НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

МАТЕРІАЛИ
ІІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

06 листопада 2025 року

Київ – 2025

УДК 620.9::[517.938::(519.718+004.056)]
ББК 31
Р-34

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 14 від 30 травня 2025 р.)

Р-34 **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.

R-34 **Resilience of** dynamic systems, III scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, November 06, 2025). Kyiv: PIMEE NAS of Ukraine, 2025. 185 p.

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

МАТЕРІАЛИ
ІІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

06 листопада 2025 року

м. Київ

2025

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

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

ПРОГРАМНИЙ КОМІТЕТ

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

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

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

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

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

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

Клименко Тетяна Михайлівна
завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

БІРЖОВІ ПІДХОДИ ФОРМУВАННЯ РОБАСТНИХ РІШЕНЬ

Ринок небалансів (imbalances) описує ціноутворення та торгівлю, а також використання резервної енергії відповідно до врегулювання (settlement) небалансу на балансуючих ринках. Ринок небалансів є елементом балансуючих ринків, які виконують функцію балансування енергетичної мережі та оптимізують використання відновлюваних джерел енергії. Він є частиною ринку енергопостачання в режимі реального часу, який пропонує послуги з виробництва та передачі електроенергії [1]. Ринку небалансів стосуються кілька зон балансування та території комунальних підприємств.

Енергетичні ринки – це товарні ринки, на яких енергетичні товари (раніше − такі прості фізичні товари, як деревина, торф, вугілля тощо) купуються та продаються [2]. З розвитком технологій розроблялися складніші енергетичні товари, торгівля якими передбачає відповідні рівні суспільної організації (яка є одним з факторів виробництва) [3]. Енергоринки є ключовим елементом балансування споживання та виробництва енергії [4]. На відміну від інших товарів, електроенергію не можна зберігати у великих кількостях [5]. Тому оператори мережі мають постійно балансувати виробництво електроенергії з попитом споживачів [6].

Можна виділяти типи енергоринків на основі ціноутворення: а) форвардний (ф'ючерсний) ринок електроенергії; б) ринок на добу наперед (РДН; аукціонний ринок); в) спотовий ринок (зокрема внутрішньодобовий); г) ринок балансу та небалансу [7].

а) На форвардних ринках електроенергія торгується за місяці або роки до її фактичної поставки, а ціни встановлюються на основі спотових ринкових цін майбутніх періодів поставки, щоб захищати покупців від коливань цін та забезпечувати стабільніші витрати.

б) РДН означає торгівлю електроенергією на наступну добу. Ціни визначаються останньою прийнятою заявкою на ринку. Ці торги є анонімними та відбуваються щодня, включаючи святкові дні.

Торгівля на РДН відбувається, наприклад, на EPEX (European Power Exchange) SPOT у м.Париж (спотовий ринок Європейської енергетичної біржі; заснований у 2008 р.), на EXAA (Energy Exchange Austria) у м.Відень (Енергетична біржа Австрії; заснована у 2001 р.) або як позабіржовий (over-the-counter (OTC)) трейдинг за контрактами, укладеними на двосторонній основі [8].

EPEX SPOT SE – це європейська біржа електроенергії, що працює в 10 державах ЄС (Австрії, Бельгії, Данії, Люксембурзі, Нідерландах, Німеччині, Польщі, Фінляндії, Франції, Швеції), а також у Великобританії, Норвегії, Швейцарії. EPEX SPOT SE є зареєстрованою згідно з європейським законодавством і має штаб-квартиру в столиці Франції з офісами у столицях Австрії, Бельгії, Великобританії, Нідерландів, Німеччини, Швейцарії. EPEX SPOT SE керує спотовими ринками електроенергії для короткострокового трейдингу в зазначених 13 державах. EPEX SPOT була заснована в 2008 р.

шляхом злиття спотових ринків електроенергії енергетичних бірж Powernext (заснована у 2001 р.) та European Energy Exchange (EEX AG; заснована у 2002 р.). Сьогодні EPEX SPOT на 51% належить EEX AG та на 49% операторам систем передачі (Transmission System Operators (TSOs)), які організовані в холдинг HGRT (Holding Gestion Reseau Transport Elec; холдинг управління електротранспортною мережею; заснований у 2001 р.), до складу якого входять Amprion GmbH (заснований у 2003 р.), APG (Austrian Power Grid) AG (заснований у 2001 р.), RTE (Réseau de Transport d'Électricité; заснований у 2000 р.), Elia (заснований у 2001 р.), Swissgrid (заснований у 2005 р.), TenneT (заснований у 1998 р.). У 2015 р. EPEX SPOT інтегрувалася з колишньою групою APX (Amsterdam Power Exchange; перший біржовий ринок електроенергії в континентальній Європі; заснований у 1999 р.), яка керувала спотовими ринками електроенергії в Бельгії (через Belpex (заснована у 2006 р.)), Великобританії, Нідерландах. У 2020 р. EPEX SPOT запровадила свої РДН та внутрішньодобовий ринок (ВДР) у Нордичному регіоні.

EPEX SPOT є одним із стейкхолдерів Єдиного європейського поєднання ринків «на добу наперед» (European Single Day-Ahead Coupling (SDAC); засноване у 2005 р.), яке сьогодні з'єднує ринки, що становлять 95% європейського споживання електроенергії. EPEX SPOT також надає послуги Угорській енергетичній біржі HUPX (Hungarian Power Exchange; заснована у 2010 р.) та Ірландській енергетичній біржі SEMOpx (Single Electricity Market Operations power exchange; заснована у 2015 р.). Крім того, EPEX SPOT надає послуги цінового поєднання для ринку трьох із чотирьох енергетичних бірж 4M Market Coupling (заснований у 2012 р.), що охоплюють Румунію, Словаччину, Угорщину, Чехію. У EPEX SPOT працює близько 200 співробітників.

EPEX SPOT SE – це компанія з дворівневою системою врядування. Акціонери призначають Наглядову раду (Supervisory Board), що складається з представників європейського енергетичного сектору, які обирають Правління (Management Board) та затверджують стратегію компанії. Наглядова рада підтримує роботу EPEX SPOT щодо інтеграції європейського ринку електроенергії та враховує зростаючу кількість спільних справ (collaborations) європейського та глобального масштабів.

Щоб забезпечувати найсучасніші правила врядування та ефективно застосовувати свою структуру акціонерів, EPEX SPOT SE створила Біржову раду (Exchange Council) як незалежний орган, який складається з учасників ринку. До Біржової ради входять 26 членів і 4 постійних (permanent) гостя, які зустрічаються щоквартально, адекватно представляють різноманіття економічних і корпоративних профілів, що існує серед понад 300 членів EPEX SPOT від різних секторів. EPEX SPOT володіє 100% дочірньої компанії EPEX SPOT Schweiz AG (започаткована у 2006 р.) у Швейцарії.

У 2024 р. обсяг торгів електроенергією на ринках EPEX SPOT становив близько 868 терават-годин (ТВт-год).

На EPEX SPOT РДН постійно організовується через аукціонний процес, що знаходить парасполучення для кривих попиту та пропозиції один раз на

добу, фіксуючи відповідні ціни анонімно, прозоро й безпечно. Члени EPEX SPOT вносять свої заявки на погодинні обсяги електроенергії до книги заявок (order book), яка закривається о 11:00 для Швейцарії та о 12:00 для всіх інших ринків. Тоді EPEX SPOT розраховує криві пропозиції та попиту, а також їх перетин для кожної години наступної доби. Результати публікуються з 9:30 за Гринвічем GMT (Greenwich Mean Time) для Великобританії, 11:10 для Швейцарії та 12:55 для всіх інших ринків.

Країни Центральної та Західної Європи, за винятком Великобританії та Швейцарії, та ринки Нордичних країн з'єднуються через механізм, що називається поєднанням ринків (Market Coupling). Цей механізм пов'язує ринки електроенергії країн-членів за допомогою рішення цінового поєднання, щоб оптимізувати використання транскордонних потужностей між цими країнами, збільшуючи суспільний добробут на всіх ринках.

EPEX SPOT також керує ВДР (intraday markets) для електроенергії у всіх вищезгаданих 13 державах, крім Польщі. ВДР організовується шляхом безперервної торгівлі, коли заявки членів EPEX SPOT постійно вносяться до книги заявок: як тільки дві заявки сполучаються, виконується торгова угода. Виходячи з контрактів, можна торгувати на погодинні, півгодинні, чвертьгодинні обсяги електроенергії до 5 хвилин до фактичної її поставки.

Система M7 на EPEX SPOT для ВДР допускає одночасну транскордонну торгівлю як через біржу, так і через OTC-операції. M7 − це сімейство торгових систем, яку розробила Deutsche Börse Group (заснована у 1992 р.) здебільшого для товарних ринків, включаючи ринки електроенергії, газу, ф'ючерсів. M7 включає різні платформи для брокерів і бірж: M7 Trading − система організації безперервної торгівлі на ВДР для електроенергії; M7 Auction − інноваційна аукціонна система для торгівлі різними товарними продуктами, яка використовується для європейських сертифікатів викидів і закупівель втрат в електромережах; M7 Capacity − система керування потужностями між транскордонними інтерконекторами електромереж; M7 XBID − сервіс у загальноєвропейському ВДР для електроенергії транскордонних мереж.

Безперервні ВДР EPEX SPOT, за винятком Великобританії та Швейцарії, поєднуються через загальноєвропейське єдине внутрішньодобове поєднання (pan-European Single Intraday Coupling).

У 2011 р. EPEX SPOT запровадила 15-хвилинні контракти на безперервному ВДР у Німеччині. Ці контракти гнучкості сприяють трейдингу з переривчастими (intermittent) джерелами енергії та допомагають підтримувати резильєнтність енергосистеми з внутрішньогодинними коливаннями виробництва та споживання. Із запуском ВДР у Швейцарії 15-хвилинні контракти були поширені на цей ринок.

У 2014 р. EPEX SPOT запустила кол-аукціон (call auction) (з похідними фінансовими інструментами (деривативами)) для 15-хвилинних контрактів на ВДР Німеччини, щоб забезпечувати надійний ціновий сигнал на чверть години. Цей аукціон о 15:00 за центральноєвропейським часом (Central European Time (CET)) надає інструмент для відповідальних за баланс сторін, щоб краще налаштовувати (fine-tune) свої портфелі на 15-хвилинній основі в

ході нарощування виробництва та прогнозувати відхилення. Таким чином, ціновий сигнал 15-хвилинних контрактів сприяє додатковій вартості (added value) гнучкості та водночас забезпечує стимули для стабілізації системи.

У 2017 р. EPEX SPOT запровадила 30-хвилинні контракти на безперервному ВДР Франції, Німеччини, Швейцарії, дозволяючи здійснювати місцеві та неявні транскордонні торги на відповідних кордонах. Ці контракти розробляються для ефективнішого менеджменту з новопосталиими питаннями гнучкості на енергоринках і допомоги учасникам ринку виконувати свої балансові зобов'язання перед TSO Франції. EPEX SPOT пропонує додаткові аукціони ВДР у Великобританії − з 2018 р., у Швейцарії − з 2019 р., в Австрії, Бельгії, Франції − з 2020 р.

Вищенаведений практичний досвід сусідніх у розвитку сучасних організованих ринків ринків електроенергії є корисним для України.

1. Горбачук, В. М., Лупей, М. І., Дунаєвський, М.С. (2022). Підходи до резильєнтності критичних інфраструктур. In A. Ostenda, V. Smachylo (eds.), *Science and Education for Sustainable Development* (pp. 87−95). Katowice, Poland: University of Technology, Katowice.
2. Gorbachuk, V. M., Suleimanov, S.-B., Batih, L. O. (2022). Integrated resilient strategies of renewable power generation and distribution, *Наука і техніка сьогодні*, 4 (4), 113−125.
3. Gorbachuk, V., Bardadym, T., Dunaievskyi, M. (2025). Digitalization of modern energy in the information society. In A. Ostenda, O. Nestorenko (eds.), *Education, Economy, and AI: Multidisciplinary Perspectives for a Digital Future* (pp. 513−527). Katowice, Poland: University of Technology in Katowice.
4. Gorbachuk, V., Bardadym, T., Rybachok, D. (2025). International practices and national transfer pricing in energy. In *Transfer Pricing in Ukraine: A System of Analytical, Digital, and Control Management* (pp. 29−56). Riga, Latvia: Baltija Publishing.
5. Gorbachuk, V., Dunaievskyi, M., Lupey, M. (2023). Innovative approaches to measuring system resilience. In V. Yuskovych-Zhukovska, O. Bogut (eds.), *Contemporary Technologies and Society: Innovations, Artificial Intelligence, and Challenges* (pp. 476−482). Katowice, Poland: Academy of Silesia.
6. 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.
7. Сулейманов, С.-Б., Рибачок, Д., Голоцукова, Т. (2025). Трансформаційний вплив цифровізації на енергетичний сектор. *Наука і техніка сьогодні*, 2025, 8 (49), 1717−1730.
8. Gorbachuk, V., Bardadym, T. (2025). Multi-level approaches to organizing sustainable energy development. In *Strategic Priorities for Sustainable Development in the Context of Global Economic Transformation* (pp. 791−816). Riga, Latvia: Baltija Publishing.

F. Korobeynikov

DIFFERENTIATING SOCIOTECHNICAL SYSTEMS VIA MULTIPLEX NETWORK THEORY

Contemporary understandings of complex systems have proved remarkably adept at articulating the interconnectedness of constituent elements, yet remain circumscribed in their capacity to discern qualitative distinctions amongst modes of systemic evolution. Within the ambit of adaptive security research, particular salience attaches to the differentiation between systems oriented towards the preservation of functional architecture and those possessed of a capacity for self-modification and adaptive transformation. The former may be designated as functionally stable; the latter as evolutionarily dynamic [1]. This distinction bears not so much a technological as an ontological character: it reflects fundamentally divergent modes of systemic response to perturbation – whether through restoration of antecedent states or through transfiguration of organisational form itself.

To formalise this ontological distinction, a suitable representational framework must be employed. Traditional network representations–monoplex in construction, prove insufficient for expressing such differentiation, inasmuch as they capture solely the connections between components whilst neglecting the interplay between organisational strata [2]. Sociotechnical systems – be they infrastructures, organisations, or societies – constitute multilevel architectures wherein technical, cognitive, institutional, and social processes are superimposed upon one another. The analysis of such systems necessitates an approach capable of reflecting both their multilayered nature and the dynamics of inter-level coordination. It is precisely these requirements that multiplex network theory addresses [3], wherein each layer represents a discrete instantiation of systemic reality, whilst the ensemble of layers constitutes its adaptive architectonics.

In contrast to traditional network representations – whether monoplex graphs, dual-layered models, or multilayered structures with fixed types of edges, the multiplex formalism enables a departure from linear and unidimensional conceptions of interaction within complex systems [3,4]. A multiplex captures the multiplicity of levels and modes of interaction among components, each of which may be governed by distinct systemic invariants – functional, organisational, social, ethical, religious, and otherwise. These invariants manifest in the form of laws, norms, traditions, beliefs, shared representations, and semantic constraints that delineate stable contours of communication and coordination within the system.

