з геополітичними процесами та нестабільністю на світових енергетичних ринках.

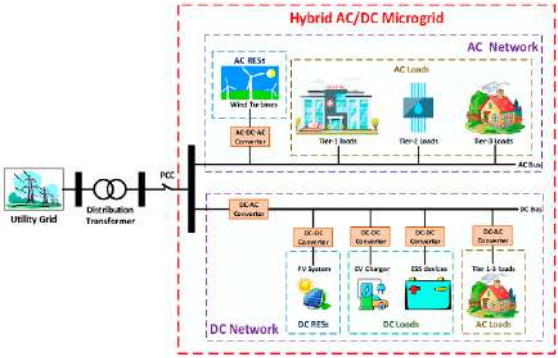


Рисунок 3. – Структура гібридної мікромережі

Висновки. У контексті сучасних воєнних загроз розвиток локальних microgrid може розглядатися як елемент формування розподіленої енергетичної оборони держави [2], [3]. На відміну від централізованої моделі енергопостачання, у якій пошкодження окремих ключових об’єктів може призвести до масштабних відключень, мережа локальних microgrid дозволяє створити енергетично автономні клітини на рівні територіальних громад. Кожна така система здатна забезпечувати електропостачання критичної інфраструктури навіть у разі пошкодження магістральних мереж. Формування мережі взаємопов’язаних microgrid на рівні громад може стати одним із напрямів підвищення стійкості національної енергосистеми та важливим елементом енергетичної безпеки держави в умовах воєнних загроз.

1. International Energy Agency. Resilience of power systems in a changing climate. IEA. 2021. https://www.iea.org/reports.

2. United Nations Development Programme. Energy resilience in times of crisis. 2022. https://www.undp.org.

3. European Commission. Energy system integration strategy. 2020. https://energy.ec.europa.eu.

4. Lasseter, R. H. MicroGrids. 2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings. 2002. pp. 305–308. https://doi.org/10.1109/PESW.2002.985003.

5. Hatziargyriou N. Microgrids: Architectures and Control. Wiley & Sons, Incorporated, John, 2013. 344 p.

6. Smart Management of Energy Losses in Distribution Networks Using Deep Neural Networks / I. Blinov et al. Energies. 2025. Vol. 18, no. 12. P. 3156. URL: https://doi.org/10.3390/en18123156.

7. Guerrero, J. M., Vasquez, J. C., Matas, J., de Vicuña, L. G., & Castilla, M. Hierarchical control of droop-controlled AC and DC microgrids. IEEE Transactions on Industrial Electronics. 2011. 58(1), 158–172. DOI: 10.1109/TIE.2010.2066534.

8. Abbasi, M.; Abbasi, E.; Li, L.; Aguilera, R.P.; Lu, D.; Wang, F. Review on the Microgrid Concept, Structures, Components, Communication Systems, and Control Methods. Energies 2023, 16, 484. https://doi.org/10.3390/en16010484.

9. IEEE Standards Association. (2018). IEEE Std 2030.7-2017: Microgrid controllers
http://www.ired2018.at/Sessions/5.2%20Standard%20micro%20contr_%20Joos.pdf.

10. Dragicevic, T., Lu, X., Vasquez, J. C., & Guerrero, J. M. D DC Microgrids–Part I: A Review of Control Strategies and Stabilization Techniques. IEEE Transactions on Power Electronics, 2016. 31(7), 4876–4891. DOI: 10.1109/TPEL.2015.2478859.

11. International Renewable Energy Agency. Innovation landscape for a renewable-powered future.2019. https://www.irena.org.

12. Electric Vehicle Outlook | BloombergNEF. BloombergNEF. URL: https://about.bnef.com/insights/clean-transport/electric-vehicle-outlook/.

13. Erickson, R. W., & Maksimović, D. (2001). Fundamentals of power electronics. Springer. https://doi.org/10.1007/b100747.

14. Maksimovic D., Erickson R. W. Fundamentals of Power Electronics (Second Edition). 2nd ed. Springer, 2001. 912 p.

15. P. Wang, X. Liu, C. Jin, P. Loh and F. Choo, "A hybrid AC/DC micro-grid architecture, operation and control," 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 2011, pp. 1-8, doi: 10.1109/PES.2011.6039453.

Т.В. Пучко

ФЕДЕРАТИВНЕ СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ РОЗВИТКУ ЕЛЕКТРОЕНЕРГЕТИКИ: ДЕЦЕНТРАЛІЗАЦІЯ ТА ЦИФРОВИЙ СУВЕРЕНІТЕТ

Розвиток електроенергетики України дедалі більше відбувається в умовах децентралізації генерації, зростання ролі приватних учасників ринку та потреби в координації між державними, комерційними й аналітичними структурами, що ставить нові вимоги до інфраструктури прогнозного моделювання електроенергетики [1, 2]. У таких умовах централізовані монолітні системи виявляються недостатньо гнучкими, складними для масштабування та вразливими з погляду кібербезпеки, тому доцільним є перехід до федеративної архітектури середовища моделювання, де незалежні учасники взаємодіють на основі інтероперабельності та суверенітету даних [3, 4].

Потреба в такому середовищі зумовлена, по-перше, необхідністю синхронізації стратегічних документів, які формуються різними органами влади та мають бути узгоджені між собою в межах довгострокового розвитку енергетики [1]. По-друге, інвестори та ринкові учасники потребують прозорих і верифіковних результатів моделювання, але водночас не готові відкривати чутливі дані про режими роботи активів, витрати та технічні параметри, що безпосередньо пов’язано з конкурентоспроможністю [2]. Саме тут постає суперечність між відкритістю, безпекою й приватністю, яку сучасні дослідження описують як трилему децентралізації, безпеки та приватності [4].

Федеративне середовище моделювання розвитку електроенергетики пропонується як інфраструктурна відповідь на цю суперечність. Його концепція спирається на децентралізоване володіння моделями та даними, відкритість стандартів, фізичне рознесення обчислень і технологічну незалежність учасників. За такого підходу конфіденційні локальні набори даних не залишають захищеного периметра власника, тоді як координаційні механізми забезпечують узгодженість сценарних припущень, повторюваність розрахунків та цілісність інформаційного простору [5]. Це створює підґрунтя не лише для підвищення якості прогнозування розвитку електроенергетики, а й для практичного втілення цифрового суверенітету в енергетичній сфері [6, 7].

Технічною основою такого середовища може бути багаторівнева структура реєстрів ресурсів, показана на рис. 1. На рівні моделей та інтерфейсів функціонують реєстр застосунків і реєстр моделей, які дають змогу відокремити користувацький доступ від конкретної реалізації алгоритмів і запускати моделі через стандартизовані програмні інтерфейси. На рівні даних та семантики діють реєстр вхідних даних, реєстр результатів

моделювання і реєстр форматів даних, що забезпечують каталогізацію параметрів, архівування результатів та уніфікацію обміну через спільні схеми й онтології. На рівні інфраструктури та обчислень працюють реєстр програмних засобів і реєстр обчислювальних ресурсів, які відкривають доступ до солверів, симуляторів, кластерів і серверів як до сервісів, а не як до локально встановлених компонентів.

Рисунок 1. – Багаторівнева структура реєстрів ресурсів

Така архітектура важлива не лише з технічного, а й з управлінського погляду. Вона дає змогу різним суб'єктам енергоринку спільно використовувати моделі, перевірені набори даних і результати розрахунків без дублювання зусиль і без централізованого передавання всіх ресурсів в один центр. У результаті децентралізація постає не як відмова від координації, а як форма організації, що підвищує адаптивність та еволюційну стійкість системи [3, 5].

За такої архітектури федеративного середовища моделювання особливого значення набуває інфраструктура довіри. Для федеративного обміну даними доцільно використовувати підходи International Data Spaces, де функції ідентифікації, сертифікації, каталогізації та аудиту розподілені між спеціалізованими ролями: Identity Provider, Certification Body, Metadata Broker та Clearing House [7]. Така модель знижує ризик концентрації повноважень, підтримує аудит транзакцій і дозволяє прив'язувати політики використання безпосередньо до даних, що є ключовим механізмом захисту цифрового суверенітету учасників екосистеми [6, 7].

Отже, федеративне середовище моделювання розвитку електроенергетики доцільно розглядати як інституційно й технологічно збалансовану платформу для прогнозування розвитку електроенергетики. Воно поєднує переваги децентралізації, інтероперабельності та контрольованого обміну даними, що створює підґрунтя для цифрового суверенітету учасників екосистеми [6, 7].

Дослідження виконано в рамках проекту 2025.07/0204 «Паралельні методи та алгоритми розв'язування задач змішаного цілочисельного лінійного програмування для планування розвитку структурно мінливих і резильєнтних електроенергетичних систем України», що виконується за рахунок грантової підтримки Національного фонду досліджень України (НФДУ).

1. Energy Charter Secretariat. (2022). *Synchronization of strategic documents in the energy sector in the context of the post-war recovery of Ukraine*. https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2022_11_15_-_Strategic_documents-_eng.pdf.

2. Stiewe, C. (2021). A Cost-efficient Deployment of Renewables. In *Reaching Ukraine's energy and climate targets* (pp. 119–135). Low Carbon Ukraine. https://www.lowcarbonukraine.com/wp-content/uploads/LCU_Reaching-Ukraines-energy-and-climate-targets.pdf.

3. Mosleh, M., Dalili, K., & Heydari, B. (2018). Distributed or Monolithic? A Computational Architecture Decision Framework. *IEEE Systems Journal*, *12*(1), 125–136. https://doi.org/10.1109/JSYST.2016.2594290.

4. Sun, Q., Ma, H., Zhao, T., Xin, Y., & Chen, Q. (2024). Break down the decentralization-security-privacy trilemma in management of distributed energy systems. *Nature Communications*, *15*(1), 4508. https://doi.org/10.1038/s41467-024-48860-7.

5. Grataloup, A., Jonas, S., & Meyer, A. (2024). A review of federated learning in renewable energy applications: Potential, challenges, and future directions. *Energy and AI*, *17*, 100375. https://doi.org/10.1016/j.egyai.2024.100375.

6. Lycklama, D. (2022). Data Space Functionality. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (pp. 521–534). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_32.

7. Pettenpohl, H., Spiekermann, M., & Both, J. R. (2022). International Data Spaces in a Nutshell. In B. Otto, M. ten Hompel, & S. Wrobel (Eds.), *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage* (pp. 29–40). Springer International Publishing. https://doi.org/10.1007/978-3-030-93975-5_3.

Ю.О. Дрейс

УДОСКОНАЛЕННЯ МЕТОДУ ОЦІНЮВАННЯ НАСЛІДКІВ ВТРАТИ ОБ'ЄКТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЗА АНТИТЕРОРИСТИЧНИМ КРИТЕРІЄМ

У роботі [1] розроблено *метод оцінювання наслідків втрати об'єкта критичної інформаційної інфраструктури (ОКІІ) узагальненими критеріями* (далі – метод) для своєчасної їх мінімізації та ліквідації, як способу попередження, виявлення, запобігання і нейтралізації загроз безпеці ОКІ та підтримки стану захищеності ОКІІ на рівні, за якого забезпечується безперервність функціонування і стійкість надання основних послуг та/або життєво важливих функцій за дев'ятьма критеріями: міжнародного та національного впливу, функцій та/або послуг, значущості, відповідальності, інформації, кіберзахисту, захисту і гарантій, кіберстійкості.

Функціональна залежність наслідків втрати ОКІІ (Consequences of Loss) від узагальнених критеріїв розраховується за виразом [1]:

$$CL = \frac{\sum_{i=1}^{n} cl_i}{n}, \qquad (1)$$

де n – кількість узагальнених критеріїв наслідків втрати ОКІІ; cl_i – коефіцієнт, який характеризує кількісну міру цих наслідків за i-м критерієм.

Таблиця 1 – Наслідки втрати ОКІІ за узагальненими критеріями

Оцінка наслідків втрати ОКІІ (*CL*)	Класифікація наслідків	Умовне позначення наслідку	Рівень негативного впливу	Категорія наслідків	Грошова шкала (€)
< 0,1	незначні	синій	1 бал	перша	< 100 тис.
0,11 ÷ 0,20	середні	зелений	2 бали	друга	100 тис.-1 млн.
0,21 ÷ 0,30	значні	жовтий	3 бали	третя	1-100 млн.
> 0,3	тяжкі	червоний	4 бали	четверта	> 100 млн.

Так як даний метод є універсальним і не обмежений кількістю критеріїв, пропонується удосконалити його за рахунок доповнення додаткового (десятого) міжсекторального критерію *за наслідками потенційних втрат (людських, економічних, екологічних та суспільно-політичних) від можливих терористичних посягань на функціонування (виробничий цикл) ОКІ та стану його системи забезпечення антитерористичної захищеності)* або скорочено як «*антитерористичний критерій*». Який, відповідно до пп. 15, 16 [2] означає, що під час формування прогнозованої загрози використовується модель терористичних посягань, спрямованих в найбільш уразливе місце об'єкта (у т.ч. ОКІ), що призводить до максимально можливих втрат, у найбільш незручний час з точки зору функціонування (виробничого циклу) об'єкта та стану його системи забезпечення антитерористичної захищеності, визначаються прогнозовані людські (К1), економічні (К2), екологічні (К3)

та суспільно-політичні (К4) втрати внаслідок терористичних посягань щодо об'єкта. Ідентифікація об'єкта проводиться шляхом визначення загального рівня потенційних втрат (**S**) від можливих терористичних посягань як [2]:

$$\mathbf{S} = \mathrm{K}1 + \mathrm{K}2 + \mathrm{K}3 + \mathrm{K}4. \quad (2)$$

Законом [3] встановлено чотири категорії критичності I (перша, A), II (друга, B), III (третя, C) і IV (четверта, D). Також за кожною категорією критичності ОКІ визначено рівень кризової ситуації (КС) до якої може призвести порушення функціонування ОКІ [3]: державний (Д), регіональний (Р), місцевий (М), об'єктовий (О) (див. критерій відповідальності у [1]).

Для отримання коефіцієнта cl_{10} за *антитерористичним критерієм*, тобто за наслідками потенційних втрат (людських, економічних, екологічних та суспільно-політичних) від можливих терористичних посягань на функціонування (виробничий цикл) ОКІ та стану його системи забезпечення антитерористичної захищеності, використаємо наступну формулу:

$$cl_{10} = \frac{t_i}{\sum_{i=1}^{n} t_i}, \quad (3)$$

де n – кількість категорій об'єкта та/або рівнів критичності ОКІ; t_i – коефіцієнт, який характеризує рівень можливих втрат за категорією об'єкта та/або рівнем критичності ОКІ від можливих терористичних посягань.

Взаємозв'язок характеристик наслідків та отримані результати за *антитерористичним критерієм* наведені у таблиці 2.

Таблиця 2. – Наслідки потенційних втрат за антитерористичним критерієм

Рівень КС	Коефіцієнт значущості втрат				Категорія об'єкта	Втрати (S)	Рівень критичності ОКІ	t_i	cl_{10}
	К1	К2	К3	К4					
Д	4	4	4	4	Перша (A)	14-16	0,82-1	0,9	0,36
Р	3	3	3	3	Друга (B)	10-13	0,57-0,81	0,715	0,29
М	2	2	2	2	Третя (C)	7-9	0,39-0,56	0,5	0,20
О	1	1	1	1	Четверта (D)	4-6	0,25-0,38	0,285	0,11

Удосконалений метод може бути корисним для політики інформаційної безпеки ОКІІ на етапі оцінки ризиків загроз для інформаційних активів ОКІ.

1. Дрейс, Ю. (2024). Метод оцінювання наслідків втрати об'єкта критичної інформаційної інфраструктури за узагальненими критеріями. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(25), 487–504. https://doi.org/10.28925/2663-4023.2024.25.487504.

2. Про затвердження Правил терористичної безпеки. Кабінет Міністрів України. Постанова, правила №1172 від 15.10.2024, https://zakon.rada.gov.ua/laws/show/1172-2024-%D0%BF#Text.

3. Про критичну інфраструктуру. Закон України від 16.11.2021 (редакція від 21.06.2024), https://zakon.rada.gov.ua/laws/show/1882-20#Text.

С.В. Сушко

АСПЕКТИ ВІДДАЛЕНОГО ВИМІРЮВАННЯ І МОНІТОРИНГУ ПАРАМЕТРІВ ЕНЕРГОМЕРЕЖІ

В світі останніми роками набувають розвитку мережі передачі електричної енергії Smart Grid [1]. [2]. Такі системи, на відміну від класичних мереж, застосовують вимірювання і передачу параметрів електричної мережі у її вузлах. Використання Smart Grid, при належній системі контролю і керування, дозволяє підвищити ефективність використання електричних мереж. Smart Grid підвищують ефективність енергосистем завдяки автоматизації, зменшуючи втрати енергії та підвищуючи стабільність постачання. Основні переваги включають інтеграцію відновлюваних джерел енергії (CEC, BEC), самовідновлення при аваріях, зниження викидів, та можливість для споживачів керувати витратами через розумні лічильники.

В контексті воєнних дій деякі з підходів Smart Grid можуть бути запозичені для надійного і ефективного використання електричних мереж, пристроїв енергетики, акумуляторів Силами Оборони України. Зважаючи на вірогідне фізичне ураження об’єктів енергосистеми під час військових дій, віддалений моніторинг елементів енергосистеми має особливий сенс. Маючи інформацію про стан мережі, рівень заряду акумулятора, наявність електричної напруги в будь-якій точці енергомережі, оператор може прийняти рішення про зміни в енергомережі, увімкнення генераторів, заряджання акумуляторів, постачання заряджених акумуляторів на бойові позиції де не можна виконати заряджання акумуляторів на місці.

Загалом, схема підключення будь-якого пристрою для віддаленого моніторингу енергомережі збігається з технологією IoT: пристрій передає дані в мережу, де вони зберігаються на сервері і можуть бути переглянуті користувачем, якому цей доступ надано. Функціональна діаграма підключення наведена на рис. 1.

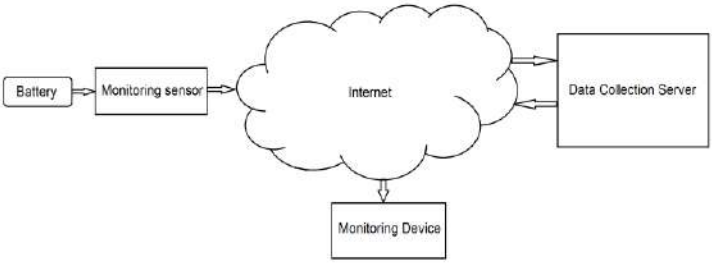


Рисунок 1. – Функціональна діаграма підключення пристроїв віддаленого моніторингу параметрів енергомережі

Важливим являється можливість віддаленого вимірювання напруги постійного струму. Використання сенсора для віддаленого вимірювання напруги дозволяє спостерігати рівень заряду акумулятора не перебуваючи поруч з ним. Автором розроблений пристрій, написано ПЗ для нього, а також зконфігуровано і налаштовано сервер для накопичення і відображення даних [3-6].

Безпосереднім пристроєм, що виконує вимірювання і пересиланням даних на сервер, обрано плату на базі мікроконтролера ESP32 та GSM модулем для зв'язку. З метою точного і стабільного вимірювання рівнів напруги використовується зовнішній АЦП ADS 1115 з розрядністю 16 біт. Структурна схема пристрою відображена на рис. 2.

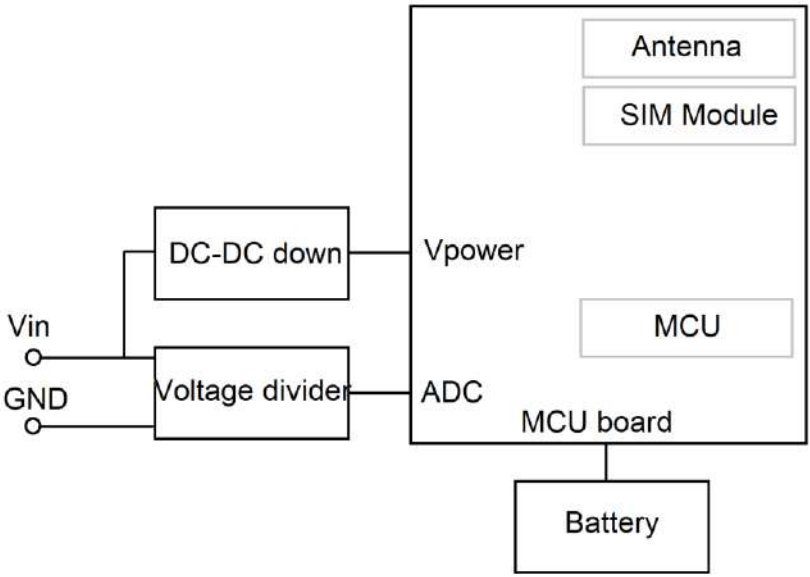


Рисунок 2. – Структурна схема пристрою для віддаленого вимірювання напруги акумулятора

Корпус для пристрою було спроектовано і роздруковано на 3D принтері. Розміри корпусу становлять 100*44*38 мм. Зовнішній вигляд пристрою та приклад підключення до батареї 51В наведено на рис. 3.

Рисунок 3. – Приклад підключення віддаленого сенсору напруги

За результатами вимірювань було отримано графіки у часі напруги на віддаленому акумуляторі. Приклад вимірювань наведено на рис. 4.

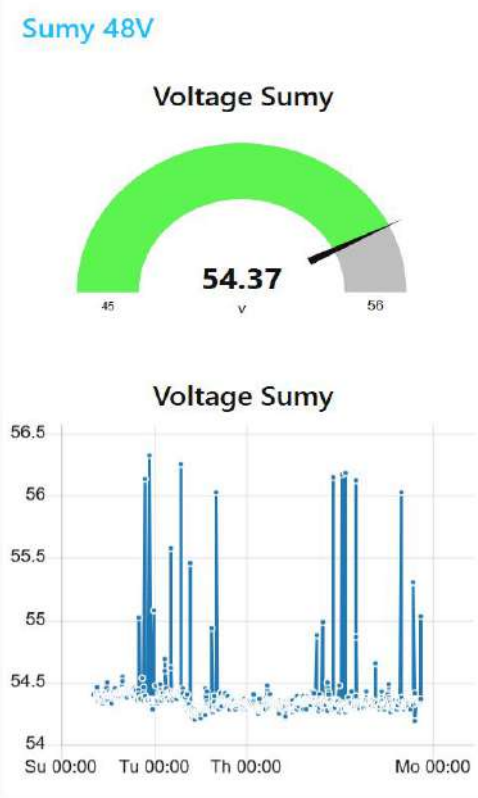


Рисунок 4. – Результати вимірювань напруги

В результаті досліджень було зпроектовано і побудовано дослідний екземпляр сенсору віддаленого вимірювання напруги. Розроблений сенсор складається із загальнодоступних і недорогих споживацьких електронних плат. Сервер містить програмний пакет Node-RED, що виконує накопичення і відображення отриманих даних. ПЗ для мікроконтролера написано власноруч, що гарантує, що виміряні дані будуть передано виключно на цільовий сервер і не будуть передані кудись де-інде на сервер виробника пристрою. Також власне ПЗ гарантує, що пристрій не може бути вимкнено за командою віддалено, чого не можна виключати для наявних на ринку пристроїв схожого призначення. Запропонована схема функціонування здатна для розширення функціональності та гнучка в контексті підключення більшої кількості пристроїв.

1. Alymov, Ivan, and Moshe Averbukh. 2024. "Monitoring Energy Flows for Efficient Electricity Control in Low-Voltage Smart Grids" Energies 17, no. 9: 2123. https://doi.org/10.3390/en17092123.

2. Kabeyi, Moses Jeremiah Barasa, and Oludolapo Akanni Olanrewaju. “Smart Grid Technologies and Application in the Sustainable Energy Transition: A Review.” 2023, International Journal of Sustainable Energy 42 (1): 685–758. doi:10.1080/14786451.2023.2222298.

3. S. Sushko and O. Chemerys. (2024) Remote Voltage Monitoring for Smart Grid. 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2024, pp. 1-5, doi: 10.1109/DESSERT65323.2024.11122237.

4. Sushko, S., Tetskyi, A., Perepelitsyn, A. (2025). Microcontroller-Based System for Balancing and Monitoring of Li-ion Battery Pack. In: Lytvynov, O., Pavlikov, V., Krytskyi, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2024. ICTM 2024. Lecture Notes in Networks and Systems, vol. 1473. Springer, Cham. https://doi.org/10.1007/978-3-031-94845-9_49.

5. Z. Chaczko and R. Braun, "Learning data engineering: Creating IoT apps using the node-RED and the RPI technologies," 2017 16th International Conference on Information Technology Based Higher Education and Training (ITHET), Ohrid, Macedonia, 2017, pp. 1-8, doi: 10.1109/ITHET.2017.8067827.

6. James, Alice & Seth, Avishkar. “IoT enabled sensor node: a tutorial paper. International Journal on Smart Sensing and Intelligent Systems.” 2020, 13. pp. 1-18, doi: 10.21307/ijssis-2020-0.

О.І. Клюзко

ПРОГНОЗУВАННЯ ОБСЯГІВ СПОЖИВАННЯ ЕЛЕКТРОЕНЕРГІЇ МЕТОДОМ «RANDOM FOREST» ІЗ ЗАСТОСУВАННЯМ «LS-ФАКТОРА» ДЛЯ МОДЕЛЮВАННЯ ВПЛИВУ РАКЕТНО-ДРОНОВИХ АТАК НА ЕНЕРГОСИСТЕМУ

За інформацією DIXI Group, упродовж періоду від лютого 2022 року до грудня 2024 року енергетична система України зазнала 13 масованих атак [1]. Ці атаки відрізнялися як за масштабом, так і за характером наслідків для функціонування енергосистеми. Частина з них спричинила значні пошкодження об'єктів енергетичної інфраструктури [2] та зумовила необхідність тривалого обмеження електропостачання споживачів. Тривалість стабілізаційних відключень, необхідних для відновлення сталої роботи системи, залежала від виду та інтенсивності уражень. Загальна тривалість відключень електроенергії для споживачів перевищила 1951 годину [3].

З огляду на те, що постачальник електричної енергії закуповує електроенергію на оптовому ринку заздалегідь для кожної окремої години розрахункового місяця, раптове зниження фактичного навантаження внаслідок аварійних або планових відключень створює суттєві економічні ризики. У таких умовах недоспожиті обсяги електроенергії доводиться реалізовувати на балансуючому ринку, що може призводити до фінансових втрат для постачальника. Це зумовлює потребу у застосуванні інструментів погодинного прогнозування електроспоживання, здатних враховувати складні взаємозв'язки між зовнішніми чинниками, які визначають поведінку споживачів. В сучасних умовах України, крім традиційних факторів впливу, такі інструменти мають враховувати також наслідки вимушених відключень, спричинених пошкодженням енергосистеми внаслідок ракетно-дронових атак.

Метою дослідження є розроблення методології прогнозування погодинних обсягів електроспоживання, яка забезпечує вищу адекватність прогнозних оцінок в умовах порушення нормального режиму функціонування енергосистеми, спричиненого ракетно-дроновими ударами.

Серед сучасних методів машинного навчання метод Random Forest належить до найбільш перспективних для задач короткострокового прогнозування електроспоживання. Це пояснюється його стабільною результативністю в межах кластерно-гібридних підходів, можливістю визначення важливості ознак, стійкістю до шумових спотворень і пропусків у даних, а також відносно невисокими вимогами до обчислювальних ресурсів. Разом із тим наявні методологічні підходи до прогнозування електроспоживання формуються з урахуванням різного набору факторів,

вибір яких визначається специфікою поставленої задачі. Для застосування таких підходів в українських реаліях доцільним є введення додаткового чинника, що відображає вимушене обмеження навантаження споживачів за графіками, запровадженими внаслідок руйнування енергетичної інфраструктури.

У період повномасштабної війни фіксуються часові інтервали істотного скорочення обсягів електроспоживання, які пов'язані з примусовим розвантаженням споживачів. Для врахування таких екстремальних режимів функціонування енергосистеми простір вхідних ознак моделі Random Forest було доповнено load-shedding-фактором (LS-фактором). Цей фактор подано у вигляді тривимірного дескриптора, що кількісно описує оперативний стан мережі за трьома характеристиками: наявністю факту розвантаження споживачів, кількістю знеструмлених фаз і часткою споживачів, які залишилися без електропостачання. Урахування LS-фактора дає змогу підвищити адаптивність моделі до нестійких режимів роботи енергосистеми та знизити прогнозну похибку в кризові періоди.

Доступ до детальної інформації про генерацію й конкретні об'єкти уражень у воєнний час обмежений, проте агреговані показники (дата, характер та географія масованих обстрілів) публікуються відкрито[1], що дало змогу синхронізувати їх із погодинними даними щодо обсягів споживання електроенергії.

Формування load-shedding-фактора було здійснено на основі щоденних оперативних даних, що публікуються на офіційних сайтах EnergyMap [1], DTEK[4], НЕК «Укренерго» [5], аналітичних бюлетенів DIXI Group [6].

Визначення load-shedding-фактору $LS(t)$ має вигляд тривимірного вектору

$$LS(t) = \left[l_1(t), l_2(t), l_3(t)\right] \tag{1}$$

- $l_1(t)$ – бінарний індикатор факту повного відключення електропостачання у годину t;
- $l_2(t)$ – порядковий рівень (0–4) оголошеної черги планових чи аварійних обмежень;
- $l_3(t)$ – кількість населених пунктів без живлення у ту саму годину.

Фактор не згортається у скаляр: кожна компонента надходить у модель Random Forest як самостійна ознака. Така подача даних зберігає повноту інформації (від самої події до її просторового масштабу), не потребує суб'єктивного нормування й легко розширюється, наприклад, тривалістю відключення або недовідпущеною потужністю.

Узгоджене тривимірне кодування дозволило об'єднати три різнорівневі характеристики (дихотомічну, рангову та масштабну), які

раніше розглядалися розрізнено. Більше того, оскільки Random Forest оцінює вагу кожної ознаки автоматично, то це дозволило уникнути ручного підбору коефіцієнтів та підвищити відтворюваність результатів прогнозування. Порівняльні експерименти засвідчили, що введення вектору $[l_1(t), l_2(t), l_3(t)]$ зменшує середню абсолютну похибку прогнозу в кризові дні на 15–25 % відносно конфігурацій, у яких проблемні часові ряди були відсутні. Отже, багатовимірний LS-фактор забезпечує суттєве підвищення адаптивності прогнозної моделі до умов, характерних для екстремальних режимів роботи енергосистеми.

Введемо одновимірні часові ряди, що надходять із SCADA-телеметрії або реєстру аварійних відключень ОСР з кроком дискретизації , згідно опису наведеного в таблиці 1:

Таблиця 1. Опис компонентів вектора load-shedding-фактора

Позначення	**Попередня назва у CSV**	**Діапазон**	**Семантика**
$l_1(t)$	load-shedding	{0,1}	індикатор повної втрати напруги у мережі споживача
$l_2(t)$	phases	{0,1,2,3,4}	кількість знеструмлених фаз (ordinal)
$l_3(t)$	deenergized	N_0	кількість споживачів, що одночасно залишилися без електроживлення

Наведені ряди об’єднуємо у вектор-спостереження:

$$LS(t) = \left[l_1(t), l_2(t), \tilde{l}_3(t) \right]^T \in R^3, \; t \in \{1,\ldots,T\}. \tag{2}$$

Оскільки $l_3(t)$ може набувати значень на кілька порядків вищих за інші компоненти, застосовуємо лінійну нормалізацію:

$$\tilde{l}_3(t)_r = \frac{l_3(t)}{\max_{1 \le s \le T} l_3(s)}. \tag{3}$$

Якщо немає відключень, $\tilde{l}_3(t) = 0$.

Для категоріальної величини $l_2(t)$ достатньо порядкового кодування – Random Forest коректно працює з ordinal-скалами, не потребуючи one-hot-розгортання, що дозволяє уникнути штучного зростання розмірності.

Нехай $X(t)$ – базовий вектор ознак (рік, місяць, день, … температура тощо):

$$X(t) = \left[x_1(t), x_2(t), \ldots, x_p(t) \right]^T \tag{4}$$

Тоді доповнений вектор, що надходить на вхід моделі, має наступний вигляд

$$X(t)\Big|=\left[x_1(t),x_2(t),\ldots,x_p(t),l_1(t),l_2(t),\tilde{l}_3(t)\right]^T \tag{5}$$

Прогнозна модель, доповнена load-shedding-фактором, демонструє суттєве підвищення адекватності прогнозу електроспоживання в період з 18 по 30 листопада 2024 року – саме в дні масштабних аварійних та стабілізаційних відключень. Розширена конфігурація відтворює не лише погодинний графік споживання електроенргії, а й характерні спади під час вимкнень, а також нерівномірність між робочими та вихідними днями. У порівнянні з базовим варіантом, МАЕ у вказаному інтервалі зменшилась з 0,122 МВт·год до 0,096 МВт·год, а відносна похибка – з 8,4 % до 6,6 %. Це зниження похибки прогнозу забезпечило орієнтовне скорочення сумарних небалансів на близько 38 %. що у грошовому вираженні відповідає скороченню витрат постачальника на закупівлю електроенергії приблизно на 16%

1. Інформація щодо масованих ударів по критичній інфраструктурі України (Ukr). URL: https://map.ua-energy.org/uk/resources/12f3148d-841a-478d-b9ed-72bf0764b286/.
2. Саух, С. і Борисенко, А. 2025. Моделювання електроенергетичної системи україни та оцінювання її резильєнтності в умовах систематичних терористичних атак. Технічна електродинаміка. 2025. №2, С. 57-70 DOI: https://doi.org/10.15407/techned2025.02.057.
3. ІНФОРМАЦІЯ ЩОДО ЗАСТОСУВАННЯ ЗАХОДІВ ОБМЕЖЕННЯ СПОЖИВАННЯ ЕЛЕКТРОЕНЕРГІЇ URL: HTTPS://MAP.UA-ENERGY.ORG/UK/RESOURCES/0F8F9882-1FB2-47C6-81DC-31FBAD914F16/.
4. Планові і аварійні графіки відключень. Офіційний сайт ДТЕК Київські Електромержі URL:https://www.dtek-kem.com.ua/ua/shutdowns (дата звернення: 15.06.2025).
5. Офіційний сат НЕК «УКРЕНЕРГО» URL: https://ua.energy/uchasnikam_rinku/ (дата звернення: 15.06.2025)
6. Проходження осінньо-зимових періодів 2022-2024: State of the Energy System. DiXi Group. Kyiv. URL: https://dixigroup.org/wp- content/uploads/2024/04/2024_ winterseasons_analysis_dixi_group_final.pdf.

В.М. Зварич, Ю.І. Гижко

ДЕЯКІ АЛГОРИТМИ ВІБРОДІАГНОСТИКИ ЕНЕРГЕТИЧНОГО ОБЛАДНАННЯ НА ОСНОВІ МОДЕЛЕЙ ЛІНІЙНИХ ВИПАДКОВИХ ПРОЦЕСІВ

Оцінка надійності роботи електротехнічного обладнання та його діагностика набувають особливого значення в повоєнний період. Для надійної роботи електростанції важливе безперебійне функціонування не тільки її основного обладнання, але і обладнання власних потреб та відповідальних вузлів такого обладнання.

Надійність роботи енергетичного обладнання тісно пов'язана з ефективними системами контролю та діагностики, якими вони оснащені. Побудова таких систем відбувається в кілька етапів: розробка математичних моделей інформаційних сигналів таких систем, виділення на основі аналізу таких моделей більш інформативних діагностичних ознак, побудова навчальних сукупностей і розв′язувальних правил, розробка алгоритмів діагностики та самої системи на основі отриманих наукових результатів.

При побудові новітніх систем моніторингу і діагностування електроенергетичних об’єктів все частіше використовується концепція Smart Grid. Застосування цієї концепції (в тому числі і у багаторівневих систем моніторингу і діагностики) передбачає, що обслуговування та ремонт енергетичного обладнання повинні здійснюватися за фактичним станом [1]. Для цього значно більша частина обладнання повинна бути охоплена системами забезпечення надійності, які повинні здійснювати постійний чи періодичний контроль його фактичного технічного стану. Крім того, самі ці системи повинні мати більше можливостей: забезпечувати двосторонній обмін інформацією на всіх рівнях, віддалений моніторинг стану, прогнозування відмов, планування необхідності у запасних частинах, оцінку залишкового ресурсу тощо.

Розробкою подібних систем займаються такі компанії як Brüel & Kjær, PCB, SPM, Deriton, Bently Nevada, Timken а також виробники великого електротехнічного обладнання – Siemens, ABB та ін. Зрозуміло, що в повоєнний час доцільно мати мобільні системи моніторингу та діагностики.

Особливо привабливим у такий час є використання бездротових технологій побудови систем контролю та діагностики. Структура цих систем залежить від того, моніторинг та діагностику якого обладнання треба проводити [2].

Лінійні випадкові процеси знаходять все ширше застосування при вирішенні задач виділення (детекції) і класифікації інформаційних сигналів в радіотехніці, геофізиці, вібродіагностиці, біомедичних дослідженнях.

Оскільки сучасні системи діагностики у своєму складі мають мікропроцесори або персональні комп'ютери, все більшого застосування в додатках набувають процеси з дискретним часом.

В доповіді в якості математичних моделей діагностичних сигналів пропонується використати лінійні процеси авторегресії. Процесом авторегресії (AR) називається процес, який можна задати наступним чином

$$\xi_t + a_1\xi_{t-1} + ... + a_p\xi_{t-p} = \varsigma_t \qquad (1)$$

або

$$\xi_t = -\sum_{i=1}^{p} a_i\xi_{t-i} + \varsigma_t$$

де $a_1,...,a_p$ - параметри авторегресії; p - порядок авторегресії ς_τ - породжуючий процес. Для лінійних (AR) процесів породжуючий процес є процесом з незалежними значеннями, що має безмежно подільний закон розподілу.

Відзначимо, що лінійний процес авторегресії відноситься до лінійних випадкових процесів з дискретним часом і може бути представлений у вигляді

$$\xi_t = \sum_{\tau=0}^{\infty} \varphi(\tau)\varsigma_{t-\tau}$$

$\{\varphi(\tau), \tau \in Z\}$- деяка числова послідовність дійсних чисел, яку називають імпульсною реакцією, або ядром лінійного випадкового процесу ξ_t. Передбачається, що виконується співвідношення

$$\sum_{\tau=0}^{\infty} \varphi^2(\tau) < \infty, \quad \varphi(\tau) \equiv 0 \quad \text{при } \tau < 0 \ . \qquad (2)$$

Ядро $\{\varphi(\tau), \tau \in Z\}$ рекурентно пов'язано з параметрами авторегресії $a_1,...,a_p$ [3]. Як правило, породжуючий процес $\{\zeta_t, t \in Z\}$ лінійних процесів авторегресії та авторегресії ковзного середнього розглядають як послідовність незалежних однаково розподілених випадкових величин. Оскільки виконується умова (2), представлення (1) має сенс і для випадку, якщо породжуючий процес $\{\zeta_t, t \in Z\}$ є послідовність незалежних не однаково розподілених, але безмежно подільних випадкових величин, однак така послідовність повинна асимптотично рівномірно сходитися до нуля (збігатися за ймовірністю) [3], тобто виконуватися умова $\forall\ \varepsilon > 0, \quad P\{|\zeta_{t,n}| > \varepsilon\} < \varepsilon$ при і $t = 1,\ldots,n..$

В доповіді розглянуто питання використання властивостей лінійних процесів для побудови розв'язувальних правил.

Показано побудову міри різниці між стаціонарними процесами авторегресії а також між гільбертовими стаціонарними та оберненими [2] процесами використовуючи ядра таких процесів. Така міра визначається відстанню $d\left[\xi_1(t),\xi_2(t)\right]$, яку можна визначити таким чином:

$$d\left[\xi_1(t),\xi_2(t)\right]=\sqrt{\sum_{\tau=0}^{\infty}\left(\varphi_{\xi 1}(\tau)-\varphi_{\xi 2}(\tau)\right)^2}\ , \qquad (3)$$

де $\varphi_{\xi 1}(\tau)$ - ядро лінійного стаціонарного процесу авторегресії $\xi_1(t)$, $\varphi_{\xi 2}(\tau)$- ядро лінійного стаціонарного процесу авторегресії $\xi_2(t)$. Зазначимо, що таким чином можна побудувати розв′язувальні правила для лінійних процесів авторегресії, що мають різний порядок авторегресії, а також побудувати розв′язувальні правила для процесів авторегресії та процесів ковзного середнього. Відповідно до [4], функція $d\left[\xi_1(t),\xi_2(t)\right]$ завжди існує і задовольняє властивостям функції відстаней тобто, вона позитивна, існує нульовий елемент і має місце нерівність трикутника.

Розглянуто приклад використання такого підходу, а також деякі інші приклади побудови розв'язувальних правил з діагностики технічного стану енергообладнання.

1. Babak V.P., Babak S.V., Myslovych M.V., Zvaritch V.N., Zaporozhets A.O. Diagnostic Systems For Energy Equipment. – Springer Nature, Switzerland AG, 2020. 134 P. https://doi.org/10.1007/978-3-030-44443-3.

2. Гижко, Ю., Зварич, В. Особливості побудови компонентів багаторівневих експертних систем вібродіагностики вузлів електротехнічного обладнання з урахуванням використання бездротових блоків зв′язку. *Технічна електродинаміка*. 5 (2024), 094. URL: https://doi.org/10.15407/techned2024.05.094.

3. V. Zvaritch, 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. https://doi.org/10.1007/978-3-031-44772-3_12.

4. Triacca U. Feedback causality and distance between ARMA models. Mathematical and Computing in Simulation, 2004, vol. 64, pp. 679-685.

С.С. Шевченко

НАДІЙНІСТЬ НАСОСНОГО ОБЛАДНАННЯ АЕС – ВАЖЛИВИЙ ФАКТОР СТІЙКОСТІ ЕНЕРГЕТИКИ УКРАЇНИ

В Україні атомна енергетика є ключовим компонентом енергетичної системи держави, що забезпечує значну частку електроенергії, особливо в умовах військових дій та обмежених можливостей теплової енергетики. Надійність та стійкість роботи атомної енергетики — це багатокомпонентний підхід, що охоплює технологічні, операційні та стратегічні аспекти для забезпечення безперебійного енергопостачання в умовах зростаючих викликів.

Насосне обладнання атомних електростанцій (АЕС) виконує технологічні функції, що безпосередньо пов'язані із забезпеченням ядерної та радіаційної безпеки: з одного боку, відмови деяких насосів можуть викликати великі аварії, а з іншого – насоси є важливими елементами різних систем безпеки [1]. Відцентрові насоси відіграють важливу роль у забезпеченні резильєнтності АЕС. Порушення потоків чи відхилення їх параметрів від необхідних значень призводять до зниження економічності блоку, а частіше створюють аварійні ситуації. Позапланові простої блоку АЕС призводять до суттєвої недоподачі в мережу електроенергії через неоптимальні режими роботи агрегатів АЕС, що призводить до величезних економічних втрат, а в умовах воєнного стану і до блекаутів.

На рис.1 наведено діаграму, що відображає розподіл дефектів насосного обладнання за типами, згідно інформації про експлуатацію насосного обладнання атомних станцій за 2015-2020 роки [2].

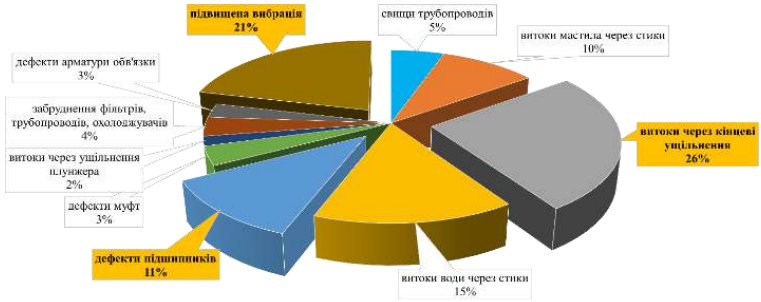


Рисунок 1. – Діаграма розподілу дефектів насосного обладнання АЕС

Як показав аналіз наведених даних найпоширенішим дефектом насосного обладнання є «витоки через кінцеві ущільнення». Основними причинами є механічне зношування ущільнюючих поверхонь внаслідок

застосування застарілих конструкцій ущільнень. Другий за кількістю дефект – «підвищена вібрація».

Для високонапірних відцентрових насосів АЕС (рис. 2) характерні високі робочі параметри: подача, тиск і швидкість обертання ротора. В результаті високонапірні відцентрові машини, як правило, високооборотні. А для таких машин проблеми динаміки роторів особливо актуальні [3]. Відповідно зростають проблеми, пов'язані із забезпеченням ефективної герметизації ущільнюваного середовища.

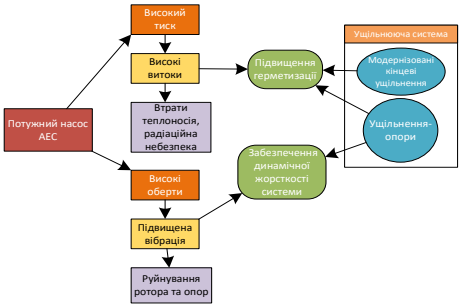


Рисунок 2. – Шлях вирішення проблеми вібрації ротора насоса [4]

Таким чином, крім власне герметизації ущільнювальні системи мають все більший вплив на загальну експлуатаційну безпеку обладнання, особливо вібраційну. Досліди, проведені на спеціально створеній установці, показали, що використання безконтактних ущільнень ротора в якості опор дозволяє зняти проблему вібрацій.

На рис. 3 показано приклади використання безконтактних ущільнень в якості опор ротора. Тобто щілинні ущільнення робочих колес, які працюють за рахунок перепаду тиску середовища, що перекачується, відіграють роль не тільки статичних, а й динамічних опор, які за рахунок тиску рідини, що ущільнюється придушують вібрації ротора. Такі насоси можуть працювати без виносних опор.

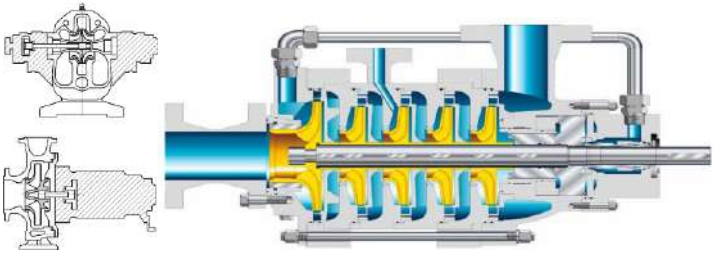


Рисунок 3. – Приклади використання безконтактних ущільнень в якості опор в енергетичних насосах

Також для забезпечення герметизації важливу роль відіграють кінцеві ущільнення ротора насоса. Практична реалізація модернізації кінцевих ущільнень ілюструється на прикладі ущільнення вертикального насоса типу КсВА атомної електростанції [5, 6] (рис. 4).

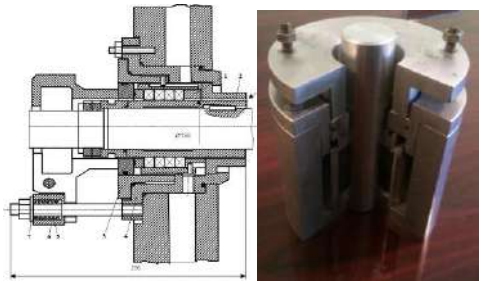


Рисунок 4. – Модернізована ущільнююча система насоса КсВА

Промислові випробування та досвід експлуатації таких ущільнень показали, що тепер ущільнення працюють без обслуговування від ППР до ППР.

За результатами проведених досліджень створено методику проектування та модернізації ущільнюючих систем відцентрового обладнання атомних електростанцій, на основі якої забезпечується стійка герметичність та вібраційна надійність насосів АЕС.

1. Марцинковський В.А., Шевченко С.С. Насосы атомних електростанцій: розрахунок, конструювання, експлуатація: монографія / під заг. ред. С.С. Шевченко. Суми: Університетська книга, 2018. 472 с. ISBN 978-966-680-866-3.
2. Шевченко О.С., Гурець Л. Л., Ковальчук М.М., Шевченко С.С. Оцінка ризику техногенних аварій насосів АЕС та їх екологічних наслідків. Ядерна та радіаційна безпека. No. 2(106), 2025. https://doi.org/10.32918/nrs.2025.2(106).06.
3. Shevchenko, S. (2025) Sealing and Vibrations of Centrifugal Machines. /First edition/ – USA, CRC Press, Taylor & Francis Group. 264 P. ISBN 9781041095040 https://doi.org/10.1201/9781003651925.
4. Шевченко С. С. Спосіб зниження вібрації ротора відцентрової машини. Патент UA 161011U публ. 29.10.2025, р., бюл. №44 – заяв. U202502046, 01.05.2025 р.
5. Шевченко С. С. Сальникове ущільнення валу. Патент UA 151398 U; F16J 15/18 публ. 13.07.2022 р., бюл. №28 – заяв. U 202200856, 23.02.2022 р.
6. Шевченко С. С. Сальникове ущільнення валу. Патент UA 152297 U; F16J 15/18 публ. 11.01.2023 р., бюл. №2 – заяв. U 202202341, 07.06.2022р.

СВІТОВІ ІНВЕСТИЦІЇ В ЕНЕРГЕТИЧНІ ІННОВАЦІЇ УКРАЇНИ

Третій щорічний Форум МЕА (на 2026 р. спільнота МЕА охоплювала близько 75% світового попиту на енергію) з енергетичних інновацій відбувся одночасно з зустріччю міністрів 18 лютого 2026 р. Форум зібрав учасників від урядів, галузей промисловості, стартапів, інвестиційних і дослідницьких спільнот, дозволяючи вести поглиблений обмін думками з питань, пов'язаних з політикою енергетичних інновацій та розвитком інноваційної екосистеми. Розглядалися теми інновацій для підтримки резильєнтних електромереж [1], технологій термоядерної енергетики [2], самопідтримуваних джерел енергії, а також теми зв'язків між інноваціями, ланцюгами постачання технологій та економічною конкурентоспроможністю [3].

19 лютого 2026 р. міністри дев'яти країн-членів МЕА (Великобританія, Данія, Канада, Латвія, Литва, Німеччина, Польща, Чехія, Швеція) та Європейська комісія (ЄК) під час Міністерської зустрічі МЕА опублікували спільну заяву, в якій підтвердили свою підтримку Програми співпраці МЕА з Україною (донорами якої є згадані країни), підкресливши важливість цієї ініціативи в умовах повномасштабної агресії в Європі, яка за тривалістю і втратами наближається до тривалості і втрат попередньої світової війни. Міністри високо оцінили роботу МЕА з Україною в рамках Програми, зазначивши, що вона підтримує короткострокову відбудову енергетичного сектору України, який залишається під значними атаками з боку РФ, і водночас допомагає сприяти довгостроковим інвестиціям, потрібним Україні для побудови нового енергетичного майбутнього. У своїй заяві міністри наголосили, що Програма співпраці МЕА з Україною (IEA–Ukraine Collaboration Programme), заснована у 2025 р., є ключовим доповненням до роботи, яку проводить МЕА в рамках своєї Спільної робочої програми з Україною (Joint Work Programme with Ukraine) на 2025–2026 рр. Співпраця МЕА з Україною поглибилася, коли 19 липня 2022 р. Україна стала асоційованим членом МЕА. Міністри наголосили, що Програма була ключовою передумовою, яка сприяла аналізу МЕА енергетичної ситуації в Україні та допомагала формувати власні зусилля України та дії її партнерів.

В рамках роботи Секретаріату МЕА через Програму, МЕА опублікувало 10-кроковий план для України щодо захисту її енергосистеми протягом зимнього періоду 2024–2025 рр., оновлену інформацію на 2025–2026 рр., дорожню карту децентралізації енергосистеми України. У лютому 2026 р. МЕА опублікувало звіт, у якому висвітлено ключові уроки України, які можуть сприяти плануванню енергетичної резильєнтності в усьому світі. Донори закликали МЕА далі посилювати роботу з уможливлення інвестицій в енергетичний сектор України, які є критично важливими для побудови безпечної, сучасної, резильєнтної та самопідтримуваної енергосистеми України, а також закликали інших членів МЕА надавати додаткове фінансування для взаємовигідного розширення Програми.

Спільна заява на підтримку Програми співпраці МЕА–Україна зазначає, що значні пошкодження критично важливої цивільної та енергетичної інфраструктури по всій Україні є прямим результатом триваючої війни РФ проти України. Посилення атак РФ на критично важливу енергетичну інфраструктуру в Україні протягом 2025 р. мало серйозні наслідки для повсякденного життя цивільного населення, а ці атаки продовжували зростати за масштабами та інтенсивністю. Програма співпраці МЕА–Україна паралельно з іншими зусиллями міжнародних донорів, включаючи зусилля, що координуються через Групу підтримки енергетики України G7+ (G7+ Ukraine Energy Support Group), є ключовою ініціативою, завдяки якій МЕА здатне підтримувати значні потреби України у відбудові енергетичного сектору та допомагати їй сприяти інвестиціям для побудови нового енергетичного майбутнього. Ця Програма також відіграє цінну роль у зміцненні відносин МЕА з Україною. Донори Програми визнають зусилля, яких докладає МЕА для допомоги Україні у формуванні стратегічного бачення безпечного та резильєнтного енергетичного майбутнього, включаючи підтримку ініціатив сприяння інвестуванню в розподілені енергетичні ресурси, а також визнають роботу МЕА з поширення ключових уроків, отриманих від України, яка працює над збереженням енергетичної безпеки та резильєнтності, незважаючи на постійні атаки на основі новітніх озброєнь. Донори Програми висловлюють вдячність за реалізацію Спільної робочої програми МЕА з Україною, яка охоплює ключові енергетичні пріоритети України, включаючи безпеку енергетичного сектору, безпеку постачання нафти і газу, енергозбереження та перехід до більш безпечної, самопідтримуваної, резильєнтної та доступної енергетичної системи, інтегрованої з Європою, а також схвалюють інтенсифікацію діяльності МЕА в рамках цієї Програми, як того вимагали міністри МЕА на зустрічі міністрів 2024 р. Донори Програми вітають і підтримують внесок МЕА у подальше посилення співпраці з Україною через Програму співпраці МЕА−Україна та звертаються до Секретаріату МЕА далі продовжувати роботу через Програму для підтримки потреб України у відбудові. Донори Програми висловлюють свою вдячність Секретаріату МЕА за продовження надання аналізу поточної енергетичної ситуації в Україні для обґрунтування міжнародних дій, визнають ключову роль, яку відіграє Програма співпраці МЕА−Україна в уможливленні такого аналізу, та консолідуючий вплив МЕА, який привертає увагу світової спільноти до потреб енергетичного сектору України.

У зв’язку з цим донори Програми звертають увагу на сучасні звіти МЕА «Енергетична безпека України та майбутня зима» [4] та «Розширення можливостей України через децентралізовану енергетичну систему» [5], в яких висвітлюються негайні дії, які Україна та її партнери можуть вживати для з’ясування нагальних вразливостей енергетичної безпеки країни та зміцнення довгострокової енергетичної резильєнтності. Ці звіти також викладають стратегічне бачення енергетичного майбутнього України, використовуючи інноваційні технології для розкриття нових можливостей, надаючи пріоритет енергетичній безпеці та самопідримуваному розвитку, зосереджуючись на

розподілених енергосистемах і підвищеній системній резильєнтності. Донори Програми закликають Секретаріат МЕА далі інтенсифікувати роботу з уможливлення інвестицій в енергетичний сектор України, які підтримуватимуть політику України, регуляторну стабільність, прозорість і належне корпоративне врядування, включаючи врядування державних підприємств, відповідно до стандартів ОЕСР та ЄС, щоб відповідати прагненням переходу до сучасної та резильєнтної енергосистеми, яка підтримує відновлення, енергетичну безпеку та довгострокову стійкість. Донори Програми підтвердили свою підтримку Програми співпраці МЕА−Україна та запросили інших членів МЕА надавати додаткове фінансування і приєднуватися до спільної заяви від 19 лютого 2026 р., а також висловили переконання, що Програма та її подальше розширення є взаємовигідними для всієї спільноти МЕА. Діалогом високого рівня було обговорення питань гарантування енергетичної безпеки епохи електроенергії (Age of Electricity) та інвестування в майбутню енергетичну безпеку України за участю першого віце-прем'єр-міністра та міністра енергетики України.

Звіт МЕА [4], підготовлений у жовтні 2025 р., передбачав нові загрози енергетичній безпеці України на зимовий період 2025−2026 рр. Новий аналіз МЕА надає практичні рекомендації щодо підтримки постраждалої енергетичної системи України в умовах зниження температури, висвітлюючи вразливості в умовах посилення атак РФ на енергетичну інфраструктуру за масштабністю та складністю. Звіт рекомендує ключові кроки для гарантування надійного доступу до електроенергії та опалення в умовах зниження температури. Аналіз містить оновлену інформацію про широкомасштабну війну в Європі, що впливає на енергетичну безпеку України, та пропонує дії, які Україна та її партнери можуть вживати негайно, щоб пом'якшувати ризики зимового періоду та зміцнювати довгострокову енергетичну резильєнтність. Звіт [4] базується на висновках візиту представників МЕА до м.Київ в жовтні 2025 р. та базується на попередній роботі МЕА з енергетичної безпеки України, опублікованій у вересні 2024 р. [6]. Запропоновані в новому аналізі дії включають: посилення фізичного захисту навколо енергетичної інфраструктури; поліпшення ланцюгів постачання обладнання для пришвидшення ремонтів; подальше збільшення децентралізованого енергопостачання країни; продовження оптимізації електромережевого з'єднання з Європою; вивчення методів розширення обсягів природного газу, що зберігається в Україні; диверсифікація імпорту газу; підготовка резервних варіантів (backup options) для зимового опалення.

Для кожної такої дії співпраця з партнерами України залишатиметься важливою. Україна приєдналася до спільноти МЕА як асоціаційована країна у 2022 р. після багаторічної співпраці з енергетичних питань. Рамки асоціації дозволяють МЕА тісно співпрацювати та поглиблювати співпрацю зі своїми країнами-партнерами, обмінюючись аналізом, даними, передовим досвідом. Попередня співпраця зосереджувалася на спільних пріоритетах, таких як реконструкція енергосистеми, енергетична безпека (зокрема шляхом ефективного використання децентралізованих енергетичних ресурсів), інтеграція технологій чистої енергії, доповнюючи діяльність в рамках програми

EU4Energy. Починаючи з 2007 р., МЕА здійснило декілька поглиблених оглядів політики й організувало заходи з питань політики та розбудови потенціалу в галузі енергетичних даних у м. Київ та м.Одеса. МЕА провело низку семінарів із зацікавленими сторонами енергетичної системи України, включаючи кілька семінарів у м.Київ. Ці заходи охоплювали такі теми, як резильєнтність енергосистеми, роль розподілених енергетичних ресурсів у підвищенні енергетичної безпеки, моделювання енергетики. МЕА тісно співпрацювало з Україною в рамках програми ЄК EU4Energy і в 2021 р. розробило дорожню карту, що вказує шляхи використання обмежень попиту на енергію [7]. EU4Energy – це регіонально орієнтована програма, яка зосереджена на шести країнах Східного партнерства ЄС. EU4Energy – це співпраця між МЕА, ЄС, цільовими країнами (Focus Countries) та іншими сторонами-виконавцями, розроблена для підтримки прагнень цільових країн щодо впровадження політики сталого розвитку енергетики та сприяння розвитку кооперативного енергетичного сектору на регіональному рівні.

Конкурентоспроможність передбачає широку міжнародну співпрацю.

1. Gorbachuk V., Shulzhenko S., Golovynskyi A. (2025). To computable decentralized heterogeneous energy market supply model. In Nexus of Sustainability. Understanding of FEWSE Systems II. A.Zagorodny, V.Bogdanov, A.Zaporozhets, T.Ermolieva (eds.). *Studies in Systems, Decision and Control (SSDC)*. 627. Cham, Switzerland: Springer, pp. 219–241.

2. Gaivoronski A., Gorbachuk V., Bardadym T., Dunaievskyi M. (2025). Digital transformations of modern energy sciences. 1st Workshop on Software Engineering and Semantic Technologies (SEST) 2025, co-located with the 15th International Scientific and Practical Programming Conference UkrPROG'2025 (May 13–14, 2025, Kyiv, Ukraine). *CEUR Workshop Proceedings*. 4053. A.Doroshenko, N.Kussul (eds.), pp. 61–71.

3. Gorbachuk V., Dunaievskyi M., Suleimanov S.-B. (2025). Cybersecurity investments in networks. In A.A. Gaivoronski, P.S. Knopov, V.I. Norkin, V.A. Zaslavskyi (eds.), *Stochastic Modeling and Optimization Methods for Critical Infrastructure Protection, Volume 2: Methods and Tools* (pp. 211−234). Wiley-ISTE.

4. Vatman, T., Gebhardt, T., Hesseling, D., Molnar, G., Warichet, J., Valentini, O. (2025). *Ukraine's Energy Security: A pre-winter assessment*. Paris, France: IEA, 13 p.

5. Hart, C., Vatman, T., Hevia-Koch, P., Al-Saffar A., Gebhardt, T., van Dedem, F., Valentini, O., Fennelly, F. (2024). *Empowering Ukraine Through a Decentralised Electricity System: A roadmap for Ukraine's increased use of distributed energy resources towards 2030*. Paris, France: IEA, 87 p.

6. Gould, T., Hart, C., Hesseling, D., Losz, A., Molnar, G., Vatman, T., Warichet, J. (2024). *Ukraine's Energy Security and the Coming Winter: An energy action plan for Ukraine and its partners*. Paris, France: IEA, 39 p.

7. Cooke, D., Vatman, T., Fager-Pintilä, M. (2021). *Harnessing Energy Demand Restraint in Ukraine: A Roadmap*. Paris, France: EU; IEA, 78 p.

Т.О. Бардадим, С.П. Осипенко

ОКРЕМІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ПРИ ДЕЦЕНТРАЛІЗАЦІЇ

Сучасне суспільство характеризується надзвичайно інтенсивною взаємодією різних потоків: міграційних, товарних, енергетичних, фінансових, інформаційних тощо. Забезпечення стійкості функціонування цих потоків є одним з головних пріоритетів незалежно від факторів, що загрожують їх нормальній взаємодії. Серед цих факторів можуть бути стихійні лиха, помилки персоналу, зловмисні дії кіберзлочинців, воєнні дії, пандемії…

Залишається вияснити, чи сприяє децентралізація забезпеченню цієї стійкості, як знайти потрібний ступінь децентралізації, які фактори впливу слід враховувати.

Так склалося, що питання децентралізації останнім часом привертали увагу переважно у зв'язку з масовим впровадженням відновлювальних джерел енергопостачання. Це торкнулося і технічних засобів організації безперебійного функціонування мереж [1], і вивчення економічних питань, пов'язаних з плануванням і проектуванням мереж розподіленої генерації [2], і кіберстійкості [3–5] і багатьох інших аспектів.

Питання, які безпосередньо стосувалися ключових уроків енергетичної стійкості України, обговорювалося на зустрічі експертів, організованої Dixi Group [6]. У підготовленому аналітичному документі [7] підсумовані напрями, що можуть забезпечити перехід від вимушеної адаптації до запроектованої стійкості. Втім, проблематика є дуже широкою, і конкретні рекомендовані напередодні вказаної події першочергові проєкти для впровадження в рамках муніципальних енергетичних планів, стосувалися лише енергозбереження [8]. Дійсно, це найперші необхідні заходи при вимушеній адаптації. Для переходу до запроектованої стійкості серед планових заходів можна згадати такі.

Визначення горизонту планування. Ця величина буде суттєво відрізнятися у ситуаціях термінового короткострокового забезпечення електроенергією, проміжних середньострокових інженерних рішень та довгострокових перспективних проектів. Відповідно буде різною і вартість подібних проектів. У короткостроковому варіанті за нагальної потреби вартість може суттєво перевищувати середньо- чи довгострокові варіанти. Наприклад, так бувало при імпорті електроенергії Україною у аварійних випадках з Польщі, Румунії, Словаччини, Угорщини, Молдови, що дозволяло пом'якшити наслідки руйнувань критичної енергетичної інфраструктури.

Визначення просторової оцінки і відповідної оцінки вартості проекту, який може стосуватися окремого домогосподарства, населеного пункту, громади, області тощо.

Вибір технічних засобів з урахуванням існуючої інфраструктури та *забезпечення інформаційної підтримки* розподіленої генерації. Дійсно, для забезпечення нормальної роботи енергетичної інфраструктури при децентралізації особливого значення набувають технічно-інформаційні рішення, що дозволяють

забезпечити балансування мереж навіть за несприятливих умов для роботи відновлювальних джерел за рахунок гнучкого регулювання попиту і пропозиції. Вихід з ладу засобів інформаційної підтримки може привести до критичних наслідків для власне енергетичної інфраструктури. І навпаки, раптове виведення з ладу генеруючих потужностей чи мереж може заблокувати роботу інформаційної критичної інфраструктури. Тому забезпечення стійкості для цих двох складових потрібно розглядати разом. Як вказується у праці [5], питання взаємовпливу технічної та інформаційної складових тільки починає турбувати суспільство: «Досліджувана проблематика є відносно новою … як в контексті наукових досліджень, так і в рамках інженерних рекомендацій щодо практичних засобів протидії». При цьому спроби моделювання потенційних наслідків руйнівних атак стримуються відсутністю доступних статистичних даних щодо впливу масових відключень електропостачання.

Підсумовуючи, зазначимо, що децентралізація, дійсно, може підвищувати стійкість енергосистем, але це передбачає суттєве збільшення генеруючих блоків та вищі вимоги до координації в мережі, до безпеки центрів обробки даних, засобів комунікації, а крім того – урахування можливого розташування спеціалізованих систем (наприклад, радарних), що можуть впливати на працездатність цивільної інфраструктури та навпаки.

1. Sun, Y., Hou, X., Lu, J., Liu, Z., Su, M., & Guerrero, J. (2022). Overview of Microgrid. In: Series-Parallel Converter-Based Microgrids. Power Systems. (pp. 1-28). Springer, Cham. https://doi.org/10.1007/978-3-030-91511-7_1.
2. UNECE (2025). Understanding the Full System Costs of the Electricity System. 114 p. Available at: https://unece.org/sites/default/files/2025-12/Understanding%20FSCOES%20Report%20-%20Quantified%20Carbon.pdf (дата звернення: 14.03.2026).
3. UNECE (2023). Digitalization in Energy: Case Study on "Cyber Resilience of Critical Energy Infrastructure". Available at: https://unece.org/info/Sustainable-Energy/pub/387073 (дата звернення: 14.03.2026).
4. UNECE (2023). Key considerations and solutions to ensure cyber resiliency in the smart integrated energy systems. Available at: https://unece.org/sites/default/files/2023-08/ECE_ENERGY_GE.6_2023_3_ECE_ENERGY_GE.5_2023_3_EN_0.pdf (дата звернення: 14.03.2026).
5. Drahuntsov, R., & Zubok, V. (2023). Modeling of Cyber Threats Related To Massive Power Outages and Summary of Potential Countermeasures. Èlektronnoe modelirovanie, 45(3), 116–128. https://doi.org/10.15407/emodel.45.03.116.
6. Розподілена генерація, стійкі мережі та інтеграція з Європою: ключові уроки енергетичної стійкості України під час війни. DiXi Group. Kyiv. 12.03.2026. URL: https://dixigroup.org/rozpodilena-generacziya-stijki-merezhi-ta-integracziya-z-%d1%94vropoyu-klyuchovi-uroki-energetichno%d1%97-stijkosti-ukra%d1%97ni-pid-chas-vijni/ (дата звернення: 14.03.2026).
7. Holding the Grid: Ukraine's Energy Resilience Playbook. DiXi Group. Kyiv. 12.03.2026. URL: https://dixigroup.org/en/pdf-en/?pdf=https://dixigroup.org/wp-content/uploads/2026/03/dixi-ukraines-energy-resilience-playbook.pdf (дата звернення: 14.03.2026).
8. DiXi Group. Аналітика. 2026. Рекомендовані першочергові проєкти для впровадження в рамках муніципальних енергетичних планів. DiXi Group. Kyiv. 09.03.2026. URL: https://dixigroup.org/analytic/rekomendovani-pershochergovi-proekti-dlya-vprovadzhennya-v-ramkah-municzipalnih-energetichnih-planiv/ (дата звернення: 14.03.2026).

Є.В. Котух

СИСТЕМА КІБЕР-КІНЕТИЧНОГО ЗАХИСТУ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Енергетична інфраструктура України зазнає безпрецедентного тиску внаслідок систематичних комбінованих кібер-кінетичних атак, що поєднують ракетно-дронові удари з кібернападами на системи управління. За даними CERT-UA, група APT44 (Sandworm) протягом 2024–2025 років здійснила цілеспрямовані атаки на понад 20 енергетичних об'єктів у 10 регіонах, синхронізуючи кіберінтрузії з кінетичними ударами. Загальна генеруюча потужність скоротилася з 37 ГВт (включаючи великі АЕС, ТЕС та ГЕС) довоєнного рівня до менш ніж 12 ГВт, а Президент України 14 січня 2026 року оголосив надзвичайний стан в енергетиці. За оцінками Світового банку, збитки перевищили 20 млрд дол. США.

Формується нова парадигма загроз - кібер-кінетична конвергенція, за якої противник використовує кіберзброю для розвідки наслідків кінетичних ударів, маніпуляції SCADA/ICS для ускладнення відновлення та координації часу кібератак із фізичними ударами. Шкідливе ПЗ Industroyer/Industroyer2 стало першим у світі прикладом автономного зловмисного коду, здатного взаємодіяти з обладнанням підстанцій через протоколи IEC 60870-5-104 та IEC 61850. За звітом Держспецзв'язку в 2025 році зловмисники почали активно застосовувати ШІ для генерації фішингових повідомлень та створення шкідливого коду.

Мета роботи полягає у розробці концептуальної архітектури інтелектуальної системи кібер-кінетичного захисту, що інтегрує методи ШІ для виявлення аномалій, прогнозування комбінованих атак та автоматизованого реагування в умовах одночасного кібернетичного та кінетичного впливу.

Така система має базуватися на трирівневій архітектурі: рівень злиття даних (Data Fusion Layer), рівень інтелектуального аналізу (AI Analysis Layer) та рівень автоматизованого реагування (Automated Response Layer). На першому рівні інтегруються гетерогенні джерела: телеметрія SCADA (напруга, частота, потужність, стан комутаційних апаратів), мережевий трафік промислових протоколів (DNP3, IEC 60870-5-104, Modbus TCP), дані систем фізичної безпеки (сейсмічні датчики, радари БПЛА) та OSINT. Критичним елементом є синхронізація часових міток між кібернетичними та фізичними сенсорами для ідентифікації кореляцій між кібернападами та кінетичними ударами.

На першому рівні інтелектуального аналізу застосовуються моделі глибокого навчання. Мережі LSTM аналізують часові ряди телеметрії SCADA для виявлення атак False Data Injection (FDI), що маскують реальний стан мережі. Фреймворк на базі LSTM та Random Forest досягає точності 99,8% при бінарній класифікації аномалій. Згорткові нейронні мережі (CNN)

класифікують просторові патерни трафіку для виявлення латерального руху зловмисника. Потенційно, може бути використана модель DeepFM, апробована на наборі даних Sherlock (2025), демонструє F1-score 0,955 для виявлення процесних аномалій у середовищах SCADA.