Such a representation allows for the analysis not only of intra-layer connectivity but also of inter-layer resonances, revealing how shifts in one invariant can induce structural rearrangements in others, thereby reconfiguring the system’s adaptive trajectory. This capability is of central importance to the differentiation of functionally stable and evolutionarily dynamic systems. In the former case, the multiplex exhibits a tendency toward synchronisation and

reduction: the structure ‘collapses’ into a single, dominant control layer, minimising inter-layer variation. In the latter, by contrast, one observes divergence, asymmetry, and redistribution of linkages across layers – a sign of internal reorganisation and the formation of novel regimes of stability. In this sense, multiplex architectonics enables the conception of adaptation not as an external imposition or descriptive parameter, but as an intrinsic property of the system – its capacity to transform its own topological configuration whilst preserving semantic and functional coherence.

This understanding, in turn, opens the way toward the formulation of differentiated security strategies. For functionally stable systems, the appropriate approaches are those grounded in structural robustness, reliability, and the capacity to maintain function under perturbation (emphasising robustness and engineering resilience). For evolutionarily dynamic systems, by contrast, strategic relevance lies in approaches based on adaptation, self-organisation, and directed transformation – wherein disturbances are construed not as threats, but as sources of renewal and systemic development (emphasising ecological resilience and transmorphance).

The adoption of a multiplex model is motivated by the need to operationalise typological distinctions between forms of connectivity while preserving computational tractability. In multigraphs, multiple edges merely encode interactional intensity without capturing qualitative differentiation; hypergraphs and simplicial complexes facilitate the representation of group-level cooperation, yet obscure the axis of layeredness as the distinguishing dimension of heterogeneous relations. Categorical constructions, for their part, tend toward excessive abstraction and prove difficult to operationalise within metric-based classification. Tensors, though useful as representations, do not in themselves constitute criteria of systemic distinction. Multiplex networks, by contrast, furnish a parsimonious yet adequate formalism capable of distinguishing between systems reducible to a single relation type and those exhibiting irreducible multilayeredness. Within the proposed approach, each layer of the multiplex corresponds to a specific type of connection among elements, defined by systemic invariants – functional, organisational, ethical, religious, social, and others. These invariants constitute normative–semantic foundations, delineating permissible classes of interaction and stabilising respective channels of coordination. Interlayer dynamics reflect the processes of alignment or contestation among these foundations, together with the mechanisms governing the transmission, amplification, or attenuation of signals across levels of organisation. The focus of analytical attention lies not upon individual nodes or edges, but upon the topology of interlayer coherence – the configuration of weighted interconnections between layers, which governs how information is distributed and synchronised throughout the system. This topology is assessed using information-structural indicators of coherence and divergence, allowing for quantitative evaluation of mutual dependence and variability across systemic strata. Under conditions of high coherence, the system evinces functional stability: its structure can be effectively reduced to a dominant layer. Rising divergence, by contrast, indicates irreducible

multiplicity and the activation of adaptive or transformational processes. Operationalising this distinction requires the introduction of formal metrics for analysing structural complexity indicators – including the entropy of interlayer connection distributions, reflecting the diversity of interaction types; agent participation across layers, capturing the depth of their integration into distinct coordination regimes; and the reducibility index, measuring information loss incurred when compressing the multiplex into a monoplex structure. Each of these metrics affords reproducible classification of systems and the identification of appropriate strategies for ensuring their security.

Multiplex network theory furnishes a rigorous analytical apparatus for the formal differentiation of socio-technical system types, grounded in the examination of their multilayered architectures. It permits not only structural characterisation of interactions, but also the quantitative assessment of such parameters as interlayer coherence, functional distribution, and the degree of adaptive integration. This, in turn, facilitates the operationalisation of a shift from qualitative typologies to measurable indicators that capture the constitutive attributes of functionally stable and evolutionarily dynamic systems.

The principal indicator in this context is the entropy of interlayer connection distribution, which quantifies the degree of diversity and balance among interaction types. When connections are concentrated within a single dominant layer, entropy approaches zero – a configuration emblematic of functionally stable systems governed by unified control structures. Conversely, when connections are evenly distributed across multiple layers, entropy is maximised – indicating structural diversity and the latent capacity for transformation.

In the generality of cases, this indicator alone suffices to distinguish between systemic types. However, the analysis may be extended by incorporating two additional measures.

The distribution of agent participation across layers allows for the evaluation of how evenly system elements are engaged in different types of interaction. Low values correspond to functional specialisation and hierarchical organisation, with agents concentrated within a single layer. High values, by contrast, suggest a multiplicity of roles, enhanced interlayer integration, and a systemic disposition toward adaptive reconfiguration.

The reducibility index reflects the informational loss incurred when a multilayered architecture is collapsed into a single aggregated layer. This measure gauges the degree to which a system's structure is irreducibly multiplex: whether it can be meaningfully represented through a singular relational modality, or whether its layeredness is essential to the preservation of systemic identity. Low reducibility denotes pseudomultiplex or effectively monoplexstructures; high reducibility attests to inner polymorphism and the constructive role of interacting invariants.

The application of the multiplex approach enables the identification of qualitative distinctions between two types of socio-technical systems: functionally stable and evolutionarily dynamic. In the former case, the network structure

exhibits high interlayer coherence, redundant linkages, and synchronised control circuits. Such systems are characterised by the sustained distribution of information flows and a dominance of feedback mechanisms oriented towards the preservation of the existing order. Adaptation in this context is either altogether absent or takes a compensatory form (resilience), whereby perturbations are dissipated through internal buffering and the structure rapidly returns to its prior state.

In the latter case, a markedly different dynamic is observed: interlayer coherence diminishes and divergence increases, indicating a redistribution of weights across invariants and the emergence of novel structural configurations. These systems evince a capacity to reorganise the topology of interactions, generate new channels of information flow, and reprioritise among functional and normative subsystems. Their mode of adaptation is evolutionary in nature (transmorphance): rather than reverting to a previous equilibrium, the system establishes new regimes of stability through the reinterpretation and recombination of its own invariants.

It bears noting that the boundary separating functionally stable and evolutionarily dynamic systems ought not to be construed as a rigid binary demarcation. Rather, it delineates a conceptually salient zone within the space of systemic configurations – a region of critical sensitivity in which systems undergoing transformation, internal ambivalence, or structural indeterminacy tend to concentrate. Nevertheless, the binary differentiation advanced herein retains considerable practical purchase, as it may be integrated into procedures aimed not only at monitoring and diagnostics, but also at the design of systems and embedded security circuits for complex socio-technical formations. Such systems are capable not merely of withstanding stochastic and sporadic high-impact, low-probability (HILP) threats, but of harnessing uncertainty as a productive resource for systemic evolution. This developmental trajectory opens the way toward the construction of architectures in which adaptation, stability, and transformation operate as mutually consonant dimensions of internal dynamics.

1. Mokhor, V., Korobeynikov, F. (2025). Transmorphance of socio-technical systems: A conceptual framework for adaptive security. International Science Journal of Management, Economics & Finance, 4(4), 71–77. https://doi.org/10.46299/j.isjmef.20250404.07.
2. Barabási, A.-L. (2016). Network science. Cambridge University Press. https://networksciencebook.com.
3. Boccaletti, S., Bianconi, G., Criado, R., del Genio, C. I., Gómez-Gardeñes, J., Romance, M., ... & Zanin, M. (2014). The structure and dynamics of multilayer networks. Physics Reports, 544(1), 1–122. https://doi.org/10.1016/j.physrep.2014.07.001.
4. Battiston, F., Amico, E., Barrat, A., Bianconi, G., Ferraz de Arruda, G., Franceschiello, B., ... & Petri, G. (2020). Networks beyond pairwise interactions: Structure and dynamics. Physics Reports, 874, 1–92. https://doi.org/10.1016/j.physrep.2020.05.004.

Г.П. Дубинський

РЕЗИЛЬЄНТНІСТЬ — ЧОТИРИ ПІДХОДИ ДО СТІЙКОСТІ ЛАНЦЮГІВ ПОСТАЧАННЯ

Вступ: Коли сильне слово стає порожнім жаргоном

Сучасний бізнес-ландшафт характеризується безпрецедентною волатильністю, де збої (від кібератак і геополітичної нестабільності до логістичних проблем і дефіциту сировини) стали "новою нормою". Компанії щодня стикаються з викликами, які вимагають миттєвої реакції.

Протягом останнього десятиліття термін **"резильєнтність" (стійкість)** перейшов з наукових праць у зали засідань. Ми вихваляємо стійкість, встановлюємо її як ключовий показник ефективності і часто використовуємо як магічне заклинання. Але — і в цьому полягає проблема — чим частіше ми повторюємо це слово, не розбираючи його на вимірні складові, тим більший ризик, що воно перетвориться на порожнє модне слово. Модні слова не зупиняють перебоїв.

Визначення: Резильєнтність ланцюга постачання — це не просто здатність повернутися до попереднього стану. Це інтегрована система, що здатна поглинати вплив, відновлюватися та функціонувати під тиском. Вона включає **абсорбційну здатність** (здатність мінімізувати падіння функціональності) та **відновлювальну здатність** (швидкість і якість повернення до норми або нової стійкої фази).

Розділ 1: Резильєнтність як Криві Відновлення та Ланцюг Фільтрів

1.1. Криві резильєнтності як перехідні функції

Криві резильєнтності є перехідними функціями, які графічно відображають зміну продуктивності системи ($f(t)$) після руйнівної події. Перехід включає фази падіння (Disruptive phase) та відновлення (Recovery phase), що ведуть до нової стабільної фази.

1.2. Механізм ланцюга фільтрів

Уявіть, що ваш ланцюг поставок — це не монолітна структура, а послідовність взаємопов'язаних **адаптивних фільтрів**. Кожен вузол (постачальник, виробничий майданчик) має свою перехідну функцію, реагуючи на вхідні шоки таким чином, що відображає його потужність, гнучкість та вразливість.

Коли трапляється збій, перший вузол модифікує «сигнал» цього збою. Можливо, він поглинає частину впливу, використовуючи резерви, або затримує його завдяки запасам. Змінений шок потім передається до наступного вузла, який застосовує свою власну криву реагування.

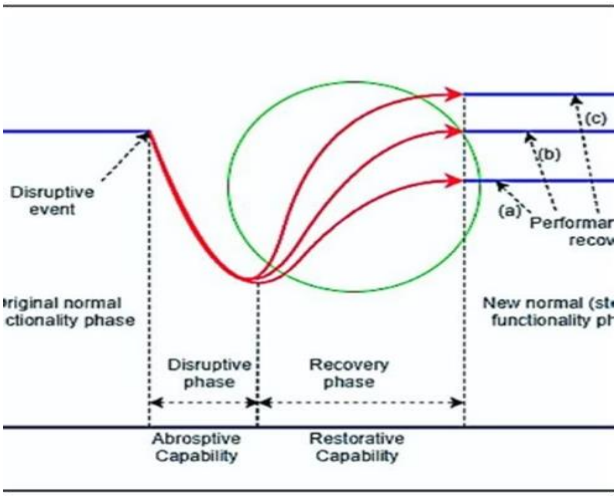


Рисунок 1. – Діаграма перехідної функції

Математично, ланцюг моделюється як послідовність N вузлів. Його вихідна продуктивність (наслідки збою) залежить від вхідного впливу $I_i(t)$ попереднього вузла $y_{i-1}(t)$, а також від його власної функції відновлюваності $h_i(\tau)$ та функції впливу:

$$y_i(t) = \int_0^\infty h_i(\tau) \cdot [I_i(t-\tau) \cdot y_{i-1}(t-\tau)] d\tau \quad (1)$$

де $h_i(t)$ — функція відновлюваності вузла, а I_i — функція впливу.

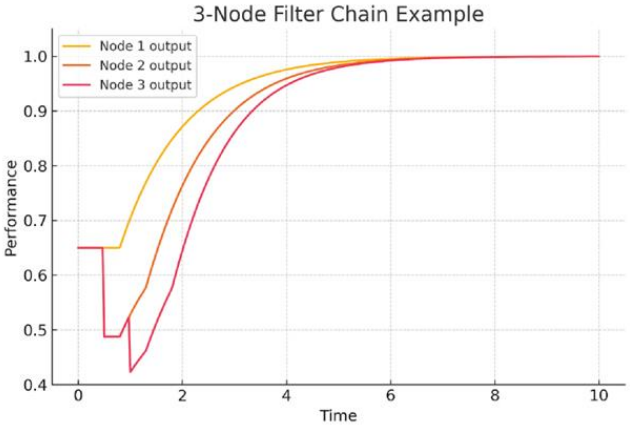


Рисунок 2. – Приклад 3-вузлового ланцюга

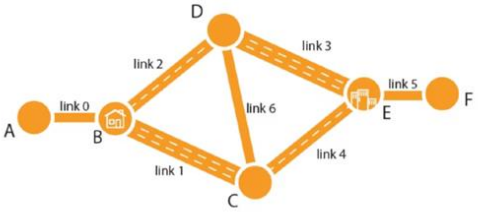
Практичний висновок: Моделювання дозволяє ідентифікувати критичні параметри, такі як швидкість відновлення (τ) та початковий вплив (Δ), дозволяючи створювати прогнозні моделі. Однак, якщо один фільтр є по суті просто широко відкритою діркою, ваші прекрасно складені рівняння будуть точно моделювати поширення катастрофи.

Розділ 2: Парадокс Браесса та Небезпека Неконтрольованого Надлишку

2.1. Суть Парадоксу Браесса

Парадокс Браесса — це добре відоме поняття в теорії мереж: **додавання додаткової потужності (надмірності) до мережі може, всупереч інтуїції, знизити загальну продуктивність.** Це відбувається, коли індивідуальні учасники (або вузли ланцюга постачання) діють, виходячи з локальної оптимізації, нехтуючи системним ефектом.

Уявіть, що ви запроваджуєте нового постачальника або маршрут експрес-доставки. Теоретично, це повинно покращити пропускну здатність. Але на практиці, без належної координації, особи, які приймають рішення, можуть надмірно використовувати нову опцію, що спричинить затори в інших місцях. Парадокс полягає в тому, що ваша «надмірність» стає єдиною точкою відмови.



link	from	to	lenght (km)	freespeed (km/h)	capacity (cars/h)
0	A	B	1	100	100
1	B	C	50	25	100
2	B	D	50	50	50
3	D	E	50	25	100
4	C	E	50	50	50
5	E	F	1	50	100
6	D	C	25	100	100

4-roads model includes links 0-1-2-3-4-5
5-roads model includes links 0-1-2-3-4-5-6

Рисунок 3. – Діаграма парадоксу Браеса

Я колись чув жартівливу аналогію: «Ми відкрили нову касу, і чомусь черга стала вдвічі довшою». Проблема була не в самій касі, а в тому, як люди відреагували на її появу.

2.2. Урок для проектування відмовостійкості

Конкретний приклад: З лютого 2022 року Україна страждала від проблем із зв'язком. Отримання 47 000 терміналів Starlink спочатку було

дивом — повне покриття, надзвичайна швидкість. Але за кілька місяців швидкість мережі різко впала, оскільки критична концентрація терміналів на одну комірку була перевищена майже вдвічі.

Стратегічний імператив: Надмірність необхідно контролювати, моніторити та інтегрувати в динамічну стратегію балансування навантаження. Більша кількість з'єднань не означає автоматично більшу стабільність. Стратегія повинна базуватися на **контрольованому надлишку**, а не на неконтрольованому.

Розділ 3: Схожість Кривих та Людський Фактор

3.1. Криві Ринку та Криві Резильєнтності

V-, U- та W-подібні відновлення є основними елементами макроекономічного аналізу, але вони однаково застосовні до стійкості ланцюгів постачання.

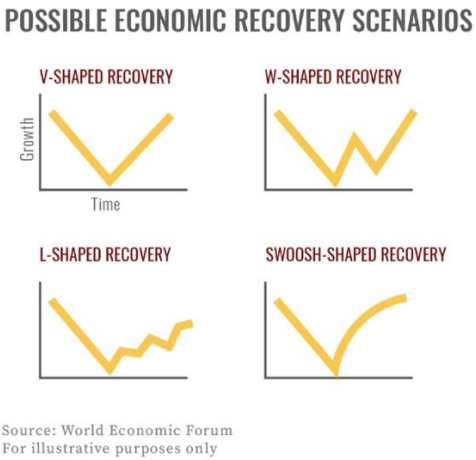


Рисунок 5. – Сценарії відновлення економіки

Форма кривої відновлення багато що говорить про внутрішню динаміку системи:

- **V-подібна:** Свідчить про швидку реакцію та ефективні механізми відновлення.
- **U-подібна:** Вказує на тривалий спад перед початком відновлення.
- **W-подібна:** Страшний «подвійний спад», що може означати вторинний шок або залежність від зовнішньої інфраструктурної допомоги.

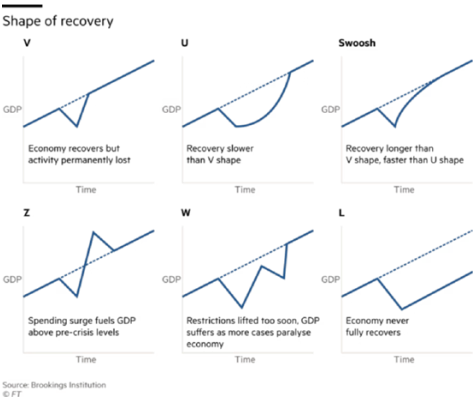


Рисунок 6. – Криві відновлення ринку

Спільні Рушійні Сили: Ці форми відновлення формуються не лише матеріальними потоками, але й психологією, очікуваннями та зворотними зв'язками. Це вказує на те, що інструменти аналізу фінансового ринку можуть бути корисними для **прогнозування відновлення** ланцюга.

Розділ 4. Ефект Даннінга-Крюґера та Ризик Самовдоволення

Сприйняття резильєнтності підпадає під вплив людської психології. Ефект Даннінга-Крюґера описує, як люди з низькою компетентністю схильні переоцінювати свої здібності.

У контексті стійкості це проявляється, коли організації переживають невеликі збитки і роблять висновок, що вони повністю готові до серйозної кризи. Це небезпечно, оскільки призводить до **самозаспокоєння** і недостатніх інвестицій.

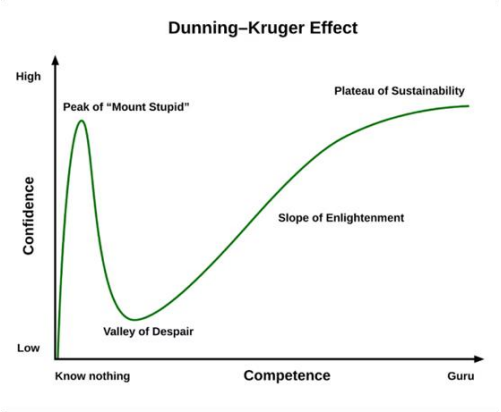


Рисунок 7. – Ефект Даннінга-Крюґера

Наочний приклад: Всі страхові компанії знають, що страхування для водіїв віком до 25 років коштує дорожче. Пережити невеликі збитки не робить вас чемпіоном світу з відновлення після катастроф; це може означати лише те, що цього разу вам пощастило.

Справжня Резильєнтність: Справжня стійкість вимагає смиренності та постійного навчання. Важливо постійно зіставляти сприйняття карти ризиків проти реальності та заповнювати прогалини в знаннях, використовуючи метапізнання та конструктивний зворотний зв'язок.

Висновок: Від Теорії до Дій

Ми розглянули стійкість через чотири різні, міждисциплінарні призми, нагадуючи, що резильєнтність — це не одна річ, а властивість, що виникає з взаємодії між інфраструктурою, процесами, рішеннями та людьми.

Резюме ключових інсайтів: Резильєнтність можна виміряти, моделювати та покращувати. Це вимагає комплексного підходу: від математичного моделювання потоків до фінансової оцінки ризиків та психологічної роботи з командою.

Без цього глибокого розуміння ми ризикуємо неправильно розподілити ресурси або просто повірити в «апостеріорну теорію стійкості», яка пояснює все, але тільки після того, як це сталося.

Заклик до дії: Керівники мають перетворити ланцюг постачання зі допоміжної функції на стратегічний важіль створення цінності, інвестуючи в:

1. **Прогнозне моделювання** (на основі Тези 1: Фільтри).
2. **Координований та керований надлишок** (на основі Тези 2: Парадокс Браесса).
3. **Фінансове обґрунтування стійкості** (на основі Тези 3: Опціонна модель).
4. **Культуру смиренності та навчання** (на основі Тези 4: Ефект ДК).

Лікуванням є **стрес-тест**: порівняння сприйманої стійкості з фактичною продуктивністю в умовах стресу. Резильєнтність — це не магія, а **математика, системний дизайн і, я б навіть сказав, філософське явище**.

С.С. Шевченко, Л.О. Митько

НАДІЙНЕ ФУНКЦІОНУВАННЯ НАСОСНОГО ОБЛАДНАННЯ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ – ВАЖЛИВИЙ КОМПОНЕНТ РЕЗИЛЬЄНТНОСТІ 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. Резильєнтність в атомній енергетиці — 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. Відцентрові насоси відіграють важливу роль у забезпеченні резильєнтності АЕС, а отже методи контролю їх стану та визначальних параметрів знаходяться під жорстким технічним та нормативним регулюванням. Надійність роботи відцентрових насосів, які перекачують рідке середовище під великим (до 50-100 МПа) тиском, залежить від забезпечення герметичності та вібраційної безпеки.

Розробка ущільнювальної техніки направлена на вирішення проблем герметизації об'єктів і створення ефективних систем ущільнень. Ущільнення роторів відцентрових насосів повинні задовольняти двом основним умовам: необхідній герметичності і підвищеній надійності при заданих перепадах тиску, частоті обертання, температурах і фізичних властивостях ущільнюваного середовища. Ротор відцентрового насоса, що обертається в щілинних ущільненнях, разом з системою авторозвантаження осьових сил являє собою особливу замкнуту гідромеханічну систему. Особливість системи обумовлена тим, що на ротор з боку ущільнень діють гідродинамічні сили (і моменти) різної природи: інерційні, дисипативні, гіроскопічні, потенційні і циркуляційні. Всі ці сили по різному впливають на коливання ротора і, в той же час, самі залежать від характеру цих коливань.

Аналіз динаміки ротора з урахуванням взаємозв'язку радіальних, кутових і осьових коливань навіть для найпростіших однодискових моделей ротора вимагає розв’язування систем диференційних рівнянь високих порядків. Розв’язувати такі системи можна лише обчислювальними методами, що ускладнює аналіз, узагальнення результатів та їх використання спеціалістами з проектування, обслуговування та ремонту відцентрових машин. Тому актуальною є побудова спрощених моделей, що відображають якісну картину впливу гідродинамічних характеристик щілинних ущільнень, а їх точність є прийнятною при проектуванні, обслуговуванні та ремонті відцентрових машин. Проблема побудови моделей ущільнень відцентрових

машин має наступні основні складові: створення моделей контактних ущільнень – сальникових і торцових механічних для розуміння механізмів герметизації і подальшого аналітичного дослідження; побудова моделі ущільнення з саморегульованим моментом в парі тертя, що пояснює механізм регулювання моменту тертя в різних конструкціях контактних ущільнень; створення моделі імпульсного торцового ущільнення, як системи автоматичного регулювання; розробка моделі жорсткого ротора з автоматичним врівноважуючим пристроєм для подальшого аналізу вимушених коливань ротора, амплітуда яких залежить від віддаленості частоти обертання від власних частот системи «ротор- врівноважуючий пристрій»; розробка моделі динамічної системи «ротор – щілинні ущільнення» та подальшого математичного аналізу динаміки системи з метою врахування при виборі конструкцій щілинних ущільнень не тільки їх прямого призначення – зменшувати об'ємні втрати, але і не менш важливу їх функцію – забезпечувати необхідні вібраційні характеристики ротора.

Побудова моделей різних типів ущільнень дозволяє оцінити вплив їх конструктивних особливостей на динамічні характеристики відцентрових машин. Розробка моделей гідромеханічних систем «ротор – ущільнення» і «ротор – врівноважуючий пристрій» дозволять знаходити розв’язок задачі підвищення вібраційної надійності відцентрових машин за рахунок правильного вибору конструктивних параметрів ущільнень. Тому методи моделювання і комп’ютерні технології побудови складних ущільнюючих систем є важливою складовою інструментальних засобів для підвищення резильєнтності відцентрових машин. [1, 2]. Аналіз процесів в ущільнюючих пристроях показав доцільність їх використання в якості динамічних опор ротора, які здатні пригнічувати коливання і, таким чином, забезпечувати вібраційну надійність та техногенну безпеку експлуатації насосного обладнання атомних електростанцій. Розробка математичних моделей та отримання аналітичних залежностей, які описують процеси в системах герметизації, є базою для створення науково обґрунтованих методик конструювання складних ущільнюючих систем для насосного обладнання, що сприяють резильєнтності АЕС.

1. Шевченко С.С. Разработка математических моделей уплотнительных систем. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. Том 31 (70) Ч. 1, № 6, 2020, с. 165–172.
2. Shevchenko, S. S. Mathematical modeling of centrifugal machines rotors seals for the purpose of assessing their influence on dynamic characteristics. "Mathematical Modeling and Computing" Lviv Polytechnic National University. Vol. 8, № 3 (2021) pp. 422 – 431.

В. Зубок, Н. Мішина

РЕЗИЛЬЄНТНІСТЬ ЯК ФАКТОР СТРИМУВАННЯ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ В КІБЕРБЕЗПЕЦІ

Поняття стримування. Кіберпростір — це оперативна сфера, офіційно визнана Північноатлантичним альянсом (НАТО) як один з п'яти доменів ведення бойових дій ще у 2016 році. Стратегія стримування в кіберпросторі для НАТО є одним із найважливіших напрямів безпекової політики в останнє десятиліття. Альянс поступово адаптував свою концепцію стримування до нових форм загроз, включаючи кібернапади, які можуть мати стратегічний вплив, навіть без фізичного втручання.

Політика стримування НАТО — багаторівнева. Кіберстримування включає три компоненти:

1) Deterrence by denial (стримування через відмову) — захист критичних систем так, щоб нападник визнав спробу атаки неефективною та відмовився від неї.
2) Deterrence by punishment (стримування через покарання) — готовність відповісти на кібератаку (не обов'язково в кіберпросторі).
3) Normative deterrence — встановлення міжнародних норм і очікувань, що атаки матимуть політичні та дипломатичні наслідки.

НАТО підтримує концепцію active cyber defence (проактивної кібероборони), що включає виявлення та нейтралізацію загроз у режимі реального часу.

Обмеження традиційних стратегій стримування в кіберпросторі. Традиційні стратегії стримування не враховують гнучкість і непередбачуваність кібертактик. Традиційні підходи до стримування виходять із припущення, що потенційного противника можна відлякати загрозою достовірної відплати (retailation) чи покарання (punishment). Але ці припущення не працюють у кіберпросторі.

Противники швидко адаптуються до нових засобів захисту, що ускладнює прогнозування їхньої поведінки. Анонімність кіберпростору й можливість використовувати інфраструктуру третіх сторін роблять покарання майже неможливим.

Проблема атрибуції в кіберпросторі. Атрибуція у кібербезпеці — це процес встановлення, хто стоїть за кіберінцидентом або атакою. Інакше кажучи, це визначення джерела, виконавця (індивіда, групи, держави) або походження атаки на основі технічних, аналітичних і розвідувальних даних.

Чітка атрибуція означає достатньо переконливе, технічно і аналітично обґрунтоване встановлення виконавця атаки, яке не залишає значних сумнівів. Вона базується на зібраних цифрових доказах (наприклад, збіги індикаторів компрометації, використання унікальних інструментів, шаблонів

командно-контрольних серверів тощо), підтверджується розвідданими (intelligence), підтримується міжнародними партнерами.

У документах НАТО та ЄС «чітка атрибуція» вважається необхідною умовою для пропорційної відповіді (наприклад, застосування санкцій або кібервідплати). Однією з головних перешкод для ефективного кіберстримування є складність атрибуції (Rogers, 2024). Визначити точне джерело атаки часто надзвичайно важко або неможливо. Зловмисники застосовують спуфінг, анонімізацію, використання проміжних серверів — усе це приховує їхню особу та місцезнаходження. Основні перепони чіткій атрибуції в кіберпросторі — це:

- анонімність в Інтернеті,
- використання проксі-серверів, VPN, ботнетів,
- викрадення чужих облікових записів чи серверів (false flag),
- політична чутливість наслідків оприлюднення висновків (публічної атрибуції).

Ці сумніви підсилюють нерішучість відплати та покарання.

Неоднозначність «червоних ліній» в кіберпросторі. На відміну від інших доменів, що саме є проявом кібервійни, або інакше — яка кібердія може бути однозначно трактована як «акт війни», залишається незрозумілим, що ускладнює визначеність пропорційного реагування. У традиційній війні наслідки — це руйнування, жертви, окупація території. У кіберпросторі — шкода нематеріальна: викрадення даних, тимчасова дестабілізація енергосистеми, зрив комунікацій або економічних процесів. Часто неможливо визначити, чи це розвідка, саботаж, тестування оборони, чи вже агресія. У Талліннському посібнику (Schmitt, 2017) експерти описали, коли кібердії можуть прирівнюватися до збройного нападу — наприклад, якщо вони спричинили людські жертви або масштабні руйнування. Але цей документ не є юридично обов'язковим, і держави трактують його по-різному.

Rogers (2024) акцентує увагу на постійному перетині нових «червоних ліній», які зачіпляють критичну інфраструктуру що належить як приватному, так і державному сектору, і що агресор не приділяє уваги цій різниці. На його думку, Китай підчас атаки Volt Typhoon суттєво ескалював перетин «червоних ліній», і це означає, що інші агресивні країни (РФ, Іран та Північна Корея), будуть стежити за відповіддю та відповідно змінювати стратегію та поведінку.