Інноваційним компонентом є модуль кібер-кінетичної кореляції, який використовує графові нейронні мережі (GNN) для моделювання взаємозалежностей між компонентами енергосистеми та застосовує ансамблеві методи для виявлення патернів комбінованих атак. Модуль аналізує часову кореляцію між кібернападами на SCADA та фізичними ударами по підстанціях, виявляючи стратегію противника, наприклад, використання кіберрозвідки для оцінки наслідків кінетичних ударів та планування повторних атак.

Третій рівень забезпечує автоматизоване реагування на основі навчання з підкріпленням (Reinforcement Learning). AI-агент оптимізує стратегію захисту в реальному часі, автоматично ізолюючи скомпрометовані сегменти, переводячи SCADA в безпечний режим з аналоговим резервуванням та ініціюючи протоколи розподіленого управління мікрогридами.

Окремим аспектом є захищеність каналів зв'язку між компонентами системи. В умовах розвитку квантових обчислень пропонується використання постквантових стандартів NIST FIPS 203 та FIPS 204 для захисту каналів передачі даних між підстанціями та центрами управління.

Досвід захисту української енергетичної інфраструктури демонструє: резильєнтність вимагає гібридних архітектур, де цифрові інновації поєднуються з аналоговою надмірністю та сегментованим управлінням. Ключовим уроком є не відмова від модернізації, а відмова від виключно цифрової модернізації. Запропонований підхід може бути адаптований до специфічних умов: обмежена пропускна здатність каналів, гетерогенність обладнання, функціонування в умовах часткового руйнування інфраструктури та дефіцит кваліфікованого персоналу. Подальші дослідження спрямовані на федеративне навчання (Federated Learning) для обміну моделями без передачі конфіденційних даних, створення цифрових двійників критичних підстанцій та розробку спеціалізованих наборів даних кібер-кінетичних атак на основі реального досвіду українських енергооператорів.

1. CERT-UA. Кіберактивність групи UAC-0002 (Sandworm/APT44) щодо енергетичних об'єктів України. Звіт CERT-UA, 2024.

2. Salazar L. et al. Industroyer and Industroyer2: How Malware Attacks Power Grids. *IEEE S&P*, 2024.

3. V. M. V. et al. AI-driven cybersecurity framework for anomaly detection in power systems. *Scientific Reports*, 15, 35506, 2025.

4. DeepFM-based intrusion detection for SCADA systems. *Scientific Reports*, 2025.

5. NIST FIPS 203: ML-KEM Standard. NIST, 2024.
6. Atlantic Council. Ukraine's wartime experience provides blueprint for infrastructure protection. Dec. 2025.
7. WEF. Global Cybersecurity Outlook 2026. Jan. 2026.
8. Khalimov, G., & Kotukh, Y. (2026). *LINEture: Novel signature cryptosystem.* arXiv preprint arXiv:2601.07071. https://arxiv.org/abs/2601.07071.
9. Kotukh, Y., & Khalimov, G. (2026). *Security parameter analysis of the LINEture post-quantum digital signature scheme*. arXiv preprint arXiv:2601.03465. https://arxiv.org/abs/2601.03465.
10. Kotukh, Y. (2025). Quantum-resistant cryptography for protecting critical infrastructure from cyber threats. In *Матеріали III науково-практичної конференції «Резильєнтність динамічних систем»* (Vol. 1, Issue 1, pp. 85–88).

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

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНКИ ПОЖЕЖНОЇ НЕБЕЗПЕКИ НАГРІВУ ПРОВОДІВ ЗІ СТАЛЕВИМИ СТРУМОВІДНИМИ ЖИЛАМИ

Масовані удари по об’єктах критичної інфраструктури, енергетичній і цивільній інфраструктурі України різними типами ракет та безпілотних літальних апаратів знищують і руйнують генерацію та мережі. Виникає необхідність у швидкому відновленні складових об’єктів та систем з мінімальними витратами при дотриманні встановлених протипожежних вимог. Централізовані системи обігріву та опалення об’єктів замінюються або доповнюються локальними системами, де часто застосовуються проводи зі сталевими струмовідними жилами (сталеві проводи).

Пожежна небезпека проводів зі сталевими струмовідними жилами обумовлена їх високим питомим опором, що призводить до сильного нагріву (у 10 разів вище міді) при високих струмах. Сталь інтенсивно нагрівається, спричиняючи руйнування ізоляції та займання, особливо у місцях перевантаження або високих перехідних опорів.

До основних факторів пожежної небезпеки можливо віднести наступні:

– високе виділення тепла – завдяки значному електричному опору сталі;

– руйнування ізоляції – нагрів призводить до плавлення або обвуглювання ізоляції проводу, що може викликати коротке замикання;

– перевантаження – сталеві проводи непридатні для великих навантажень та швидко перегріваються;

– небезпека у з'єднаннях – високий перехідний опір у місцях контактів проводу підвищує ризик займання.

Таким чином, розробка математичної моделі оцінки пожежної небезпеки нагріву проводів зі сталевими струмовідними жилами є актуальною науковою задачею.

У доповіді зазначено, що температура нагріву сталевих проводів визначається як параметрами матеріалу провідника (провідністю, щільністю, теплоємністю, перерізом), так і параметрами ізоляційного матеріалу (густиною, теплоємністю, товщиною шару).

Суттєве зростання температури нагріву сталевих проводів у процесі експлуатації може супроводжуватися: розм'якшенням або розплавленням струмовідної жили; розм'якшенням та загорянням ізоляції проводу та руйнацією контактів та іншими пошкодження електричного обладнання.

При цьому, для оцінювання пожежної небезпеки проводів на основі визначення їх температури нагріву необхідно враховувати як їх параметри безпосередньо, так і умови експлуатації. У свою чергу, умови експлуатації

обумовлені призначенням кабельних виробів, при цьому слід зауважити, що основним призначенням проводів зі сталевими струмовідними жилами є не тільки передача електричної енергії, але й обігрів об'єктів промисловості. Дані напрямки використання сталевих проводів є досить важливими для відповідних галузей.

Запропоновано математичну модель оцінки пожежної небезпеки нагріву проводів зі сталевими струмовідними жилами на основі критерію тепловиділення. Модель дозволяє визначити часові інтервали при оцінки пожежної небезпеки проводів та розраховувати температуру нагріву проводів у визначені моменти часу при різних значеннях струму навантаження.

Представлено результати розрахунків, що отримані при використанні програмного математичного пакету MAHTCAD. Наведено відповідні графіки зростання температури нагріву з часом для одножильних проводів зі сталевою струмовідною жилою при обраних значеннях струму навантаження.

Таким чином, за запропонованою математичною моделлю можливо оцінити пожежну небезпеку нагріву одножильного сталевого проводу з полівінілхлоридною одношаровою ізоляцією на основі критерію тепловиділення.

1. Катунін А.М., Коломійцев О.В., Д'яков А.В., Кожушко М.І. Оцінювання впливу домішок марганцю в мідних жилах проводів на температуру їх нагріву в процесі експлуатації *Collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical Conference, June 21, 2024. Coventry, United Kingdom: International Center of Scientific Researchє* – 2024. – pp. 52-56. https://doi.org/10.36074/scientia-21.06.2024.

2. Катунін А.М., Коломійцев О.В., Зарічняк Є.М., Мусаїрова Ю.Д., Куравський М.В., Челак В.В. Оцінювання температури нагріву навантаженого алюмінієвого проводу із домішками хрому в матеріалі жили. *Sectoral research XXI: characteristics and features: collection of scientific papers «SCIENTIA» with Proceedings of the IX International Scientific and Theoretical Conference*, December 20, 2024. Chicago, USA: International Center of Scientific Research. – pp. 73-78. https://doi.org/10.36074/scientia-20.12.2024.

3. Катунін, А., Коломійцев, О., Кулаков, О., Панченко, В., Олійник, Р. і Кожушко, М. (2025). Модель оцінки впливу хімічного складу струмовідних жил на експлуатаційні характеристики ізольованого електричного проводу. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, (3(25), С. 109-117. https://doi.org/10.37701/dndivsovt.25.2025.14.

4. Катунін А.М., Коломійцев О.В., Д'яков А.В., Зарічняк Д.І., Роянов О.М., Богатов О.І., Сметана Є.А., Зарічняк Є.М., Маляренко О.С., Артюнов С.В., Семенченко С.В. Оцінювання пожежної небезпеки алюмінієвих проводів із полівінілхлоридною та поліетиленовою ізоляцією для зразків автобронетанкової техніки. *ГРААЛЬ НАУКИ*: *міжнар. наук. журнал*. – Вінниця : ГО «Європейська наукова платформа»; НУ «Інститут науково-технічної інтеграції та співпраці», 2025. – No 53. – С. 492-500. https://doi.org/10.36074/grail-of-science.20.06.2025.

О.В. Коломійцев, В.В. Пустоваров, Ю.В. Бреславец

МОДЕЛЬ АНАЛІЗУ ДАНИХ ПРО ПОКАЗНИКИ ЕЛЕКТРОЕНЕРГІЇ З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Для запобігання нештатним ситуаціям, аваріям обладнання та простоям у виробництві необхідний постійний моніторинг якості електроенергії. Він забезпечує виявлення відхилень напруги, частоти тощо, що дозволяє вчасно вжити заходів безпеки та підвищити надійність енергопостачання як для промисловості, так і населення. До основних переваг постійного моніторингу якості електроенергії можливо віднести наступні:

– запобігання аваріям – раннє виявлення відхилень (просадки, сплески напруги тощо), що допомагає уникнути виходу з ладу чутливого обладнання;

– безперервність процесів – моніторинг допомагає уникнути нештатних зупинок виробництва та котелень;

– оцінка мережи – дозволяє оцінити якість технічного обслуговування електричних мереж та вжити заходів для їх покращення;

– оптимізація – допомагає аналізувати баланс виробництва-споживання та покривати максимальні навантаження.

Постійний моніторинг якості електроенергії дозволяє у реальному масштабі часу отримувати дані про напругу, струм та частоту, забезпечуючи виявлення відхилень, запобігання аварійним ситуаціям та оптимізацію роботи мереж. Моніторинг гарантує контроль за станом електричної системи, виявляє перевитрати енергії, технічні несправності та покращує енергоефективність, переходячи від реактивного до проактивного управління. Крім того, безперервний моніторинговий аналіз дозволяє дослідникам отримати знання про явища якості електроенергії.

Вимірювання якості електроенергії дають велику кількість даних. Дані про якість електроенергії можливо віднести до великих даних не лише за їх об’ємом, а й за іншими складнощами: швидкість, різноманітність та надійність. Ручний аналіз даних про якість електроенергії можливий, але трудомісткий. Крім того, звіти про дані, засновані на стандартизованих індексах та класичних статистичних методах, можуть приховати важливу інформацію про змінну у часі поведінку при вимірюванні якості електроенергії.

На даний час штучний інтелект, у рамках відповідних інформаційних технологій, зокрема з використанням методів та моделей машинного навчання, відіграє провідну роль у наданні автоматичних інструментів для належного аналізу великих даних про якість електроенергії.

Таким чином, розробка моделі аналізу даних про показники електроенергії з використанням алгоритмів машинного навчання є актуальною науковою задачею.

У доповіді проведено аналіз відомих моделей оцінки температури нагріву навантажених проводів, а також підходів щодо інтелектуального аналізу даних якості електроенергії (PQ) для цифровізації енергосистем та формування великих масивів вимірювальної інформації (PQ Big Data). Здійснено систематизацію відомих (класичних) та сучасних методів, визначення їх сильних та слабких сторін для потокових PQ-даних. Огляд класів методів інтелектуального аналізу показує доцільність поєднання базових стандартних індикаторів із методами без вчителя, самонавчанням та інтерпретованими моделями, здатними працювати за неповної розмітки, витримувати дрейф режимів та надавати пояснювані висновки для інженерного застосування.

Обґрунтовано вимоги до моделей, які використовуються в умовах реального часу, неповних спостережень, шумів вимірювання та дрейфу режимів. Нормативно-метрологічні вимоги визначають показники, часові вікна та правила агрегації, а коректна організація даних і метаданих (синхронізація часу, паспорт записів, версіонування, маски якості) є передумовою відтворюваності експериментів і достовірної валідації аналітичних результатів.

Представлено розроблену модель аналізу даних про показники електроенергії з використанням алгоритмів машинного навчання та удосконалену архітектуру глибинного автоенкодера для некерованого вилучення ознак PQ-даних. Показано, що автоенкодер здатний скоротити розмірність вхідних даних до компактного вектору основних ознак, зберігаючи при цьому інформацію про характерні варіації сигналу. Приведено аналітичні вирази для проведення розрахунків.

За результатами машинного моделювання досягнуто малої похибки реконструкції, що підтверджує адекватність вибраної архітектури та параметрів навчання.

1. Катунін А.М., Коломійцев О.В., Зарічняк Є.М., Мусаїрова Ю.Д., Куравський М.В., Челак В.В. Оцінювання температури нагріву навантаженого алюмінієвого проводу із домішками хрому в матеріалі жили. *Sectoral research XXI: characteristics and features: collection of scientific papers «SCIENTIA» with Proceedings of the IX International Scientific and Theoretical Conference*, December 20, 2024. Chicago, USA: International Center of Scientific Research. – pp. 73-78. https://doi.org/10.36074/scientia-20.12.2024.

2. Катунін, А., Коломійцев, О., Кулаков, О., Панченко, В., Олійник, Р. і Кожушко, М. (2025). Модель оцінки впливу хімічного складу струмовідних жил на експлуатаційні характеристики ізольованого електричного проводу. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*, (3(25), С. 109-117. https://doi.org/10.37701/dndivsovt.25.2025.14.

Ю.А. Гусак, С.В. Базарний

МЕТОД ОПТИМАЛЬНОГО УПРАВЛІННЯ СТІЙКІСТЮ ДЕРЖАВНОЇ СИСТЕМИ ЯК СКЛАДНОГО ДИНАМІЧНОГО ОБ'ЄКТА В БАГАТОДОМЕННОМУ ПРОСТОРІ

Сучасна еволюція збройних конфліктів характеризується радикальним переходом від лінійних форм боротьби до інтегрованого багатодоменного протистояння. Характерною ознакою новітніх форм воєнного протистояння, особливо в контексті широкомасштабної збройної агресії рф проти України, є системне використання мультивекторного впливу, що охоплює: фізичний, інформаційний, кібернетичний, когнітивний домени. У цих умовах інформаційний домен набуває статусу системоутворювального, який безпосередньо впливає на стійкість державного управління та здатність сектору безпеки і оборони до виконання завдань за призначенням. Управління державою у таких умовах має розглядатися як складна динамічна, але керована система, динаміка якої визначається нелінійними міждоменними взаємодіями.

В концепції багатодоменних операцій (Multi-Domain Operations, далі – MDO) [2], яка відображена у стратегіях НАТО та США, наголошується на синхронізованому застосуванні засобів впливу в усіх доменах задля досягнення оперативної переваги над противником. В Україні напрямок еволюції воєнного розуміння закріплено у низці документів: Стратегія воєнної безпеки України [1] та ін., які визначають фізичний, кібернетичний та інформаційний компоненти як критичні домени оборони держави.

Попри те, що Україна перебуває в умовах інтенсивного багатодоменного протистояння, науковий та методичний інструментарій управління такими операціями залишається недостатньо дослідженим. Основна проблема полягає у невідповідності між практичним досвідом бойових дій та наявною теоретико-методологічною базою. На сьогодні в Україні бракує теоретичних механізмів ідентифікації критичних фаз міждоменної дестабілізації, які призводять до втрати керованості у складних інформаційних та когнітивних просторах. Відсутній єдиний нормативний документ для системної формалізації усіх доменів за логікою MDO, що змушує використовувати фрагментарні концепції з різних сфер безпеки. Наявні аналітичні підходи мають переважно описовий характер, який не визначає математично обґрунтований апарат для оптимального управління та прогнозування системного колапсу на стратегічному рівні. Недостатньо досліджена нелінійна динаміка взаємодії доменів не дозволяє кількісно оцінити синергетичний ефект від одночасного впливу у фізичному, кібернетичному та когнітивному просторах. Відсутність інтегрованих математичних моделей ускладнює проектування ефективних систем підтримки прийняття рішень (DSS), для забезпечення стійкого функціонування держави в умовах інформаційного перенасичення та високої адаптивності противника.

Метою цієї роботи є розроблення методу оптимального управління функціональною стійкістю державної системи, який базується на векторно-матричній формалізації нелінійної динаміки доменів. Це дозволить перейти від реактивного реагування до проактивного керування в межах динамічного протистояння. Наукове завдання полягає у побудові інтегрованої математичної моделі, що поєднує підходи військової аналітики, когнітивного моделювання та прикладної математики для ідентифікації моментів переходу системи зі стабільного режиму у стан управлінського колапсу через аналіз фазових переходів.

Розроблення методу базується на формалізації державної системи як складної динамічної керованої системи, стан якої в кожний момент часу детермінується нелінійною взаємодією внутрішніх параметрів доменів, інтенсивністю зовнішніх дестабілізаційних впливів противника та вектором відновлювальних управлінських дій [4]. Логічність методу передбачає перехід від спостереження за окремими вимірами до цілісної формалізації, що дозволяє описувати стан усієї державної інфраструктури як єдину точку у багатовимірному фазовому просторі. У межах математичної моделі стійкість управління розглядається як здатність системи утримувати свою фазову траєкторію в межах заданої області допустимих відхилень «коридору стійкості», попри синергетичний тиск багатодоменних впливів.

Метод формалізує міждоменні каскадні ефекти через матрицю інтенсивності впливу (реактивності), де зміна стану в одному домені (кібернетичному, інформаційному, тощо) [3] спричиняє нелінійну деградацію в інших, що є важливим для ідентифікації точок втрати керованості. Особливу роль відіграє вектор когнітивного проникнення, який виступає модулятором амплітуди впливу, що кількісно оцінює здатність системи до інформаційних та психологічних операцій, що за певних умов призводить до фази когнітивного резонансу та системного збою при ухваленні рішень. Математичний опис цих параметрів забезпечує можливість оцінювання синергетичного ефекту, за якого сумарна дестабілізація перевищує арифметичну суму окремих впливів у різних доменах.

Розроблення методу потребує переосмислення самої природи державного управління в сучасній війні. Система управління держави не має розглядатися як сукупність автономних секторів або інституцій, що функціонують ізольовано один від одного. У багатодоменному протистоянні вона виступає як адаптивна система, де будь-яка зміна в одному домені здатна ініціювати нелінійні перетворення в інших. Саме тому управління стійкістю набуває системного характеру і має ґрунтуватися на цілісному розумінні взаємозалежностей між доменами.

У цьому контексті функціональна стійкість трактується як динамічна властивість системи підтримувати керованість, структурну цілісність та стратегічну спрямованість в умовах постійного тиску (впливу). Вона визначається здатністю державних інституцій зберігати логіку ухвалення

рішень, координацію між рівнями управління та довіру суспільства навіть за умов синхронізованих інформаційних, кібернетичних і фізичних впливів.

Багатодоменний простір характеризується високою швидкістю змін, асиметричністю загроз та наявністю когнітивних ефектів, які можуть значно перевищувати за масштабом фізичні наслідки бойових дій. Інформаційний домен у таких умовах виступає каталізатором або мультиплікатором впливу, здатним трансформувати локальні події в системні кризи. Саме тому метод оптимального управління має враховувати безпосередні матеріальні втрати, технічні збої, зміну поведінкових параметрів цільової аудиторії – як державних, так і суспільних.

Ключовим елементом запропонованого підходу є інтеграція стратегічного, операційного та когнітивного рівнів аналізу. Стратегічний рівень охоплює довгострокові цілі держави, її геополітичну позицію та ресурсний потенціал. Операційний рівень відображає поточну конфігурацію взаємодії доменів та ефективність механізмів координації. Когнітивний рівень включає сприйняття, мотивації та наративні структури, що визначають поведінку суб'єктів управління та населення. Взаємодія цих рівнів формує загальну динаміку системи, а їх дисбаланс може стати передумовою управлінського колапсу. Особливістю сучасних збройних конфліктів є поява каскадних ефектів, коли незначна подія в одному домені здатна ініціювати масштабну дестабілізацію в інших. Наприклад, локальна кібератака на об'єкти критичної інфраструктури може спричинити інформаційний резонанс, зниження довіри до органів влади та зміну поведінкових моделей населення. Такі ефекти не є лінійними і часто мають накопичувальний характер. Відтак метод управління має передбачати механізми раннього виявлення критичних точок, у яких система наближається до межі допустимих відхилень. Оптимальність системи управління у запропонованому методі означає досягнення балансу між інтенсивністю управлінського впливу та ресурсними обмеженнями. Надмірна централізація або реактивність можуть призвести до перевантаження системи й зниження її адаптивності. Водночас недостатність або запізнення корегуючих дій збільшує ризик переходу системи в режим нестійкості. Таким чином, оптимальне управління передбачає гнучке коригування управлінських стратегій та використання механізмів зворотного зв'язку.

Стійкість системи управління держави в багатодоменному просторі значною мірою залежить від здатності різних органів влади діяти в єдиній логіці та обмінюватися інформацією в режимі реального часу. Фрагментація управлінських процесів, дублювання функцій або конкуренція між відомствами знижують ефективність реагування та створюють додаткові вразливості. Отже, оптимальне управління має включати механізми синхронізації міждоменних зусиль та інтеграції аналітичних центрів у єдину систему підтримки прийняття рішень. У прикладному вимірі реалізація методу передбачає застосування цифрових інструментів (технологій) [5], здатних агрегувати дані з різних доменів, виявляти закономірності їх взаємодії та формувати прогностичні сценарії розвитку ситуації. Такі технології мають працювати як інтелектуальні

підсистеми, що підтримують керівника, зберігаючи за нею технічну можливість на ухвалення стратегічного рішення. Основою розробленого методу є впровадження інтегрального індикатора – коефіцієнта управлінського колапсу (далі – КУК), який кількісно оцінює ризик фазового переходу державної системи до стану некерованості. Фізичний зміст КУК полягає у функціональному зіставленні матриці допустимих ресурсних інтервалів управлінських рішень із вектором необхідних змін, зумовлених сумарною інтенсивністю багатодоменної дестабілізації.

Наукова новизна методу полягає у переході від дискретного оцінювання загроз до синтезу інваріантного управління, що досягається розв'язанням варіаційної задачі мінімізації функціонала ризику управлінського колапсу при дотриманні обмежень на ресурсну місткість компенсаційних дій. Запропонований математичний апарат (модель) здійснює динамічний перерозподіл пріоритетів між фізичною обороною, кіберзахистом та когнітивними заходами залежно від поточної фазової швидкості деградації системи, що забезпечує максимізацію загальної життєздатності держави в умовах асиметричного конфлікту.

Отже, метод оптимального управління стійкістю державної системи в умовах багатодоменних операцій ґрунтується на системному баченні взаємозалежностей, динамічному трактуванні стійкості, інтеграції різнорівневого аналізу та впровадженні механізмів адаптивного коригування. Його застосування створює передумови для переходу від фрагментарного реагування на окремі загрози до цілісного стратегічного управління складною динамічною системою в умовах гібридної війни високої інтенсивності.

1. Про Стратегію воєнної безпеки України : Указ Президента України від 25 березня 2021 р. № 121/2021. – Чинний з 2021–03–25. https://zakon.rada.gov.ua/laws/show/121/2021.

2. Multi-Domain Operations: The Evolution of Combined Arms / Army University Press. – 2022. – (Military Review). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2022/MDO/.

3. Multi-Domain Operations : Allied Command Transformation Concepts / NATO ACT. – 2024. – URL: https://www.act.nato.int/activities/multi-domain-operations/.

4. Complexity and Resilience in Multi-Domain Operations / NATO Science and Technology Organization. – 2023. – (STO-MP-SAS-161). https://www.sto.nato.int/publications/STOPublications/STOPubsDefault.aspx.

5. Mathematical model of multi-domain interaction based on game theory / S. Bazarnyi, Y. Husak, T. Voitko, F. Aliew, S. Yevseiev // Advanced Information Systems (Сучасні інформаційні системи). – 2025. – Т. 9, № 3. – С. 22–31. https://doi.org/10.20998/2522-9052.2025.3.03.

Є.О. Сенюк, В.Е. Мельничук

ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ ШІ У ЯКОСТІ БАЛАНСУВАЛЬНИКА НАВАНТАЖЕННЯ У ЕЛЕКТРОМЕРЕЖІ

Ключові слова: штучний інтелект, балансування навантаження, економічна доцільність, енергосистема, оптимізація, енергозбереження.

Вступ. Сучасні електромережі стикаються з підвищеною невизначеністю через зростання частки відновлюваних джерел енергії, розподіленої генерації та варіативності споживчого попиту. Традиційні методи балансування (механічні регулятори, статичні алгоритми) часто не забезпечують достатньої гнучкості та передбачуваності. Інтелектуальні системи на основі машинного навчання та алгоритмів прогнозування можуть підвищити якість управління мережею, зменшити втрати та оптимізувати використання ресурсів.

Методологія оцінки. Для оцінювання економічної доцільності запропоновано комбінований підхід: аналіз капітальних витрат (CAPEX), операційних витрат (OPEX), потенційного зниження втрат електроенергії та скорочення санкцій за небаланси. Основні елементи моделі: 1) інвестиції в апаратне та програмне забезпечення; 2) вартість інтеграції та навчання моделей; 3) економія від зниження пік-навантажень і втрат; 4) додаткова вартість підвищення надійності (зниження частоти аварій). Розрахунки виконуються у вигляді простих дисконтованих грошових потоків (NPV), термін окупності (Payback) та внутрішня норма рентабельності (IRR) [1].

Формалізація вигод. Нехай ΔC_oper — річне скорочення операційних витрат завдяки впровадженню ШІ, ΔL — річне зменшення втрат у МВт·год, p — середня ціна електроенергії (грн/МВт·год), I — початкові інвестиції. Тоді річна економія S і чиста приведена вартість (NPV) за період T обчислюються приблизно як:

$$S = \Delta C_{oper} + p \cdot \Delta L \quad (1)$$

$$NPV = -I + \sum_{t=1}^{T} \frac{S_t}{(1+r)^t} \quad (2)$$

де S — річна економія (грн/рік), ΔC_{oper} — скорочення OPEX (грн/рік), ΔL — скорочення втрат (МВт·год/рік), p — середня ціна електроенергії (грн/МВт·год), I — інвестиції (грн), r — ставка дисконту, T — період аналізу (роки) [2].

Приклад спрощеного розрахунку. Розглянемо умовну підстанцію з річними втратами 500 МВт·год і середньою ціною 2000 грн/МВт·год. При впровадженні ШІ досягається зниження втрат на 5% та скорочення операційних витрат на 200 000 грн/рік. Інвестиції в систему становлять 1 200 000 грн, ставка дисконту 8%, період аналізу 7 років. Тоді ΔL = 25 МВт·год, $p \cdot \Delta L = 25 \cdot 2000 = 50\,000$ грн/рік; $S = 50\,000 + 200\,000 = 250\,000$ грн/рік. NPV обчислюється класично за формулою (2).

Таблиця з результатами (приклад).

Таблиця 1. Результати спрощеного розрахунку економічної доцільності

Показник	Вхідні дані	Результат (рік)
Річні втрати (МВт·год)	500	
Зменшення втрат (%)	5%	25 МВт·год
Економія від зниження втрат (грн)	—	50 000
Скорочення OPEX (грн/рік)	—	200 000
Річна загальна економія S (грн)	—	250 000

Аналіз ризиків та чутливості. Основні ризики: похибка прогнозів, витрати на підтримку моделей, ризики кібербезпеки та регуляторні обмеження. Важливо проводити аналіз чутливості NPV по параметрам ΔL, ΔC_{oper} і r. Для прийняття рішення рекомендовано сценарний підхід: песимістичний, базовий та оптимістичний сценарії з відповідними значеннями S і ймовірностями їх настання [3].

Соціально-економічний вплив. Використання ШІ для балансування дозволяє підвищити ефективність використання існуючих мережевих ресурсів, відкласти капітальні інвестиції у нові потужності та зменшити викиди CO_2 завдяки зниженню непотрібного виробництва. Також можливий вплив на зайнятість через автоматизацію рутинних операцій — це вимагає перепідготовки персоналу [4].

Висновки. 1) Технічно та економічно доцільне впровадження ШІ-рішень для балансування навантаження у випадку достатнього обсягу можливих енергозбережень та доступних даних для якісного навчання моделей. 2) Рекомендується проводити попередні пілотні проєкти з вимірюванням ΔL і ΔC_{oper} протягом 6–12 місяців для уточнення економічної моделі. 3) Необхідна увага до кібербезпеки та регуляторної відповідності.

1. Brown, T., & Smith, J. (2020). Artificial Intelligence for Power Grid Management. Energy Policy, 145, 111-123.

2. Ivanchenko, I., Petrenko, P. (2019). Optimization of Load Balancing in Distribution Networks. Proceedings of the Ukrainian Energy Conference.

3. DSTU 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.

4. Khan, S., & Lee, J. (2020). Machine Learning Approaches for ESG Risk Assessment. Sustainability Analytics, 8(2), 101–119.

К.Ю. Бровко, О.В. Великогорський, Д.Р. Подопригора

МЕТОДОЛОГІЧНІ ЗАСАДИ СТВОРЕННЯ ЦИФРОВИХ ДВІЙНИКІВ ЕНЕРГЕТИЧНИХ СИСТЕМ З АДАПТИВНОЮ ІДЕНТИФІКАЦІЄЮ ПАРАМЕТРІВ

Концепція використання цифрових двійників в енергетиці формується як відповідь на зростаючу складність сучасних енергетичних систем, інтеграцію відновлюваних джерел енергії, цифровізацію мереж та підвищені вимоги до надійності, безпеки й ефективності функціонування енергетичних об'єктів [1]. Умови переходу до Smart Grid, децентралізації генерації та активного впровадження інформаційно-комунікаційних технологій потребують нових інструментів аналізу, прогнозування та управління, одним із яких є цифровий двійник. Первинно концепція Digital Twin отримала розвиток у аерокосмічній галузі, зокрема в проєктах NASA, однак сьогодні вона активно впроваджується провідними світовими технологічними компаніями, такими як Siemens, General Electric та ABB, у сфері енергетики, промислової автоматизації та інфраструктурних систем.

Цифровий двійник енергетичного об'єкта являє собою інтегровану інформаційно-математичну систему, що відтворює у віртуальному середовищі фізичні, теплові, електричні, механічні та інші процеси, які відбуваються в реальному об'єкті, із забезпеченням двостороннього обміну даними в режимі реального часу. На відміну від традиційної математичної моделі або імітаційної симуляції, цифровий двійник передбачає постійне оновлення параметрів на основі фактичних експлуатаційних даних, що надходять від систем вимірювальних датчиків, SCADA-комплексів, інтелектуальних вимірювальних пристроїв та систем моніторингу. Таким чином формується кіберфізична система, у якій цифрова копія не лише відображає стан об'єкта, а й дозволяє прогнозувати його поведінку, оцінювати залишковий ресурс, моделювати аварійні режими та оптимізувати режими роботи.

В енергетиці цифрові двійники можуть застосовуватися на різних рівнях – від окремого елемента обладнання до енергоблоку, підстанції або всієї енергосистеми. Для генеруючих установок цифровий двійник дає можливість аналізувати термодинамічні цикли, контролювати параметри навантаження, виявляти відхилення від номінальних режимів і переходити від планово-попереджувального до предиктивного технічного обслуговування [2]. В атомній енергетиці така концепція особливо актуальна для складних і відповідальних систем, де необхідне безперервне оцінювання технічного стану активної зони, теплообмінного обладнання та допоміжних систем. У мережевій інфраструктурі цифровий двійник підстанції або вузла розподілу дозволяє моделювати перехідні процеси, прогнозувати перевантаження, оптимізувати перетоки потужності та підвищувати стійкість до збурень (рис. 1).

Рисунок 1. – Багаторівнева кіберфізична архітектура цифрового двійника енергетичного об'єкта з контуром адаптивної ідентифікації

У системах з відновлюваними джерелами енергії цифрові двійники застосовуються для прогнозування генерації з урахуванням погодних умов, аналізу деградації обладнання та оптимізації роботи накопичувачів енергії.

Ключовою особливістю концепції є поєднання фізико-математичного моделювання з методами обробки великих даних та алгоритмами машинного навчання. Це дозволяє створювати адаптивні моделі, здатні самокоригуватися відповідно до реального стану системи. У такій парадигмі цифровий двійник виступає не лише інструментом візуалізації або моніторингу, а й активним елементом системи підтримки прийняття рішень. Він може використовуватися для оцінки сценаріїв розвитку аварій, визначення оптимальних стратегій керування, аналізу ефективності модернізації обладнання та обґрунтування інвестиційних рішень.

Разом із перевагами впровадження цифрових двійників в енергетиці існують і суттєві виклики. До них належать необхідність високої якості первинних даних, стандартизація протоколів обміну, забезпечення кібербезпеки, інтеграція з існуючими системами автоматизації та значні початкові інвестиції. Крім того, створення адекватної цифрової копії складного енергетичного об’єкта потребує глибокої міждисциплінарної взаємодії фахівців у галузі енергетики, математичного моделювання, інформаційних технологій та аналізу даних.

У стратегічній перспективі використання цифрових двійників може стати основою переходу до проактивного управління енергетичними системами, коли рішення приймаються не на основі фіксації вже реалізованих відхилень, а на підставі прогнозних оцінок майбутнього стану об’єкта. Такий підхід сприяє підвищенню надійності, економічності та безпеки функціонування енергетичної інфраструктури, що є особливо важливим в умовах енергетичної трансформації та зростання вимог до стійкості енергосистем. Таким чином, концепція цифрового двійника виступає одним із ключових інструментів цифрової трансформації енергетики, забезпечуючи інтеграцію фізичних процесів, інформаційних потоків та інтелектуальних алгоритмів у єдиному керованому середовищі.

1. Budanov, P., Brovko, K., Melnykov, V., Yakymchuk, M., Kononov, V., Kyrysov, I., Nosyk, A., Karpenko, O., Kalnoy, S., & Khomiak, E. (2025). Construction of an information model of the digital twin of the technological process in a power unit at a nuclear power plant. *Eastern-European Journal of Enterprise Technologies, 4*(9(136)), 39–49. https://doi.org/10.15587/1729-4061.2025.335712.

2. Бровко, К. Ю., Буданов, П. Ф., Великогорський, О. В., & Винокурова, Н. Д. (2025). Забезпечення кількісної оцінки якості управління технологічним процесом енергоблоку АЕС засобами цифрового двійника. Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях, 3(25), 3–12. https://doi.org/10.20998/2413-4295.2025.03.01.

С.Ф. Гончар

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ РОЗПОДІЛЕНИХ ЕНЕРГЕТИЧНИХ СИСТЕМ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Перехід до децентралізованих енергетичних систем вводить нові складнощі забезпечення їх кібербезпеки, які кидають виклик традиційним парадигмам енергетичної безпеки. Розподілені системи відновлюваної енергії, що включають сонячну фотоелектрику, вітрові турбіни, мікромережі та акумуляторні батареї, за своєю суттю децентралізовані, об'єднані в мережу та залежать від передових цифрових технологій для моніторингу, контролю та оптимізації в режимі реального часу. Хоча ці системи забезпечують гнучкість та резильєнтність, вони також розширюють “поверхню атаки” для кіберзагроз завдяки пристроям Інтернету речей (IoT), хмарним обчисленням, протоколам двонаправленого зв'язку, системам SCADA, блокчейнам та представляють високі ризики для стабільності і надійності таких систем [1-4].