Концепція "Резильєнтність як фактор стримування". Отже, у кіберпросторі, де атаки є частими, а атрибуція або покарання нападників ускладнене, резильєнтність відіграє критичну роль як засіб стримування. Існує інший підхід: якщо мережі та інфраструктура є резильєнтними завдяки сильній кібергігієні, резервним системам, швидкому реагуванню на інциденти — нападники сумніватимуться у своїй здатності завдати тривалих збитків та в ефективності витрачання власних ресурсів, і це їх зупиняє. Розглянемо, чи обґрунтовані ці сподівання.

У сучасному світі гібридних загроз, резильєнтність, як «здатність готуватися до, протистояти, реагувати на та швидко відновлюватися після шоків і перебоїв в роботі» (NATO, 2024), дедалі частіше розглядається не лише як інструмент реагування на атаку чи кризу, а й як стратегічний фактор стримування. Як зазначено в аналітичному дослідженні Європейського центру передового досвіду з протидії гібридним загрозам: «стримування шляхом відмови спрямоване на підрив здатності супротивника досягти своєї мети — наприклад, шляхом підвищення захисту або резильєнтності проти певних типів атак.» (Monaghan, 2022). Моргус та ін. (2020) підкреслюють: «стримування через відмову в кіберпросторі має акцентувати важливість створення потужних захисних спроможностей і резильєнтності для протидії атакам» (Morgus R. et. al, 2020).

Деякі науковці навіть ототожнюють «недопущення вигоди» з резильєнтністю, стверджуючи, що зміцнення резильєнтності фактично дорівнює стратегії стримування через відмову. Ця ідея часто описується як «стримуюча резильєнтність» або «стримування шляхом недопущення через резильєнтність» (Resilience Rising, 2020). Так у звіті Європейського центру передового досвіду з протидії гібридним загрозам зазначається: «стримування шляхом недопущення через резильєнтність формує міцну основу для протидії гібридним загрозам.» (Monaghan, 2022).

Концепція «стримуючої резильєнтності» базується на ідеї, що формування високої резильентності – «здатності готуватися до загроз і небезпек, адаптуватися до змінних умов, протистояти перебоям в роботі і швидко відновлюватися після них» (Citron D. K., Eichensehr K. E., 2023) – саме по собі може стримувати супротивників, позбавляючи їх очікуваних переваг від атаки (Bendiek A.; Pander M. E., 2021).

Нижче наведено визначення та пояснення, що ілюструють, як резильентності сприяє стримуванню:

- Стратегічна концепція НАТО 2022: «… резильєнтність є важливим аспектом стримування через відмову: стримування супротивника від нападу шляхом переконання його, що атака не досягне поставлених цілей» (Federal Public Service Foreign Affairs, Foreign Trade and Development Cooperation of the Kingdom of Belgium, 2024).
- Національна оборонна стратегія США 2022 року чітко використовує концепцію «стримування резильєнтністю». У ній пояснюється, що «заперечення переваг агресії також вимагає резильєнтность – здатності протистояти, боротися та швидко відновлюватися після збоїв» (U.S. Department of Defense, 2022).
- Забезпечуючи, щоб збройні сили США та критично важливі системи могли продовжувати діяти під атакою та швидко відновлюватися, США сигналізують супротивникам, що атаки не принесуть бажаних переваг, тим самим стримуючи ці атаки.
- Стратегічний огляд оборони Великої Британії від 2023 року також визначає резильєнтність як критично важливу складову сучасного

стримування. Документ закликає до розбудови національної резильєнтності, щоб «витримувати атаки та швидко відновлюватися [після них], а також позбавляти супротивників потенційних переваг» (Ministry of Defence of the United Kingdom, 2025).

- Європейський Союз також значною мірою спирається на стримування шляхом недопущення через резильєнтність. Стратегія кібербезпеки ЄС наголошує на побудові «кіберрезильєнтного» єдиного ринку та критично важливої інфраструктури, чітко прагнучи «досягти стримування резильєнтністю». На практиці це означає загальноєвропейські стандарти кібербезпеки, обмін інформацією для покращення реагування на інциденти та загальні вимоги до операторів критичних об'єктів та послуг щодо планів забезпечення резильєнтності (Директиви NIS2 та CER). Логіка полягає в тому, що якщо критичні об'єкти ЕС можуть швидко ізолюватися та відновлюватися після кіберінцидентів, ворожі суб'єкти вважатимуть атаки набагато менш привабливими. Оскільки вони не зможуть легко створити хаос або використати тривалу шкоду на власну користь (Bendiek, A., and Pander M. E., 2021).

Висновки. Незважаючи на широке впровадження заходів кіберзахисту, всеосяжна й ефективна концепція кіберстримування досі залишається недосяжною. Хоча стримування може залишатися орієнтиром у формуванні безпекової поведінки, особливо в кібердормені, воно вже не може бути єдиною стратегією. Натомість резильєнтність пропонується як неодмінне доповнення — якщо не альтернатива — до стримування. Кіберрезильєнтність підкреслює здатність організації підтримувати основні функції та швидко відновлюватися після інцидентів. Такий підхід зміщує фокус із запобігання атакам на здатність їх витримувати та адаптуватися до них. Підвищення «видимої» резильєнтності пропонується поряд зі стратегіями, які накладають відчутні витрати на противників.

Динамічний, адаптивний підхід до резильєнтності є необхідним для протидії складному ландшафту сучасних кіберзагроз.

1. Bebber, R. (2018). There is No Such Thing as Cyber Deterrence. Please Stop. The Cipher Brief. URL: https://www.thecipherbrief.com/column_article/no-thing-cyber-deterrence-please-stop.
2. Bendiek A.; Pander M. E. (2021). The EU's cybersecurity policy: Building a resilient regulatory framework. European Repository on Cyber Incidents (EUREPOC). URL: https://eurepoc.eu/publication/the-eus-cybersecurity-policy-building-a-resilient-regulatory-framework/.
3. Citron D. K., Eichensehr K. E. (2023). Resilience in the digital age. Reimagining National Security. University of Chicago Legal Forum. URL: https://legal-forum.uchicago.edu/print-archive/resilience-digital-age.

4. Federal Public Service Foreign Affairs, Foreign Trade and Development Cooperation of the Kingdom of Belgium (2024). North Atlantic Treaty Organisation (NATO). URL: https://diplomatie.belgium.be/en/policy/policy-areas/peace-and-security/international-organisations/north-atlantic-treaty-organisation-nato.
5. Ministry of Defence of the United Kingdom. (2025). The Strategic Defence Review 2025 - Making Britain Safer: secure at home, strong abroad. Policy Paper. URL: https://www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad#prime-ministers-introduction.
6. Monaghan, S. (2022). Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. Hybrid CoE Paper 12. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf.
7. Morgus R. et. al. (2020). Deterrence by denial: The missing element in U.S. cyber strategy. Lawfare. URL: https://www.lawfaremedia.org/article/deterrence-denial-missing-element-us-cyber-strategy.
8. NATO (2024). Resilience and Article 3. North Atlantic Treaty Organization. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm.
9. Pernik, P. (2021). Cyber Deterrence: A Strategic Analysis. ybrid CoE Paper 8. URL: https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211012_ Hybrid_CoE_Paper_8_Cyber_deterrence_WEB.pdf.
10. Resilience Rising. (2020). Resilience and deterrence. https://resiliencerisingglobal.org/resilience-and-deterrence/.
11. Rogers, M.S. (2024). Deterrence in Cyberspace Proving to be a Difficult Exercise. Claroty NEXUS. URL: https://nexusconnect.io/articles/deterrence-in-cyberspace-proving-to-be-a-difficult-exercise.
12. Schmitt, M.N. (Ed.) (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. URL: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf.
13. Taddeo, M. (2020). How to Deter in Cyberspace. Hybrid CoE Paper 9.: URL: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-Analysis-9-Taddeo.pdf.
14. U.S. Department of Defense. (2022). 2022 National Defense Strategy of the United States of America, including the Nuclear Posture Review and Missile Defense Review. URL: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.

Д.І. Симонов, С.В. Єршов, Є.Д. Симонов, І.П. Кутова, І.О. Деменко

ВПЛИВ АНОМАЛІЙ НА ЕВОЛЮЦІЮ СКЛАДНИХ ДИНАМІЧНИХ СИСТЕМ

Вступ

Складні динамічні системи (СДС) характеризуються нелінійністю, багатокомпонентністю та високою чутливістю до збурень, що виникають у процесі взаємодії агентів СБС. У реальних мережах – соціальних, техногенних, біологічних – ключовим чинником втрати стійкості виступають аномалії: рідкісні або нетипові події, які здатні ініціювати фазові переходи, деградаційні каскади або структурну реорганізацію системи. Метою дослідження є розроблення методології виявлення, класифікації та моделювання впливу аномалій на траєкторію еволюції СДС, що забезпечує підвищення її резильєнтності та можливість передбачення критичних точок деградації (втрати рівноваги). Необхідність такого підходу зумовлена обмеженнями класичних методів аналізу (лінійних статистик, PCA, регресій), які не враховують структурно-топологічну та ентропійну природу збурень, властиву реальним адаптивним системам.

1. Теоретичні засади моделювання аномалій у СДС

У контексті складних динамічних систем (СДС) аномалія визначається як збурення, що порушує інваріантність траєкторії у фазовому просторі або спричиняє топологічну реконфігурацію структури взаємодій агентів. Формально множину таких збурень можна описати як:

$$A(t) = \left\{ x_i(t) \,|\, \left\| x_i(t) - \bar{x}(t) \right\| \geq \delta_{\text{crit}} \right\}, \tag{1}$$

де $\bar{x}(t)$ – ансамблева траєкторія системи; δ_{crit} – критичний поріг відхилення від колективної динаміки.

Розрізняють аномалії стану $x_i(t)$ та аномалії взаємодії $A_{ij}(t)$, що впливають відповідно на локальну та топологічну еволюцію.

Для кількісного аналізу впливу таких подій запроваджується ентропійна енергія збурення:

$$E_{\text{anom}}(t) = -\sum_i p_i(t) \log \frac{p_i(t)}{p_i(t - \Delta t)}, \tag{2}$$

яка вимірює темп зміни інформаційної невизначеності у часі. На відміну від статичної ентропії Шеннона, цей функціонал відображає інерційність перерозподілу ймовірностей станів і дає змогу локалізувати момент переходу від нормальної динаміки до нестійкої.

У запропонованому алгоритмі $E_{\text{anom}}(t)$ використовується як тригер еволюційного оператора F : при досягненні порога $\partial_t E_{\text{anom}} > e_c$ система переходить у режим адаптивної реконфігурації зв’язків. Така інтеграція

забезпечує прогностичну детекцію аномалій, зменшуючи час реакції моделі порівняно з класичними метриками еволюційної стабільності системи.

2. Методологія дослідження впливу аномалій

Розроблена методологія базується на гібридній операторній моделі, що інтегрує два взаємопов'язані рівні опису складної динамічної системи: локальну еволюцію станів та глобальну реконфігурацію топології. Такий підхід забезпечує одночасне відтворення мікродинаміки агентів і макроструктурних змін мережі. Загальний еволюційний оператор системи має вигляд:

$$x_{t+1} = \mathrm{F}\left(x_t, A_t, \xi_t\right) = f\left(x_t\right) + g\left(x_t\right) + e\xi_t, \tag{3}$$

де x_t – вектор станів агентів, A_t – матриця зв'язків, ξ_t – стохастичний вектор збурень, а функціонали f та g калібруються за емпіричними аномальними сценаріями.

Ключовим компонентом моделі є аналітичний модуль аномалій (*Anomaly Impact Module, AIM*), що виконує адаптивне оцінювання чутливості системи до зовнішніх і внутрішніх збурень. Для кожного елемента системи визначається локальний показник:

$$k_i = \frac{\partial x_i}{\partial \xi_t}, \tag{4}$$

який характеризує зміну стану у відповідь на імпульсне відхилення. Водночас топологічна реакція оцінюється через каскадну ентропію зв'язків:

$$\Delta H_t = H\left(A_{t+1}\right) - H\left(A_t\right), \tag{5}$$

що відображає масштаб структурної дестабілізації.

3. Сценарії моделювання

Для демонстрації адекватності запропонованої моделі проведено серію симуляцій у трьох різних предметних доменах, які репрезентують техногенну, біологічну та кіберсоціальну динаміку.

a) Енергетична мережа (smart-grid, $n = 2 \times 10^3$) – аномалії створювались у вигляді короткочасних перевантажень окремих вузлів. Операторна модель дозволила простежити каскадне поширення фазових коливань напруги й виділити критичні генератори з максимальним показником жорсткості $k_i > 0.7$. AIM-модуль забезпечив локалізацію джерела дестабілізації до моменту системної синхронізації, скоротивши час виявлення у 10-20 разів.

b) Модель міжвидової взаємодії (екосистема "хижак-жертва") – аномалії вводилися як імпульсні зміни параметрів росту популяцій. Під час моделювання спостерігався зсув траєкторій у фазовому просторі $\left(x_{\text{pred}}, x_{\text{prey}}\right)$, що інтерпретується як втрачання локальної стійкості. Функціонал $\mathrm{E}_{\text{anom}}\left(t\right)$ виявив ранні ознаки біфуркації типу Гопфа при $\partial_t E_{\text{anom}} > 0.04$.

c) Кіберінформаційна мережа (аналітика атак і самозахисту) – аномалії відображали несанкціоновані пакети трафіку, які порушують баланс

вхідних/вихідних потоків. Ентропійний індикатор ΔH_t виявив топологічний "зсув" у графі комунікацій задовго до фактичної втрати доступності вузлів.

4. Результати

Отримані результати демонструють здатність моделі відтворювати як технічні, так і біологічні або інформаційні механізми деградації структури при збереженні уніфікованої архітектури оператора F .

Таблиця 1. – Результати дослідження

Тестовий сценарій	MAPE (%)	R^2	EMR (×)	ERR	Speedup (×)
Smart-grid	2.4	0.982	1.41	0.76	×35
Predator-prey	2.8	0.973	1.29	0.68	×27
Cyber-network	2.3	0.986	1.57	0.83	×43

Отримані результати свідчать, що гібридна CPU–GPU реалізація забезпечує стабільну точність прогнозів (середня похибка <3%) при прискоренні симуляцій у 20–40 разів. Динамічна ентропійна метрика $E_{\text{anom}}(t)$ демонструє високу кореляцію з реальною швидкістю фазових зрушень $R^2 > 0.97$, підтверджуючи її ефективність як предиктора еволюційних фазових переходів. Аналіз показника ERR засвідчив, що адаптивна реконфігурація системи знижує ентропійне навантаження на 30–45%, підвищуючи стійкість до повторних збурень. Таким чином, запропонована модель підтвердила універсальність математичного ядра й здатність масштабуватися між енергетичними, біологічними та кібернетичними процесами.