Через постійні атаки на великі об'єкти енергетики Україна взяла курс на децентралізацію енергетичних систем та розбудову розподіленої генерації. За інформацією Віце-прем’єр-міністра з відновлення України – Міністра розвитку громад та територій в Україні триває посилення розподіленої генерації: станом на березень 2026 року в Україні уже експлуатується 465 одиниць обладнання загальною потужністю 651,5 МВт для підприємств житлово-комунального господарства [5].

Попри явні переваги децентралізація енергетичних систем створює нові проблеми для забезпечення кібербезпеки таких систем, основними з яких є:

- розширення поверхні атак: величезна кількість пристроїв IoT (розумні лічильники, інвертори, сенсори) створює тисячі нових точок входу для хакерів;
- вразливість промислових протоколів: багато об'єктів використовують застарілі або незахищені протоколи передачі даних, які не мають вбудованого шифрування;
- ризики ланцюжка постачання: шкідливе програмне забезпечення може бути впроваджене ще на етапі виробництва обладнання або через оновлення прошивок від сторонніх вендорів;
- відсутність єдиних стандартів: гетерогенність систем (різні виробники, технології та власники) ускладнює впровадження уніфікованої політики безпеки;
- специфічні атаки, як наприклад:
- FDI (False Data Injection): інжекція неправдивих даних для маніпуляції частотою або напругою мережі;
- DDoS-атаки: перевантаження каналів зв'язку мікромереж для блокування оперативного управління.

Пропонуються наступні шляхи вирішення проблем забезпечення кібербезпеки розподілених енергетичних систем:

- застосування моделі Zero Trust;

- використання технологій штучного інтелекту для моніторингу;
- сегментація мережі;
- застосування блокчейн-технології;
- кібер-фізичний моніторинг;
- державне регулювання.

Застосування моделі Zero Trust передбачає, що жоден пристрій або користувач у мережі не вважається безпечним за замовчуванням; кожна дія потребує безперервної верифікації.

Використання технологій штучного інтелекту для виявлення аномалій у реальному часі дозволяє ідентифікувати атаки на ранніх стадіях з точністю до 96,5% [2].

Сегментація мережі забезпечує розподіл енергосистеми на ізольовані сегменти, щоб у разі зламу одного об'єкта атака не поширилася на всю мережу.

Застосування блокчейн-технології дозволить використання децентралізованих реєстрів для безпечного обміну даними, ідентифікації пристроїв та захисту цілісності команд керування.

Кібер-фізичний моніторинг забезпечить відстеження не лише цифрових логів, а й фізичної поведінки обладнання (наприклад, нетипові зміни кута нахилу лопатей турбін), що допомагає виявити приховані втручання.

Державне регулювання передбачає впровадження обов'язкових стандартів кібербезпеки для всіх учасників ринку розподіленої генерації (на кшталт стандартів NERC CIP або відповідних постанов НКРЕКП тощо).

1. 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. https://doi.org/10.30574/wjarr.2025.26.3.2232.

2. Alshammari, A. Securing smart microgrids with a novel multi-layer cybersecurity framework for Industry 4.0 renewable energy systems. Discov Computing 28, 2025. https://doi.org/10.1007/s10791-025-09600-7.

3. Szczepaniuk, E.K.; Szczepaniuk, H. Cybersecurity of Smart Grids: Requirements, Threats, and Countermeasures. Energies 2025, 18, 5017. https://doi.org/10.3390/en18185017.

4. 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.

5. 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).

В.М. Мацука

SMART-MANAGEMENT ЕНЕРГЕТИЧНИХ СИСТЕМ В УМОВАХ ВОЄННИХ ЗАГРОЗ

Енергетична інфраструктура є однією з ключових складових критичної інфраструктури держави. Її стабільне функціонування забезпечує роботу промисловості, транспорту, систем зв'язку, медичних установ та інших важливих секторів економіки. В умовах воєнних загроз енергетичні об'єкти часто стають пріоритетною ціллю атак, що може спричинити масштабні перебої в електропостачанні та суттєво вплинути на національну безпеку.

Сучасні конфлікти демонструють, що загрози для енергетичних систем можуть мати комплексний характер. Окрім фізичного руйнування енергетичних об'єктів, значну небезпеку становлять кібератаки на системи управління енергетичною інфраструктурою. У таких умовах традиційні моделі управління енергетикою часто виявляються недостатньо ефективними, що обумовлює необхідність впровадження нових підходів до управління.

Одним із перспективних напрямів є використання smart-management – сучасної моделі управління, що базується на використанні цифрових технологій, автоматизованих систем моніторингу, аналітики даних та інтелектуальних електромереж.

У наукових дослідженнях значна увага приділяється питанням цифровізації енергетики, розвитку інтелектуальних електромереж та підвищення стійкості енергосистем до кризових ситуацій. У багатьох країнах світу активно впроваджуються концепції smart grid, що дозволяють підвищити ефективність управління енергетичними потоками та забезпечити гнучкість енергосистеми.

Водночас сучасні виклики, пов'язані з воєнними загрозами, потребують поєднання технологічних інновацій із новими управлінськими підходами, які дозволяють забезпечити швидке реагування на аварійні ситуації та ефективну координацію між різними учасниками енергетичного сектору.

Метою дослідження є вивчення особливостей застосування smart-management у системі управління енергетичними системами в умовах воєнних загроз, а також аналіз міжнародного досвіду та практичних кейсів України у цій сфері.

Функціонування енергетичних систем у кризових та воєнних умовах характеризується високим рівнем ризиків та невизначеності. Руйнування електростанцій, пошкодження підстанцій і ліній електропередач, нестабільність навантаження на мережі та кіберзагрози створюють складні умови для управління енергетичною інфраструктурою. У таких умовах особливого значення набуває впровадження smart-management, який забезпечує використання цифрових технологій для оперативного моніторингу та управління енергетичними системами [1;2].

Smart-management передбачає інтеграцію інформаційних технологій, систем автоматизованого управління та аналітики даних у процеси управління генерацією, передачею та розподілом електроенергії. Завдяки цьому забезпечується постійний контроль за станом енергетичних об'єктів, оперативне виявлення пошкоджень та швидке реагування на аварійні ситуації.

Світова практика демонструє ефективність використання інтелектуальних енергетичних систем для підвищення стійкості енергетичної інфраструктури. Наприклад, у багатьох країнах Європейського Союзу активно розвиваються системи smart grid, які дозволяють автоматично балансувати енергосистему та оптимізувати розподіл електроенергії між регіонами. У разі аварій або пошкодження енергомереж такі системи здатні автоматично перенаправляти потоки електроенергії, що дозволяє зменшити масштаби відключень.

У США та країнах Європи активно впроваджуються мікромережі – локальні енергетичні системи, які можуть функціонувати автономно від центральної енергомережі. Такі системи використовуються для забезпечення енергопостачання лікарень, центрів управління та інших об'єктів критичної інфраструктури у випадку надзвичайних ситуацій [3].

Подібні підходи поступово впроваджуються і в Україні, особливо в умовах повномасштабної війни. Важливу роль у забезпеченні стабільності енергосистеми відіграє оператор системи передачі електроенергії – НЕК «Укренерго». Під час масованих атак на енергетичну інфраструктуру у 2022–2023 роках компанія активно використовувала цифрові системи диспетчерського управління для балансування енергосистеми та координації роботи енергетичних об'єктів.

Завдяки використанню сучасних систем моніторингу стало можливим оперативно визначати місця пошкоджень у мережі та здійснювати перерозподіл електроенергії між регіонами. Це дозволило зменшити тривалість аварійних відключень та забезпечити стабільність роботи енергосистеми [4].

Важливим елементом підвищення стійкості енергетичної системи України стала її синхронізація з європейською мережею ENTSO E. Це рішення дозволило забезпечити можливість аварійного імпорту електроенергії з країн Європейського Союзу та підвищити гнучкість енергосистеми.

Значний внесок у розвиток цифрового управління енергетичною інфраструктурою здійснюють і енергетичні компанії. Зокрема, компанія ДТЕК впроваджує сучасні системи дистанційного моніторингу електромереж. Під час пошкодження підстанцій або ліній електропередач такі системи дозволяють швидко визначити місце аварії та організувати ремонтні роботи, що значно скорочує час відновлення електропостачання [5].

Ще одним важливим напрямом smart-management є розвиток децентралізованої генерації енергії. В Україні, як і в багатьох країнах світу, поступово розвиваються локальні джерела енергії – сонячні електростанції, системи накопичення енергії та резервні генератори. Такі рішення дозволяють

забезпечити автономне електропостачання окремих громад або об'єктів критичної інфраструктури у разі пошкодження центральної енергомережі.

У низці українських міст впроваджуються сучасні системи диспетчеризації міських енергетичних мереж. Вони дозволяють у режимі реального часу відстежувати стан електромереж, контролювати навантаження та оперативно реагувати на аварійні ситуації [6;7].

Окремим напрямом smart-management є забезпечення кібербезпеки енергетичної інфраструктури. Цифровізація енергетики створює нові можливості для ефективного управління, але водночас підвищує ризики кібератак. Україна вже має значний досвід протидії таким загрозам, тому енергетичні компанії впроваджують сучасні системи захисту інформаційних мереж, моніторингу кіберінцидентів та реагування на кіберзагрози [8;9].

Таким чином, міжнародний досвід та практика України демонструють, що використання smart-management є ефективним інструментом підвищення стійкості енергетичних систем та забезпечення безперебійного функціонування енергетичної інфраструктури навіть у складних кризових умовах [10].

Smart-management є важливим інструментом модернізації системи управління енергетичною інфраструктурою в умовах воєнних загроз. Використання інтелектуальних електромереж, цифрових систем моніторингу та аналітики даних дозволяє підвищити ефективність управління енергетичними системами та забезпечити їхню стійкість до зовнішніх впливів.

Поєднання міжнародного досвіду та практичних кейсів України свідчить про те, що впровадження цифрових технологій у сфері енергетики дозволяє швидко реагувати на аварійні ситуації, оптимізувати управління енергетичними потоками та забезпечувати відновлення пошкодженої інфраструктури у короткі строки.

Подальший розвиток smart-management має бути спрямований на розширення цифрової інфраструктури енергетичного сектору, розвиток децентралізованої генерації, підвищення рівня кібербезпеки та поглиблення інтеграції з європейськими енергетичними мережами. Це сприятиме зміцненню енергетичної безпеки держави та підвищенню стійкості критичної інфраструктури в умовах сучасних загроз.

1. Закон України «Про критичну інфраструктуру» № 1882-IX (2021, 16 листопада). *Відомості Верховної Ради України*, (5), 23. https://zakon.rada.gov.ua/laws/show/1882-20#Text.

2. Закон України «Про ринок електричної енергії» № 2019-VIII (2017, 13 квітня). *Відомості Верховної Ради України*, (27-28), 17. https://zakon.rada.gov.ua/laws/show/2019-19.

3. DER Deployment. (2024). *2024 Smart Grid System Report. https://www.energy.gov/sites/default/files/2024-02/2024%20Smart%20Grid%20System%20Report_untagged.pdf.*

4. Екодія. (2018, 25 грудня). *Інфографіка Енергетика України 2050: перехід на відновлювані джерела.* https://ecoaction.org.ua/ukraine-energy-2050.html?gad_source=1&gad_campaignid=23391459760&gbraid=0AAAAACVR_NRWxt1623XGt0Vg_-EttU5Rt&gclid=Cj0KCQiAk6rNBhCxARIsAN5mQLtnP-WjXxD8QZl0-bVblmdBeOoq2pQbQB1_kHs3EuA9SqCB8CuCD84aAjchEALw_wcB.

5. ДТЕК України. (2024). *Битва за світло. Звіт про діяльність 2024*. https://dtek.com/content/upload/report/DTEK%202024%20Action%20Report%20Ukrainian%20250221.pdf.

6. Balabanyts, A.V, Haponiuk, O.I., Horbashevska, M.O., Kyslova, L.A., Matsuka, V.M., Omelchenko, V.Ya, Osypenko, K.V., Perepadia, F.L., & Semkova, L.V. (2020). *Management of financial and economic security of the state and ways to prevent external and internal threats.* Mariupol MDU. https://repository.mu.edu.ua/jspui/bitstream/123456789/1746/1/upravlinnia_finansovo-ekonomichnoiu.pdf.

7. Балабаниць, А.В., Мацука, В.М. (2022). Сучасна парадигма механізму управління фінансово-економічною безпекою держави. *Економіка та суспільство*, (39). https://doi.org/10.32782/2524-0072/2022-39-65.

8. Стойка, А.В., Верительник, С.М., & Мацука, В.М. (2025). Діджиталізація управління проєктами і вплив на світову економіку та інвестиції. *Збірник наукових праць «Вчені записки»,* 39(2), 45-58. http://doi.org/10.33111/vz_kneu.39.25.02.04.026.032.

9. Cherep, A.V., Dashko, I.M., Ohrenych, Yu.O, & Cherep, O.H. (2024). *Theoretical and Methodological Foundations for the Use of Digital Technologies in Ukraine through the Implementation of EU Experience: collective monograph*. Zaporizhzhia publisher of FOP Mokshanov V.V. URL: https://dspace.znu.edu.ua/xmlui/handle/12345/24080.

10. Мацука, В.М., & Коваль, О.А. (2023). Маркетинговий менеджмент у діяльності енергопідприємств. У Є.І. Зубцов (Ред.), Технологія-2023 (с.285-287). Київ Східноукр. нац. ун-т ім. В. Даля.

С.В. Гасич

ЕНЕРГЕТИЧНА ІНФРАСТРУКТУРА ЯК ОБ'ЄКТ СТРАТЕГІЧНОГО ВПЛИВУ У СУЧАСНИХ ВОЄННИХ КОНФЛІКТАХ

У сучасних воєнних конфліктах енергетична інфраструктура відіграє одну з ключових ролей у стабільному функціонуванні держави. Від надійної та безперебійної роботи енергетичного сектору залежить діяльність промислових підприємств, транспортної інфраструктури, медичних установ, комунальних служб та оборонного комплексу. Саме тому енергетична інфраструктура є пріоритетною ціллю в театрі бойових дій. Ураження енергетичних систем в основному використовується елемент тиску на державу та її населення з метою подальшого примусу до відмови від ведення бойових дій.

Формування ідеї знищення (виведення з ладу) енергетичної інфраструктури як стратегічної цілі бере початок у першій половині XX століття. У 1930-х роках у школі для льотчиків Повітряного корпусу США проводилися дослідження щодо визначення ключових об'єктів стратегічного бомбардування. Дослідники припускали, що повне знищення або тимчасове виведення з ладу важливих енергетичних центрів здатне суттєво послабити економічний потенціал противника та обмежити його здатність продовжувати війну [1]. Хоча ці ідеї не були офіційно закріплені у військових нормативних документах, вони стали основою для формування стратегій повітряних бомбардувань під час Другої світової війни.

Досвід бойових дій другої половини XX століття продемонстрував ефективність впливу на енергетичну інфраструктуру як одного з ключових інструментів стратегічного тиску на державному рівні. Порушення функціонування енергосистеми призводить до дестабілізації соціальної ситуації та зменшення поценціалу держави підтримувати військові операції [2].

Показовим прикладом використання такої стратегії стала військова операція НАТО проти Югославії у 1999 році. У цій кампанії була застосована тактика енергетичного тискку в ході якої застосовувалася високоточна зброя для ураження об'єктів енергетичної інфраструктури, зокрема електростанцій та елементів системи передачі електроенергії. Основною метою було тимчасове виведення з ладу енергетичної системи, що дозволяло паралізувати економічну діяльність держави та обмежити її можливості продовжувати військові дії [2].

Російська Федерація у російсько-українській війні взяла за основу тактику дій НАТО в Югославії. З початку повномасштабного вторгнення наносить удари по енергетичній інфраструктурі України, але з іншим тактичним підходом. На відміну від югославського конфлікту, атаки Росії на

енергетичну інфраструктуру України мають більш руйнівний і тривалий характер. Використання ракет великої потужності та ударних безпілотників спрямоване не лише на тимчасове знеструмлення, а й на фізичне знищення об'єктів генерації та передачі електроенергії. Це ускладнює відновлення системи та значно підвищує гуманітарні ризики, особливо в осінньо-зимовий період.

Спільною рисою обох конфліктів є використання енергетичних атак як інструменту психологічного тиску на населення та засобу примусу політичного керівництва до прийняття вигідних агресору рішень. Водночас міжнародна реакція на ці дії була різною: якщо дії НАТО в Югославії викликали гострі дискусії щодо відповідності міжнародному гуманітарному праву, то удари Росії по енергетичних об'єктах України отримали широку міжнародну критику та були однозначно засуджені як порушення принципів захисту цивільної інфраструктури. Масовані атаки ракетами та безпілотними літальними апаратами спрямовані на системне пошкодження енергетичних об'єктів. Це призводить до масштабних відключень електроенергії, порушення роботи промислових підприємств та функціонування критичної інфраструктури. Крім того, такі дії створюють серйозні гуманітарні ризики для цивільного населення.

Отже, аналіз сучасних воєнних конфліктів свідчить про еволюцію підходів до використання енергетичної інфраструктури як інструменту стратегічного впливу. Якщо наприкінці XX століття переважала стратегія тимчасового паралічу енергосистеми, то у XXI столітті спостерігається тенденція до системного фізичного руйнування енергетичних об'єктів. У таких умовах особливої актуальності набуває підвищення стійкості енергетичних систем та розроблення комплексних механізмів захисту критичної інфраструктури.

1. Griffith T. Strategic Attack of National Electrical Systems. Air University Press Maxwell Air Force Base, Alabama, 1994. 64 p., https://surli.cc/pwmneo.

2. Military technical courier, issue 3 electrically conductive fibers in cluster bomblets which targeted the electric power system of fr yugoslavia, 2020, 68 p, https://www.researchgate.net/publication/343087286_Electrically_conductive_fibers_in_cluster_bomblets_which_targeted_the_electric_power_system_of_FR_Yugoslavia_in_1999.

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

ВЕРИФІКАЦІЯ СУМІСНОСТІ IoT-КОМПОНЕНТІВ МІКРОМЕРЕЖІ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ РОЗПОДІЛЕНИХ ЕНЕРГОСИСТЕМ

Децентралізація енергопостачання через мікромережі (Microgrids) є стратегічною відповіддю на вразливість централізованих енергосистем за умов воєнних та техногенних загроз. Мікромережа як автономний кластер генерації, накопичення та розподілу енергії функціонує на основі розвиненої IoT-інфраструктури (InternetofThings): датчики, актуатори, шлюзи та контролери обмінюються даними на основі протоколів прикладного рівня MQTT (MessageQueuingTelemetryTransport) та CoAP (ConstrainedApplicationProtocol). Надійність такої взаємодії визначає здатність кластера переходити в острівний режим, балансувати навантаження та зберігати управління в критичних ситуаціях.Водночас гетерогенність обладнання різних виробників, різні версії протоколів та рівні QoS (QualityofServices) породжують ризики міжкомпонентної несумісності, які за традиційного підходу виявляються лише в ході експлуатації системи.

Забезпечення резильєнтностімікромережі вимагає перенесення контролю сумісності компонентів з етапу аварійного діагностуваннядо етапупроєктування [1]. Контроль (верифікацію) сумісності зведено до встановлення істинності твердження:

$$M, \sigma| = \phi \ , \tag{1}$$

де M – модель системи, на основі якої здійснюємо контроль сумісності компонентів на прикладному рівні мережевої моделі OSI (OpenSystemsInterconnection); σ – обчислення як послідовність станів, що відтворює поведінку системи на моделі M ; ϕ – темпоральна формула, призначена приймати істинне значення для кожного із елементів послідовності σ .

У якості моделі М обрано структуру Кріпке на множині атомарних висловлювань AP :

$$M = (S, S_0, R, L), \tag{2}$$

де S – тотальна множина станів; $S_0 \subset S$ – множина початкових станів; $R \subseteq S^2$ – множина переходів між станами; $L: S \to 2^{AP}$ – функція розмітки станів.

Формалізація сполучень між компонентами виконується шляхом використання засобів темпоральної логіки дій TLA (TemporalLogicofActions); при цьому одержуються ієрархічні подання [2].Відповідні концепції «дій» (Actions) формують нижній ієрархічний рівень. Проміжний рівень складають специфікації функціональних характеристик системи. Верхній рівень – результуюча темпоральна формула на основі елементів проміжного рівня.

Множину AP формуємо наступним чином:

$$AP = V \times D = AP' \cup AP'', \quad (3)$$

де V – множина змінних станів системи переходів, що будується і опрацьовується у процесі формальної верифікації методом перевірки на моделі в автоматизованому режимі; D – множина допустимих значень змінних; $AP' = \{ap_i'\}$ – множина передумов для дій: $ap_i' = (v_i, \mathbf{0}) \in AP' \subset AP$; $AP'' = \{ap_i''\}$ – множина пост-умов: $ap_i'' = (v_i, \mathbf{1}) \in AP'' \subset AP$; $i = 1,2,...,m \in N$; $v_i \in V$.

Для випадку IoT-мікромережі, компоненти програмної складової якої взаємодіють згідно протоколу MQTT QoS 2 (QualityofServices),матимемо наступну множину змінних станів:

$$V = \left\{ v_i \middle|_{i=1}^{4} \right\}. \quad (4)$$

де $v_1 \in V$ –«PUBLISH», $v_2 \in V$ –«PUBREC», $v_3 \in V$ –«PUBREL», $v_4 \in V$ –«PUBCOMP» (рис. 1).

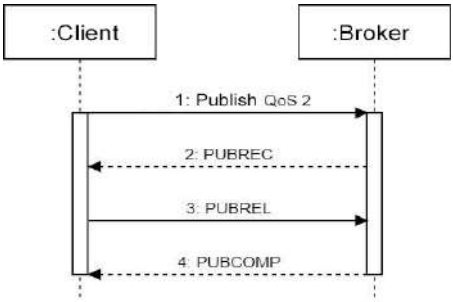


Рисунок 1 – Діаграма послідовності взаємодії згідно QoS 2

Враховуючи аспектиQoS 2, множина значень змінних становитиме $D = \left\{ d_r \middle|_{r=0}^{2} \right\}$. Отже маємо $|S| = 3^4 = 81$ станів системи переходів. Глибина обходу простору станів при цьому – 8.

Розроблений і застосований метод контролю сумісності компонентів мікромережі на рівні протоколів взаємодії полягає у наступному: компоненти мікромережі у частині їх сумісності перевіряються попарно – шляхом топологічного співставленнявідповідних систем переходів.

Метод контролю сумісності реалізовано у формі програмного модуля у складі комплексу програмних засобів IoTSim-Edge [2].

Дослідження проведено в середовищі IoTSim-Edge шляхом імітаційного моделювання мережі температурних датчиків (10–50 пристроїв). Міжкомпонентну взаємодію забезпечено на основі протоколів MQTT (QoS 0–2) та CoAP [3, 4].

Архітектурну складову програмної реалізації моделей компонентів досліджуваної системи представлено на рисунку 2.

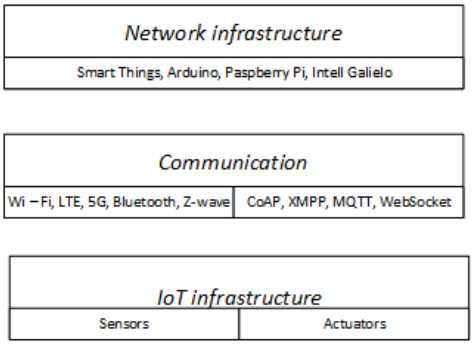


Рисунок 2. – Подання архітектури компонентівIoTSim-Edge

Отримані результати: для випадку 30 компонентів, що взаємодіють між собою на основі протоколу MQTTQoS 2, значення показника успішності контролю сумісності склало ~90 %. Для випадку застосування протоколу CoAP це значення становило~88 %. Вбачається, що отримані оціночні значення можуть бути використані проєктувальникам громадських мікромереж у якості орієнтирів у частині підбору протоколів взаємодії відповідних компонентів.

Отже, розроблений метод верифікації сумісності IoT-компонентів є дієвим інструментом сприяннярезильєнтностімікромереж у частині закладання відповідних засад на архітектурному рівні: на етапі проєктування у складі етапів процесу розроблення програмної складової мікромереж. Цей аспект набуває особливої ваги у контексті залучення у якості компонентів мікромереж відновлювальних джерел та підсистем накопичення енергії, що характеризуються значною гетерогенністю на рівні апаратної і програмної складових.

1. Timenko, A. V., Shkarupylo, V. V., Oliinyk, A. O., &Hrushko, S. S. (2019). Formal model for checking the interoperability between the components of the IoT system. *ProblemeleEnergeticiiRegionale*, *40*(1-1), 69–78. https://doi.org/10.5281/zenodo.3239196 .

2. Jha, D. N., et al. (2020). IoTSim-Edge: A simulation framework for modeling the behavior of Internet of Things and edge computing environments. *Software: Practice and Experience*, *50*(6), 844–867. https://doi.org/10.1002/spe.2787.

3. Lamport, L. (1994). The temporal logic of actions. *ACM Transactions on Programming Languages and Systems*, *16*(3), 872–923.

Shkarupylo, V., Kudermetov, R., Timenko, A., &Polska, O. (2019). On the aspects of IoT protocols specification and verification. *PIC S&T'2019*, 93–96. https://doi.org/10.1109/PICST47496.2019.9061406.

G.P. Kostenko, A.O. Zaporozhets

RAPID RESPONSE STRATEGIES FOR ENERGY DEFICITS USING SECOND-LIFE EV BATTERIES

The rapid transformation of modern power systems is driven by two key factors: the increasing penetration of renewable energy sources and the growing exposure of energy infrastructure to external disruptions. In many regions, including Ukraine, recent events have demonstrated that power systems must operate under conditions of uncertainty, where both generation and network availability may be constrained [1].

Renewable energy sources such as wind and solar introduce variability and intermittency into power systems, requiring additional flexibility to maintain system balance. At the same time, infrastructure disruptions -whether caused by physical damage, technical failures, or extreme operating conditions - can lead to short-term power imbalances that may occur locally or at the system level and require rapid response mechanisms [2].

Energy deficits and power imbalances may arise from several sources, including sudden loss of generation capacity, network constraints, variability of renewable energy sources, and peak demand conditions. In disrupted energy systems, such deficits may occur simultaneously at multiple nodes, requiring distributed and rapidly deployable response mechanisms. Traditional solutions, such as dispatchable generation or reserve capacity, are often limited by ramp rates, fuel availability, or economic constraints. Therefore, energy storage systems are increasingly recognized as key enablers of flexibility. In this context, the concept of using second-life EV batteries (SLB) for rapid response applications becomes particularly relevant [3].

The objective of this study is to develop and evaluate rapid response strategies for mitigating short-term power imbalances in modern power systems using SLB.

Second-Life EV Batteries as a Resource

SLB originate from electric vehicles that have reached the end of their automotive service life, typically when their state of health decreases to approximately 70-80%. Although these batteries no longer meet the strict requirements of electric mobility, they retain sufficient capacity for stationary applications. The main characteristics of SLB that make them suitable for rapid response applications include residual energy capacity sufficient for short-term balancing tasks; reduced cost compared to newly manufactured battery systems; modularity and scalability of deployment; availability driven by the growth of electric vehicle fleets.

In stationary energy storage systems, operating conditions are generally less demanding than in electric vehicles. Charge-discharge cycles are more stable, power requirements are lower, and thermal conditions can be better controlled.

These factors enable the effective reuse of batteries that would otherwise be directed to recycling.

The operation of SLB systems in rapid response applications can be represented through a simple control logic based on real-time power balance assessment. Depending on the difference between renewable generation and load demand, the battery system operates in either discharge mode to compensate deficits or charge mode to absorb surplus energy. This approach enables dynamic balancing of power flows and supports system stability under variable operating conditions (Fig. 1).

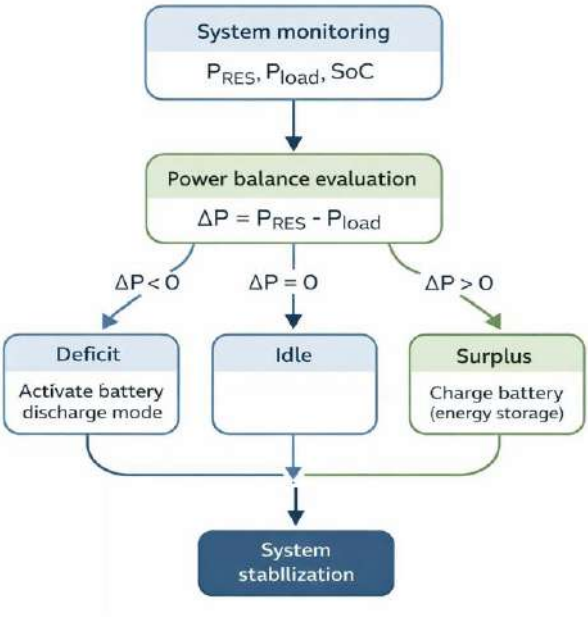


Figure 1. – Control logic for rapid response using second-life EV batteries

Rapid Response Strategies for Energy Deficits

SLB can be integrated into power systems through several rapid response strategies, depending on the type of deficit and system conditions [4].

Local Buffer Storage

Distributed battery systems can be deployed at weak grid nodes or in microgrids to provide local balancing of supply and demand. These systems respond within seconds, compensating for short-term imbalances and preventing voltage or frequency deviations. Such systems are particularly effective in distribution networks with limited flexibility, where local imbalances can lead to voltage instability or supply interruptions. The deployment of SLB in these nodes enables decentralized control and reduces dependence on centralized balancing resources.

Peak Load Support

SLB can be used to reduce peak demand by supplying energy during high-load periods. This strategy decreases stress on network infrastructure and reduces the need for additional generation capacity. This approach is especially relevant in urban energy systems with highly variable demand profiles. By reducing peak loads, SLB also contribute to extending the lifetime of grid infrastructure.

Renewable Generation Smoothing

In systems with high shares of renewable energy, SLBcan mitigate fluctuations in generation output. By absorbing excess energy and supplying it during deficits, they improve the stability of energy flows. This function is critical in systems with a high share of solar and wind generation, where fluctuations may occur over short time intervals. Battery-based smoothing reduces the need for curtailment and improves the efficiency of renewable energy utilization.

Backup Supply for Critical Loads

Second-life battery systems can provide emergency power to critical infrastructure such as hospitals, communication systems, and control centers. Their fast response time makes them particularly suitable for such applications. In emergency conditions, such systems can operate independently from the grid, forming the basis for resilient microgrids. Their rapid activation ensures continuity of supply during critical system disturbances.

The practical implementation of rapid response strategies based on SLBrequires consideration of several technical and organizational factors. These include battery aggregation methods, control system architecture, and integration with existing grid infrastructure. Reliable diagnostics and state-of-health estimation are essential for ensuring safe and efficient operation. In addition, standardized data formats and monitoring systems play a key role in enabling scalable deployment. The economic feasibility of such systems depends on battery acquisition costs, operational strategies, and market participation mechanisms.

To address power imbalances, second-life EV batteries can be deployed within a set of rapid response strategies depending on system conditions and operational requirements. These strategies differ in terms of function, application context, and response time, but all are aimed at ensuring fast and flexible compensation of power imbalances. The main types of rapid response strategies based on SLB deployment are summarized in Table 1.

Table 1. Rapid response strategies using second-life EV batteries

Strategy	Function	Application context	Response time
Buffer storage	Local balancing of supply and demand	Microgrids, weak nodes	Seconds
Peak support	Reduction of peak demand	Urban grids	Minutes
RES smoothing	Compensation of variability	High RES systems	Seconds–minutes
Backup supply	Emergency power	Critical infrastructure	Immediate

Rapid Response Adequacy Index

The deployment of second-life EV batteries in rapid response applications requires a clear criterion for assessing their ability to compensate short-term power imbalances. In practical conditions, the effectiveness of such systems depends not only on the available energy capacity, but also on the magnitude of the deficit and the required response time. Therefore, a simple adequacy indicator that links these parameters is necessary to evaluate whether a battery system can provide sufficient support within a given time interval. The introduction of a rapid response adequacy index allows for a straightforward assessment of the capability of second-life battery systems to cover power deficits and supports decision-making in the selection and design of appropriate response strategies.

$$RRAI = \frac{E_{avail}}{P_{def} t_{resp}},$$

where:

E_{avail} - available energy capacity of the second-life battery system, kWh;

P_{def} - power deficit, kW;

t_{resp} - required response duration, h.

Interpretation

$RRAI \geq 1$ - the battery system is capable of covering the power deficit within the specified response time;

$RRAI < 1$ - the available energy is insufficient, and additional resources or alternative response strategies are required.

The proposed strategies demonstrate that second-life EV batteries can significantly contribute to improving the flexibility and resilience of power systems. From a technical perspective, their fast response time allows them to address short-term imbalances more effectively than conventional generation sources. From an economic perspective, SLB provide a cost-effective alternative to new storage systems. Their reuse extends the lifecycle of battery materials, reduces waste, and aligns with circular economy principles.

However, several challenges must be considered. These include variability in battery condition, uncertainty in remaining useful life, and the need for reliable diagnostic systems. In addition, standardized data on battery performance is essential for ensuring safe and efficient operation.

Conclusions:

SLB represent a viable and scalable solution for addressing short-term power imbalances in modern energy systems. Their deployment within rapid response strategies enhances system flexibility, supports renewable energy integration, and improves overall system resilience. The use of SLB is particularly relevant in conditions of infrastructure vulnerability, where fast and distributed solutions are required. By enabling the reuse of existing battery resources, such approaches also contribute to the development of sustainable and circular energy systems. The proposed rapid response framework highlights the importance of combining technological solutions with appropriate operational strategies for effective deficit management.

1. Zaporozhets, A., Babak, V., Kostenko, G., Zgurovets, O., Denisov, V., & Nechaieva, T. (2024). Power System Resilience: An Overview of Current Metrics and Assessment Criteria. In V. Babak, A. Zaporozhets (Eds.), Systems, Decision and Control in Energy VI, 561 (pp. 35–58). Springer, Cham. https://doi.org/10.1007/978-3-031-68372-5_2.

2. Paul Denholm, Maureen Hand, Grid flexibility and storage required to achieve very high penetration of variable renewable electricity, Energy Policy, Volume 39, Issue 3, 2011, Pages 1817-1830, https://doi.org/10.1016/j.enpol.2011.01.019.

3. Kostenko, G., Zaporozhets, A., Babak, V., Uruskyi, O., Titko, V., Denisov, V. (2025). Second-Life EV Batteries Application in Energy Storage Systems for Sustainable and Resilient Power Sector. In: Systems, Decision and Control in Energy VII, vol 595. Springer, Cham. https://doi.org/10.1007/978-3-031-90466-0_1\..

4. Zaporozhets, A., & Kostenko, G. (2025). Second-Life Electric Vehicle Batteries in Ukraine's Energy Sector: SWOT Analysis and Market Evaluation. *Science and Innovation*, *21*(6), 19–37. https://doi.org/10.15407/scine21.06.019.

І.П. Каменева

АНАЛІЗРЕЗИЛЬЄНТНОСТІСОЦІАЛЬНИХ СТРУКТУР ВУМОВАХ ВІЙНИ ТА ЕНЕРГЕТИЧНОЇ КРИЗИ

Вступ. Нагадаємо, що термін «резильєнтність» походить від англійської resilience, що перекладається як «стійкість». В фізиці це означає здатність пружних тіл відновлювати свою форму після механічної дії.