5. Обговорення та наукова новизна

Запропонований підхід формує єдиний аналітичний формалізм, що інтегрує аналіз аномалій, ентропійні критерії та операторну еволюційну модель у гібридному CPU–GPU середовищі. Наукова новизна полягає у введенні динамічної міри впливу аномалії $E_{\text{anom}}(t)$, яка відображає темп втрати інформаційної рівноваги, та у формулюванні оператора $\mathrm{F}\left(x_t, A_t, \xi_t\right)$, що описує узгоджену еволюцію станів і топології. Розроблений модуль AIM поєднує предиктивну оцінку стійкості з контролем топологічних змін, забезпечуючи ідентифікацію критичних фазових переходів у реальному часі. Отримані результати розширюють класичне трактування резильєнтності:

вона розглядається не як здатність системи повертатися до рівноваги, а як активна властивість її інформаційної архітектури, що забезпечує самоорганізовану реконфігурацію під впливом аномалій.

Висновки

Аномалії у складних динамічних системах постають не лише як джерело ризику, але й як каталізатор еволюційних перетворень, що активізують механізми самоорганізації. Розроблена гібридна операторна модель забезпечує кількісне оцінювання енергетичної та ентропійної ваги збурень, дозволяє прогнозувати фази втрати стійкості й переходу до нових топологічних режимів, а також підвищує ефективність симуляцій на порядок у порівнянні з традиційними CPU-реалізаціями. Результати підтверджують, що ентропійно-операторний підхід здатний відтворювати ранні ознаки дестабілізації системної динаміки, забезпечуючи високу точність і економію часу. Подальші дослідження зосереджуватимуться на побудові універсальної карти аномальних фазових переходів, яка інтегрує аналітичні та нейромережеві моделі у спільну систему адаптивного управління резильєнтністю в енергетичних, біологічних та інформаційних процесах.

1. Symonov, D. I. (2021). Alhorytm vyznachennia optymalnoho potoku v lantsiuhakh postachannia z urakhuvanniam bahatokryterial′nykh umov ta stokhastychnosti protsesiv [Algorithm for determining the optimal flow in supply chains considering multicriteria conditions and process stochasticity]. Visnyk Kyivs′koho natsional′noho universytetu imeni Tarasa Shevchenka. Seriia Fizyko-matematychni nauky, (2), 109–116. https://doi.org/10.17721/1812-5409.2021/2.15.
2. Chen, Z., Dehmer, M., & Shi, Y. (2014). A note on distance-based graph entropies. Entropy, 16(10), 5416–5427. https://doi.org/10.3390/e16105416.
3. Symonov, D., Palagin, O., Symonov, Y., & Zaika, B. (2025). Optimisation of training samples with KLE and mutual information. In Proceedings of the Eighth International Workshop on Computer Modeling and Intelligent Systems (CMIS 2025) (Vol. 3988, pp. 296–306). CEUR-WS.org. https://ceur-ws.org/Vol-3988/paper23.pdf.
4. Kumaran, K., Ponjeyakumar, R., Savitha Sree, A., & Vasanth, V. (2025). Automated detection of algal blooms in satellite images using K-means clustering with NDVI and NDWI indices. In Proceedings of the 2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (pp. 1–6). IEEE. https://doi.org/10.1109/ICDSAAI65575.2025.11011625.
5. Sriram, K. P., Kola Sujatha, P., Athinarayanan, S., Kanimozhi, G., & Joel, M. R. (2024). Transforming agriculture: A synergistic approach integrating topology with artificial intelligence and machine learning for sustainable and data-driven practice. In Proceedings of the 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS) (pp. 1350–1354). IEEE. https://doi.org/10.1109/ICSCSS60660.2024.10625446.

M.V. Prazian

THE ROLE OF THE HUMAN FACTORS FOR THE RESILIENCE OF DYNAMIC SYSTEMS

Unlike technical systems, socio-technical systems are more complex to understand due to their intangible causes and the intricate relationships between these causes and their effects. Leveraging human adaptability and strengths can significantly improve a dynamic system's resilience, recovery, and safety. Human factors have traditionally been viewed as liabilities, with a focus on human weaknesses. This socio-technical complexity makes it challenging to enhance the resilience of European physical and critical infrastructures against a wide range of large-scale disruptions.

In 2025, the European Union (EU) launched the call HORIZON-CL3-2025-01-INFRA-02, which emphasizes the role of human factors in enhancing the resilience of critical infrastructure [1]. Within Horizon Europe Cluster 3 – Civil Security for Society, the goal is to improve infrastructure resilience against civil security threats through interdisciplinary research. The Horizon fund provides five million euros per project, categorized as an innovation action (IA), which can include cross-border cooperation across multiple countries or sectors. The EU taxonomy related to human factors is based on taxonomies derived from scientific studies and a set of standards, including [2]. A core element of Horizon, the EU encourages interdisciplinary research by integrating Social Sciences and Humanities (SSH) with Science, Technology, Engineering, and Mathematics (STEM) [3]. The report shows that 88% of current EU projects include at least one SSH partner, while STEM partners constitute 78% of all partners. The United States (US) has a long-standing tradition of managing human factors, also called 'ergonomics.' Human Factors combines ideas from disciplines like psychology, anatomy and physiology, social sciences, engineering, design, and organizational management. It merges these areas to improve understanding of how socio-technical systems interact. These systems, along with their operational contexts, encompass people, products, technology, organizations, and environments. Here are the selected standards and regulations [4][5][6].

The Pukhov Institute for Modelling in Energy Engineering (PIMEE), in collaboration with Mykolas Romeris University (MRU) and as part of the Impress-U project consortium, continues its research and has identified key gaps: (i) inadequate alignment between human and technological factors; (ii) a high level of autonomy, or silos, between technological and human practices, which hinders innovation; (iii) a mismatch in the maturity levels of technologies, skills, regulations, law enforcement, and research programs. Additionally, the author argues that human-technological systems should not only become more resilient, achievable, and nuanced through the integration of the prepare, absorb, recover, and adapt phases, but also that critical systems should become threat-agnostic in dynamic environments [7]. The author recommends the following measures:

1. Create Cross-Disciplinary Platforms.

The US Department of Transportation (DoT) has founded the Human Factors Coordinating Committee (HFCC), which serves as a multi-modal team with government-wide liaisons to promote human factors and to address crosscutting human factors issues in transportation. A working group led by the US Department of Defence (DoD) includes a total of 38 members as of 2019, from the Air Force - 2, Army - 1, Navy - 4, Department of Energy (DoE) - 10, Federal Aviation Administration (FAA) - 1, National Aeronautics and Space Administration (NASA) – 4, Industry - 10, and Academia - 6. The North Atlantic Treaty Organization (NATO) developed Network Enabled Capabilities (NEC), enabling platforms and Command and Control (C2) systems to integrate with Human System Integration (HSI). HSI considers human abilities and limitations in system definition, design, development, and evaluation to enhance overall system performance in operational environments. Overall, it is part of a comprehensive systems engineering approach to analysis, design, development, and testing for key decision-makers in the defence sector (e.g., war fighters, policymakers, capability developers, acquisition managers, systems engineers). A similar approach could be effective for stakeholders across public, private, and civil sectors in many fields.

2. Achieve The Human Readiness Level (HRL), Technology Readiness Level (TRL), and Manufacturing Readiness Level (MRL) Alignment

American National Standards Institute (ANSI), together with the Human Factors and Ergonomics Society (HFES), developed a standard, HFES 400. The standard defines nine levels of the Human Readiness Level (HRL) scale and guides the application of the HRL scale in existing systems engineering and human systems integration (HSI) processes. The HRL mirrors the existing Technology Readiness Level (TRL) and Manufacturing Readiness Level (MRL) scale and is designed to evaluate, track, and communicate a technology's readiness for human use. It fully incorporates the human element throughout the entire system lifecycle. Table 1 provides a unified view of the alignment between HRL, TRL, and MRL across various development phases, highlighting the integration of human, technological, and manufacturing readiness.

Table 1. - The Human Readiness Level (HRL), Technology Readiness Level (TRL), and Manufacturing Readiness Level (MRL) Alignment

Level	**Phase**	**TRL**	**HRL**	**MRL**
1	R&D	Basic Principles Observed/ Reported	Basic Human Research	Basic Manufacturing Implications and Studies
2	R&D	Technology Concept and Application	Design Guidelines	Manufacturing Concepts Identified
3	R&D	Analytical or Experimental Proof	Requirements for Human	Manufacturing Proof of Concept
4	T&D	Components in a	Modeling,	Prototype

		Laboratory	Part-Task, Studies	Components in a Laboratory
5	T&D	Components Demonstrated	Evaluation of Prototypes	Prototype Components - a Production-Relevant
6	P&D	System Model or Prototype Operational	Design Fully Matured	Subsystems in a Prototype
7	P&D	Completed Through Prototype Tests	Design Fully Tested	Subsystems/ Components in a Production Design
8	P&D	Completed Through Actual Systems Tests	Design Verified /Approved	Pilot Line, Manufacturing Proven
9	P&D	Proven Through Actual System Operation	Operational Use and Monitoring	Low Rate Production
10	FRP	N/A	N/A	Full Rate Production

R&D: Research and Development, T&D: Technology Demonstration, P&D: Production and Deployment. The author's assessment refers to ANSI/HFES [8][9].

3. Develop Human Factors in Modelling and Studies

These studies demand significant time and resources, making careful planning essential to ensure a positive human impact and prevent human errors with serious consequences. Practical frameworks can be proposed, such as the HUNTER (Human Unimodel for Nuclear Technology to Enhance Reliability)—a computation-based human reliability analysis framework developed by the US Department of Energy (DoE). The Human Factors Analysis and Classification System (HFACS) is a framework used for analyzing and categorizing human errors in incidents [10]. It aims to explain why incidents occur through hierarchical taxonomies. Conversely, HUNTER[11] employs quantitative models that incorporate system and human dynamics. The modelling, data collection, measurement, metrics, training, operational, legal, and ethical aspects are discussed in works[12][13][14][15].

As sub-modules of design, the 'human factors for' (HF4) dynamic systems will help researchers integrate HF4Resilience, HF4Recovery, HF4Energy, HF4Modelling, HF4Cyber, HF4Hesma, and others to ensure the resilience of critical infrastructure in a changing environment. Empirical studies remain key milestones for human factors' role surveys, case studies, or controlled experiments.

1. EC. (2025). HORIZON-CL3-2025-01-INFRA-02. Open topic for the role of the human factor in the resilience of critical infrastructures. HORIZON-CL3-2025. https://ec.europa.eu/info/funding-tenders/opportunities/portal.

2. ISO/IEC. (2010). *ISO 9241-210:2010(en), Ergonomics of human-system interaction - Part 210:Human-centred design for interactive systems*. https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en.
3. EC. (2025). *First monitoring report on SSH-flagged projects funded under Pillar II of Horizon Europe – 2021-2023* (No. 1; p. 45). Directorate-General for Research and Innovation. https://data.europa.eu/doi/10.2777/6733555.
4. DoT. (2021). *Better transportation through human factors: Strategic plan.* (p. 6). Human Factors Coordinating Committee. https://hfcc.dot.gov/publications/docs.
5. ANSI/HFES. (2021). *Human readiness level scale in the system development process* (p. 106). American National Standards Institute/Human Factors and Ergonomics Society. https://www.my.hfes.org/online-store/publications.
6. NATO. (2010). *Human Systems Integration for Network Centric Warfare. Report No. TR-HFM-155.* (p.306). https://apps.dtic.mil/sti/tr/pdf/ADA524077.pdf.
7. Trump B., Mitoulis S., Argyroudis S., Kiker G., Palma-Oliveira J., Horton R., Pescaroli G., Pinigina E., Trump J., Linkov I. (2025). *Threat-Agnostic Resilience: Framing and Application for Critical Infrastructure*. https://doi.org/10.48550/arXiv.2501.01318.
8. DoD. (2025). *Technology Readiness Assessment Guidebook.* (Unclassified No. DOPSR Case # 25-T-1398.; p. 98). Office of Systems Engineering and Architecture/Office of the Secretary of Defense for Research and Engineering. https://www.cto.mil/sea/.
9. DoD. (2020). *Manufacturing Readiness Level (MRL) Deskbook* (Versio 2020). Office of the Secretary of Manufacturing Technology Program. https://www.dodmrl.org.
10. Shappell S.A. & Wiegmann D.A. (2000). *The Human Factors Analysis and Classification System-HFACS*. https://www.researchgate.net/publication/247897525.
11. Park J. & Boring R. L. (2025). Dynamic human reliability analysis using the EMRALD dynamic risk assessment tool. *Reliability Engineering & System Safety, 264*(111260), 22. https://doi.org/10.1016/j.ress.2025.111260.
12. Mokhor V., Korchenko O., Honchar S., Komarov M., Onyskova A. (2021). Research of the impact on the ecology of the state of cybersecurity of the critical infrastructure objects. *E3S Web*, https://doi.org/DOI:252010.1051/e3sconf/202128009009.
13. Magoua J., Wang F., Li N., & Fang D. (2023). Incorporating the human factor in modeling the operational resilience of interdependent infrastructure systems. *Automation in Construction*, *149*, 48. https://doi.org/10.1016/j.autcon.2023.104789.
14. Stanton N., Salmon P., Rafferty L., Walker G., Baber C., Jenkins D. (2013). *Human Factors Methods: A Practical Guide for Engineering and Design* (2nd ed.). CRC Press. https://doi.org/10.1201/b16289.
15. FAA. (2019). *Dynamic Regulatory System* (Advisory Circulars (AC) No. AC 00-74). AIR-626B: Avionics Navigation & Flight Deck. https://drs.faa.gov.

А.В. Павлюк

МОДЕЛЮВАННЯ РЕЗИЛЬЄНТНОСТІ СКЛАДНИХ СИСТЕМ НА ГІБРИДНИХ АРХІТЕКТУРАХ

Вступ

Резильєнтність складних систем визначається як їхня здатність зберігати рівновагу та цілістність під впливом зовнішніх або внутрішніх збурень, тобто мінімізувати відхилення $\|u(t)-u^*(t)\|$ між поточним станом системи $u(t)$ та її номінальною траєкторією $u^*(t)$ за умов наявності випадкових варіацій параметрів. Такий підхід є ключовим для аналізу сучасних систем, що характеризуються множиною взаємопов'язаних елементів і нелінійними динаміками – від логістичних мереж постачання та кіберфізичних комплексів до енергетичних і транспортних інфраструктур та соціально-економічних систем [1-2].

Основна складність полягає в тому, що кількість змінних у таких моделях перевищує $n>10^5$, а простір можливих сценаріїв зростає експоненційно. Це робить традиційні CPU-орієнтовані методи непридатними для оперативного аналізу стійкості та самоорганізації. Використання гібридних CPU–GPU архітектур забезпечує істотне прискорення обчислень без втрати точності, що відкриває можливості для реалістичного моделювання резильєнтності та прогнозування поведінки складних систем у реальному часі [3].

1. Теоретичні засади моделювання резильєнтності складних систем

Формальна модель складної системи розглядається як орієнтований зважений граф $G=(V,E,W)$, де множина вершин $V=\{v_n\}$ відображає елементи системи, множина дуг $E\subseteq V\times V$ – їхні взаємодії, а матриця ваг $W=\left[w_{ij}\right]$ визначає силу та тип впливу між елементами.