Вже в минулому сторіччі цей термін досить активно застосовували в психології та медицині, де резильєнтність визначали як здатність людини протистояти складним життєвим обставинам та знаходити ресурси для відновлення після стресових подій або важких втрат [1]. Загалом,в своєму первинному значенні резильєнтність визначили як сукупність притаманних суб'єкту якостей, які допомагають долати стреси та екстремальні умови конструктивним шляхом. Пізніше цей термін почали також використовувати для аналізу проблем в сфері політики, бізнесу та економіки. Зокрема, резильєнтність економіки країни – це її здатність адаптуватися до нових умов та швидко відновлюватися після криз та екстремальних подій.

Рисунок 1. – Сумні наслідки руйнування інфраструктури

На жаль, в Україні вкрай важкий і турбулентний період продовжується вже кілька років, що вимагає від управлінських структур, соціальних органів та всіх верств населення особливої стійкості та ефективних механізмів адаптації до складних умов. Зокрема, наслідки руйнування важливих енергетичних підприємств та критичний стан інфраструктури в цілому потребують як оптимального перерозподілу енергетичних ресурсів, так і пошуку нових джерел для підтримки енергопостачання окремих регіонів.

Отже, серед найбільш актуальних задач щодо аналізу і підвищення резильєнтності на соціальному рівні в умовах війни та енергетичної кризи необхідно відзначитиоцінювання та прогнозування стійкості соціальних структур до актуальних загроз і руйнацій, ідентифікаціюкритичних параметрів в межах окремих регіонів, визначення адаптаційних можливостейна системному рівні в цілому тадослідження механізмів резильєнтності для окремих (більш вразливих) категорій населення.

Особливості резильєнтностісоціально-природних систем.

Резильєнтність починається з розуміння гібридних загроз, які постійно змінюють свої параметри. Відтак, для країни як цивілізаційного суб'єкта та суб'єкта міжнародних відносин одночасно потрібна динамічна ідентифікація потенційних гібридних ризиків, які обчислюютьсяна основі всебічного вивчення зовнішнього та внутрішнього середовища[2]. Якщо національна безпека – це стан захищеності ідентичності держави, її права на існування, реалізації її національних інтересів, то резильєнтність можна розглядати як доволі ефективну стратегію та основу національної безпеки.

Соціально-політична й правова резильєнтність передбачає аналіз й нейтралізацію викликів і загроз в контексті розвитку внутрішньої політики, взаємодії державних структур і громадянського суспільства, а також правової та правоохоронної систем, їх місця в міжнародно-правовій архітектурі.

Отже, випередження й нейтралізація на ранніх етапах стає своєрідною профілактикою серйозних наслідків, що ведуть до деформації цивілізаційної суб'єктності. Така профілактика є значно менш затратною, ніж подальше відновлення. Іншими словами, якщо ми припустимо, що національна безпека держави є необхідним мінімумом цивілізаційної суб'єктності, то національна резильєнтність сьогодні є одним з найкращих її каталізаторів[2].

В країнах з високим рівнем екологічної культури слід відзначити поширення досліджень резильєнтності на рівні соціосистем (соціально-природних систем), тобто комплексних утворень, де людська спільнота розглядається як невід'ємна частина природи. Відповідно, актуальності набули концепції, що пов'язують воєдино соціальні та екологічні системи, демоделюються соціальні механізми забезпечення резильєнтності для даного типу комплексних систем в цілому [3, 4].

Підкреслимо, що поняття *резильєнтності* на соціальному рівні включає додаткові можливості для переходу на інші режими функціонуваннявсієї структури в цілому та окремих її частин для забезпечення основних потреб населення, удосконалення існуючих та створення нових засобів підтримки життєздатності соціальних систем на регіональному та локальному рівні.

Забезпеченнярезильєнтностіпередбачаєбільш широкі можливості для виживання та відновлення соціальних і природних систем після ворожих атак та руйнувань. З позицій математичного моделювання цеможна визначити як здатність системи та її окремих частин за рахунок певних механізмів та засобів

підтримувати стан рівноваги (тобтобаланс і взаємодію основних складових) на відповідному рівні для даного діапазону значень.

Адаптаціядо нових умов включає особливий механізм пристосування, або налаштування, що забезпечує соціальній системі певну стабільність щодо впливу негативних змін зовнішнього середовища. Якщо відомі певні тенденції щодо зміни середовища, то засоби моделювання допомагають передбачити тенденції у зміні параметрів системи в цілому[5]. Її динаміка обмежена«коридором» значень, що відповідають зовнішнім впливам.

Зокрема, для дослідження процесу адаптації регіональної енергетичної системи заумов постійних загроз івисокого ризику необхідно визначити значення параметрів, які відповідаютьмаксимально можливимрівням навантажень(із врахуванняматок та значних пошкоджень).

В межах окремого регіону управлінські структури мають відповідати за забезпечення гнучкого балансускладових енергосистеми, тобтооперативновизначати ефективний розподіл енергетичних ресурсів (згідно значенням основних параметрів)для підтримки енергопостачання, тепла та інших життєво необхідних умов населення.

Для аналізу та прогнозуваннярезильєнтності окремих складових енергосистеми на регіональному або локальному рівні можна адаптувати імовірнісні моделі подання знань, розроблені для задач екологічної безпеки (зокрема, задач прогнозування рівня забруднення повітря) [6].

Психологічні та індивідуальні аспекти резильєнтності

В умовах війни, постійних загроз, вибухів, руйнувань такритичних обмежень щодо елементарних норм енергопостачання, відключення світла, води та інших комунальних послуг особливої уваги потребує підтримка психологічного стану окремих категорій населення, врахування особливостей індивідуального сприйняття загроз та ризиків.

Отже, серед механізмів індивідуальної та соціальної адаптації в умовах екстремальнихнавантажень необхідно враховувати психоемоційний стан населення, яке вже тривалий час не може повернутись до нормального життя.Зрозуміло, що під тиском таких обставинпереважна більшість населення відчуває тривожність і дискомфорт, що ведуть до психічних зривів, хвороб серця, інсультів або інших негативних наслідків. Відомо, що в екстремальних умовах на основізакладених програм виживання формуються індивідуальні адаптивні програми, зумовлені особливостями реактивності організму.

На психофізіологічному рівні визначено дві протилежні стратегії взаємодії організму із середовищем: стратегія відкритості (синтаксичні процеси) та стратегія закритості (кататоксичні процеси). Синтаксична система є основою збереження та розвитку організму в несприятливих умовах середовища. До неї належать механізми взаємодії з вірусними, бактеріальними, токсичними та іншими факторами.При занадто високих навантаженнях включаються механізми закритості, тобто виведення, нейтралізація негативних агентів тощо. Клітинний імунітет можна вважати

еволюційно вимушеним механізмом, що виник під впливом *синтаксичних* стратегій. На жаль, збільшення ступеня закритості призводить до зниження зовнішньої роботи організму та подальшого його виснаження (так званої адаптації через захворювання), що потребує термінової допомоги.

Щоб вчасно запобігти збільшенню негативних наслідків для фізичного та психічного здоров'я людей, які найбільше постраждали від екстремальних умов, потрібна кваліфікованадопомога фахівців та ефективна психологічна підтримка найбільш вразливих верств населення.

В останні роки збільшилась кількість публікацій в галузі психології та медицини, де досліджується стійкість та резильентністьлюдини в умовах високого стресу, воєнного станута невизначеності [7, 8 тощо]. Зокрема, в монографії [8] наведено засоби оцінювання життєстійкості і резильєнтності людини в сучасних умовах. На основікількісних показників побудованошкали життєстійкості для окремих категорій населення.

Важливим напрямком подальших досліджень залишається набуття досвіду адаптації до екстремальних умов, його систематизація для подолання енергетичної кризи та відновлення нормального життя. Адже унікальність і цінність досвіду, набутого в роки війни в Україні, важко переоцінити [9].

1. Мельничук І.Я. Теоретико-методологічні основи розвитку та корекції резильєнтності. №2 (2024) Наукові записки. Серія: Психологія https://journals.cusu.in.ua/index.php/psychology/article/view/469.

2. Божок Є. Резильєнтність: Стратегія виживання в умовах гібридних загроз https://www.ukrinform.ua/rubric-society/3265105-rezilentnist-strategia-vizivanna-v-umovah-gibridnih-zagroz.html.

3. Волошина О. В. Резильєнтність соціальних систем в кризових станахВісник Національного університету оборони України 4 (74) /2023.

4. «Resilience Alliance». URL: https://www.resalliance.org/glossary.

5. Nikolis, G., Prigogine, I. Exploring complexity: An introduction. W.H. Freeman and Company, New York, 1989. – 328 c.

6. Каменева І.П., Артемчук В.О., Яцишин А.В, Владимирський О.А. Імовірнісні моделі подання знань для підтримки прийняття рішень в умовах ризику та невизначеності на прикладі галузі охорони атмосферного повітря // Електронне моделювання, 2024, 46, № 1, с. 3–20.

7. Стівен М. Саутвік, ДеннісС. Чарні, ДжонатанМ. Резилієнтність: мистецтво долати найбільші виклики життя. Виданнят ретє. «Манускрипт», Львів, 2024. – 44 с.

8. Кокун О. М. Життєстійкість і резильєнтність людини в сучасному світі: теорія, дослідження, практика : монографія. Київ : Інститут психології імені Г. С. Костюка НАПН України, 2025. – 214 с.

9. Кузьма Наталія Як українці вибудували власні стратегії виживання, Високий замок, Львів, 25.09.2025.

https://wz.lviv.ua/statti/539819-innovatsii-u-roboti-z-ptsr-ukrainskyi-dosvid-syly-iakyi-vyvchaie-svit.

А.О. Лєпатьєв

РОЗРОБКА КОНСТРУКТОРА ТРЕНАЖЕРНИХ ЗАНЯТЬ ДЛЯ ОПЕРАТИВНОГО ПЕРСОНАЛУ ПІДПРИЄМСТВ РОЗПОДІЛЬЧИХ МЕРЕЖ ЗА ДОПОМОГОЮ ІНСТРУМЕНТУ UNITY

Unity – інструмент для розробки застосунків і відеоігор. Інструмент дозволяє завантажувати користувальницькі медіафайли (зображення, звуки і тощо) що дозволяє використовувати Unity для багатьох цілей, включно з розробкою конструктора тренажерних занять в області енергетики. Щоб почати розробку конструктора, потрібно створити новий проєкт[1]. Проєкт тренажера складається з сцен, ігрових об'єктів, скриптів. У тренажері сцени — це приміщення енергетичних мереж, панелі й інші компоненти мережі. Ігрові об'єкти — це основні об'єкти Unity, що представляють елементи користувацького, програмного та апаратного інтерфейсу. За замовчуванням ігрові об'єкти не мають жодних властивостей; властивості об'єктів налаштовуються в проєкті Unity.

Скрипт - файл із програмним кодом, який можна прив'язати до проєкту, сцени та ігрового об'єкта. Наприклад, скрипт переходу між приміщеннями й об'єктами, який прив'язується до кнопок навігації. Візуальний вигляд сцен та ігрових об'єктів визначає розробник через завантаження файлу зображення у проєкт Unity. Наприклад, фотографію приміщення мережі можна завантажити у проєкт Unity, і вона слугуватиме заднім фоном сцени. Для відображення зміни вимикача завантажуються дві фотографії вимикача у двох різних станах (увімкнено та вимкнено); при натисканні на них під час тренування змінюється їхній візуальний вигляд.

Для відображення зміни значення режиму мережі використовуються скрипти, які прив'язуються до вимикачів та роз'єднувачів, а також до об'єктів відображення значення режиму (амперметр, вольтметр, тощо). Наприклад, скрипт, який реагує на стан вимикачів та перемикачів і залежно від станів змінює положення стрілки об'єкта відображення режиму. Дані щодо значень режиму мережі можна розрахувати за допомогою моделі розрахунку режиму. Модель розрахунку режиму розраховується за допомогою скрипт файлу, який знаходиться усередині проекту. В середині скрипт файлу знаходиться програмний код, який розраховує напругу та струму у мережі. Скрипт виконується при запуску моделі, а також значення перераховується при зміні режиму. Також зміну режиму можна відобразити через метод повноформатних графічних зрізів. Зріз являє собою набір масиву графічних компонентів, масиву станів комутаційних компонентів (вимикачі, роз'єднувачі) та масиву значень режиму. Графічні компоненти містять зображення об'єктів і приміщень, які присутні в мережі.

1. Unity: Develop, Deploy, and Grow | The World's Leading Game Engine. (б. д.). Unity. https://unity.com.

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

COMPREHENSIVE TRANSFORMATION OF MANAGED TELECOMMUNICATION SERVICES THROUGH THE INTEGRATION OF ARTIFICIAL INTELLIGENCE ALGORITHMS

The main goal of this work is the fundamental transformation of Managed Telecommunication Services in order to provide a higher level of operational efficiency, better quality of the services provided and improved customer experience. This is achieved by means of the systematic identification of factors with negative impact and their relevant assessment, through the incorporation of a structured approach based on methods derived from productivity improvement and the application of Quality Management principles. In this sense, the main contribution of this investigation refers to the elaboration of a new organizational model aligned with the international [1].

Artificial Intelligence (AI) is no longer an evolution of technology in this globalized era of business and therefore must be considered as a revolution. In the era of communication, telecommunication networks and towers are at the heart of communication. These networks require effective management in order to provide a quality experience to the customers. With the explosion of data in our networks, they cannot be managed reactively; infrastructure management cannot afford to have any down time. Thus, the aim of this research is to validate the implementation of AI in telecommunication managed services through a holistic approach combining Predictive Maintenance, Network Planning, Incident Management and Resource Provisioning.

Several studies have been conducted to investigate the researches that are related to the AI in the context of the digital transformation of telecommunication sector. However, little work has been done to investigate the synergetic effects of the different AI applications such as fault prediction and traffic routing in the context of unified managed services (UMS) [2]. In fact, most of existing works are focused on the technical aspect, while there is a need for a holistic approach that evaluates the degree of digital transformation and its impact on KPIs.

The proposed paper presents a method for integrating condition monitoring based maintenance decision making tools. The proposed method involves a loop process starting from data audit and preparation stage. It requires reliable maintenance records, network performance data and incident reports. The data has to be validated, normalized and cleaned to be available in a reliable database. Finally, the model development stage recommends the application of Random Forests for predictive maintenance using the historical condition monitoring data and LSTM networks for forecasting the future values in the time series data of the network elements.

In the most general mathematical sense [3], the hardware node reliability gain provided by predictive maintenance algorithms can be characterized by an optimal availability factor.

$$A_{opt} = \frac{MTBF + \Delta T_{ai}}{(MTBF + \Delta T_{ai}) + (MTTR - \Delta t_{res})}, \quad (1)$$

The factors A opt, *MTBF*, ΔT_{ai}, *MTTR* and Δt_{res} are defined as: A_{opt} – optimized equipment availability factor MTBF – mean time between failures ΔTai – additional uptime gained by using the AI forecasting *MTTR* – mean time to recovery Δt_{res} – time saved by using automated incident detection.

In conclusion, the use of AI in telecommunication managed services is no longer a technological issue, but rather a business decision. Through the results obtained, it is possible to validate the statements presented in the introduction. As a result, telecommunication infrastructure providers have moved from the traditional reactive mode of service management to a more proactive approach. The proposed AI-based tools and techniques contribute to a significant reduction in the role of human intervention in the management of network failures while reducing operational costs and improving the level of service quality in line with the requirements of the digital era.

1. Prihatmanto, A. S., Sukoco, A., Santoso, E., Susilo, E., Adriansyah, A., Jokonowoft, B., & Budiyono, A. (2023). Unlocking Transformation: AI Implementation for Enhanced Telecommunication Managed Services. Journal of Instrumentation, Automation, and Systems, 10(2), 68-76.

2. Bakhtiiarov D., et al. Distribute load among concurrent servers // CEUR Workshop Proceedings. 2024. Vol. 3826. P. 260–266.

3. O. Solomentsev, et al., A Procedure for Failures Diagnostics of Aviation Radio Equipment, Proceedings - International Conference on Advanced Computer Information Technologies, ACIT (2023) 100–103. doi: 10.1109/ACIT58437.2023.10275337.

4. Kotyk, B., Bakhtiiarov D., et al. (2025). Neural network approach to 5G digital modulation recognition. CEUR Workshop Proceedings, 3925, 82-92.

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

DYNAMIC PERFORMANCE OPTIMIZATION OF TELECOMMUNICATION NETWORKS BASED ON REINFORCEMENT LEARNING AND GENETIC ALGORITHMS

The dynamic performance optimization of telecommunication networks is one of the key problems to be solved in the next generation networks. Network performance optimization is generally implemented by adjusting some control variables such as transmission power, bit rate, transmission route, etc in a pre-designed scope based on previous experience in practice. The variables to be adjusted are generally limited and fixed, and the adjustment range is also limited [1].

The digital world is changing at a speed that is unparalleled in history and so are the 5G standards. The requirements of flexibility and bandwidth on telecom infrastructure have never been higher. The static settings on the tower level have already been exhausted [2]. This calls for implementation of more dynamic solutions to handle the heterogeneous nature of today's traffic and the unpredictable variations in required bandwidth. In this paper, we propose to use Artificial Intelligence (AI) techniques, particularly reinforcement learning and genetic algorithms, to achieve dynamic load balancing and resource management in telecom towers.

In the previous section we started to describe the approach to develop the intelligent system. In this section we will continue that description. The first step in this approach is an audit to the telecommunications infrastructure. In the next stage, the data obtained from the switches and base stations has to be cleaned, transformed and normalized in what is called the data pre-processing stage, so that the data is in a format that can be worked with in the stage of machine learning to develop the models for the optimization of the network infrastructure. For this stage the models for the optimization of the network infrastructure will be based on Reinforcement Learning (RL) algorithms [3]. The basic idea of this type of architecture is based on a software agent that acts in the network environment and through a process of trial and error, it achieves the desired performance through instant feedback in the form of a reward that is given after each action, and in this context, this reward is always related to the performance of the network [4].

The expected reward function of the AI agent during channel bandwidth optimization can be written as: where denotes the minimum throughput required for each user, denotes the maximum number of users that can be supported over the whole network, and denotes the transmission bandwidth assigned [5]:

$$J(\theta) = \mathbb{E}_{\pi_\theta}\left[\sum_{t=0}^{T} \gamma^t R(s_t, a_t)\right], \quad (1)$$

The objective function for the policy is given by: $J(\theta)$, γ, $R(s_t, a_t)$ where $J(\theta)$ is the objective function of the parameterized policy θ, γ is the discount factor, and $R(s_t, a_t)$ is the reward function which aims to minimize latency and maximize the number of transmitted packets in state s_t under action a_t.

The validity of the developed models will be verified within the framework of the stress-testing phase for maximum load and different topologies. The models and tools will be connected to current systems by implementing the corresponding APIs and by synchronization of real-time data.

Our test trials and analysis of real-world networks also confirm the success of our solution. In our implementation, the algorithm that manages the parameters of the networks is based on the current traffic and user behavior. Our measurements showed an improvement of 15% in network performance indicators, such as throughput, which translates into faster speeds and greater network stability and therefore reduced peak hour congestion. Network administrators will no longer have to spend most of their time patrolling the networks in search of failures and will be able to dedicate themselves to expanding the infrastructure [6].

The use of self-learning optimization algorithms enables the migration from manual setup to Self-Organizing Networks (SONs). As a result, it is possible to achieve better quality of service and a more reliable network architecture that can manage surprising peak loads in the traffic.

1. Kotyk, B., Bakhtiiarov D., et al. (2025). Neural network approach to 5G digital modulation recognition under a priory uncertainty of parameters. CEUR Workshop Proceedings, 4024, 119–132.

2. R. Odarchenko, V. Pevnev, A. Pinchuk, O. Polihenko, Optimization of the integrated video surveillance system with elements of data analysis, CEUR Workshop Proceedings 3925 (2025) 47–63.

3. M. Abdollahi, R. Sabzalizadeh, S. Javadinia, S. Mashhadi, S. S. Mehrizi, A. Baniasadi, Automatic modulation classification for nlos 5g signals with deep learning approaches, in: Proceedings of the 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, Istanbul, Turkiye, 2023, pp. 1–6.

4. K. S. Mayer, C. Müller, J. A. Soares, F. C. C. de Castro, D. S. Arantes, Deep phase-transmittance rbf neural network for beamforming with multiple users, IEEE Wireless Communications Letters 11 (2022) 1498–1502.

5. M. Zaliskyi, et al., Model building for diagnostic variables during aviation equipment maintenance, in: International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 2022, pp. 160–164.

6. B. Kotyk, D. Bakhtiiarov, O. Lavrynenko, B. Chumachenko, V. Antonov, V. Fesenko, V. Chupryn, Neural network approach to 5g digital modulation recognition, in: Proceedings of the Workshop on Cyber Hygiene Conflict Management in Global Information Networks, volume 3925 of CEUR Workshop Proceedings, 2025, pp. 82–92.

V.V. Telnykh, D.I. Bakhtiiarov, B.P. Kotyk

AUTOMATION OF INCIDENT DETECTION AND CLASSIFICATION IN MANAGED TELECOMMUNICATION SERVICES INFRASTRUCTURE

Network management is mission critical for managed service providers. Managing telecommunication system incidents is a time-consuming task, requiring a lot of log file and ticket analysis before the root cause of an incident can be identified and the incident escalated. With the increasing complexity of networks, traditional incident routing practices have led to longer mean time to recovery and a poorer customer experience. This paper discusses the integration of Artificial Intelligence (AI) in the form of Convolutional Neural Networks (CNNs) into network management layer to automatically and in real-time discover telecommunication system incidents, classify them and send notifications to stakeholders [1, 3, 7].

The automation of the incident management process is only possible if the historical log data, network outage reports and security audit records are integrated. The process involves the vectorisation of the incident descriptions, feature engineering in order to train the neural network and to discover the connections between the variables [2]. The classification process is implemented through the AI-based system, using the features extracted from the data by the CNNs. The classifier manages to identify the type of incident (hardware failure, software bug on the base station or attack from external sources to the network defence systems) [3, 4].

Efficiency gained by the automated incident triage system can be modeled by reducing the Mean Time To Recovery (MTTR).

$$MTTR_{opt} = \sum_{i=1}^{N} P(I_i) \left[\Delta t_{AI}^{detect}(I_i) + \Delta t_{AI}^{triage}(I_i) + t_{human}^{repair}(I_i) \right], \quad (1)$$

where $P(I_i)$ is the probability of an incident of type i occurring; Δt_{AI}^{detect} and Δt_{AI}^{triage} denote the time expended by AI on automated detection and routing (which approaches zero relative to human processing); and t_{human}^{repair} is the actual time required to physically or software repair.

Initial results from lab tests and field case studies show that Smart CMMS solutions lead to a productivity gain in the maintenance service activities in a much greater extent than what is achieved using conventional CMMS systems. The accuracy of failure type detection in the Smart CMMS system has reached an accuracy of over 90% in a wide range of scenarios [1, 3, 6]. The operational analysis of three real scenarios, which correspond to three different maintenance service interventions carried out by the maintenance staff of a large Spanish

distributor, show that the total time to attend to each failure has been reduced by 40% thanks to the almost instantaneous and automatic detection and escalation of the failure that needs to be attended to, thereby bypassing the time and effort required for the maintenance staff to manually decide which type of intervention is needed (triage).

Rapid incident processing is not the main use case for AI in telecommunication operations, but the technology has proven to be very effective for the root cause analysis of recurring problems in the network. Instead of being flooded with the same type of problems, again and again, the operator can now proactively act. An intelligent incident processing system that is incorporated into a managed telecommunication service will lead to operational cost reductions.

1. Kotyk, B., Bakhtiiarov D., et al. (2025). Neural network approach to 5G digital modulation recognition under a priory uncertainty of parameters. CEUR Workshop Proceedings, 4024, 119–132.
2. N. Yehorov, M. Zaliskyi, B. Chumachenko, D. Bakhtiiarov, A method for deterministic signal detection on the background of noise based on the neural network, in: Proceedings of the 2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek), IEEE, Kharkiv, Ukraine, 2024, pp. 1–6. doi:10.1109/KhPIWeek61434.2024.10878073.
3. Bakhtiiarov D., et al. Distribute load among concurrent servers // CEUR Workshop Proceedings. 2024. Vol. 3826. P. 260–266.
4. R. Odarchenko, A. Pinchuk, O. Polihenko, A. Skurativskyi, A comparative analysis of cyber threat intelligence models, CEUR Workshop Proceedings 3925 (2025) 3–12. URL: https://ceur-ws.org/ Vol-3925/paper01.pdf.
5. P. Sadhukhan, J. Bhaumik, Automatic modulation classification using convolutional neural network with batch normalization: A novel approach, in: Proceedings of the 2024 4th International Conference on Computer, Communication, Control & Information Technology (C3IT), IEEE, Hooghly, India, 2024, pp. 1–4. doi:10.1109/C3IT60531.2024.10829439.
6. B. Kotyk, D. Bakhtiiarov, O. Lavrynenko, B. Chumachenko, V. Antonov, V. Fesenko, V. Chupryn, Neural network approach to 5g digital modulation recognition, in: Proceedings of the Workshop on Cyber Hygiene Conflict Management in Global Information Networks, volume 3925 of CEUR Workshop Proceedings, 2025, pp. 82–92.
7. M. Zaliskyi, Y. Petrova, M. Asanov, E. Bekirov, Statistical data processing during wind generators operation, International Journal of Electrical and Electronic Engineering and Telecommunications 8 (2019) 33–38. doi:10.18178/ijeetc.8.1.33-38.

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

ФОРМАЛІЗАЦІЯ КІБЕРНЕТИЧНОЇ СКЛАДОВОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ШЛЯХ ЗАБЕЗПЕЧЕННЯ РЕЗИЛІЄНТНОСТІ

Поточний рівень розвитку методологічної складової формальних методів і супутніх засобів, у тому числі інструментальних засобів автоматизації процесу верифікації і синтезу формалізованих подань – формальних специфікацій (ФС) [1], є достатнім для їх результативного застосування у контексті численних критичних сфер діяльності сучасного суспільства на індустріальному рівні [2]. Показовою при цьому є сфера атомної енергетики Фінляндії, де методи перевірки на моделі (Model Checking) і супутні засоби автоматизації було успішно застосовано у якості засобів контролю розроблюваного критичного програмно-алгоритмічного забезпечення (ПАЗ) за показником несуперечливості [3].

У частині критичних сфер застосування комп'ютерних систем, у тому числі у рамках вирішення актуальних задач енергетики, що постають у кібернетичній площині, визначального значення набуває аспект усунення небажаного впливу людського фактору, також у процесі розроблення ПАЗ означених систем. Стосовно названого процесу, у контексті розгляду критичної енергетичної інфраструктури у межах кібернетичної складової, пропонується стримувати вказаний вплив шляхом залучення формальних методів і супутніх засобів, включно із засобами автоматизації, у якості інструментів контролю ПАЗ за показником несуперечливості вже на етапі проєктування у складі етапів процесу розроблення ПАЗ.

Формалізацію пропонується розглядати як шлях забезпечення уніфікованої і однозначної інтерпретації змістового навантаження артефактів, створюваних і застосовуваних розробниками ПАЗ на етапі проєктування. У якості означених артефактів погоджено опрацьовувати блок-схеми алгоритмів, UML-діаграми дій, станів (Unified Modeling Language) [4].

У якості засобів формалізації пропонується використовувати такі, що базуються на основі математичного апарату темпоральної логіки дій TLA (Temporal Logic of Actions), представленої лауреатом премії Тюрінга Л. Лемпортом (Leslie Lamport) [5]. При цьому до обігу залучається концепція «абстрактної програми» (abstract program), формою подання якої є ФС на основі виразних засобів математично строгого модульного формалізму TLA+ [6]. Означена і супутні концепції (дій, поведінок) застосовуються у процесі синтезу і аналізу ФС при проєктуванні ПАЗ, у тому числі при вирішенні актуальних задач енергетики, до складу яких входить проведення автоматизованого контролю несуперечливості ПАЗ, базуючись на формальних методах і супутніх засобах [7].

Специфіка поточного деструктивного впливу на енергетичну інфраструктуру держави, обумовленого неспровокованим триваючим

повномасштабним вторгненням, постає, у тому числі, у комплексності такого впливу, що полягає в охопленні обох основоположних концептуальних площин енергетичної інфраструктури – і кібернетичної, і фізичної – при розгляді означеної інфраструктури як кіберфізичної системи [8].

Результати проведеного аналізу підходів до забезпечення резилієнтності критичної енергетичної інфраструктури показали, що визначальним чинником впливу на резилієнтність системи є, зокрема, відповідна архітектурна складова (структура та зв'язки між компонентами структури) [9]. Даний висновок охоплює і архітектурну складову у частині ПАЗ.

Пропонується закладати основи забезпечення резилієнтності критичної енергетичної інфраструктури як кіберфізичної системи у частині опрацювання відповідного ПАЗ вже на етапі проєктування процесу розроблення шляхом комплексного залучення формальних методів і засобів, що базуються на основі темпоральної логіки дій TLA. При цьому постає ефект експоненційного зростання просторів станів систем переходів, що будуються і використовуються у процесі автоматизованої формальної верифікації методом перевірки на моделі в автоматизованому режимі [10]. Даний ефект проявляється у площинах і обчислювальних, і просторових витрат, супутніх процесу формальної верифікації методом перевірки на моделі, застосовуваним до ФС [11]. Зменшувати небажаний вплив означеного ефекту пропонується шляхом проведення стратифікації складових ФС і варіювання рівня деталізації ФС за рахунок вибіркового опрацювання шляхів (поведінок) у межах граф-подань систем переходів у процесі проведення формальної верифікації на основі методу перевірки на моделі TLC (TLA Checker). Характер вибірки шляхів, призначених для опрацювання, при цьому окреслюється значенням відповідного показника, яке задається розробником ПАЗ з урахуванням, у тому числі, комплексності ПАЗ, попереднього досвіду, обчислювальних і просторових ресурсів наявної обчислювальної системи [12].

Дослідження проведено у рамках вирішення задач наступних науково-дослідних робіт, виконуваних в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: НДР № 0125U000326 «Розвинення теоретичних засад формалізації подань процесів опрацювання оперативної інформації в енергетиці» (2025–2029 рр.); 0125U002837 «Розвинення теоретичних засад забезпечення резильєнтності критичної енергетичної інфраструктури» (2025–2026 рр.); «Методи та засоби управління інформаційними активами об'єктів критичної інфраструктури як основа забезпечення їх кібербезпеки» (Гранти НАН України дослідницьким лабораторіям/групам молодих вчених НАН України для проведення досліджень за пріоритетними напрямами розвитку науки і техніки 2026–2027 рр.); у рамках наукової роботи «Методологія та інструментарій формальної перевірки несуперечливості артефактів проєктування критичних систем», поданої на конкурс на призначення іменних стипендій Верховної Ради України імені Бориса Патона для молодих учених – докторів наук на 2026 рік.

1. Шкарупило, В. В. & Душеба, В. В. (2024). *Комп'ютерна програма «Програмний комплекс засобів автоматизації процесу синтезу і опрацювання формальних специфікацій» («ФОРМ-TLA»)*. (Свідоцтво про реєстрацію авторського права на твір № 131670). Український національний офіс інтелектуальної власності та інновацій (УКРНОІВІ). https://sis.nipo.gov.ua/uk/search/detail/1839768/.

2. Clarke, E. M., Grumberg, O., Kroening, D., Peled, D., & Veith, H. (2018). *Model checking: 2nd ed*. The MIT Press.

3. Pakonen, A., Buzhinsky, I., & Vyatkin, V. (2024). Evaluation of visual property specification languages based on practical model-checking experience, *Journal of Systems and Software*, 216. https://doi.org/10.1016/j.jss.2024.112153.

4. Shkarupylo, V., Blinov, I., Dusheba, V., & Alsayaydeh, J. A. J. (2023). Case driven TLC model checker analysis in energy scenario. *CEUR Workshop Proceedings*, 3392, 65–75. https://doi.org/10.32782/cmis/3392-6.

5. Lamport, L. (2002). *Specifying systems: The TLA+ language and tools for hardware and software engineers*. Addison-Wesley Longman Publishing Co., Inc.

6. Lamport, L. (2026). *A science of concurrent programs*. Cambridge University Press.

7. Shkarupylo, V. V., Blinov, I. V., Chemeris, A. A., Dusheba, V. V., & Alsayaydeh, J. A. J. (2022). On applicability of model checking technique in power systems and electric power industry. In: A. Zaporozhets (Eds.), *Systems, Decision and Control in Energy III. Studies in Systems, Decision and Control* (pp. 3–21), 399. Springer, Cham. https://doi.org/10.1007/978-3-030-87675-3_1.

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

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

10. Шкарупило, В. В., Чемерис, О. А., & Душеба, В. В. (2020). Оцінювання просторової складності задачі формальної верифікації, вирішуваної методом перевірки на моделі. *Вчені записки Таврійського національного університету імені В.І. Вернадського, серія «Технічні науки»*, 31(70), 5, 147–151. https://doi.org/10.32838/2663-5941/2020.5/24.

11. Shkarupylo, V. V., Tomičić, I., Kasian, K. M., & Alsayaydeh, J. A. J. (2018). An approach to increase the effectiveness of TLC verification with respect to the concurrent structure of TLA+ specification. *International Journal of Software Engineering and Computer Systems*, 4(1), 48–60. https://doi.org/10.15282/ijsecs.4.1.2018.4.0037.

12. 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. 1–4). https://doi.org/10.1109/IDAACS68557.2025.11322075.

.

M. Gardus

THE POLITICAL ECONOMY OF RUSSIA'S SHADOW TANKER FLEET: THE ROLE OF INDIVIDUAL COUNTRIES IN CIRCUMVENTING OIL SANCTIONS

Since 2022, restrictions on seaborne oil exports from the Russian Federation have been based on a combination of the European Union's embargo and a price cap mechanism, which permits the provision of maritime services for Russian oil only if it is sold at or below the limit.

In response, a parallel transport infrastructure has emerged – a 'shadow' fleet of ageing tankers with opaque ownership, 'flags of convenience', alternative insurance and practices to conceal the movement and origin of cargo (STS transhipments, AIS anomalies).

The paradox lies in the fact that a significant portion of 'Western' tonnage and maritime services has historically been concentrated in EU shipping centres – notably in Greece, Cyprus and Malta – that is, in jurisdictions which simultaneously formulate sanctions rules and have economic interests in the maritime industry.

What is the role of these countries?

Firstly, a structural role in global shipping. Greek shipowners own the largest tanker fleet in the world. Even after sanctions were imposed, some of the vessels transporting Russian oil are linked to Greek companies or were sold through Greek brokers to older vessels, which then became part of the shadow fleet. This does not constitute a direct breach of sanctions, but it shows that it is through this market that a reserve of older tankers has been established.

Secondly, the role of flag states. Malta and Cyprus are among the largest ship registries in the EU. Some of the tankers that subsequently ended up in the 'shadow fleet' previously sailed under their flags, and before becoming involved in the schemes, changed their registration to Panama, Liberia or other open registries. In other words, they act more as a hub in the global system of ship registration and resale.

Thirdly, the political stance of these countries within the EU. During discussions on sanctions against Russian oil in 2022, it was Greece, Malta and Cyprus that insisted on exemptions for shipping. Ultimately, this led to the introduction of a price cap mechanism, which allows the transport of Russian oil provided it is sold below the set price.

Fourthly, maritime services. Part of the critical infrastructure – ship management, brokerage services, insurance, technical management – has also historically been concentrated in Greece and Cyprus. Even when a vessel changes flag or owner, such services may remain within European jurisdiction.

The European Commission's official guidelines detail attestations along the supply chain, record-keeping requirements and the risk of 'price masking' through freight/insurance and other ancillary costs [1]. The Updated Advisory Price Cap

Coalition identifies risk indicators: opaque corporate structures, frequent changes of ownership/flag, STS operations, AIS anomalies and problematic insurance [2].

Institutional reviews (notably the European Parliamentary Research Service [3], EPRS) systematise typical evasion tactics and highlight that Malta is mentioned among the 'top flags' for shadow tankers, and that the presence of vessels flying EU flags creates an internal regulatory challenge.

The empirical data (flags, STS incidents, assessment of the shadow segment) is supplemented by the Kyiv School of Economics Institute (KSE Institute) [4].

The political-economic 'money trail' is reflected in the OCCRP investigation into the sale of old tankers and the role of shell intermediaries [5].

The analytical framework is based on the premise that sanctions create a 'circumvention market': the difference between compliant logistics and sanctions-risky logistics generates a rent ('sanctions premium') that private actors seek to monetise.

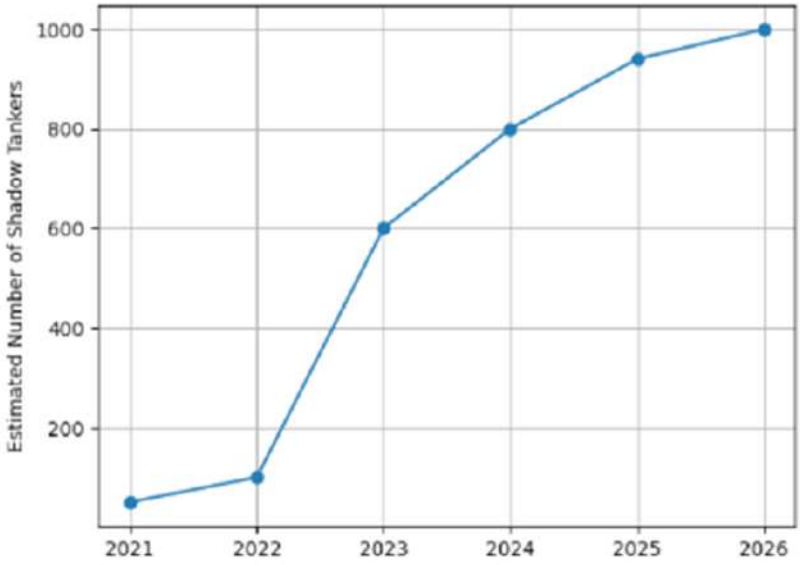
Table 1. Main mechanisms used by Russia to circumvent oil sanctions

Mechanism	Description of the scheme	Main participants	Consequences
Shadow fleet	Use of aging tankers operating without Western insurance or services	Russia, UAE, India, China	Makes enforcement and monitoring of sanctions more difficult
Ship-to-ship transfer	Transfer of oil between vessels at sea to obscure cargo origin	Private traders	Conceals the origin of oil
Flag switching	Frequent re-registration of vessels under different flags	Panama, Liberia, Marshall Islands	Complicates vessel tracking
Alternative insurance	Insurance provided outside the G7 insurance system	Russian and Asian insurers	Circumvention of the oil price cap

In a fragmented maritime governance framework (flag/port/coastal states plus private insurance and classification societies), regulatory arbitrage arises: actors choose jurisdictions and contractual arrangements that minimise oversight and liability.

In such a system, the state can simultaneously act as a regulator of sanctions and a beneficiary of maritime sector revenues, which explains the political complexity of strict enforcement.

Mechanisms of the shadow fleet's operation



Shadow logistics is reproduced through a combination of six mechanisms.

Figure 1. – Estimated Growth of Russia's Shadow Tanker Fleet (2021–2026)

Firstly, **ownership structures**: multi-tiered ownership/management chains and 'single vessel' companies conceal the ultimate beneficiary and obscure accountability.

Secondly, **flag hopping** as a means of evading compliance; in the KSE Institute's tracking, Panama, Gabon and the Cook Islands are cited as the top flags for crude oil.

Thirdly, **STS transhipments** as a means of obscuring or 'breaking' the documented origin and chain of control; the findings of LEG 110 of the International Maritime Organisation highlight the high risk posed by STS operations on the high seas to safety and liability regimes.

Fourthly, **AIS manipulation** (switching off/spoofing) to reduce the transparency of voyages.

Fifth, **insurance and service 'divergence'** from traditional compliance frameworks (alternative insurers, non-transparent certificates).

Sixthly, **the secondary market for old tonnage** as an economic 'gateway' to the shadow fleet: OCCRP has documented at least $6.3 billion in revenue for Western shipowners from the sale of hundreds of old tankers to shell companies, after which the vessels entered the 'shadow' circuit; a significant proportion of these sales is linked to Greek-operated companies.

The role of European shipping jurisdictions

Europe's role manifests itself in two areas.

The first is **control over tonnage and maritime services**: more than a third of Russian oil is exported using 'Western' tankers and services linked to EU shipping nations – notably Greece, Cyprus and Malta; the EU/G7 discussed replacing the price cap with a complete ban on maritime services [9].

A sector analysis by Lloyd's List[10] suggests that such a ban would drive the remainder of the 'European' segment of Russian oil transport into the shadow fleet.

The second dimension is **institutional architecture** (registers, management, compliance practices): the EPRS emphasises that the presence of the Maltese flag among the 'top flags' and, more generally, the proportion of vessels flying EU flags, create an internal political and administrative challenge to strengthen enforcement without harming the maritime business.

The shadow fleet increases the risks of accidents and environmental disasters, as it often consists of old vessels with insufficient technical condition checks and problematic/non-transparent insurance [8].

At the same time, the impact of sanctions is diminishing: Chatham House shows that the price cap can be 'eroded' through transfer pricing (in particular, inflated freight and insurance costs), which preserves the Russian Federation's revenues even without an explicit breach of FOB logic.

Recommendations

1) **UBO transparency as a standard for access:** promote disclosure requirements for beneficial owners, ISM managers and insurance providers for high-risk vessels as a condition for access to ports/partner services.

2) **From 'vessels' to 'networks':** enforce secondary sanctions against intermediaries (ship management firms, brokers, insurers) that repeatedly divert tonnage into the shadow trade.

3) **Port State Control + insurance checks:** validity of P&I/certificates, vessel class, AIS/STS history; AIS blackouts and suspicious STS patterns – triggers for in-depth inspections and subsequent designations.

4) **Closing transfer pricing loopholes:** audit of ancillary costs and discussion of CIF approaches or limits on freight/insurance to reduce the possibility of hidden price increases.

5) **Data sharing:** institutionalise the exchange of data regarding changes in flag, manager, insurance and STS events, using regular trackers for timely sanctions submissions.

Conclusions

The shadow fleet is not merely a 'Russian' tactic, but a product of the global political economy of shipping: the secondary tanker market, offshore structures, 'flags of convenience' and fragmented governance transform sanctions restrictions into rent for intermediaries.

The centrality of Greece, Cyprus and Malta lies in their role as hubs for shipownership and management, and in their political weight in sanction decisions; consequently, the effectiveness of sanctions depends not only on formal prohibitions, but also on the ability to make beneficiaries and service chains visible and accountable, and to ensure that port and insurance controls are systematic.

1. International Maritime Organization. Legal Committee, 110th Session (LEG 110), 27–31 March 2023.
https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/Legal-Committee%2C-110th-session.aspx.
2. Dubrovskiy, V., Nixey, J. (2025). Tightening the Oil Price Cap to Increase Pressure on Russia. Chatham House.
https://www.chathamhouse.org/sites/default/files/2025-09/2025-09-04-tightening-oil-price-cap-increase-pressure-russia-dubrovskiy-nixey.pdf.
3. Price Cap Coalition. (2024). Advisory for the Maritime Oil Industry and Related Sectors.
https://finance.ec.europa.eu/document/download/3d23e169-8904-4057-b621-0d3b26546019_en?filename=price-cap-coalition-advisory-maritime-safety-2024_en.pdf .
4. Organised Crime and Corruption Reporting Project (OCCRP). (2024). European Ships Keep Russia's Shadow Fleet Afloat.
https://www.occrp.org/en/investigation/european-ships-keep-russias-shadow-fleet-afloat.
5. European Commission. (2024). Guidance on Russian Oil Price Cap.
https://finance.ec.europa.eu/system/files/2024-01/guidance-russian-oil-price-cap_en.pdf.
6. Reuters. (2025). EU, G7 Weigh Ban on Maritime Services for Russian Oil Exports, End to Price Cap.
https://www.reuters.com/business/energy/eu-g7-weigh-ban-maritime-services-russian-oil-exports-end-price-cap-2025-12-05/.
7. Lloyd’s List. (2025). EU Sanctions Plan Will Complete Russia’s Shift into the Shadow Fleet.
https://www.lloydslist.com/LL1156314/EU-sanctions-plan-will-complete-Russia%E2%80%99s-shift-into-the-shadow-fleet.
8. European Parliament Research Service. (2024). Russia’s “Shadow Fleet”: Bringing the Threat to Light.
https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI%282024%29766242_EN.pdf.
9. Kyiv School of Economics. (2024). Russian Oil Tracker: Monthly Report, October 2024.
https://kse.ua/wp-content/uploads/2024/11/ROT_Oct24.pdf
10. International Institute for Strategic Studies (IISS). (2025). Russia’s “Shadow Fleet” and Sanctions Evasion.
https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf.

Т.Т. Бондарук

АКТУАЛЬНІ ЗАДАЧІ ПРОГНОЗУВАННЯ ЗБОЇВ ВЕБ-РЕСУРСІВ ЕНЕРГЕТИКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ З ЗАСТОСУВАННЯМ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. У контексті гібридних загроз, що поєднують кібератаки на системи управління з фізичним руйнуванням інфраструктури, веб-ресурси енергетичних компаній України (портали диспетчерських служб, корпоративні сайти, клієнтські сервіси та системи моніторингу) залишаються критичними елементами захисту цифрового суверенітету. Збої в їхній роботі не тільки порушують управління електропостачанням, але й спричиняють фінансові втрати, паніку серед населення та ескалацію політичної напруги. За даними звіту Європейського агентства з кібербезпеки (ENISA) Threat Landscape 2025 (період липень 2024 – червень 2025), DDoS-атаки домінують у ландшафті загроз (близько 77% інцидентів), переважно через hacktivist-активність, з акцентом на державно-орієнтовані (state-aligned) операції та неідентифіковані інциденти. Енергетика входить до топ-5 секторів, цільованих state-aligned групами (включно з Russia-nexus), хоча основний обсяг DDoS спрямований на public administration [1]. Традиційні системи моніторингу не завжди справляються з швидкістю та комбінованістю таких атак, тому штучний інтелект стає ключовим інструментом для прогнозування збоїв веб-ресурсів, швидкого реагування та відновлення стійкості в електроенергетичній інфраструктурі.

Сучасний стан проблеми. Дослідження демонструють, що для прогнозування збоїв у веб-ресурсах енергосистем ефективно застосовуються моделі, які моделюють мережеву структуру (вузли як сервери, з'єднання як трафік даних). Такі підходи, що комбінують ансамблеві методи, моделі уваги для аналізу часових залежностей та графові нейронні мережі (GNN) для врахування топологічних особливостей, досягають високої точності (часто понад 95–98% на тестових датасетах, наприклад, у гібридних моделях типу GraphFedAI чи GCTNetwork) і працюють з прийнятними обчислювальними витратами [2]. Їх доповнюють часовими моделями для послідовного аналізу подій та механізмами уваги для фокусу на критичних сегментах трафіку. Гібридні методи дозволяють не лише прогнозувати, але й пропонувати миттєві заходи реагування.Для веб-ресурсів прогноз базується на метриках, як кількість запитів за секунду (QPS), час відповіді, рівень відмов та помилок. Моделі ШІ можуть виявляти аномалії за 5–15 хвилин наперед, пропонуючи дії: перерозподіл трафіку, активацію резервних серверів або перехід на альтернативні домени. ШІ допомагає операторам розуміти причини прогнозу, сприяючи швидким рішенням.Інтеграція технічних даних (логів серверів, мережевого трафіку) з відкритими джерелами (соціальні мережі, новини) є критичною, оскільки кібератака на веб-сайт може

ескалувати до фізичного пошкодження. У випадках атак на українські енергокомпанії кібероперації часто використовуються для збору розвідки та оцінки пошкоджень/ремонтів (наприклад, діяльність групи Sandworm, яка в 2025–2026 роках дедалі більше фокусується на розвідці для підтримки подальших фізичних ударів, включаючи аналіз відновлення енергосистеми) [4]. У 2024 році кібератаки на Україну зросли на 69.8% (з 2541 до 4315 інцидентів), з фокусом на критичну інфраструктуру, включаючи енергетику [5].Рішення включають оптимізацію алгоритмів, апаратне покращення (наприклад, спеціалізовані GPU) та розподілені обчислення для зменшення навантаження на енергосистему під час атак [3]. ШІ вже застосовується для захисту фізичної інфраструктури, але для веб-ресурсів українських компаній актуально фокусуватися на прогнозі DDoS, автоматичному відновленні та інтеграції з кібер-кінетичною обороною.

Актуальні задачі. У контексті кібер-кінетичної оборони, базуючись на аналізі, виділяються такі задачі:

Розробка гібридних моделей ШІ, що інтегрують дані трафіку з відкритими джерелами для реального часу прогнозу збоїв веб-ресурсів і автоматичного реагування [6].

Створення адаптивної моделі для українських енергокомпаній, що враховує мережеву структуру, послідовність подій і швидкі обчислення, з фокусом на DDoS-атаки.

Моделі для прогнозу перевантажень через дезінформацію, з інтеграцією аналізу соцмереж для виявлення фейкових кампаній.

Забезпечення explainability ШІ для надання операторам чітких рекомендацій і уникнення помилок під час інцидентів.

Оптимізація енергоспоживання ШІ-моделей через розподілені обчислення і алгоритмічні покращення, з урахуванням впливу на енергобаланс під час гібридних загроз.

Розробка алгоритмів для автоматичного відновлення: перерозподіл трафіку, блокування IP, активація резервів під час атаки.

Інтеграція з відновлюваною енергетикою: прогноз збоїв з урахуванням даних про погоду, сонячну/вітрову генерацію та екологічні ризики для адаптації веб-систем.

Розвиток self-healing систем ШІ, що поєднують прогноз з автономним відновленням без людського втручання.

Врахування етичних аспектів: справедливість, приватність даних і соціальні наслідки (вплив на населення), для уникнення посилення криз, з акцентом на прозорість та справедливість у енергетичному переході [3].

Висновки. Прогнозування збоїв веб-ресурсів енергетики в умовах гібридних загроз є ключовим елементом кібербезпеки України. У рамках кібер-кінетичної оборони ШІ-моделі переходять від пасивного моніторингу до проактичного захисту, дозволяючи передбачати атаки, мінімізувати наслідки та швидко відновлювати функціональність. Подальші дослідження

мають фокусуватися на реальних даних українських порталів, тестуванні гібридних моделей і поширенні на інші сектори для посилення стійкості в умовах гібридної війни.

1. European Union Agency for Cybersecurity. (2025). ENISA threat landscape 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

2. Agarwal, L., Jaint, B., & Mandpura, A. K. (2025). Hybrid AI framework for detecting cyberattacks and predicting cascading failures in power systems. Sustainable Computing: Informatics and Systems, 48(Suppl C), Article 101222. https://doi.org/10.1016/j.suscom.2025.101222.

3. Zhu, R. R., & Ma, J. (2026). Artificial intelligence and the energy transition: Towards ethical and equitable future power systems. Energy Research & Social Science, 132, Article 104564. https://doi.org/10.1016/j.erss.2026.104564.

4. Ukraine says cyberattacks on energy grid now used to guide missile strikes. (2026, February 19). The Record. https://therecord.media/ukraine-cyberattacks-guiding-russian-missile-strikes.

5. Institute of Mass Information. (2025, January 9). Cyber attacks on Ukraine spiked by 70% in 2024. https://imi.org.ua/en/news/cyber-attacks-on-ukraine-spiked-by-70-in-2024-i65939.

6. Sakr, H. A., El-Afifi, M. I., El-Mowafy, M. A., & Ibrahim, H. M. (2025). Detecting DDoS threats in IoT-driven 6G-energy hubs networks using machine learning algorithms. Discover Applied Sciences, 7, Article 1002. https://doi.org/10.1007/s42452-025-06716-9.

V. Tiutiunnikova

MICROCLUSTER MODEL OF A RESILIENT NATIONAL ENERGY SYSTEM

Ukraine's energy sector operates on a centralised hub-and-spoke architecture, in which the bulk of electricity is generated at a small number of large facilities and transmitted via high-voltage trunk lines. This topology is a direct inheritance from the Soviet-era Unified Energy System, designed around very large nuclear and coal plants requiring long-distance bulk transmission [1]. Nuclear generation alone accounts for approximately 50% of Ukraine's total electricity output [2], meaning that a handful of facilities underpin the stability of the entire system. The consequence is a compounding vulnerability – simultaneously structural, in that radial transmission creates cascade dependencies, and physical: by mid-2023, Russian strikes had disabled approximately 51% of Ukraine's generating capacity and 45% of its transmission capacity [3]. At the same time, Ukraine's energy trajectory is inseparable from its accelerating integration into the European energy space. Ukraine's alignment with the European Green Deal whose strategic goal is climate neutrality by 2050 is no longer merely a political declaration: it has a concrete technical foundation. On 16 March 2022, Ukraine's national power grid was integrated with ENTSO-E a full year ahead of the originally planned schedule effectively placing Ukraine on the European energy map [4]. By the end of 2023, ENTSO-E confirmed that Ukrenergo had achieved compliance with all requirements for permanent synchronisation, and on 1 January 2024 Ukrenergo became the 40th full member of the association [5]. This is not a symbolic gesture: since the beginning of the war, the total volume of electricity imported from European countries increased by 94% from 415 million kWh in 2021 to 935 million kWh demonstrating that the interconnection already functions as an operational buffer against infrastructure destruction [5]. In this context, the transition to a distributed energy architecture is not only a resilience imperative but a market integration requirement: a decentralised, modular grid is structurally compatible with the EU Clean Energy Package and with the operational standards of the continental European network to which Ukraine now formally belongs.

In its report “Empowering Ukraine Through a Decentralised Electricity System” (2024), the International Energy Agency establishes a direct relationship between the architecture of an energy system and its resilience. Specifically, it states that large centralised facilities are structurally more vulnerable, while distributed generation offers advantages that cannot be achieved with a centralised topology [6]. The IEA identifies the formation of a diversified portfolio of distributed energy resources such as rooftop solar generation, small wind turbines, modular turbines and battery systems as a key vector for development. Fundamentally, the agency views this transition not as a temporary solution, but as a long-term architectural framework compatible with the goals of decarbonisation

and Ukraine's integration into the European energy market. Decentralisation and the green transition in this concept are solved by a single architectural solution, a system built around a multitude of small autonomous nodes. Such a system is modular, scalable and resistant to point failures by its very nature. The IEA's technical case for decentralisation thus establishes not merely an engineering preference, but a systemic imperative: distributed architecture is the only topology that is simultaneously resilient, scalable, and compatible with decarbonisation goals. This technical consensus has since been elevated to the level of political commitment. The G7+ joint statement translates the IEA's architectural logic into an intergovernmental obligation, anchoring Ukraine's decentralisation within the broader framework of EU Clean Energy Package integration, thereby transforming a technical recommendation into a binding strategic vector [7]. The European Commission formulates a three-tiered logic for transformation. Distributed generation reduces systemic vulnerability; integration with the EU market provides buffer imports during periods of shortage; reforms create conditions for long-term investment. Yet political commitment and engineering design, taken alone, do not explain how a system undergoing radical structural transformation maintains coherence and identity across the transition. This is precisely the theoretical gap addressed by concept of adaptive security [8]. Unlike classical resilience theory, which frames recovery as a return to a prior state, their framework redefines system health as the capacity for transmorphance - structural transformation that preserves functional identity while fundamentally reconfiguring internal architecture. Applied to Ukraine's energy sector, this means that each disruption to a microcluster node is not a failure event to be corrected, but an adaptive signal that triggers redistribution of resources and reformation of connections across the remaining network. Unlike resilience, which implies a return to the initial state, transformation results in the system becoming different and more adaptable, without losing its original identity. During failures in systems of this type, resources are redistributed and connections are restructured, so such models can be considered morphological - structurally plastic. Consequently, failures in such systems do not cause degradation, but rather trigger a process of adaptation, which in turn signifies the development of the system. Taken together, these three frameworks form a single argumentative chain: the IEA establishes what architecture is needed; the G7+ consensus establishes why it must happen now and under what international obligations; and adaptive security theory explains how such a system sustains itself through the very instability it is designed to withstand.

Considering all of the above, the energy system should become distributed, horizontal, and self-organising. The essence of the proposed concept is as follows: a second layer is built on top of the existing centralised system - a network of autonomous microclusters, where each participant (household, enterprise, local community) is capable of independently generating, storing and consuming electricity. The microcluster acts as a local energy unit that performs the processes of generation, storage and consumption. Each microcluster functions as an autonomous node and, if necessary, can switch to island mode, i.e. operate

separately from the main grid. In this way, they operate as a closed circuit, cooperating with the external system, which is centralised only in terms of surplus exchange or deficit coverage. Microclusters are connected to each other by microgrids, so the failure of one node does not cause a cascade collapse of the entire system. Moreover, in the event of failure of any of the clusters, new connections are formed between the remaining ones, which stimulates the overall development of the system, as each failure becomes an impulse for the restructuring and strengthening of the remaining nodes. Compared to a centralized system, such a structure consisting of thousands of autonomous nodes cannot be instantly shut down, either physically or administratively. Therefore, a microcluster energy system is even an institutional solution. It is essential that the concept does not involve dismantling the existing infrastructure, but rather building a new layer on it as a second level of resilience, reducing the load on the transmission network under normal conditions and ensuring the autonomous functioning of critical nodes in the event of a failure. The legal framework for the self-organisation of participants in such clusters operates at three reinforcing levels. At the domestic level, the primary instrument is the Law of Ukraine 'On the Electricity Market' [9], which establishes the foundational rules for electricity market participation, including the construction and grid connection of generating facilities. Subsequent amendments have enabled electricity consumers to become active market participants through self-generation - installing capacity for their own needs and selling surplus electricity to the grid at free market prices. Critically, Ukrainian legislation has also introduced formal definitions of 'microgrid', 'microgrid island mode', 'microgrid energy management system', and 'demand response' - establishing the precise regulatory vocabulary needed to govern distributed cluster architectures [10]. At the EU harmonisation level, Draft Law No. 12087-d introduces fundamental amendments to the Electricity Market Law to transpose EU Directive 2019/944 [11] and Regulation 2019/943, and by establishing a legal framework for energy communities, opens the electricity market to cooperative, locally-rooted actors [12]. At the European framework level, Directive (EU) 2019/944 grants final customers the right to act as active participants - selling self-generated electricity, participating in flexibility programmes, and joining citizens' energy communities - without being subject to disproportionate or discriminatory technical requirements [11]. Together, these three layers - domestic market law, its ongoing EU harmonisation, and the European Clean Energy Package - provide a coherent and already operational legal basis for microcluster self-organisation, one grounded in energy law rather than civil association law.

The cluster network has a further structural advantage: it requires no centralised authorisation to launch. A single enterprise or micro-neighbourhood is sufficient to establish the first microcluster node, and once operational, its example exerts a demonstrative effect that no policy document can replicate. The microcluster scales through proof, not permission. This bottom-up logic does not, however, diminish the role of the state - it redefines it. A state that clings to

centralised generation as a source of institutional control is not protecting energy security; it is actively undermining it. Regulatory capture of the energy sector, through restrictive grid connection procedures, discriminatory tariff structures, or the absence of a prosumer framework - functions, in effect, as a subsidy to vulnerability. The constructive role of government is therefore enabling, not gatekeeping: fair tariffs for surplus electricity fed into the grid, tax incentives for distributed generation and storage, and genuinely simplified connection procedures for microcluster participants. This means transposing the prosumer rights enshrined in EU Directive 2019/944 [12] not as a bureaucratic exercise but as a genuine reallocation of market power toward citizens and local communities. Under these conditions, participation in a microcluster becomes the rational economic choice rather than an act of civic voluntarism. The transition to a distributed infrastructure does not then depend on individual initiative or institutional goodwill - it becomes the path of least resistance, systemically encoded into the market design itself.

1. Nies, S., & Savytskyi, O. (2024). Six options to boost power transfers from Continental Europe to Ukraine, for the next two winters Ukraine´s power network integration with the EU. Green Deal Ukraïna. https://greendealukraina.org/assets/images/reports/grid-solutions-ukraine-next-winters-final.pdf.
2. Nuclear Power in Ukraine. (2026). World Nuclear Association. https://world-nuclear.org/information-library/country-profiles/countries-t-z/ukraine.
3. Ukraine Energy Damage Assessment. (2023). UNDP. https://www.undp.org/ukraine/publications/ukraine-energy-damage-assessment.
4. Ukraine's Power Network Integration with EU ENTSO-E. (n. d.). Ministry of Energy of Ukraine. https://mev.gov.ua/en/reforma/ukraines-power-network-integration-eu-entso-e
5. Two years since Ukraine and Moldova synchronised electricity grids with EU. (2024). ENTSO-E. https://www.entsoe.eu/news/2024/03/15/two-years-since-ukraine-and-moldova-synchronised-electricity-grids-with-eu/.
6. Empowering Ukraine Through a Decentralised Electricity System – Analysis - IEA. (2024). IEA. https://www.iea.org/reports/empowering-ukraine-through-a-decentralised-electricity-system.
7. Statement of the G7+ Ukraine Energy Coordination Group and the Government of Ukraine promoting sustainable green recovery of Ukraine's energy system. (2024). European Commission. https://energy.ec.europa.eu/news/statement-g7-ukraine-energy-coordination-group-and-government-ukraine-promoting-sustainable-green-2024-11-15_en.
8. Korobeynikov, F., & Mokhor, V. (2026). Adaptive security: strategic principles for complex socio-technical systems. Royal Society Open Science, 13(1). https://doi.org/10.1098/rsos.251481
9. Law of Ukraine 'On Electricity Market'. (2017). Official website of the Parliament of Ukraine. https://zakon.rada.gov.ua/laws/show/en-ga/2019-19.
10. One step closer to the implementation of “smart grids”. (2024). GOLAW Law Firm. https://golaw.ua/insights/energy-alert/na-krok-blizhche-do-vprovadzhennya-rozumnih-merezh/.
11. Directive (EU) 2019/944 of the European Parliament and of the Council on common rules for the internal market for electricity and amending Directive 2012/27/EU. (2019). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02019L0944-20220623.
12. Ukraine moves toward market coupling with the EU energy market. (2025). Lexology. https://www.lexology.com/library/detail.aspx?g=2f54f9eb-f160-4c9b-bbe5-c53375291067.

А.А. Ублінських

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СТРИМУВАННЯ ДЕСТРУКТИВНОГО ВПЛИВУ НА ЕНЕРГЕТИЧНУ ІНФРАСТРУКТУРУ

Енергетичні системи з кожним роком стають дедалі складнішими, а традиційні підходи до керування ними вже не демонструють тієї ефективності, яку забезпечували раніше. Розвиток розподіленої генерації, цифровізація енергетичних мереж і зростання вимог до безперервності постачання електроенергії формують нові виклики для операторів енергосистем. У таких умовах виникає об'єктивна потреба у впровадженні інтелектуальних методів аналізу, прогнозування та підтримки прийняття рішень.

Як зазначено у джерелі [1], інтеграція відновлюваних джерел енергії додає до процесів планування низку нових змінних, передусім пов'язаних із погодними умовами, що безпосередньо впливають на ефективність генерації. Це ускладнює балансування виробництва та споживання електроенергії, підвищує вимоги до точності прогнозування та адаптивності систем керування. Водночас залишаються актуальними ризики природних лих, які можуть спричиняти масштабні перебої у функціонуванні енергетичної інфраструктури та значні економічні втрати для бізнесу і населення.

До зазначених вразливостей додаються загрози штучного характеру, насамперед кібератаки, спрямовані на порушення стабільної роботи енергетичних мереж як об'єктів критичної інфраструктури держави. Джерело [2] зазначає, що лише за перший квартал 2024 року було виявлено 1038 кібератак на об'єкти критичної інфраструктури. Ці приклади підтверджують, що традиційні засоби захисту часто не забезпечують достатнього рівня проактивного виявлення та оперативного реагування на складні й динамічні загрози.

Отже, впровадження нових інструментів на основі штучного інтелекту для протидії як усталеним, так і новим ризикам є необхідною умовою підвищення надійності та безпеки енергосистем. У цій роботі розглянуто сучасні методи застосування штучного інтелекту (ШІ) для підвищення кіберстійкості та забезпечення надійного функціонування енергетичної інфраструктури.

Метою даної роботи є огляд існуючих методів і архітектур впровадження ШІ для керування, моніторингу та відновлення енергетичних мереж, а також для захисту їх від кіберзагроз.

У контексті критичної інфраструктури надійність визначається як здатність системи виконувати свої функції в заданих параметрах і часових межах із високою ймовірністю успішної роботи протягом визначеного періоду [2]. Для енергетичної інфраструктури це означає не лише стабільність окремих компонентів, а й передбачувану взаємодію між ними в

умовах штатної експлуатації, відхилень і зовнішніх збурень. Відповідно, оцінювання надійності має спиратися на кількісні підходи до аналізу відмов і деградації, зокрема статистичні методи, такі як Weibull analysis, Markov chains та Monte Carlo simulation [2].

Разом із цим доцільно розширювати визначення надійності через часову динаміку функціональності системи під впливом критичних подій. Згідно з [1], resilience в енергосистемах доцільно аналізувати в межах п'яти послідовних фаз: pre-event state, degradation state, during-event state, restoration state та recovery (post-event) state. Така фазова модель демонструє, що стійкість системи формується не лише швидкістю післяаварійного відновлення, а й якістю підготовки до потенційної події та ефективністю дій безпосередньо під час дестабілізації.

Важливим висновком для подальшого обґрунтування ролі ШІ є обмеженість традиційних підходів, які часто мають реактивний характер. Як зазначено у [3], традиційні методи, зокрема load shedding (LS) та frequency response analysis (FRS), зазвичай реагують уже після виникнення порушення. Така логіка управління створює часову затримку у реагуванні на загрози та збої і підвищує ймовірність погіршення ситуації. Натомість підходи на основі штучного інтелекту, зокрема predictive analytics та time series analysis, забезпечують можливість прогнозування небажаних станів системи і створюють основу для завчасних керуючих дій [3]. Таким чином, для енергетичної інфраструктури принципово важливим є перехід від реактивної моделі забезпечення надійності до проактивної, орієнтованої на раннє виявлення ризиків, запобігання каскадним порушенням і скорочення часу відновлення системи.

Описано методи штучного інтелекту та їх практичне застосування в енергосистемах з урахуванням їх сильних і слабких сторін. Автор розглядає такі методи, як Artificial Neural Networks (ANN), Fuzzy Logic (FL), Expert Systems та Evolutionary Methods (зокрема Genetic Algorithms і метаевристичні оптимізаційні методи). На основі технічних характеристик кожного підходу визначено найбільш доцільні сфери їх застосування в енергетичних мережах. Більшість операцій в енергетичних мережах можуть бути описані як near-linear, що дає змогу застосовувати швидкі чисельні методи. Однак зі зростанням навантажень у системі посилюється вплив нелінійних процесів, з якими традиційні інструменти справляються значно гірше. Натомість підходи на основі ШІ демонструють високу ефективність у виявленні нелінійних залежностей [3].

Автор також зазначає значний потенціал використання ANN та FL для захисту енергосистем від кібератак завдяки їх здатності моделювати складні закономірності та імітувати елементи людського процесу прийняття рішень. Крім того, згадуються моделі штучного інтелекту на основі support vector machines (SVM), decision trees (DT), convolutional neural networks (CNN) та recurrent neural networks (RNN), які можуть ефективно застосовуватися для реалізації систем моніторингу енергосистем у режимі реального часу [3].

Як приклад практичного застосування ШІ розглядається поєднання технології wavelet transformation з artificial neural networks. Wavelet transformation представлено як ключовий підхід для аналізу аварійних режимів у лініях електропередачі, особливо в тих випадках, коли класичне перетворення Fourier transform (FT) має обмеження через фіксовану роздільну здатність і недостатню локалізацію в часово-частотній області. Використання такого підходу підвищує точність і швидкодію систем релейного захисту, а також покращує надійність діагностики в умовах шуму, змін навантаження та складних режимів роботи мережі [3].

Описано підхід до зменшення або повного усунення негативних ефектів, притаманних окремим методам штучного інтелекту. Запропонованим рішенням є використання гібридних моделей ШІ, які поєднують декілька різних методів у межах однієї системи. Такий підхід дає змогу зменшити кількість хибних спрацьовувань та підвищити загальну ефективність системи. Як приклад автори наводять поєднання Random Forests (RF) з deep neural networks (DNN), що дозволило підвищити ефективність роботи системи та зменшити кількість помилкових спрацювань [4].

Запропоновано комплексний підхід до впровадження штучного інтелекту в системи захисту критичної інфраструктури (Critical Infrastructure Protection, CIP), у межах якого поєднуються моделі оцінювання надійності та практичне розгортання ШІ-рішень [2].

Запропонований підхід базується на фреймворку Markov chains. У цій моделі інфраструктура розглядається як система станів із ймовірнісними переходами між ними, що дає змогу кількісно оцінювати надійність і безпеку за допомогою таких показників, як Mean Time To Failure (MTTF), Mean Time To Recovery (MTTR) та інших пов'язаних метрик. У межах цього підходу не здійснюється чітке розмежування між атаками та технічними помилками, оскільки обидва типи подій призводять до виведення системи з робочого стану. Даний підхід можна описати як модель Main System – Disaster Recovery (MS–DR), де одночасно враховуються як технічні відмови, так і кібератаки. Для енергетичної інфраструктури це є особливо важливим, оскільки дозволяє оцінювати її стійкість як єдиного кіберфізичного середовища [2].

Операційну частину впровадження ШІ автори описують через життєвий цикл LLM, який включає: визначення цілей і сфери застосування; вибір або адаптацію моделі; налаштування продуктивності; ітераційне оцінювання та продуктивне розгортання з постійним моніторингом. У результаті формується практична схема інтеграції ШІ у системи CIP, де Markov chains framework визначає математичну основу оцінювання ризиків, а LLM lifecycle – послідовність впровадження AI-рішень у реальну експлуатацію [2].

З огляду на те, що моделі штучного інтелекту все ще можуть демонструвати некоректні рішення, у практичних системах часто

застосовується технологія Digital Twin. Вона передбачає створення віртуальної моделі енергетичної мережі, що дозволяє моделювати результати майбутніх змін та перевіряти можливі сценарії розвитку подій. Завдяки цьому оператор енергомережі може попередньо оцінити коректність прийнятого рішення та зменшити ризик негативних наслідків [4].

Попри значний технологічний прогрес у сфері штучного інтелекту протягом останніх років, існує низка обмежень, які потребують подальшого дослідження та вдосконалення. До таких обмежень належать: ефект «чорної скриньки», коли складно пояснити причини прийняття конкретного рішення моделлю ANN; можливість так званого AI poisoning – цілеспрямованого навчання моделі на хибних даних, що може призвести до небезпечних результатів; а також відносно невелика кількість практичних впроваджень таких систем. Зокрема, станом на 2024 рік було реалізовано лише шість інтеграцій ШІ в енергосистеми [3].

Таким чином, незважаючи на зазначені обмеження та майбутні виклики, потенціал штучного інтелекту для оптимізації та підвищення надійності енергосистем є надзвичайно значним. Однією з ключових переваг ШІ є можливість безперервного моніторингу стану енергетичних мереж з метою раннього виявлення відхилень, збоїв або кібератак і своєчасного реагування на них. Завдяки використанню інтелектуальних алгоритмів стає можливим виявлення прихованих взаємозалежностей у роботі системи, які можуть сигналізувати про потенційні відмови, що дозволяє здійснювати превентивні управлінські дії ще до виникнення критичних подій.