Стан системи у момент часу t описується вектором $x(t)\in\mathbb{R}^n$, а її еволюція – оператором:

$$x_{t+1}=\mathrm{F}\left(x_t,\theta,\xi_t\right), \tag{1}$$

де θ – параметри керування системою; ξ_t – випадкові збурення, що моделюють невизначеність середовища.

Резильєнтність системи визначається як багатокритеріальна функція:

$$\mathrm{R}=\alpha_1 S_{\text{struct}}+\alpha_2 S_{\text{dyn}}+\alpha_3 S_{\text{ctrl}}, \tag{2}$$

де S_{struct} – змінна, що характеризує структурну зв'язність графа (наприклад, через спектральний радіус $\rho(W)$); S_{dyn} – змінна, що характеризує динамічну стійкість системи; S_{ctrl} – потенціал самовідновлення системи під дією керуючих впливів; α_i – вагові коефіцієнти.

Аналітичне обчислення (2) потребує великої кількості ітераційних апроксимацій та статистичних експериментів з різними наборами θ і ξ_t. Для моделей розмірності $n > 10^5$ таке моделювання на CPU стає обчислювально непідйомним, тому використання паралельних обчислень на гібридних архітекторах є необхідною умовою для досягнення прийнятної часової складності без втрати точності моделювання.

2. Гібридна обчислювальна архітектура

Запропонована гібридна архітектура CPU–GPU реалізує багаторівневу схему оброблення даних, орієнтовану на масштабне моделювання резильєнтності складних систем. Центральний процесор (CPU) виконує функції керування сценаріями, ініціалізації параметрів, оброблення метаданих та синхронізації потоків, тоді як графічний процесор (GPU) забезпечує масово-паралельну еволюцію станів системи, а також обчислення показників R , S_{dyn} і S_{struct}. Обмін даними між рівнями здійснюється за схемою *state* → *kernel* → *reduction* → *feedback*, що забезпечує мінімальні накладні витрати на комунікацію[4].

Для реалізації архітектури використано бібліотеки Numba/CUDA, OpenCL та PyTorch tensors, що оптимізують матричні та тензорні операції з урахуванням апаратної специфіки GPU. Структура графа зберігається у представленні CSR/COO, що знижує обсяг пам'яті та покращує пропускну здатність шин. Динамічний менеджер задач розподіляє навантаження між CPU та GPU у реальному часі, мінімізуючи сумарний час обчислень:

$$T_{\text{tot}} \approx \min\left(T_{\text{CPU}}, T_{\text{GPU}}\right), \tag{3}$$

і забезпечуючи стійку продуктивність навіть при різкій зміні розмірності або параметрів системи.

3. Алгоритмічна схема оцінювання резильєнтності

Розроблений операторний метод оцінювання резильєнтності поєднує аналітичне наближення та стохастичне моделювання динаміки системи. Еволюція станів описується рівнянням:

$$x_{t+1} = \mathrm{L}_h\left(x_t, \theta\right) + \eta_t, \tag{4}$$

де $\mathrm{L}_h(\cdot)$ – оператор локальної еволюції; η_t – шум або збурення, що моделює випадкові впливи середовища на систему.

Підхід (4) дозволяє досліджувати стабільність і відновлюваність системи через еволюційні траєкторії, не потребуючи повного перебору

параметрів. Для оцінювання навантаження на GPU введено метрику миттєвої енергії обчислень:

$$E_{\text{comp}}(t) = \sum_i c_i \left| \frac{\partial x_i(t)}{\partial \theta_i} \right|^2, \tag{5}$$

де c_i – коефіцієнти, що визначають локальну вагу змінних у процесі обчислення.

Рівняння (5) використовується для балансування точності й швидкодії за рахунок адаптивного розподілу ресурсів.

Загальна обчислювальна складність методу становить $O(n \log n)$ для структурних метрик і $O(nm/p)$ для динамічних експериментів, де p – кількість GPU-ядер, що гарантує масштабованість алгоритму на великих моделях.

4. Експериментальні результати та апробація

Для перевірки ефективності розробленого методу проведено серію тестових експериментів на трьох типових сценаріях: (1) мережа постачання з коеволюційною логістикою при $n = 10^3$ вузлах; (2) маршрутизація БПЛА з 512 агентами, що моделюють адаптивну взаємодію у просторі; (3) соціальна мережа впливу, де ваги зв'язків динамічно змінюються залежно від локальної реакції системи з $n = 10^5$. У всіх випадках гібридна реалізація CPU–GPU продемонструвала прискорення часу обчислень у діапазоні ×15–×40 порівняно з базовою CPU-версією при збереженні середньої похибки менше ніж 3 %.

Таблиця 1. – Результати дослідження

Тестовий сценарій	Розмірність (n)	MAPE (%)	R^2	Прискорення (×)	Енергія (ΔE, %)	Пам'ять (ΔM, %)
Мережа постачання	10^3	2.8	0.982	28	-35	-42
динамічні агенти (БПЛА)	512	2.1	0.989	22	-31	-38
Соціальна мережа впливу (адаптивна)	10^5	2.5	0.977	18	-29	-36

Оцінка точності виконувалась за метриками MAPE, R^2 та energy/memory ratio, що підтвердило високу узгодженість між аналітичними та чисельними результатами. Крім того, алгоритм продемонстрував здатність ідентифікувати критичні вузли (critical nodes) та прогнозувати момент деградації системи вже після 10–20 % від тривалості повної симуляції, що свідчить про його придатність для реального аналізу резильєнтності складних систем.

5. Наукова новизна та практична значимість

У роботі вперше запропоновано операторну модель резильєнтності для великих гетерогенних систем, яка поєднує аналітичні та стохастичні підходи в єдиній формальній структурі. Розроблено метод адаптивної дискретизації для систем із локальною жорсткістю, що забезпечує стійкість і точність чисельних розв'язків у багатошарових моделях. Реалізовано гібридну обчислювальну схему CPU–GPU з динамічним балансуванням навантаження, яка мінімізує часові витрати та енергоспоживання при великомасштабному моделюванні.

Запропонований підхід забезпечує оцінювання стабільності й відновлюваності реальних кіберфізичних систем у режимі реального часу, зокрема міських інфраструктур (urban systems), енергетичних мереж (energy grids) та кооперативних роїв БПЛА (UAV networks), підвищуючи їхню керованість і надійність.

6. Висновки та перспективи

Гібридний підхід до моделювання резильєнтності складних систем забезпечує масштабованість, високу точність і стійкість чисельних обчислень навіть для моделей великої розмірності і стохастичності. Подальші дослідження спрямовуються на розширення методу для коеволюційних систем, інтеграцію з AI-керованими симуляціями, а також оптимізацію енергоефективності обчислень з урахуванням динамічного розподілу навантажень у гібридних обчислювальних середовищах.

1. Khimich, O. M., Popov, O. V., Chistyakov, O. V., et al. (2023). Adaptive Algorithms for Solving Eigenvalue Problems in the Variable Computer Environment of Supercomputers. Cybernetics and Systems Analysis, 59, 480–492. https://doi.org/10.1007/s10559-023-00583-1.
2. Khimich, O. M., Popov, O. V., Chistyakov, O. V., et al. (2020). A Parallel Algorithm for Solving a Partial Eigenvalue Problem for Block-Diagonal Bordered Matrices. Cybernetics and Systems Analysis, 56, 913–923. https://doi.org/10.1007/s10559-020-00311-z.
3. Shevchenko, I., & Crisan, D. (2024). On Energy-Aware Hybrid Models. Journal of Advances in Modeling Earth Systems, 16(8), e2024MS004306. https://doi.org/10.1029/2024MS004306.
4. Xu, T., Liu, D., Hao, P., & Wang, B. (2023). Variational Operator Learning: A Unified Paradigm Marrying Training Neural Operators and Solving Partial Differential Equations. Journal of the Mechanics and Physics of Solids, 190, 105714. https://doi.org/10.1016/j.jmps.2024.105714.

О.А. Даниленко, Т.П. Мельник

HR-МЕТРИКИ СТАВЛЕННЯ ПРАЦІВНИКІВ ДО ПІДПРИЄМСТВА ЯК ПОКАЗНИКИ СОЦІАЛЬНОЇ РЕЗИЛЬЄНТНОСТІ ТРУДОВИХ КОЛЕКТИВІВ

Сучасні соціально-економічні процеси характеризуються високим рівнем невизначеності, динамічністю змін і частими кризовими явищами, що зумовлює необхідність формування резильєнтнихорганізаційних структур, тобто структур «…здатних відновлювати стабільний стан після його порушення зовнішніми чинниками» [1]. У цьому контексті особливої ваги набуває вивчення соціальної резильєнтності трудових колективів, яку можна визначити як здатністьколективу зберігати ефективність діяльності, внутрішню згуртованість і позитивний соціально-психологічний клімат навіть за умов зовнішнього тиску, криз чи трансформацій. Це визначення грунтується на думці Кухарук О. Ю., що «…під час надзвичайної ситуації спільнота набуває спільної ідентичності, яку поділяє більшість її членів (shared identity). Відчуття психологічної єдності з іншими під час надзвичайних ситуацій є основою здатності надавати і приймати підтримку, діяти разом із спільним розумінням того, що є практично й морально необхідним, і сприймати становище інших як пов'язане з нашим власним, а не як протилежне» [2].

Одним із важливих індикаторів такого стану виступають HR-метрики ставлення працівників до підприємства, що відображають рівень задоволеності, лояльності, залученості та довіри до підприємства [3].HR-аналітика в сучасному менеджменті персоналу перетворюється на ключовий інструмент підтримки управлінських рішень. Вона дозволяє не лише оцінити ефективність процесів управління персоналом, а й глибше зрозуміти соціальні настрої колективу, виявити потенційні ризики демотивації, вигорання або плинності працівників. Саме тому HR-метрики ставлення працівників до підприємства можуть розглядатися як своєрідний «барометр» соціальної стійкості підприємства. Вони відображають глибину емоційного, ціннісного та поведінкового зв'язку між працівником і підприємством, що безпосередньо впливає на здатність колективу протистояти викликам.

На основі аналізу наукових джерел [3-7] можна узагальнити HR-метрики для оцінювання ставлення працівників до підприємства:

– індекс задоволеності працівників (Employee Satisfaction Index), який вимірює ступінь задоволення умовами праці, винагородою та можливостями розвитку;

– індекс лояльності (Employee Net Promoter Score, eNPS), що демонструє готовність працівників рекомендувати підприємство як привабливого роботодавця;

– індекс залученості (Employee Engagement Index), який показує рівень емоційної включеності працівників у робочі процеси;

– показники довіри до керівництва, сприйняття справедливості та ідентифікації з корпоративними цінностями;

– показники вигорання (за методикою BAT [7]) як наслідок хронічного стану енергетичного виснаження, що охоплюють емоційні, когнітивні й поведінкові аспекти:

– виснаження (exhaustion) –відображає фізичне, емоційне та когнітивне спустошення, втрату енергії, хронічну втому, відсутність сил для виконання роботи,

– психічна дистанція (mental distance) –проявляється у байдужості, цинізмі, втраті інтересу до професійної діяльності, відчутті «внутрішнього відключення»,

– порушення емоційного контролю (emotional impairment) –може проявлятися у підвищеній дратівливості, нетерпимості, емоційних сплесках, зниженні здатності до співчуття,

– порушення когнітивного контролю (cognitive impairment) – стосується ослаблення концентрації уваги, пам'яті, прийняття рішень, людина може відчувати, що «мислення сповільнюється», зростає кількість помилок і складніше зосередитися,

– психологічне дистанціювання– відчуження від колег і роботи,

– відчуття неефективності– зниження самооцінки професійної компетентності,

– фізичні симптоми– порушення сну, головні болі, соматичні прояви стресу;

– рівень плинності кадрів (TurnoverRate), що відображає стабільність трудового колективу та ефективність політики менеджменту персоналу; висока плинність може свідчити про проблеми із задоволеністю роботою, корпоративною культурою, умовами праці чи управлінням персоналом.

HR-метрики оцінювання ставлення працівників до підприємства та формування організаційної резильєнтності дозволяють:

– своєчасно виявляти групи ризику серед працівників;

– аналізувати зв'язок між рівнем вигорання та залученістю персоналу;

– оцінювати ефективність програм добробуту (well-being) і профілактики стресу;

– підтримувати **соціальну резильєнтність** колективу, запобігаючи виснаженню й зниженню командної ефективності.

З позицій теорії соціальної резильєнтності, високі показники залученості та лояльності працівників свідчать про наявність у колективі соціального капіталу, тобто взаємної довіри, взаємопідтримки та ефективної комунікації. Ці чинники стають ключовими у періоди трансформацій, коли саме згуртованість і мотиваційна єдність команди визначають здатність організації адаптуватися без суттєвих втрат. Навпаки, низькі показники задоволеності або підвищення плинності персоналу можуть сигналізувати про послаблення соціальної згуртованості колективу та зниження його резильєнтності.

Аналітичне опрацювання HR-метрик дає змогу менеджменту не лише виявляти проблемні зони, але й прогнозувати соціальні ризики. Наприклад, систематичне відстеження eNPS дозволяє оцінити, наскільки працівники готові рекомендувати своє підприємство як надійного роботодавця, а динаміка цього показника може слугувати індикатором морального клімату та довіри до лідерства. Аналіз даних про залученість допомагає визначити, які фактори найбільше впливають на продуктивність – внутрішня мотивація, можливості розвитку, визнання досягнень чи справедливість винагороди.

Використання таких інструментів, як пульс-опитування (PulseSurveys),

зворотний зв'язок 360° (360° Feedback), AI-моделі ризику звільнення (AI Attrition/TurnoverRiskModels), аналітика корпоративних соціальних мереж тощо, поглиблює розуміння соціальної динаміки колективу. На основі цих даних формується комплексна картина психологічного клімату та соціального добробуту працівників організації. Збалансоване використання кількісних і якісних метрик ставлення працівників до підприємства дозволяє перейти від реактивного управління персоналом до превентивного, що відповідає принципам резильєнтності – передбачати та готуватися до змін, а не лише реагувати на них.

Важливо зазначити, що HR-метрики ставлення працівників до підприємства виконують не лише діагностичну, але й стратегічну функцію. Вони стають підґрунтям для розроблення політик корпоративної культури, програм розвитку лідерства, систем нематеріальної мотивації. Саме через вимірювання соціально-психологічних аспектів трудової взаємодії підприємство здатне підтримувати сталий розвиток, баланс між економічною ефективністю та людським потенціалом.

Таким чином, HR-метрики ставлення працівників до підприємства можна розглядати як індикатори соціальної резильєнтності трудових колективів. Вони відображають ступінь узгодженості цінностей, рівень довіри й комунікаційної ефективності, що визначають здатність колективу витримувати зовнішні стреси та адаптуватися до змін. Упровадження системного підходу до збору та аналізу таких даних створює основу для підвищення гнучкості, згуртованості та конкурентоспроможності підприємства в умовах сучасних викликів.

1. Резилентність. Wikipedia. https://uk.wikipedia.org/wiki/Резилентність.
2. Кухарук О. Ю. Ідентичнісний вимір соціальної резильєнтності: визначення, підходи, можливості прогнозування. *Проблеми політичної психології.* 2022. № 12(26). С. 77-90. DOI : https://doi.org/10.33120/popp-Vol26-Year2022-107.
3. Даниленко О. А. HR-метрики як інструмент HR-аналітики соціально-психологічного клімату колективу підприємства. *Проблеми сучасних трансформацій. Серія: економіка та управління.*2023. №8. DOI : https://doi.org/10.54929/2786-5738-2023-8-07-01.
4. Saks, A. M. (2019). Antecedents and consequences of employee engagement revisited. *Journal of Organizational Effectiveness: People and Performance*, 6(1), 19–38. DOI: https://doi.org/10.1108/JOEPP-06-2018-0034.
5. Lesener, J., Gusy, B., &Wolter, C. (2019). The job demands-resources model: A meta-analytic review of longitudinal studies. *Work & Stress*, 33(1), 76–103. DOI: https://doi.org/10.1080/02678373.2018.1529065.
6. Bakker, A. B., & Albrecht, S. L. (2018). Work engagement: current trends. *Career Development International*, 23(1), 4–11. DOI: https://doi.org/10.1108/CDI-11-2017-0207.
7. Schaufeli, W. B., Desart, S., & De Witte, H. (2020). Burnout Assessment Tool (BAT): Development, validity, and reliability. *International Journal of Environmental Research and Public Health*, 17(24), 9495. DOI: https://doi.org/10.3390/ijerph17249495.

І.С. Кузнєцов, А.В. Міщенко, А.В. Ільєнко

ТЕОРЕТИЧНИЙ ПІДХІД ДО СТВОРЕННЯ ЗАХИЩЕНОГО РОЗПОДІЛЕНОГО ХМАРНОГО СЕРЕДОВИЩА НА ОСНОВІ ТЕХНОЛОГІЇ BLOCKCHAIN

Актуальність

Резильєнтність, тобто здатність системи передбачати, протистояти, відновлюватися та адаптуватися до несприятливих впливів, визначається у сучасних підходах системної інженерії безпеки як інтегральна властивість життєвого циклу системи [1]. Зростання залежності від хмарних обчислень підвищує значущість резильєнтності: відмова чи атака на інфраструктуру може спричинити масштабні простої та втрати даних. Вітчизняні й міжнародні дослідження підкреслюють, що у складних інформаційних системах критичними стають єдині точки відмови та централізовані контури довіри [2]. У традиційних хмарних платформах користувач змушений довіряти одному провайдеру щодо зберігання та обробки чутливих даних, що створює ризики компрометації конфіденційності та доступності; огляди вказують на обмеження централізованого керування доступом та переваги розподілених підходів у хмарі [3]. На цьому тлі блокчейн розглядається як інноваційна технологія усунення централізованих вразливостей завдяки децентралізованій верифікації, незмінності записів і прозорості операцій, що сумарно підсилює довіру й кіберстійкість [4], а також доповнює класичні механізми резервування та відновлення [1], [3].

Огляд підходів до забезпечення резильєнтності

Класично резильєнтність розподілених систем забезпечують надлишковістю, георознесенням, відмовостійкими архітектурами та планами відновлення. Однак у централізованих моделях зберігається залежність від критичних вузлів (ідентифікація/автентифікація, контролери керування), компрометація яких здатна вплинути на значну частину екосистеми [3]. Сучасні тенденції зміщуються до децентралізації та інтелектуалізації: застосування AI/Big Data для проактивного виявлення аномалій поєднується з блокчейн, що усуває центри довіри й дозволяє колективно верифікувати зміни стану. Практика децентралізованого хмарного зберігання свідчить, що розподіл даних між багатьма вузлами з криптографічним контролем цілісності та журналюванням у реєстрі зменшує вплив одиничних збоїв і підвищує спостережуваність процесів [4]. У підсумку, поєднання відмовостійкого обладнання з криптографічно захищеною, консенсусною логікою керування формує нову парадигму забезпечення резильєнтності [1], [3], [4].

Концептуальна модель захищеного хмарного середовища на основі Blockchain

Архітектурна ідея. Блокчейн інтегрується як базовий шар керування станом розподіленої хмарної інфраструктури. Вузли хмари (сервери/кластери

в різних локаціях) виступають учасниками мережі реєстру; будь-які операції (виділення ресурсу, зміни конфігурацій, керування доступом) оформлюються як транзакції, що підписуються та верифікуються множиною вузлів. Після досягнення консенсусу транзакції входять до блоку, який послідовно приєднується до ланцюга — утворюючи незмінний журнал змін стану системи [1], [3].

Ключові компоненти. 1) *Розподілене зберігання/контроль цілісності*: критичні артефакти або їх хеші реплікуються між вузлами; відсутній єдиний репозиторій, чия відмова паралізує систему [4]. 2) *Розподілене керування доступом*: права й політики фіксуються і виконуються через смарт-контракти, що усуває одиничний центр авторизації і підвищує прозорість аудиту [3]. 3) *Смарт-контракти резильєнтності*: автоматизовані тригери (ізоляція дефектного вузла, ініціація відновлення з відомо коректного знімка, перемикання на резервні ресурси) активуються за заздалегідь визначеними правилами [1], [3].

Приклади й прототипи. У промислових сценаріях показано доцільність поєднання блокчейн із мережевими технологіями керування: наприклад, архітектура DistB-SDCloud для Industrial IoT демонструє, як розподілений реєстр забезпечує безпеку, конфіденційність і цілісність у хмарі, а SDN додає гнучке балансування та стабільність мережі [5]. З іншого боку, корпоративні підходи до децентралізованого хмарного зберігання демонструють, що ресурси можна надавати через peer-to-peer пул із реєстрацією та оплатою транзакцій у блокчейні; це зменшує залежність від одного постачальника та знімає окремі «вузькі місця» керування [4]. Актуальні огляди підтверджують, що такі інтеграції практично здійсненні для підсилення живучості розподілених хмарних сервісів [5].

Теоретичне обґрунтування ефективності підходу

Децентралізація як основа відмовостійкості. Відсутність єдиного критичного вузла і наявність реплік даних/стану у множини учасників забезпечують продовження функціонування навіть за відмови окремих компонентів; відновлення з коректних копій відбувається без порушення глобальної цілісності [1], [4].

Консенсус і толерантність до збоїв/зловмисних дій. Алгоритми класу BFT та інші приватні (permissioned) механізми згоди дозволяють досягати узгодженого стану навіть у разі недобросовісних або дефектних вузлів — недійсні транзакції відкидаються більшістю [8]. Це знижує ефективність атак на контури керування і унеможливлює тихе «переписування історії» без колективної згоди.

Незмінність та аудит як чинники скорочення MTTR. Криптографічна незмінність записів і повна трасованість операцій скорочують час виявлення й локалізації інцидентів; практичні демонстрації у суміжних інфраструктурах (енергосистеми) показують, що блокчейн-журнал прискорює фіксацію несанкціонованих змін та ідентифікацію джерела відхилення [7]. У хмарному

контексті це інтегрується з розподіленим керуванням доступом, підвищуючи перевірюваність і керованість ризиками [3].

Компроміс, продуктивність та безпека. Розподілений консенсус створює накладні витрати (затримки, трафік). Втім, у приватних мережах із контрольованою довірою сучасні протоколи згоди дозволяють досягати прийнятних характеристик латентності, зберігаючи властивості незмінності та толерантності до збоїв [8]. Гібридні підходи (on-chain метадані й політики, off-chain масиви даних) дають змогу збалансувати цілісність, прозорість і пропускну здатність [1], [3], [5].

Висновки

Запропоновано теоретичний підхід до підвищення резильєнтності динамічних систем через побудову блокчейн-орієнтованого розподіленого хмарного середовища. Децентралізація, консенсус і незмінність записів підсилюють відмовостійкість, скорочують час виявлення/відновлення та зменшують вплив атаки або збоїв окремих компонентів. Перспектива практичної реалізації підходу підтверджується експериментальними демонстраціями та прототипами, а інженерний успіх залежатиме від добору алгоритмів згоди й архітектурних рішень, що збалансовують безпеку й продуктивність.

1. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (NIST SP 800-160 Vol. 2 Rev. 1). NIST.
2. Lysenko, S. M., Kharchenko, V. S., Bobrovnikova, K. Yu., & Shchuka, R. V. (2020). Резильєнтність комп'ютерних систем в умовах кіберагроз: таксономія та онтологія. Radioelectronic and Computer Systems, (1)(93), 17–28. https://doi.org/10.32620/reks.2020.1.02.
3. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing, 13(1), 146. https://doi.org/10.1186/s13677-024-00697-7
4. Kumar, K. (2018). Distributed Cloud Storage with Blockchain Technology. Dell EMC Proven Professional Knowledge Sharing Article.
5. Aryan, N. (2025). Enhancing cloud security with blockchain: A decentralized approach to strengthening data integrity, privacy, and resilience against cyber threats in distributed computing environments. International Journal of Research Publication and Reviews, 6(4), 721–727.
6. Rahman, A., Islam, M. J., Band, S. S., & Muhammad, G. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks, 9, 411–421. https://doi.org/10.1016/j.dcan.2022.11.003.
7. Walton, R. (2022, November 28). DOE tests blockchain technology to ensure grid security, resilience in first-of-its-kind demonstration. Utility Dive.
8. Gramoli, V., Guerraoui, R., Lebedev, A., & Voron, G. (2024). Blockchain fault tolerance. arXiv:2409.13142.

Я.П. Лукашевич, А.В. Полухін

SWOT-ОЦІНКА ТА ШЛЯХИ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГОСИСТЕМИ УКРАЇНИ В УМОВАХ ВОЄННИХ ВИКЛИКІВ

Резильєнтність енергосистем визначає її здатність зберігати функціонування та швидко відновлюватися під впливом зовнішніх і внутрішніх збурень. У сучасних умовах війни та енергетичних викликів України питання формування резильєнтної енергосистем стає критично важливим. Тому метою дослідження є оцінка резильєнтності енергосистеми України в умовах війни та визначення шляхів її підвищення.

Резильєнтність енергосистем включає надійність інфраструктури, гнучкість для адаптації до змін, інтеграцію відновлюваних джерел енергії, енергетичну безпеку, ефективне управління та стійкість до зовнішніх викликів. Ці компоненти забезпечують функціональність системи навіть за умови відмови окремих її елементів.

Надійність інфраструктури включає фізичну міцність обладнання, здатність витримувати екстремальні умови, а також рівень модернізації мереж. Надійність інфраструктури в Україні значно постраждала через військові дії. Руйнування ліній електропередач, трансформаторних підстанцій та генеруючих об'єктів суттєво знизили її стійкість. Значна частина інфраструктури залишається застарілою і потребує модернізації. Рівень зносу обладнання досягає критичних значень, що збільшує ризик аварійних ситуацій. Водночас можливості для швидкого оновлення обмежені через дефіцит фінансування та складну логістику доставки нових компонентів в умовах воєнного стану. Моніторинг технічного стану обладнання здійснюється, однак масштаби руйнувань ускладнюють ефективну профілактику аварій.

Гнучкість системи визначає її здатність адаптуватися до змін у споживанні або виробництві електроенергії. Це включає інтеграцію відновлюваних джерел енергії (станом на 2024 рік частка електроенергії, що вироблена з ВДЕ, становить 11% [1]), розвиток мікромереж, здатних функціонувати автономно, а також впровадження систем зберігання енергії.

Після 602 російських ударів по енергетичній інфраструктурі України з 2022 по середину 2025 року 76% бізнесу зазнали впливу відключень електроенергії. У відповідь підприємства масово переходять на власні джерела енергії та підвищують енергоефективність – 73,6% з опитаних мають генератори, 59% побудували або будують власну генерацію (переважно СЕС та газопоршневі/газотурбінні установки), 41% впровадили системи зберігання енергії. [1] Також цього року в Україні планується ввести в експлуатацію системи накопичення енергії ємністю 500 МВт*год, а наступного року – ще 1000 МВт*год. [2]

Енергетична безпека – залишається вразливою, незважаючи на прогрес у диверсифікації джерел енергії. Україна значно скоротила залежність від імпорту російських енергоресурсів, проте забезпечення енергетичної автономії вимагає подальшого розвитку внутрішніх ресурсів. Натомість, через російські обстріли і знищення або пошкодження інфраструктури, Україна змушена збільшити залежність від європейських електроенергії, газу, вугілля. Захист критичної інфраструктури посилюється, однак масштаби військових атак ускладнюють повноцінну реалізацію заходів безпеки. Залишаються актуальними питання кібербезпеки, адже автоматизовані системи управління також є потенційними цілями атак.

Ефективність управління в Україні у поточних умовах демонструє позитивну динаміку завдяки підтримці міжнародних партнерів. Залучення іноземних грантів та кредитів дозволяє фінансувати модернізацію та ремонт інфраструктури. Водночас оперативність реагування на аварії залишається на високому рівні, що свідчить про ефективність кризового менеджменту. Проблемним залишається питання цифровізації, адже далеко не всі регіони забезпечені сучасними системами моніторингу та управління. Інвестиції в цю сферу є недостатніми, хоча саме цифрові технології можуть значно підвищити стійкість системи. Залучення нових міжнародних партнерів для фінансування таких ініціатив повинно стати одним із пріоритетів.

Стійкість до зовнішніх впливів є серйозним викликом для України. Військові дії стали основним фактором, який суттєво знизив цей показник. Зруйнована інфраструктура, ускладнена логістика, а також загроза подальших атак ставлять під загрозу стабільність енергосистеми. Розвиток «зеленої» енергетики гальмується, в тому числі через недостатнє фінансування і невиконання держави покладених на неї обов'язків, але її підтримка є критично важливою для зниження залежності від традиційних ресурсів і підвищення стійкості системи до зовнішніх викликів.

На жаль, наразі недоступні чисельні показники для аналізу резильєнтності енергосистеми України, через чутливість такої інформації під час війни. Тому для детального аналізу показників резильєнтності електроенергетики України виконаємо SWOT-аналіз, який дозволяє оцінити внутрішні та зовнішні чинники, які функціонування енергосистеми. Цей підхід дасть змогу оцінити та зрозуміти, як максимально використовувати переваги системи, мінімізувати недоліки та адаптуватися до зовнішніх викликів.

Групою експертів були визначені основні компоненти, що характеризують стан енергосистеми України сьогодні.

В табл. 1 розписані сильні, слабкі сторони енергосистеми України та можливості та загрози, що на неї впливають.