1. Zahraoui, Y., Korõtko, T., Rosin, A., Mekhilef, S., Seyedmahmoudian, M., Stojcevski, A., & Alhamrouni, I. (2024). AI Applications to Enhance Resilience in Power Systems and Microgrids—A Review. Sustainability, 16(12), 4959. https://doi.org/10.3390/su16124959.

2. Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., Tihanyi, N., & Janicke, H. (2025). Generative AI and LLMs for Critical Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities. Sensors, 25(6), 1666. https://doi.org/10.3390/s25061666.

3. Alhamrouni, I., Abdul Kahar, N. H., Salem, M., Swadi, M., Zahroui, Y., Kadhim, D. J., Mohamed, F. A., & Alhuyi Nazari, M. (2024). A Comprehensive Review on the Role of Artificial Intelligence in Power System Stability, Control, and Protection: Insights and Future Directions. Applied Sciences, 14(14), 6214. https://doi.org/10.3390/app14146214.

4. Rana, S. (2025). ai-driven fault detection and predictive maintenance in electrical power systems: a systematic review of data-driven approaches, digital twins, and self-healing grids. American Journal of Advanced Technology and Engineering Solutions, 1(01), 258–289. https://doi.org/10.63125/4p25x993.

Є.І. Котляров, Т.І. Салашенко, І.В. Шульга

ПРОБЛЕМИ РОЗБУДОВИ РОЗПОДІЛЕНИХ ЕНЕРГЕТИЧНИХ СИСТЕМ [1]

Проблема створення децентралізованих розподілених енергетичних систем (далі – ЕС) активно обговорюється в наукових колах протягом останніх років. Свідченням цього є, наприклад, проведення щорічних тематичних конференцій Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, наприклад [1, 2 та інші]. Актуальність зміни підходу з централізованого до децентралізованого енергозабезпечення споживачів викликана чинниками, наведеними в табл. 1.

Таблиця 1. Чинники, що обумовлюють необхідність розвитку децентралізованих розподілених ЕС

Чинник	Характеристика
Військові загроза з боку рф	Орієнтація ракетно-дронових ударів на об'єкти критичної інфраструктури
Вимоги ЄС щодо реформування ринку електроенергії	Директива (ЄС) 2024/1711 [3] та Регламент (ЄС) 2024/1747 [4] містять вимоги щодо розвитку децентралізованих енергетичних систем
Зобов'язання України в сфері енергетики та клімату	Зниження викидів парникових газів може бути досягнуто шляхом більш широкого використання альтернативних джерел енергії, які притаманні саме невеликим потужностям енергогенерації

Переорієнтація енергозабезпечення на децентралізацію ЕС є логічною реакцією на російську агресію, яка спрямована, в першу чергу на об'єкти критичної енергетичної інфраструктури (об'єкти електро- і теплогенерації, потужності з транспортування і постачання відповідних енергоносіїв).

Необхідність реформування централізованих електричних систем випливає з вимог нової реформи європейської моделі ринку електроенергії в ЄС, оголошеної у 2024 р. Директивою (ЄС) 2024/1711 [3] та Регламентом (ЄС) 2024/1747 [4]. Завданнями цієї реформи, крім іншого, є встановлення права на енергетичний шерінг (спільне використання) активними споживачами енергії з відновлюваних джерел енергії (далі – ВДЕ), розбудова енергетичних кооперативів тощо.

Національним планом з енергетики та клімату [5] (далі – НПЕК)

[1] Тези доповідей 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».

передбачено індикативні цілі ВДЕ у валовому кінцевому споживанні енергії до 2030 р.: опалення та охолодження – 35 %, електроенергія – 25,4 %.

Розбудова енергетики України, яка враховує всі перелічені чинники (табл. 1), передбачає зміну пріоритетів подальшого розвитку. Замість орієнтації на великі генеруючі потужності, що працюють на викопному паливі, пріоритетом повинно стати створення сукупності децентралізованих ЕС, які працюють на ВДЕ і не замінюють, а доповнюють об'єднану ЕС України.

Виділення поняття локальної ЕС передбачає обмеженість її дії певною територією, тобто певною територіальною громадою (далі – ТГ). На наш погляд, майбутня система енергозабезпечення країни повинна мати наступний укрупнений вигляд –рис. 1.

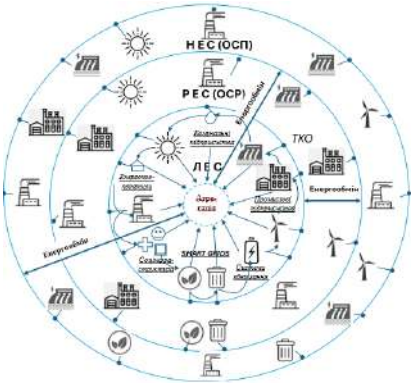


Рисунок 1. – Агрегований вид локальних ЕС ТГ в об'єднаній ЕС України

Примітка: НЕС – національна ЕС, яка керується оператором систем передачі (ОСП); РЕС – регіональна ЕС, яка керується оператором систем розподілу (ОСР); ЛЕС – локальна ЕС, оператори відсутні; ТКО – точки комерційного обліку

При побудові таких локальних ЕС, орієнтованих на самозабезпечення енергоресурсами окремих ТГ, існує ряд проблем, вирішення яких потребує проведення подальших наукових досліджень і внесення змін до діючого нормативно-правового поля.

Перш за все, розвиток низьковуглецевої енергетики розглядається виключно як будівництво нових потужностей, які працюють на ВДЕ. При цьому ігнорується те, що необхідна величина цих потужностей визначається потребами споживачів. Тобто, керування попитом необхідно розглядати як інструмент управління обсягами виробництва. В «Довгостроковій стратегії термомодернізації будівель на період до 2050 року» [6] передбачено завдання скоротити кінцеве споживання енергії в секторі будівель до 2030 р. на 15 %. Але, «Державна цільова економічна програма енергетичної модернізації підприємств - виробників теплової енергії, що перебувають у державній або комунальній власності, на період до 2030 року» [7]

встановлює обсяги реконструкції, модернізації та будівництва нових об'єктів і не містить жодної згадки про потенційне зниження потреб в теплоенергії.

Виконані розрахунки [8] показують, що при випереджаючій термомодернізації будівель: потреба в теплоенергії може бути знижена на 40 % [6], при подальшій модернізації систем розподілу (зниженні втрат при транспортуванні принаймні на 10 %) необхідна потужність котельні знижується практично на 50 % з відповідним зменшенням потреби в природному газі і викидів парникових газів.

Ще одним прикладом неузгодженості нормативно-правових актів є Стратегія розподіленої генерації [9], в якій основну увагу приділяється будівництву та введенню в експлуатацію об'єктів з гарантованою потужністю, які працюють на природному газі, що не узгоджується з цілями НПЕК [5] щодо декарбонізації енергетики.

Також необхідно зауважити на наступне. Стрімкий розвиток енергетики на ВДЕ в Україні протягом останніх десятиріч пов'язаний з законодавчо гарантованим викупом вироблених обсягів електроенергії за цінами, які підвищувалися на коефіцієнт «зеленого» тарифу [10]. На даний час на території багатьох ТГ існують потужності з відновлюваної енергетики, які передають вироблену електроенергію до Об'єднаної ЕС України. Тобто, ці потужності спрямовані не на потреби ТГ, на території яких вони розташовані, а на задоволення вимог Об'єднаної ЕС України, яка диспетчерізує їхнє навантаження. Але, стимулюючі коефіцієнти «зелених» тарифів діють до кінця 2029 р. [10]. Після цього терміну створюються умови для переорієнтації принаймні невеликих електростанцій, що працюють на ВДЕ, з загальнодержавного на місцеві ринки електроенергії. За таких умов необхідним становиться розробка організаційно-економічного механізму узгодження інтересів ТГ з інтересами власників потужностей, що працюють на ВДЕ. Такий механізм повинен включати необхідне інструментально-інституціональне забезпечення, спрямоване на стимулювання створення локальних ЕС, орієнтованих на забезпечення потреб окремих ТГ за рахунок використання наявних місцевих ВДЕ.

Окремо потребує розробки механізм взаємодії локальних ЕС між собою та з Об'єднаною ЕС, який повинен містити комплекс організаційних та технічних заходів, спрямованих на забезпечення стійкості як локальних, так і Об'єднаної ЕС.

Таким чином, завершення дії стимулюючих коефіцієнтів «зелених» тарифів у 2029 р. формує об'єктивні умови для стратегічної переорієнтації малих генеруючих потужностей ВДЕ із загальнодержавного на місцеві енергетичні ринки, що зумовлює необхідність розробки комплексного організаційно–економічного механізму узгодження інтересів ТГ і власників генерації, впровадження інструментально-інституціонального забезпечення для розбудови локальних ЕС, а також створення дієвих засобів технічної та організаційної взаємодії між локальними вузлами та Об'єднаною ЕС України задля гарантування стійкості та живучості енергетичної інфраструктури.

1. Живучість та резильєнтність критичної інфраструктури – 2023: збірник матеріалів міжнародної науково-практичної конференції, м. Київ, 19 жовтня 2023 р., ІПМЕ ім. Г.Є. Пухова НАН України. – 2023. – 173 с. URL : https://ipme.kiev.ua/wp-content/uploads/2023/11/%D0%9C%D0%B0%D1%82%D0%B5%D1%80i%D0%B0%D0%BB%D0%B8_%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86i%D1%97_Survivability_and_Resilience-2023-4.pdf.

2. Резильєнтність динамічних систем, ІІІ науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 06 листопада 2025 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2025. 185 с. URL : https://ipme.kiev.ua/wp-content/uploads/2025/11/%D0%9C%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D0%B8-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%97-%D0%A0%D0%94%D0%A1-2025.pdf.

3. Directive (EU) 2024/1711 of the European Parliament and of the Council of 13 June 2024 amending Directives (EU) 2018/2001 and (EU) 2019/944 as regards improving the Union's electricity market design. URL : https://eur-lex.europa.eu/eli/dir/2024/1711/oj/eng.

4. Regulation (EU) 2024/1747 of the European Parliament and of the Council of 13 June 2024 amending Regulations (EU) 2019/942 and (EU) 2019/943 as regards improving the Union's electricity market design. URL : https://eur-lex.europa.eu/eli/reg/2024/1747/oj/eng.

5. Національний план з енергетики та клімату на період до 2030 року. Схвалено розпорядженням Кабінету Міністрів України від 25.06.2024 р. № 587–р. URL: https://me.gov.ua/view/bb0b9ef5-ea96-4b8a-8f2f-471faf32c9df.

6. Деякі питання стратегічного розвитку енергетичної ефективності будівель. Розпорядження КМУ від 29.12.2023 № 1228-р. URL : https://mindev.gov.ua/npas/deiaki-pitannia-strategicnogo-rozvitku-energeticnoyi-efektivnosti-budivel?__cf_chl_tk=KSlA9N5NYTZL.OA.BdNNYLTFG1napzoSDupx8zD8978-1773475602-1.0.1.1-mWXVdPJxDxvCTw2tHuzRKAiS_JiyKIUKPgjL58fJo1w.

7. Про затвердження Державної цільової економічної програми енергетичної модернізації підприємств - виробників теплової енергії, що перебувають у державній або комунальній власності, на період до 2030 року. Розпорядження Кабінету Міністрів України від 01.10. 2025 р. № 1083-р. URL : https://zakon.rada.gov.ua/laws/show/1083-2025-%D1%80#Text.

8. Кизим М. О., Котляров Є. І. Обґрунтування комплексного підходу до модернізації систем централізованого теплопостачання і теплоспоживання населених пунктів. Проблеми економіки. 2022. №4. С. 46–58. https://doi.org/10.32983/2222-0712-2022-4-46-58.

9. Стратегія розвитку розподіленої генерації на період до 2035 року. Схвалено розпорядженням Кабінету Міністрів України від 18.07.2024 р. № 713–р. URL : https://zakon.rada.gov.ua/laws/show/713-2024-%D1%80#Text.

10. Про альтернативні джерела енергії. Закон України від 20.02.2003 р. № 555-IV. URL : https://zakon.rada.gov.ua/laws/show/555-15#Text.

С.Б. Бурченко, І.І. Сватовський

CYBER-KINETIC DEFENSE В ЕНЕРГЕТИЦІ - ЦИФРОВОЙ СУВЕРЕНІТЕТ, ГІБРИДНІ ЗАГРОЗИ ТА РОЛЬ ШІ В КРИЗОВОМУ РЕАГУВАННІ

Cyber-kinetic загрози стали нормою для енергетики України.

З 2022 року росія системно поєднує кібератаки на підприємства паливно-енергетичного комплексу з ракетно-дроновими ударами по електростанціях, підстанціях та мережах передачі, що призводить до втрати до половини доступної генеруючої потужності в окремі періоди [1],[2].

Це не лише енергетична, а й інформаційно-цифрова війна за здатність держави керувати власною інфраструктурою.

Кіберфаза часто передує кінетичній фазі.

Аналіз подій безпеки в українському кіберпросторі останнього часу показує, що інтенсивність атак на енергетичні компанії (в т.ч. з боку APT-груп) зростала напередодні хвиль ракетних ударів, для виконання завдання розвідки, тестування захисту та підготовки до можливих деструктивних дій по ICS/SCADA [3]

Ці сценарії нагадали елементи відомого кейсу атак на енергетичні компанії України минулих років типу BlackEnergy, які використовували троян для доставки руйнівного компонента KillDisk (виявлено компанією ESET у 2015 році [18]). Аналітичні висновки щодо техніки проведених атак були підтверджені також іншими авторитетним організаціями (наприклад – в аналізі Cyber-Attack Against Ukrainian Critical Infrastructure [19]).

Таким чином формується повний cyber-kinetic kill chain: від кіберрозвідки — до фізичного знищення об’єктів.

Масштаб та інтенсивність кіберзагроз по енергетиці зростає.

Кількість кібератак на Україну у 2024 році зросла приблизно на 70%, при цьому критична інфраструктура (енергетика, транспорт, комунікації) залишається однією з ключових цілей [4].

Паралельно міжнародні дослідження фіксують десятки інцидентів в енергетичному секторі щороку, з трендом на зростання деструктивних операцій [5].

Цифровий суверенітет енергетики як новий вимір безпеки постачання.

Традиційне розуміння «безпеки постачання» (генерація, резерви, фізична мережа) вже не працює без контролю над цифровими платформами, даними, SCADA/EMS/DMS та хмарними сервісами, на яких вони побудовані [6].

Цифровий суверенітет означає спроможність енергетичного сектору діяти автономно та без зовнішнього примусового впливу у цифровому просторі: від зберігання й обробки даних до можливості змінити платформу чи постачальника без втрати керованості системи [7], [6].

Vendor lock-in та «несуверенні» хмари як фактор вразливості.

Залежність від закордонних хмарних провайдерів, пропрієтарних EMS/DMS/MDM-рішень без чітких exit-стратегій та з обмеженою прозорістю створює додаткові ризики: від правової доступності даних іноземними юрисдикціями до неможливості швидко мігрувати в умовах війни чи санкцій [8], [6].

Тож потрібні суверенні хмарні рішення та «sovereign AI clouds» для енергетики:

- Моделі: національні/галузеві хмари, data-spaces, multi-cloud та hybrid-cloud стратегії для критичної інфраструктури [12], [6], [7].
- Політики доступу до даних і управління ключами в умовах війни й санкцій.

ШІ як інструмент прогнозування та стійкості енергосистеми.

Моделі ML/AI вже дають змогу точніше прогнозувати попит на енергію та генерацію відновлюваних джерел енергії (ВДЕ), перевантаження ліній та «слабкі місця» в мережі, що дозволяє заздалегідь планувати перемикання, локалізувати ризики та уникати каскадних відмов [9], [10].

Військові умови лише підсилюють цінність таких інструментів для оперативного планування ремонтів, резервування та сценарного моделювання.

Generative AI та агентні системи для кризового управління.

Окремий клас рішень — генеративні моделі та агентні системи, які можуть:

- моделювати рідкісні «tail events» (екстремальні погодні та бойові події),
- інтегрувати телеметрію SCADA, метеодані, кібералерти та OSINT,
- формувати для оператора узагальнені сценарії дій, рекомендації щодо перемикання та відновлення мережі в режимі наближеного реального часу [11], [12].

AI-Enhanced SOC/OT-SOC для кібер-кінетичного середовища.

Класичний SOC, орієнтований на IT-логіку, недостатній в умовах OT/IC. SOC, які доповнюються штучним інтелектом, представляють собою підхід «людина в циклі», де штучний інтелект покращує робочі процеси аналітиків, а не замінює людський досвід. Сучасні впровадження SOC, які доповнені штучним інтелектом, повинні відповідають фреймворку MITRE ATT&CK для забезпечити повного охоплення всіх потенційних тактик зловмисників [16], [17].

Модель доповненої SOC є доцільною там, де ефективні операції безпеки вимагають поєднання обчислювальної потужності ШІ з людським розумінням, судженнями та можливостями прийняття оперативних управлінських рішень.

ШІ-підходи дозволяють:

- виявляти аномалії в телеметрії технологічних процесів (частоти, напруги, режими навантаження),

- корелювати їх з мережевими подіями (неавторизовані команди, зміни конфігурації PLC, відхилення у VPN-сесіях операторів),

- знижувати «alarm flood» за рахунок інтелектуального пріоритезування інцидентів для диспетчерів та кібер-аналітиків [10], [11].

Інтеграція ШІ в ситуаційні центри: людино-центричний дизайн та довіра.

Ключове завдання — не замінити диспетчерів, а зменшити когнітивне навантаження та пришвидшити ухвалення рішень: чат-інтерфейси для технічної документації, напівавтоматичні «playbooks», рекомендаційні панелі для режимів мережі, візуалізація сценаріїв «що-якщо» [10], [11].

Потрібні чіткі принципи «human-in-the-loop», пояснюваність моделей та перевірка їх стійкості до маніпуляцій противника. Необхідно чітко визначити ролі, де ШІ займається обробкою великих масивів даних та початковим їх аналізом, а оператори проводять керівні функції та прийняття наступних рішень відповідно контекстуальної усвідомленості ситуації в операціях забезпечення безпеки.

Нормативний та стратегічний вимір (NIS2, KRITIS, нацстратегії).

Європейське регулювання (NIS2, KRITIS, вимоги до критичної інфраструктури) вже прямо прив'язує вимоги кіберстійкості, управління ризиками постачальників та прозорості ланцюжків поставок до забезпечення безпеки постачання енергії [6].

Для України питання гармонізації цих підходів із власною моделлю цифрового суверенітету енергетики є стратегічним на період повоєнного відновлення.

Уроки України для союзників.

Багатомісячна оборона електромережі під масованими cyber-kinetic ударами дає унікальний практичний матеріал для США, ЄС та інших партнерів щодо:

- архітектур Defense-in-Depth,

- процедур швидкого відновлення та ротації обладнання,

- моделей взаємодії між операторами мереж, CERT/CSIRT та силовими структурами [2], [13].

Вектор майбутніх досліджень: від цифрових двійників до суверенних «GridGPT».

Перспективні напрями — цифрові двійники енергосистеми для моделювання гібридних атак, національні доменно-специфічні LLM/agent-frameworks для керування мережею («суверенні GridGPT»), а також формалізовані методики оцінки цифрового суверенітету енергетики на рівні держави та окремих операторів [12], [11].

1. Attacks on Ukraine's Energy Infrastructure: Harm to the Civilian Population https://ukraine.ohchr.org/sites/default/files/202412/ENG_Attacks_on_Ukraine's_Energy_Infrastructure_Harm_to_the_Civilian.pdf.

2. Attacks On Ukraine's Electricity Infrastructure Threaten Key Aspects of Life As Winter Approaches. https://ukraine.ohchr.org/en/Attacks-On-Ukraines-Electricity-Infrastructure .

3. Cybersecurity Threat Landscape of Ukraine in 2023. https://understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_en.pdf.

4. Cyber attacks on Ukraine spiked by 70% in 2024. https://imi.org.ua/en/news/cyber-attacks-on-ukraine-spiked-by-70-in-2024-i65939.

5. Cyber threats and energy security: Development and analysis of an incident dataset for the period 2022–2024.
https://www.sciencedirect.com/science/article/pii/S0301421525004203.

6. Digital Sovereignty in the Energy and Utilities Industry.
https://www.arvato-systems.com/blog/digital-sovereignty-in-the-energy-and-utilities-industry.

7. Trusted cybersecurity to ensure your digital sovereignty. https://www.stormshield.com/towards-sovereign-cyber-security/ .

8. Digital Sovereignty Strategies for Every Nation.
https://www.acigjournal.com/pdf-184285-105043?filename=Digital-Sovereignty-Strat.pdf.

9. How to Prevent Power Outages: Tech Solutions for Grid Resilience.
https://eleks.com/expert-opinion/technological-solutions-power-grid-resilience/.

10. AI for the Grid: Opportunities, Risks, and Safeguards. https://www.csis.org/analysis/ai-grid-opportunities-risks-and-safeguards.

11. Generative AI for Power Grid Operations. https://docs.nrel.gov/docs/fy25osti/91176.pdf.

12. AI for Grid Resilience and Security Challenge. https://techconnect.org/ai-for-grid-resilience-and-security-challenge.

13. Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience. https://www.congress.gov/crs-product/R48067

14. Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities. https://www.gssc.lt/wp-content/uploads/2024/05/v03_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf.

15. Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber War. https://www.rnbo.gov.ua/files/НКЦК/2024 06 Cyber digest_ENG.pdf .

16. MITRE ATT&CK ICS Techniques. https://attack.mitre.org/techniques/ics/.

17. MITRE ATT&CK Enterprise Techniques. https://attack.mitre.org/techniques/enterprise/.

18. BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry. https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.

19. Cyber-Attack Against Ukrainian Critical Infrastructure. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01сучасному.

О.О. Бакалинський

КРИТИЧНА ІНФРАСТРУКТУРА, ДОСВІД ЗАХИСТУ

Коли ракетний удар поєднується з кібератакою на енергомережу чи банківську систему, дата-центр, питання стійкості стає питанням національного виживання. Український досвід демонструє, що критична інфраструктура країни — енергетична, фінансова та цифрова — здатна витримувати постійні кібер та комбіновані атаки з 2014 року, при цьому одночасно покращуватись та розвиваючись.

Необхідно зазначити, що операційні технології (OT) та промислові системи управління (ICS) мають специфічні вразливості, в зв'язку з тим, що вони побудовані без вбудованим механізмів кіберзахисту, що роблять їх привабливими для атак. Системи управління включають диспетчерські системи, програмовані логічні контролери та людино-машинні інтерфейси, через які зловмисники можуть впливати на фізичні об'єкти: трансформатори, генератори, лінії електропередач.

У 2015–2016 роках українська енергетична інфраструктура зазнала серії специфічних кібератак, зокрема на «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Масштабні атаки за допомогою BlackEnergy та Industroyer продемонстрували поєднання класичних кіберзагроз і фізичних впливів, таких як вимкнення підстанцій і блокування кол-центрів. Ці інциденти стали каталізатором не лише технічних змін, а й перегляду державної політики у сфері захисту критичної інфраструктури, включаючи централізований моніторинг, вимоги до резервування та координацію операторів енергосистеми. Після певної частини успішних для ворога кібератак, швидке відновлення енергосистем стало можливим завдяки саме не повністю автоматизованим процесам та системам управління електромережою чи окремими її сегментами чи системами, а навпаки збереженим (іноді дійсно архаїчним) можливостям здійснювати підключення саме вручну, і саме це є той кейс, який можливо додасть вартість новому обладнанню, але залишить спроможність швидкого відновлення атакованого сегменту мережі, забезпечивши можливість підключення підстанцій, електромереж, їх окремих сегментів вручну [1-3].

Окремо необхідно врахувати приклад кіберстійкості, який продемонструвала національна банківська система України. Незалежний статус Національного банку України [4, 5], багаторічна діяльність якого базується виключно на ризик-менеджменті, послідовне слідування найсучаснішим практикам кіберзахисту, відповідальне ставлення керівництва до питань забезпечення кіберстійкості та спроможність утримувати високопрофесійний персонал дозволило та дозволяє швидше реагувати на загрози та координувати дії банків і платіжних систем, ніж це можливо на рівні держави в цілому.

Ця автономія обґрунтована високою залежністю фінансового сектору від цифрових послуг, необхідністю забезпечення безперебійного функціонування мереж іта х кіберзахисту. Завдяки незалежності регулятора:

- оперативно впроваджуються тимчасові заходи (як заходи із кіберзахисту, так і інші ініціативи) захисту інформаційних ресурсів та платіжних систем;
- прискорюється координація з правоохоронними та компетентними органами;
- розбудовуються спроможності CSIRT-NBU, забезпечується розвиток власних IT-системи, резервування даних та відновлення роботи критичних сервісів;
- швидше відбувається нормативно-правове унормування найсучасніших рішень із забезпечення стабільної роботи ІКС та кіберзахисту інформаційної інфраструктури;
- забезпечується безперервна робота банківської інфраструктури навіть під час масштабних атак.

Прикладом комплексного підходу до питань стійкості надання банківських фінансових послуг, який варто враховувати, слугує ініціатива Power Banking, яка забезпечує роботу спільної мережі банківських відділень, що була створена за ініціативи Національного банку України. Виконання правил, які пропонує ініціатива, забезпечує роботу банківських послуг під час тривалих відключень електроенергії. До мережі входять відділення, обладнані альтернативними джерелами енергії та зв'язку, посиленою інкасацією та додатковим персоналом. Ці відділення можуть надавати послуги, такі як отримання готівки, платежі, обмін валют та консультації.

Таким чином, українська банківська система демонструє ефективну організаційну та технічну стійкість, що може слугувати моделлю для інших секторів критичної інфраструктури.

Разом з тим, кінетичні та кібератаки часто поєднуються у «dual-domain» сценарії: одночасно пошкоджуються фізичні об'єкти і цифрові системи керування. У випадку України такі атаки охоплювали:

— фішингові кампанії та розповсюдження шкідливого ПЗ для отримання доступу до SCADA та OT-систем;

— зловмисні команди для відключення або спотворення роботи підстанцій;

— атаки на кол-центри та комунікаційні канали, щоб унеможливити повідомлення про аварії.

Сучасні загрози критичній інфраструктурі характеризуються високим рівнем комплексності та взаємопов’язаністю кібер та фізичних ризиків, що зумовлює необхідність інтегрованого підходу до забезпечення її захисту та підвищення резильєнтності [6].

Ефективність захисту енергетичних, фінансових та інших систем, що забезпечують життєзабезпечення залежить від застосування узгоджених

організаційно-технічних і управлінських заходів, які мають базуватись на наступних принципах:

1.Спільний кіберфізичний моніторинг – передбачає інтеграцію даних із сенсорів операційних технологій (OT), мереж SCADA та інформаційних систем (IT) для забезпечення своєчасного виявлення, аналізу та реагування на потенційні атаки.

2.Децентралізовані системи управління – спрямовані на підтримання функціональності критичних об'єктів у разі локального порушення або виведення з ладу окремих компонентів інфраструктури.

3.Публічно-приватне партнерство – забезпечує системний обмін інформацією про кіберзагрози, а також координацію дій між державними інституціями та приватними операторами критичних систем.

4.Резервування та аварійне відновлення – включає дублювання каналів живлення, резервне копіювання даних та реалізацію планів безперервності діяльності (Business Continuity Planning).

5.Формування культури кібербезпеки та підготовка персоналу – охоплює регулярне проведення навчань, тренувальних симуляцій кібератак і підвищення рівня обізнаності щодо методів соціальної інженерії.

6.Таким чином, забезпечення стійкості критичної інфраструктури вимагає синергетичного поєднання технічних, організаційних і людських факторів, спрямованих на мінімізацію ризиків та швидке відновлення функціонування систем у разі інцидентів.

Досвід функціонування держави в умовах війни показали, що: комбіновані атаки є реальними та ефективними, якщо вони не зустрічають достатнього опору; підготовка персоналу, автономія регулятора, наявна регуляція та протоколи взаємодії, надають можливість швидко визначати тактики та техніки протидії кібератакам, а наявність галузевої високопрофесійної команди реагування CSIRT прискорює реагування та підвищує резильєнтність секторів; міжнародна кооперація і обмін досвідом з партнерами допомагають впроваджувати сучасні моделі захисту; резервування критичних систем і розподілена архітектура значно зменшують ризики від одночасних кібератак і фізичних ушкоджень.

Необхідно зауважити що поширення досвіду інших секторів захисту критичної інфраструктури, спроможність секторальних органів їх швидко враховувати, імплементувати та адаптувати забезпечить достатньо високий ступінь резільєнтності держави в наступні роки важкої війни та відновлення.

Таким чином, отриманий Україною досвід захисту критичної інфраструктури пропонує глобальну модель для інших країн:

поєднання кібер- та фізичного захисту є обов'язковим у сучасних умовах;

автономія ключових регуляторів і швидка реакція підвищують стійкість критичних секторів;

інтеграція енергетики, фінансів та телекомунікацій у єдину систему моніторингу і управління забезпечує стабільність під час криз;

публічно-приватне партнерство і навчання персоналу формують культуру безпеки, яка протистоїть складним атакам.

Зазначені висновки необхідно враховувати при розробці законопроектів, які спрямовані на імплементацію в національне українське законодавство європейських директив із стійкості критичної інфраструктури, забезпечення високого рівень безпеки мережевих та інформаційних систем у Європейському Союзі та регламенту з операційної цифрової стійкості фінансового сектору.

1. E-ISAC & SANS Institute Analysis of the Cyber Attack on the Ukrainian Power Grid (2016), https://www.sans.org/reading-room/whitepapers/critical/analysis-cyber-attack-ukrainian-power-grid-37712/.

2. Dragos, CrashOverride / Industroyer Analysis, https://www.dragos.com/resource/crashoverride-analysis-of-the-threat-to-electric-grid-operations/.

3. ICS-CERT, Alert (IR-ALERT-H-16-056-01), https://www.cisa.gov/news-events/ics-alerts /.

4. Закон України «Про Національний банк України», https://zakon.rada.gov.ua/laws/show/679-14#Text.

5. Постанова Національного банку України «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах», https://zakon.rada.gov.ua/laws/show/v0064500-18#Text.

6. ENISA Cybersecurity in the Energy Sector https://www.enisa.europa.eu/publications.

Л.М. Товстенко, О.А.Товстенко, М.А. Косовець

ОБГРУНТУВАННЯ ЗАСТОСУВАННЯ ЕЛЕКТРОННИХ ПЛАТФОРМ ДЛЯ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ЕНЕРГЕТИКИ ЯК РЕЗИЛЬЄНТНА СТРАТЕГІЯ ВИЖИВАННЯ

Вступ

Застосування електронних платформ є критичною умовою для переходу від ієрархічної до децентралізованої енергосистеми, де споживачі стають активними учасниками ринку. Наведемо ключові аргументи на користь їхнього впровадження:

1. Ефективне управління мікромережами. Електронні платформи на базі IoT та штучного інтелекту дозволяють у реальному часі балансувати попит і пропозицію всередині локальних мереж. Це мінімізує втрати при передачі електроенергії (які в централізованих мережах можуть сягати 8%) та забезпечують автономність громад під час масштабних відключень.

2. Пряма торгівля енергією (P2P Trading)та використання технології Blockchain створює прозоре середовище для купівлі-продажу надлишків енергії без посередників. Це дає змогу: монетизувати приватні сонячні або вітрові станції; зменшити цінову волатильність для кінцевих споживачів; гарантувати безпеку транзакцій за допомогою смартконтрактів.

3. Згідно з концепцією «Інтернету енергії», платформи інтегрують розподілені джерела (ВДЕ) у єдину інтелектуальну мережу. Це підвищує кіберстійкість системи та дозволяє оперативно реагувати на критичні навантаження через механізми Demand Response (управління попитом).

1. Розроблення інформаційної моделі взаємодії учасників на інтегрованих ринках електроенергії через нормативні регулювання.

Моделі базуються на стандартах CIM (Common Information Model) для забезпечення сумісності між локальними мікромережами та загальнонаціональною системою.

- Нормативне регулювання: Впровадження правил РДН/ВДР (Ринок «на добу наперед» / внутрішньодобовий ринок) для малих виробників через агрегаторів.
- Інтеграція з ЄС: Синхронізація інформаційних протоколів з європейським ринком для транскордонної торгівлі енергією.
- Сфери застосовності: Визначено межі між гуртовим ринком, ринком допоміжних послуг та локальними ринками гнучкості.

Моделювання підтвердило, що використання єдиного семантичного простору даних дозволяє інтегрувати малу генерацію в загальну енергосистему без втрати керованості. Визначено функції цифрового регулятора як «арбітра» даних, що забезпечує недискримінаційний доступ до мереж.

Перехід до децентралізації вимагає відходу від статичних ієрархічних моделей. Для інтеграції децентралізованих одиниць (мікромереж) у загальний ринок розроблено модель «Гнучкого вузла». Вона дозволяє регулятору виділити сфери застосованості. Модель адаптована для роботи на ринку допоміжних послуг та балансуючому ринку. Визначено три рівні взаємодії: *локальний* (P2P у межах мікромережі), *регіональний* (ринок послуг гнучкості) та *глобальний* (інтеграція в ОЕС України).

• Функції регуляторів: Модель передбачає автоматизацію нагляду через «регуляторні пісочниці», де правила ринку адаптуються автоматично на основі аналізу великих даних (Big Data). Посередники (агрегатори) тепер виконують роль цифрових хабів, що конвертують технічні параметри (кВт·год, напруга) у ринкові заявки автоматично.

• Результат: Створено семантичну модель на основі IEC 62325, що забезпечує бачити розподілену генерацію як єдиний віртуальний ресурс, безшовну» передачу даних між оператором системи розподілу (ОСР) та агрегаторами.

2. Розроблення методів та інформаційних технологій для організації взаємодії учасників енергоринків.

Автоматизація документообігу між учасниками (виробниками, операторами мереж, споживачами) через використання кваліфікованого електронного підпису (КЕП) та платформ типу *ETS/UA* для швидкої реєстрації та укладання угод. Централізовані реєстри гарантій походження «зеленої» енергії. Розроблено технологію автоматизованого укладання договорів приєднання та купівлі-продажу. Реалізація на базі децентралізованих реєстрів, де кожен договір має унікальний хеш-ідентифікатор, що унеможливлює його підробку.

Традиційні паперові договори є бар'єром для динамічного енергоринку. Впроваджено методику динамічного профілювання договірних умов, де параметри (обсяги, цінові коридори) можуть змінюватися автоматично. Використовуємо розподілені реєстри (DLT) для фіксації юридичних прав та зобов’язань. Це створює незмінну історію взаємовідносин, доступну для аудиту в реальному часі. Розробляється методика автоматизованого життєвого циклу енергетичного контракту. Використовуємо розподілені реєстри (DLT) для верифікації прав власності на енергію. Електронний договір інтегрує в собі технічні умови приєднання та комерційні умови постачання. Кожна транзакція підписується КЕП на рівні протоколу зв'язку лічильника, що робить договір «живим» документом, який автоматично оновлюється при зміні тарифів або обсягів споживання.

Розробляється методика динамічного контрактного управління на базі DLT (Distributed Ledger Technology). Де замість статичних PDF-документів впроваджуємо "структуровані об'єкти даних", що містять алгоритмічні умови (наприклад, зміна ціни залежно від часу доби). Реалізація на базі приватного

блокчейну дозволяє фіксувати факт укладання угоди миттєво, що критично для ринків, які працюють у реальному часі (Real-time markets).

Впроваджено методику динамічного контрактування на основі розподілених реєстрів. Використовуємо кваліфіковані електронні позначки часу та хешування умов договору в блокчейн-ланцюг. Таким образом договір стає "цифровим об'єктом", який автоматично активує постачання при виконанні технічних умов приєднання, зафіксованих IoT-датчиками.