Таблиця 1. – SWOT-аналіз резильєнтності енергосистеми України

Strengths	**Opportunities**
Поступове відновлення генерації	Залучення міжнародних інвестицій та грантів
Поступове відновлення енергетичної інфраструктури	Інтеграція з європейськими енергетичними ринками
Оперативне реагування на аварії	Розвиток мікромереж, систем зберігання енергії та цифрових рішень в Україні та світі
Поступова інтеграція нових альтернативних джерел енергії в енергосистему	Підвищення захисту інфраструктури за допомогою сучасних технологій та підтримки міжнародних експертів
Поступове впровадження таких технологій як мікромережі і системи накопичувачів	Позбавлення залежності від російських та білоруських енергоресурсів
Синхронізація енергосистеми України з електромережею ENTSO-E	
Weaknesses	**Threats**
Руйнування об'єктів генерації та інфраструктури	Російська агресія
Зношеність інфраструктури	Ризик кібератак
Низька частка відновлюваних джерел у загальному енергобалансі	Економічна нестабільність (недостатнє фінансування)
Недостатній розвиток систем зберігання енергії	Залежність від імпорту енергоресурсів
Вразливість до атак	Бюрократичні обмеження
Недостатній рівень цифровізації та використання застарілих технологій	Зміни клімату та глобальні енергетичні кризи

SWOT-аналіз показує, що резильєнтність енергосистеми України базується на поступовому відновленні генерації та інфраструктури, синхронізації з європейськими мережами та інтеграції альтернативних джерел енергії. Водночас система стикається зі значними викликами через руйнування об'єктів, зношеність мереж та низький рівень цифровізації. Можливості для посилення включають міжнародну підтримку, розвиток сучасних технологій захисту та інтеграцію з енергетичними ринками ЄС. Основними загрозами залишаються військові дії, кіберризики, кліматичні зміни та економічна нестабільність, що впливають на здатність до адаптації.

На основі вище наведених компонентів була складена SWOT-матриця (рис. 1). шляхом перехресного оцінювання сильних і слабких сторін, можливостей і загроз. Такий аналіз дозволив зрозуміти, наскільки суттєвими перевагами й недоліками є сильні та слабкі сторони, а також оцінити важливість загроз і можливостей зовнішнього середовища.

		Strengths						Weaknesses						Всього
		Поступове відновлення генерації	Поступове відновлення енергетичної інфраструктури	Оперативне реагування на аварії	Поступова інтеграція нових альтернативних джерел енергії в енергосистему	Поступове впровадження таких технологій як мікромережі і системи накопичувачів	Синхронізація енергосистеми України з електромережею ENTSO-E	Руйнування об'єктів генерації та інфраструктури	Зношеність інфраструктури	Низька частка відновлюваних джерел у загальному енергобалансі	Недостатній розвиток систем зберігання енергії	Вразливість до атак	Недостатній рівень цифровізації та використання застарілих технологій	
Threats	Російська агресія	7,3	8,5	9,2	6,8	8,0	8,5	10,0	6,5	6,0	8,7	8,8	4,3	93
	Ринок кібератак	4,8	5,5	8,8	5,7	7,5	7,0	4,2	3,3	2,5	3,8	8,5	8,3	70
	Економічна нестабільність (недостатнє фінансування)	7,3	7,3	8,5	7,2	6,2	7,7	6,5	8,7	6,8	9,7	8,2	8,3	92
	Залежність від імпорту енергоресурсів	8,7	8,7	7,8	7,7	7,2	2,8	4,7	5,2	6,8	7,8	6,5	3,7	78
	Бюрократичні обмеження	2,0	2,0	2,2	2,8	2,2	2,0	4,5	4,5	4,3	5,2	2,0	4,5	38
	Зміни клімату та глобальні енергетичні кризи	6,0	5,7	6,2	7,5	8,0	5,3	3,8	4,3	4,0	4,7	2,7	3,0	61
Opportunities	Залучення міжнародних інвестицій та грантів	9,5	9,5	8,2	9,0	9,2	5,8	8,2	9,0	7,7	9,5	7,8	8,5	102
	Інтеграція з європейськими енергетичними ринками	6,7	6,5	5,8	7,0	6,8	9,7	6,2	5,0	6,0	6,5	5,5	5,2	77
	Розвиток мікромереж, систем зберігання енергії та цифрових рішень в Україні та світі	4,7	6,0	7,5	7,8	9,7	6,2	7,5	8,5	6,8	8,7	8,2	6,8	88
	Підвищення захисту інфраструктури за допомогою сучасних технологій та підтримки міжнародних експертів	7,2	8,2	8,2	7,7	8,5	5,5	6,5	6,8	3,7	4,2	9,2	8,7	84
	Позбавлення залежності від російських та білоруських енергоресурсів	6,3	6,3	5,2	6,8	6,7	7,8	4,0	5,5	5,3	6,3	6,3	4,0	71
Всього		71	74	78	76	80	68	66	67	60	75	74	65	

Рисунок 1. – SWOT-матриця резильєнтності енергосистеми України

Відсортувавши сильні сторони, слабкі сторони, можливості та загрози за кількістю набраних балів, було визначено наскільки суттєвими перевагами й недоліками є сильні та слабкі сторони, а також оцінено важливість загроз і можливостей зовнішнього середовища (табл. 2). Таблиця кількісно відображає важливість кожного чинника, що допомагає визначити пріоритети для подальших дій.

Таблиця 2. – Результати SWOT-аналізу резильєнтності енергосистеми України

Strengths	**Бали**	**Opportunities**	**Бали**
Поступове впровадження таких технологій як мікромережі і системи накопичувачів	**80**	Залучення міжнародних інвестицій та грантів	**102**
Оперативне реагування на аварії	**78**	Розвиток мікромереж, систем зберігання енергії та цифрових рішень в Україні та світі	**88**
Поступова інтеграція нових альтернативних джерел енергії в енергосистему	**76**	Підвищення захисту інфраструктури за допомогою сучасних технологій та підтримки міжнародних експертів	**84**
Поступове відновлення енергетичної інфраструктури	**74**	Інтеграція з європейськими енергетичними ринками	**77**

Поступове відновлення генерації	**71**	Позбавлення залежності від російських та білоруських енергоресурсів	**71**
Синхронізація енергосистеми України з електромережею ENTSO-E	**68**		
Weaknesses	**Бали**	**Threats**	**Бали**
Недостатній розвиток систем зберігання енергії	**75**	Російська агресія	**93**
Вразливість до атак	**74**	Економічна нестабільність (недостатнє фінансування)	**92**
Зношеність інфраструктури	**67**	Залежність від імпорту енергоресурсів	**78**
Руйнування об'єктів генерації та інфраструктури	**66**	Ризик кібератак	**70**
Недостатній рівень цифровізації та використання застарілих технологій	**65**	Зміни клімату та глобальні енергетичні кризи	**61**
Низька частка відновлюваних джерел у загальному енергобалансі	**60**	Бюрократичні обмеження	**38**

Висновки. Основні переваги полягають у поступовому впровадження технологій (мікромережі і системи накопичувачів), оперативному реагуванні на аварії, інтеграції нових альтернативних джерел енергії в енергосистему. Разом з міжнародною підтримкою, а саме фінансовою допомогою, можливістю залучення інвестицій та грантів, розвитком мікромереж, систем зберігання енергії та і цифрових рішень можливо вирішити ключові виклики та нівелювати виплив загроз

Разом з тим, резильєнтність енергосистеми України перебуває на етапі трансформації під впливом безпрецедентних викликів, спричинених воєнними діями. Незважаючи на масштабні руйнування інфраструктури, дефіцит ресурсів та економічну нестабільність, українська енергетика демонструє здатність до адаптації й відновлення.

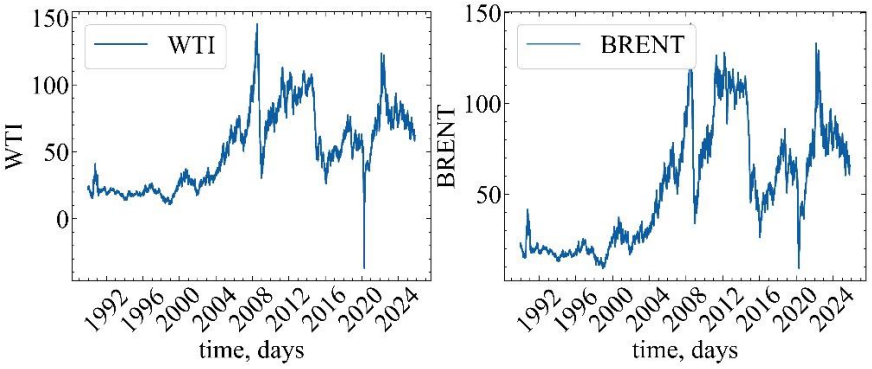
Підвищення резильєнтності енергосистеми України можливе лише за умови синергії технічних, організаційних і соціальних заходів, міжнародної підтримки та активної участі місцевих громад у формуванні децентралізованих енергетичних рішень. Саме поєднання технологічних інновацій із соціальною відповідальністю стане основою для формування стійкої, безпечної та автономної енергосистеми України.

1. Енергетичний перехід URL:https://www.topleadprojects.com/ukraine-energy-transition-2025-ukr (дата звернення: 30.10.2025).
2. Сектор відновлюваної енергетики України до, під час та після війни URL: https://forbes.ua/news/tsogorich-v-ukraini-zapustyat-500-mvt-sistem-nakopichennya-energii-u-2026-rotsi-tsey-pokaznik-podvoitsya-gerus-24102025-33606 (дата звернення: 30.10.2025).

ANALYZING RESILIENCE IN CRUDE OIL PRICES USING BOX-COUNTING RECURRENCE DIMENSION AND RECURRENCE LACUNARITY

Understanding how energy markets absorb shocks and reorganize is central to the theme of the resilience of dynamical systems. Crude oil prices exhibit multiscale variability, clustered volatility, and regime shifts that challenge linear diagnostics. We propose a recurrence-plot–based characterization of the development and resilience of the WTI and Brent benchmarks by combining two geometric descriptors of the recurrence structure: (i) the **box-counting (fractal) dimension** of the recurrence plot (RP) as a compact measure of scaling richness, and (ii) **lacunarity** as a multiscale gauge of "gappiness"/heterogeneity in recurrence patterns. Together, they reveal how recurrent temporal patterns fragment under stress and re-cohere during recovery, offering interpretable proxies for resistance, recovery speed, and reconfiguration – three pillars of resilience. Together these descriptors reveal how recurrent temporal patterns fragment under stress and re-cohere during recovery, linking geometric changes in the RP to resistance, recovery speed, and post-shock reconfiguration – three pillars of resilience. Foundationally, RPs were introduced by Eckmann, Kamphorst & Ruelle and later systematized by Marwan et al. [1, 2]

We analyze crude oil prices of WTI and Brent for the period from 1 January 1990 to 27 October 2025, and their prices are standardized. Given the documented interconnection and contagion between WTI and Brent, especially post-2010, we interpret asymmetries in resilience jointly with known co-movement dynamics. The dynamics of the studied indices is presented in Figure 1.



(a) (b)

Figure 1. – WTI (a) and Brent (b) crude oil prices (daily, USD/bbl) for the period 1990-2025

For each series we reconstruct state space by time-delay embedding. We then compute recurrence plots R_{ij} using a fixed ε threshold (ε=0.3). In this case, the embedded states are considered to be recurrent if they remain within ε. Reconstruction details are justified by Takens' theorem [3].

For each sliding window we apply square boxes of size w to the $T \times T$ RP and count the number $N(w)$ of boxes containing at least one recurrence point. The **recurrence fractal dimension** D_B is estimated from the slope of log$N$(w) vs. log($1/w$) over an admissible scaling range. Intuitively, larger D_B indicates richer cross-scale occupancy of the recurrence pattern; lower D_B indicates sparser, more homogeneous recurrence organization.

We compute **lacunarity** $\Lambda(w)$ for each box size w by the gliding-box mass statistics of black pixels (recurrences) within boxes [4, 5]. Given the mass distribution $P_w(M)$, we use the first two moments $Z^{(1)}(w)$, $Z^{(2)}(w)$ to form $\tilde{\Lambda}(w)=Z^{(2)}(w))/[Z^{(1)}(w)]^2 = 1+(\sigma^2(w)/\mu^2(w)$, and then normalize it using the following equation: $\Lambda(w)=2 - (1/(\tilde{\Lambda}(w)) + 1/(\tilde{\Lambda}^{\wedge\dagger}(w))$.

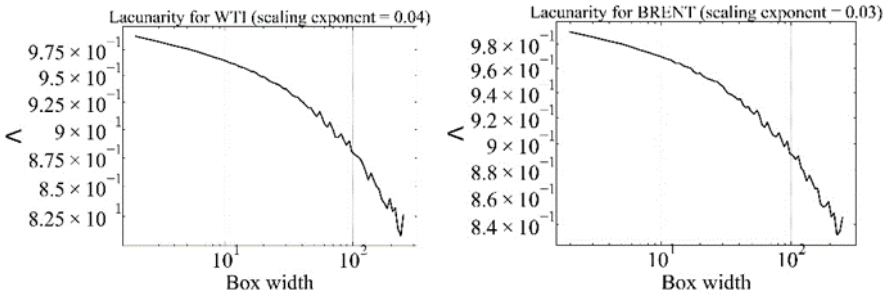
This recurrence lacunarity (RL) quantifies multiscale heterogeneity (large, variable gaps leads to higher Λ).

Most classical RQA indicators summarize line structures (e.g., diagonal/vertical lines), which can miss non-linear microstructures or be sensitive to thresholding/edge effects; lacunarity complements them by capturing geometric heterogeneity across scales without relying on minimum line lengths or specific microstates.

Prior work [6] shows that RL provides a robust multiscale detector of regime transitions, since it does not rely on line-length thresholds and captures heterogeneity directly in the RP geometry.

Both benchmarks exhibit clear power-law scaling in w vs. $N(w)$ and very close fractal dimensions (D_B^{WTI}=1.37 vs. D_B^{Brent}=1.35). The slightly higher D_B for WTI suggests a marginally more space-filling (multiscale) recurrence structure, consistent with stronger mixing of temporal scales. As emphasized in the study, box-counting dimension captures overall scaling richness, while lacunarity will discriminate differences in gap heterogeneity between WTI and Brent.

Figure 2 presents log-log lacunarity $\Lambda(w)$ versus box width w (gliding-box method).



(a) (b)

Figure 2. – Lacunarity of the WTI recurrence plot (a) and Brent recurrence plot (b)

Both benchmarks display clear power-law-like decay of lacunarity, consistent with multiscale heterogeneity in their recurrence geometry. The slightly larger exponent for WTI (0.04 > 0.03) implies a little stronger scale dependence: WTI's gap structure homogenizes faster as the observation scale coarsens, whereas Brent retains heterogeneity more persistently across scales. Combined with the nearly equal box-counting dimensions, these lacunarity results suggest that the subtle differences between WTI and Brent lie neither in the overall filling of repetition space nor in how the heterogeneity of gaps disappears with increasing scale.

Conclusions. Recurrence-plot geometry provides a compact, scale-aware view of crude-oil market development and resilience. Both benchmarks display clear power-law behavior in the box-counting curves with fractal dimensions, evidencing similarly rich multiscale recurrence structure. Taken together, the near-equal D_B lacunarity slopes show that there are less differences in both overall space-filling of recurrences and in how gap heterogeneity collapses with scale. Results should be validated with bootstrap confidence intervals, robustness to embedding/recurrence-rate choices and scaling-window selection, and event-aligned, sliding-window analysis [7, 8] around 1998, 2008