В результаті маємо практичні результати та переваги.

- Скорочення транзакційних витрат: Автоматизація укладання договорів знижує адміністративні видатки енергокомпаній на 30-50%.
- Масштабованість: Можливість одночасного обслуговування мільйонів мікроугод (P2P-торгівля між сусідами), що неможливо в ручному режимі.
- Юридична безпека: Незмінність записів у розподіленому реєстрі виключає можливість рейдерського захоплення активів або підробки умов постачання.

Традиційні методи документообігу не здатні забезпечити динамічність децентралізованого ринку. Розроблений метод ієрархічного структурування умов енергозабезпечення перетворює договір на набір виконуваних правил:

- Метод атрибутивного підписання: Використання КЕП (кваліфікованого електронного підпису) не лише для суб'єкта (директора/власника), а й для об'єкта (інтелектуального лічильника/інвертора), що підтверджує технічну спроможність виконання договору.
- Метод динамічних додатків: Основна частина договору фіксує юридичні засади, а техніко-економічні додатки (ціна, графік, ліміти) оновлюються автоматично на основі ринкових сигналів.
- Метод автоматичного комплаєнсу: Перевірка нормативних обмежень (наявність ліцензій, "зеленого" тарифу, технічних умов приєднання) інтегрована в процес укладання договору як обов'язкова верифікація метаданих.
- Використання Blockchain для автоматичного виконання умов без посередників.
- Використання Смарт-контрактів, які забезпечують миттєву оплату при досягненні певних обсягів генерації або споживання.
- Можливість застосування алгоритмів криптографічного захисту.
- Створено програмні алгоритми для автоматичного клірингу (розрахунків) на основі фактичних даних лічильників.
- Моделювання: Експерименти на базі архітектури Ethereum/Hyperledger показали здатність системи обробляти до 10 000 мікротранзакцій за секунду. Експерименти проводилися в середовищі Ethereum-compatible (EVM) мереж. Доведено, що використання алгоритму

консенсусу Proof of Authority (PoA) дозволяє проводити розрахунки між сусідами за < 2 секунди.

• Смарт-логіка: Контракт автоматично перераховує кошти від покупця до продавця в момент фіксації передачі енергії, нівелюючи ризики неплатежів.

• Специфікація смарт-контрактів для P2P-торгівлі та алгоритми прогнозування генерації в умовах динамічного середовища оновлюють механізм розрахунків та мінімізує фінансові ризики, робить прозорими процеси взаємодії між IoT-пристроями. Одним із ключових елементів цієї технології є смарт-контракти.

• Функціонал: Смарт-контракт виконує роль ескроу-рахунку: кошти блокуються при замовленні енергії та миттєво перераховуються виробнику за фактом підтвердження генерації датчиками IoT.

Смарт-контракти усувають потребу в довірі між незнайомими контрагентами та зменшують транзакційні витрати. Доведено, що смарт-контракти знижують операційні витрати на білінг на 40-60%, оскільки оплата відбувається автоматично за сигналом лічильника.

3. Розроблення методів та інформаційні технології для організації взаємодії учасників енергоринків з динамічним зовнішнім середовищем.

Розроблена система на базі Artificial Intelligence (AI) для прогнозування генерації ВДЕ (сонячні, вітрові станції). Адаптована для використання методів Demand Response(управлінн я попитом) для балансування мережі в умовах нестабільності.

Моніторинг прогнозування включає онлайн-аналіз топології мережі та автоматичне відновлення після збоїв, математичну модель оцінки вразливості енергоринків до зовнішніх шоків (кібератак, погодних аномалій, різких коливань цін).

• Аналіз вразливості: Виявлено, що децентралізовані платформи на 40% стійкіші до каскадних відмов порівняно з централізованими.

• Метрики стійкості: Впроваджено технологію вимірювання Resilience Score, яка в реальному часі оцінює здатність системи до самовідновлення (Self-healing). Децентралізовані системи більш вразливі до кіберзагроз, але стійкіші до фізичних руйнувань. Впроваджено коефіцієнт автономності мікромережі та індекс живучості системи.

• Вразливість: Розроблено модель «атаки на відмову» (DoS) та методику захисту через розподілений консенсус.

• Технологія: Використання цифрових двійників (Digital Twins) для прогнозування поведінки системи під впливом екстремальних погодних факторів.

Система моніторингу та оцінки стійкості до зовнішніх шоків (кібератаки, погодні аномалії) включає:

• Моделювання вразливості: Розроблено математичні моделі прогнозування каскадних відмов у децентралізованих мережах.

• Технології вимірювання: Впроваджено індекс Resilience Score, який обчислюється на основі швидкості самовідновлення (self-healing) локальних сегментів після зовнішнього втручання.

• Використання Bayesian Networks для моделювання вразливостей при різких змінах погодних умов або кібератаках.

• Вимірювання загальної стійкості через індекс R-SI (Resilience Stability Index), що дозволяє системі автоматично переходити в ізольований (острівний) режим, динамічний показник, що вимірює швидкість відновлення ринкових операцій та фізичного балансу після зовнішнього шоку.

• Метрика автономності (Self-Sufficiency Ratio): Розрахунок здатності окремих кластерів (Microgrids) переходити в ізольований режим роботи зі збереженням внутрішнього ринку.

• Технологія реального часу: Використання Stream Analytics для постійного вимірювання параметрів якості енергії та швидкості клірингу транзакцій, що дозволяє виявляти деградацію системи до моменту настання аварії.

Розроблення розподілена інформаційна технологія для розподілених систем енергетики на базі архітектури Microgrids, де кожен вузол має власну систему керування та збереження даних. Інтеграція систем зберігання енергії (BESS) та grid-forming рішень для стабілізації частоти. Обробка даних безпосередньо на пристроях обліку для мінімізації затримок. Реалізовано систему керування об'єктами малої генерації (сонячні СЕС, вітрові ВЕС, системи зберігання BESS). Як технологічне рішення використано Multi-Agent Systems (MAS), де кожна енергоустановка діє як автономний агент, що максимізує прибуток власника при дотриманні технічних обмежень мережі.

Централізована обробка даних від мільйонів датчиків створює критичні затримки. Для їх мінімізації впроваджено архітектуру Edge Computing (периферійні обчислення). Розумні лічильники самостійно приймають рішення про скидання навантаження або активацію накопичувачів.

Реалізовано алгоритми синхронізації інверторів у безінерційних мережах, що дозволяє підтримувати стабільну частоту 50 Гц без магістральних станцій.

Розподілена обробка даних (Edge Computing) дозволяє сонячним інверторам та системам зберігання (BESS) приймати рішення про стабілізацію напруги локально, не чекаючи команди з центрального диспетчерського пункту. Це забезпечує можливість роботи мікромережі в режимі «острова» під час аварій в основній мережі, підтримуючи критичне навантаження через внутрішні ресурси.

Для переходу від централізованого диспетчерського управління до ієрархічно-розподіленого розроблено архітектуру "Multi-Agent Cloud-Edge", яка забезпечує обробку даних максимально близько до джерела генерації.

Для рівня кластера мікромережі розроблено Метод Fog Computing (Туманні обчислення), де здійснюється локальна координація між сусідніми вузлами (P2P) без участі центрального хмарного сервера, що забезпечує працездатність системи при обриві магістральних каналів зв'язку.

4. Розроблення розподілених інформаційних технологій для цифрових платформ енергетики.

Для реалізації розробки децентралізованої енергосистеми обґрунтовано впровадження наступних методів та технологій:

- Розробка єдиної цифрової екосистеми, що об'єднує фізичну інфраструктуру та ринкові механізми.
- Використання хмарних технологій та API для підключення нових гравців (електромобілі, розумні будинки).
- Розробка платформи для токенізації енергетичних активів та залучення інвестицій через «зелені» аукціони.

Розроблено та протестовано архітектуру цифрової платформи для децентралізованої системи енергетики. Реалізовано кейс «Енергетична громада», де учасники через мобільний додаток керують споживанням своїх приладів, автоматично продаючи надлишки енергії сусідам у пікові години. Платформа побудована на мікросервісній архітектурі з використанням Docker/Kubernetes. Підтверджена можливість зниження вартості електроенергії для кінцевого споживача на 15-20% за рахунок оптимізації локального споживання. Кінцевим результатом якої є діюча екосистема взаємодії.

Створено діючий прототип цифрової платформи MVP (Minimum Viable Product) для децентралізованої платформи. Прототип включає користувацький інтерфейс (мобільний застосунок), модуль блокчейн-білінгу та шлюзи інтеграції з розумними приладами обліку. Платформа дозволяє створювати «Енергетичні кооперативи», де громади можуть спільно інвестувати в генерацію та розподіляти прибутки через автоматизовані цифрові інструменти без залучення сторонніх бухгалтерських сервісів. Модель забезпечує спільну мову для локальних громад та магістральних мереж. Вона дозволяє автоматично агрегувати дані від дрібних виробників у єдиний ринковий лот.

Впроваджено цифрові профілі ролей, де Регулятор має доступ до "незмінних логів" ринку для аудиту ціноутворення в реальному часі. Забезпечено 100% сумісність даних при транскордонному обміні енергією з країнами ЄС. Компонентами забезпечення обміну є: Marketplace для P2P-торгівлі між сусідами, Asset Management для відстеження стану обладнання, Tokenization Engine для обліку "зелених" сертифікатів.

Розроблено архітектуру хмарно-орієнтованої цифрової платформи як сервісу (PaaS). Прототип платформи об’єднує API для білінгу, Marketplace для торгівлі та модуль прогнозування генерації на базі Machine Learning. Платформа дозволяє громадам створювати "віртуальні електростанції" (VPP), підвищуючи дохідність приватних сонячних станцій на 20-30%.

Розробка інформаційних моделей для інтегрованих ринків електроенергії в умовах децентралізації вимагає створення єдиного семантичного простору, де технічні параметри енергосистеми синхронізовані з нормативними правилами ринку. В основу моделі покладено розширення стандарту Common Information Model (CIM), що дозволяє уніфікувати обмін даними між магістральними мережами (TSO), розподільчими мережами (DSO) та новими учасниками (агрегаторами, prosumer-ами).

Висновки

Розроблені методи дозволяють створити автономні енергетичні громади, де розрахунки відбуваються без участі людини, а енергосистема сама себе балансує економічними стимулами, закладеними в код смарт-контракту.

Впровадження цих методів дозволяє перетворити енергоринок із "реактивного" (що реагує на події, які вже сталися) на "проактивний" (що передбачає та нівелює загрози до їх виникнення). Це підвищує загальну стійкість системи на 35-45% у порівнянні з традиційними ієрархічними моделями керування.

Розроблення розподілених інформаційних технологій для розподілених систем енергетики розподіленого керування перетворює з пасивної енергомережі на інтелектуальну екосистему Microgrids.

- Впровадження цих методів дозволяє підвищити практичні результати, а саме: Підвищення надійності: Час відновлення електропостачання (SAIDI) скорочується на 60% завдяки локальній автоматизації.
- Масштабованість: Можливість інтеграції до 100 000 нових вузлів генерації на рік без модернізації центральних центрів обробки даних.

Розроблена архітектура та програмна реалізація цифрової платформи, що інтегрує фізичні активи енергетики в єдине інформаційне середовище, методика агрегації розподілених ресурсів (СЕС, вітряки, електромобілі) у єдиний керований об'єкт.

- Алгоритм централізованого завдання (Dispatching): Платформа формує єдиний графік навантаження для тисяч малих учасників, виступаючи для системного оператора (Укренерго) як один великий енергоблок.
- Оптимізація портфеля: Використання методів лінійного програмування для максимізації прибутку учасників платформи при мінімальних витратах на балансування.

Розроблені технології створюють цифровий фундамент для децентралізованої енергосистеми України. Вони дозволяють перетворити

енергетику з інертної інфраструктури на гнучкий ринок послуг, де кожен громадянин може бути активним гравцем, підвищуючи енергонезалежність держави.

Інформаційні моделі взаємодії учасників на інтегрованих ринках електроенергії через нормативні регулювання. Обгрунтування та моделювання сфер застосовності різних ринків електроенергії, умов їх сумісності та ефективної інформаційної взаємодії, функцій регуляторів і посередників.

Для переходу від централізованого диспетчерського управління до ієрархічно-розподіленого розроблено архітектуру "Multi-Agent Cloud-Edge", яка забезпечує обробку даних максимально близько до джерела генерації.

Розроблено та впроваджено наступні програмно-технологічні рішення:

1. Мультиагентна система керування (MAS): Кожен об'єкт розподіленої генерації (PV-інвертор, вітроустановка) представлений інтелектуальним агентом. Агенти використовують протоколи консенсусу (наприклад, Raft або Paxos) для узгодження обсягів видачі потужності в мережу.

2. Розподілені системи моніторингу (WAMS на низькій напрузі): Використання технології синхронізованих векторних вимірювань (Phasor Measurement Units, PMU), адаптованої для розподільчих мереж. Це дозволяє бачити динамічні процеси в мікромережах з точністю до мілісекунд.

3. Віртуальні електростанції (VPP) на базі мікросервісів: Технологія об'єднання тисяч дрібних установок у єдиний інформаційний профіль для участі у балансуючому ринку. Реалізовано через контейнеризацію (Kubernetes), що забезпечує миттєве масштабування при підключенні нових prosumer-ів.

Обґрунтовано метод горизонтального балансування, при якому надлишок енергії в одному сегменті мережі автоматично компенсує дефіцит в іншому через локальні IT-команди, минаючи верхні рівні управління. Це знижує навантаження на магістральні мережі та зменшує втрати енергії на 12-15%.

В результаті виконаних досліджень ми оримали програмно-апаратний комплекс розподіленого керування об'єктами малої генерації, що забезпечує автономну роботу енергорайону (Microgrid) у режимі "острова" прягом необмеженого часу, що дозволило отримати можливість платформи підтримувати внутрішній енергобаланс громади в режимі "острова" при повному відключенні від зовнішньої мережі. Вперше реалізовано концепцію "Енергетичного Інтернету" (IoE) на рівні локальної громади України, де інформаційні потоки та фінансові розрахунки повністю синхронізовані з фізичними потоками у реальному часі.

В.Ю. Зубок, А.В. Давидюк

ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНОГО СЕКТОРУ ПІД ВПЛИВОМ КОМПЛЕКСНИХ ЗАГРОЗ ШЛЯХОМ ВОЄННО-ІГРОВОГО МОДЕЛЮВАННЯ

Вступ. Енергетичний сектор перебуває під постійним впливом гібридних атак, де кібер, фізичні, інформаційні та політичні загрози взаємодіють, підсилюючи одна одну та сприяючи каскадній ескалації наслідків. Постає завдання інтегровано відтворювати складні багатодоменні сценарії, аналізувати взаємозалежності та тестувати управлінські рішення, постійно вдосконалювати міжвідомчу координацію та формувати проактивні стратегії підвищення резильєнтності в умовах невизначеності. Зручним інструментом для виконання таких завдань в безпечному середовищі (без впливу на реальні системи) постає воєнно-ігрове моделювання [1].

Воєнно-ігрове моделювання (wargaming) – це метод моделювання сценаріїв конфлікту із метою аналізу рішень, поведінки сторін і можливих наслідків. У сучасному професійному контексті це аналітичний інструмент підтримки прийняття рішень, до якого входять рольові сценарії, моделювання ескалації, тестування стратегій і планів, оцінка стійкості (резильєнтності) систем [2], [3].

Методологія. Пропонується проведення воєнно-ігрового моделювання (ВІМ) для відпрацювання практичних рішень з підвищення резильєнтності енергетичного сектору під комплексними загрозами (кібер, фізичних, інформаційних, політичних). Аудиторія ВІМ – керівники енергетичних компаній, кіберкоманди, фахівці зі стратегічних комунікацій, урядові представники, фасилітатор. У результаті проведення ВІМ має сформуватись більш адаптивна та проактивна модель управління резильєнтністю в умовах високої невизначеності. *Ключові сутності* ВІМ перелічені в табл.1.

Таблиця 1. Пояснення основних сутностей ВІМ

№	Сутність	Опис
	Раунди	Етапи сценарію, що починаються з внесення питання чи опису події, та завершуються ухваленням рішення
	Рішення	Консенсусне обрання одного з варіантів реагування, що пропонуються сценарієм
	Треки	Сфери компетенцій
	Інжекти	Додаткові варіації сценарію
	Наслідки	Закладені в сценарії результати прийняття рішень
	Фасилітатори	Особи, що не входять до складу гравців, але виконують функції ведучого, вносять інжекти, слідкують за дотриманням порядку ухвалення рішень, нараховують бали тощо

Однією з ключових сутностей є рішення, що ухвалюються гравцями. З метою напрацювання навичок взаємодії пропонується така *система ухвалення рішень*. Рішення повинні прийматись консенсусом. Фасилітатор слідкує за рівноправним доступом до висловлення думок. Однак час на прийняття рішень лімітовано. Неприйняття рішення у відведений для раунду час оцінюється найнижчим балом по треку, який є найбільш важливим в раунді.

Можливі *треки* (сфери компетенцій):

OPER – операційна стійкість енергосистеми: фізична резильєнтність, дії персоналу, швидкість відновлення.

CYBER – кіберрезильєнтність : захищеність автоматизованих систем управління технологічними процесами, ефективність команд кіберзахисту (SOC).

COORD – координація стейкхолдерів (галузева команда реагування на комп'ютерні інциденти, уряд, регулятор, партнери).

TRUST – довіра: «інформаційний фронт», комунікації з громадськістю, медіа, персоналом.

INST – інституційна цілісність: внутрішня єдність, керованість і спроможність виконувати свої функції в умовах кризи.

Система оцінювання передбачає оцінку впливу кожного рішення на кожен трек у вигляді балів. Таблиця нарахування балів відома лише фасилітаторам. Приблизний вигляд таблиці з для нарахування балів приведено в табл. 2.

Таблиця 2. Приклад нарахування балів за один раунд BIM

	Варіант відповіді	**OPER**	**CYBER**	**TRUST**	**INST**
A	Організувати threat hunting і red team	0	+2	+1	+1
B	Посилити моніторинг без зміни процесів	+1	+1	0	0
C	Ігнорувати	0	0	-1	-1
D	Повідомити уряд і залучити галузевий CERT	-1	+2	+1	+2
F	Делегувати кіберзахист підряднику	0	+1	+1	0
Z	Нема спільного рішення	0	-2	0	-1

Для зведення результатів нарахування балів необхідно створити рейтингову систему оцінювання, де певним діапазонам балів надаються пояснення. Наприклад, оцінка суми балів по треку OPER (операційна стійкість) S_o:

$5 \leq S_o \leq 8$: система стійка, відновлення швидке.

$1 \leq S_o \leq 4$: система вціліла, але потребує вдосконалень.

$S_o \leq 0$: серйозні проблеми з відновленням та каскадні ефекти.

Висновок. Запропонований підхід до проведення воєнно-ігрового моделювання створює структуроване середовище для відпрацювання взаємодії та оцінювання рішень в умовах гібридних загроз і обмеженого часу, з урахуванням міждоменних залежностей та потенційної каскадної ескалації. Поєднання багатотрекової системи оцінювання та консенсусного ухвалення рішень дозволяє сформувати узгоджені практики реагування.

1. Sarjakivi, P., Ihanus, J., and Moilanen, P. (2024) Using Wargaming to Model Cyber Defense Decision-Making: Observation-Based Research in Locked Shields. European Conference on Information Warfare and Security, ECCWS, pp. 453–460.

2. Business Wargaming Explained in Depth (online). URL: https://strategicmanagementinsight.com/tools/business-wargaming-explained/ (доступ 20.03.2026).

3. Callagan, P., and Fiadotau, M. (2024) Using Meaningful Choices and Uncertainty to Increase Player Agency in a Cybersecurity Seminar Game. Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 14475 LNCS, pp. 23–32.

С.В. Матвєєв, І.В. Івченко

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ФОРМУВАННІ СТІЙКОЇ АРХІТЕКТУРИ ЕНЕРГОСИСТЕМИ УКРАЇНИ

Анотація У статті розглядається трансформація енергетичної системи України станом на 2026 рік у відповідь на воєнні виклики та структурні зміни в енергетиці. Показано, що поєднання децентралізації та штучного інтелекту (ШІ) створює нову модель енергосистеми, яка є більш гнучкою, стійкою та адаптивною. Особлива увага приділяється ролі розподіленої генерації, систем накопичення енергії та концепції віртуальних електростанцій (VPP - Virtual Power Plant). Обґрунтовано, що масове впровадження побутових накопичувачів може частково замінити втрачену теплову генерацію, а ШІ виступає ключовим інструментом координації цих ресурсів.

Після 2022 року енергетична система України опинилася в умовах безпрецедентного навантаження. Руйнування великих електростанцій, регулярні атаки на інфраструктуру та нестабільність енергопостачання змусили переглянути сам підхід до побудови енергосистеми. Як показують дослідження Міжнародного енергетичного агентства (IEA, 2024), централізована модель із великими вузловими електростанціями є вразливою в умовах сучасних загроз. У відповідь на це Україна фактично почала перехід до нової моделі - більш розподіленої, цифрової та гнучкої [1].

Традиційно енергосистема будувалася навколо великих електростанцій - теплових, атомних, гідро. Така модель добре працює в стабільних умовах, але має критичний недолік: уразливість. Коли одна велика станція виходить з ладу, система втрачає значний обсяг потужності. Саме це стало ключовою проблемою для України після масованих атак на енергетичну інфраструктуру.

Натомість сучасна модель поступово переходить до комбінованої архітектури, яка включає: централізовану базову генерацію (АЕС, ГЕС), розподілену генерацію (сонячні та вітрові установки), локальні накопичувачі енергії, мікромережі та цифрові системи управління. Такий підхід дозволяє не лише підвищити надійність, а й зробити систему більш резильєнтною - здатною працювати навіть при часткових пошкодженнях.

У міру ускладнення енергосистеми традиційні методи управління стають недостатніми. Тут на перший план виходить штучний інтелект, який використовується для: прогнозування споживання електроенергії; передбачення генерації з ВДЕ; управління накопичувачами; балансування системи в реальному часі.

Інакше кажучи, ШІ виконує роль «диспетчера нового покоління», який здатен обробляти величезні обсяги даних і приймати рішення швидше за людину [2]. Особливо важливо, що ШІ дозволяє об’єднати тисячі малих енергетичних об’єктів у єдину керовану систему.

Однією з найважливіших тенденцій останніх років стало стрімке зростання ринку накопичувачів енергії. За оцінками галузевих джерел у 2025

році було введено близько 500 МВтгод накопичувачів, у 2026 році очікується ще ≈1000 МВтгод. Таким чином, загальний обсяг може сягати 1,5 ГВтгод [3]. Цей зріст відбувається не лише за рахунок великих проєктів, а й завдяки масовому встановленню систем у домогосподарствах і бізнесі. Причини очевидні: нестабільність електропостачання, потреба в автономності, здешевлення технологій, розвиток ринку $LiFePO_4$-акумуляторів.

Раніше балансування енергосистеми забезпечували теплові електростанції. Сьогодні, коли значна частина цих потужностей втрачена, на зміну приходить новий підхід - розподілене балансування. Уявімо, що лише 10% домогосподарств мають накопичувачі по 10 кВтгод, тоді сумарний потенціал сягає 15 ГВтгод. Це величезний ресурс, який можна використовувати для покриття пікових навантажень, стабілізації мережі та аварійного резервування. Фактично, мільйони малих батарей можуть виконувати ту саму функцію балансування енергосистеми, що раніше виконували великі теплоелектростанції.

Ключ до ефективного використання цих ресурсів - їх об'єднання. Тут з'являється концепція Virtual Power Plant (VPP) - віртуальної електростанції, яка об'єднує: домашні батареї, сонячні панелі та інші об'єкти малої генерації. ШІ координує роботу цієї системи, визначаючи: коли заряджати батареї; коли віддавати енергію в мережу; як мінімізувати навантаження. За оцінками IEA (2024), такі системи можуть зменшити пікове навантаження на 20 - 30% [1].

Попри великий потенціал, існують і серйозні виклики: потреба в сучасній цифровій інфраструктурі, ризики кібербезпеки, відсутність чітких правил для VPP, необхідність значних інвестицій. Також важливо забезпечити стандартизацію та інтеграцію нових технологій у національну енергосистему.

Україна фактично перебуває у точці переходу до нової енергетичної моделі. Централізована енергосистема поступається місцем гібридній. ШІ стає ключовим елементом управління. Накопичувачі енергії набувають статусу стратегічного ресурсу. Побутові батареї можуть частково замінити балансуючі можливості теплової генерації. VPP формує основу енергосистеми майбутнього. У підсумку формується нова парадигма: енергосистема як мережа інтелектуально керованих розподілених ресурсів.

1. International Energy Agency. (2024). *Empowering Ukraine through a decentralised electricity system.* https://www.iea.org/reports/empowering-ukraine-through-a-decentralised-electricity-system.

2. Mastoi, M. S., et al. (2026). *AI-driven optimization in smart grids. Energy Reports*. https://greendealukraina.org/assets/images/reports/gdu-technologies-for-ua-grid.pdf.

3. AES ET UA. (2026). *Зима 2026: іспит на автономність та бум на накопичувачі.* https://aesetua.com/zyma-2026-ispyt-na-avtonomnist-ta-bum-na-nakopychuvachi/.

О.В. Немикіна, Д.Н. Капля, Б. Ю. Худолій. О.С. Немикіна

ОЦІНКА ВИРОБНИЦТВА ЕЛЕКТРОЕНЕРГІЇ ДАХОВОЇ СОНЯЧНОЇ СТАНЦІЇ

Для власників невеликих будівель, комунально-побутових споживачів, промислових споживачів найбільш актуальної є встановлення дахової сонячної електричної станції для зниження споживання електричної енергії. Калькулятор PVWatts® розраховує місячне та річне виробництво електроенергії фотовольтаїчною системою за допомогою погодинного моделювання протягом одного року, припускаючи , що в одному році є 8760 годин. Це дозволяє домовласникам, власникам невеликих будівель, комунально-побутових споживачів, промисловим споживачам легко оцінювати продуктивність потенційних фотоелектричних установок [1]. Нижче наведено опис алгоритму, який PVWatts® використовує для розрахунку годинної генерації електроенергії фотоелектричної системи.

- Обчислення погодинної площі сонячного опромінення (ПСО) на основі горизонтального опромінення, широти, довготи та часу для даних сонячних ресурсів, а також на основі вхідних даних типу масиву, нахилу й азимута.
- Розрахування ефективного опромінення ПСО для врахування втрат на відбиття від поверхні модуля залежно від кута падіння сонячного світла.
- Розрахування температури комірки на основі типу масиву, опромінення ПСО, швидкості вітру та температури навколишнього середовища. Модель температури комірки передбачає висоту модуля 5 метрів над землею та встановлену номінальну робочу температуру комірки 49°C для варіанту фіксованого кріплення на даху і 45°C для інших параметрів масиву.
- Обчислення постійного струму на виході масиву відповідно до потужності системи постійного струму при стандартному освітленні ПСО 1000 Вт/м² і розрахованій температурі комірки, припускаючи, що еталонна температура комірки становить 25°C.
- Обчислення вихідної потужність змінного струму системи на основі обчисленого вихідного струму постійного струму та втрат системи та номінальної вхідної ефективності інвертора (96 % за замовчуванням) з коригуванням ефективності інвертора при частковому навантаженні, отриманому з емпіричних вимірювань продуктивності інвертора.

Калькулятор PVWatts складається з наступних меню :

- ДАНІ ЩОДО СОНЯЧНИХ РЕСУРСІВ;
- ІНФОРМАЦІЯ ПРО СИСТЕМУ;
- РЕЗУЛЬТАТИ.

Розташування фотовольтаїчної системи в м. Київ для отримання **ДАНИХ ЩОДО СОНЯЧНИХ РЕСУРСІВ** . У вікні «ІНФОРМАЦІЯ ПРО СИСТЕМУ» вводимо наступні вхідні дані.

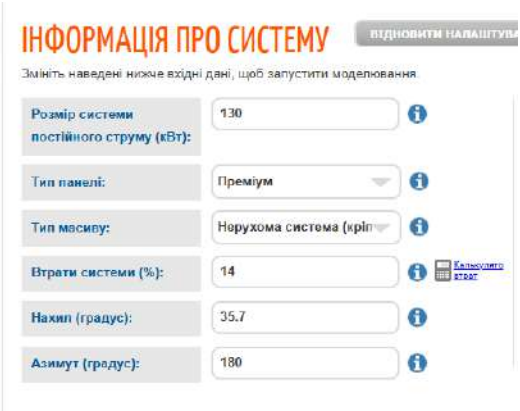


Рисунок 1. – Ввод параметрів в ІНФОРМАЦІЯ ПРО СИСТЕМУ

Тип сонячного масиву- фіксований тип . Оптимальний цілорічний кут нахилу сонячних модулів прийняти з калькулятора розрахунку кута нахилу PV панелей [2-4].

Місяць	Сонячне випромінювання (кВт·год/м²/день)	Енергія змінного струму (кВт·рік)
Січень	1.50	4794
Лютий	2.58	7 025
Березень	3.75	11 566
Квітень	4.89	14 018
Травень	5.65	16 274
Червень	6.12	16 744
Липень	6.06	17 038
Серпень	5.83	16 527
Вересень	4.46	12 458
Жовтень	2.60	7 894
Листопад	0.97	2860
Грудень	0.63	1908
За рік	3.76	129 707

Рисунок 2. – Результат розрахунку сонячної інсоляції та виробництво електроенергії PV системою

Місцезнаходження та ідентифікація станції	
Запит на локацію	Київ
Джерело даних про погоду	Широта, Довжина: 50.45, 30.54 0.7 милі
Широта	50,45° пн.ш.
Довгота	30,54° сх. д.
Технічні характеристики фотовольтаїчної системи	
Потужність системи постійного струму	130 кВт
Тип панелі	Преміум
Тип масивний	Нерухома система (кріплення на даху)
Втрати системи	14%
Нахил масиву	35,7°
Азимут масиву	180°
Коефіцієнт поточного та змінного струму	1.2
Ефективність інвертора	90%
Коефіцієнт покриття землі	0,4
Альбедо	0,2
Двосторонній	Ні (0)
Щомісячна втрата випромінювання	січень 0% лютий 0% березень 0% квітень 0% Травень 0% Червень 0% Липень 0% серпень 0% вересень 0% жовтень 0% листопада 0% грудень 0%
Показники продуктивності	
Коефіцієнт потужності постійного струму	11,4%

Рисунок 3. – Специфікація для PV системи для фіксовоного масиву

Таблиця 1. Характеристики фотоелектричної системи.

Параметр	Значення
Тип сонячної електростанції	Мережева під власне споживання
Локація	Киев (50°27′)
Номінальна потужність інвертора, кВт	100
Потужність сонячного масиву (СМ), кВт	130
Напруга підключення змінного струму, В	380 ± 20%
Напрям встановлення по азимуту	Південь (180º)
Кут встановлення сонячного масиву, град	35,7
Площа встановлення сонячного масиву, м^2	1512
Площа даху цеха, м. кв.	3250
Тип даху	Плоский
Площа СМ відносна площі даху цеха,%	1512/3250*100%=46,5%
Втрати системи,%	14
Ефективність інвертора, %	90
Тип фотомодуля	Преміум, Кристалічний кремній, ККД=21%

Аналітичний розрахунок виробництва електроенергії фотовольтаїчною системою. Струм сонячних панелей є постійним (Direct current). Для його перетворення в змінний струм (Alternating current) використовується інвертор.

Електроенергія постійного струму (DC), що генерується PV панелями фіксованого масиву (нерухома система), Вт·год:

- протягом доби:

$$W_{\text{ген\_DC}} = k \cdot E \cdot P_{\text{мод}\Sigma} / 1000 , \quad (1)$$

- на протязі місяця:

$$W_{\text{ген\_мес\_DC}} = W_{\text{ген}} \cdot n , \quad (2)$$

де E – сонячна радіація, яка потрапляє на поверхню Землі для обраної території за добу, Вт· год/м^2; в грудні E=630 Вт· год /м^2/ за добу, рис 2 .

k – коефіцієнт, що враховує втрату потужності PV панелей при перетворенні енергії (наприклад: Забруднення PV панелі); його величина становить близько 0,7÷ 0,85, k =0,86 втрати потужності становитиме 14% [5].

$P_{\text{мод}\Sigma}$ - сумарна потужність фотоелектричних (PV) панелей (масиву), Вт ;

n – кількість днів на місяці.

Енергія змінного струму (AC) з урахуванням ККД інвертору

$$W_{\text{ген\_мес\_AC}} = W_{\text{ген\_мес\_DC}} \cdot \eta_i \quad (3)$$

де η_i – ККД інвертору у відносних одинцях, η_i =0,9, рис 3.

Генерація електроенергії постійного струму (DC) PV панелями:

$W_{\text{ген\_DC}} = 0,86 \cdot 130 \cdot 10^3 \cdot 630 / 1000 = 70,43$ кВт · год (за добу);

$W_{\text{ген_мес_DC}} = 70,43 \cdot 31 = 2183,45$кВт · *год* (за місяць)

Енергія змінного струму (AC) з урахуванням ККД інвертору, вираз (3):

$W_{\text{ген\_мес\_AC}} = 2183,45 \cdot 0,9 = 1965,1$ к Вт· год

Чисельний розрахунок енергії змінного струму із використанням PVWatts складає 1908 к Вт· год (за місяць-грудень).

Аналіз місячних даних, як для сонячної інсоляції, так і для виробництва енергії, чітко показує сильну сезонну залежність. Генерація є максимальною в літні місяці (наприклад, у червні-серпні) та мінімальною у зимові місяці (грудень-січень) через зміну висоти сонця та тривалості світлового дня.

Було проведено порівняння результатів чисельного моделювання в PVWatts з аналітичним розрахунком для нерухомої системи за грудень. Результати виявилися дуже близькими. Мінімальна розбіжність, близько 2%. підтверджує коректність застосованої аналітичної моделі для попередніх оцінок генерації.

Таким чином, калькулятор PVWatts є зручним та точним інструментом для швидкої оцінки потенціалу сонячної електростанції з урахуванням її типу та географічного розташування.

1. PVWatts®Calculator https://pvwatts.nrel.gov/pvwatts.php.
2. Single Axis Trackers https://sinovoltaics.com/learning-center/csp/single-axis-trackers/.
3. Немикіна О. В., Демченко Б. С., Немикіна О. С. ОЦІНКА ВИРОБЛЕННЯ ЕЛЕКТРОЕНЕРГІЇ ФОТОПАНЕЛЯМИ ЗА УМОВ РІЗНИХ ТИПІВ КРІПЛЕННЯ МАСИВУ ФОТОПАНЕЛЕЙ Електроенергетика, електромеханіка та технології в АПК: [Електронний ресурс] : матеріали Міжнар. наук.-практ. конф., 9 листопада 2023 р. / Держ. біотехнологічний ун-т. – Харків, 2023. – 81-82 с. – Електронні текстові дані. – Режим доступу : http://btu.kharkov.ua/nauka/konferentsiyi/.
4. Немикіна О. В. Поновлювальні та альтернативні джерела енергії: навчальний посібник / О. В. Немикіна. - Запоріжжя: Видавництво НУ «Запорізька політехніка», 2020 – 187 с. http://eir.zntu.edu.ua/handle/123456789/6657.

ЗМІСТ

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ВІДДІЛЕННЯ ЕНЕРГЕТИКИ
ТА ЕНЕРГЕТИЧНИХ ТЕХНОЛОГІЙ

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

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ЕНЕРГЕТИЧНИЙ ФРОНТ: ШОСТИЙ ТЕАТР ВОЄННИХ ДІЙ»
(стратегія захисту, управління та відновлення)

27 березня 2026 року

м. Київ

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua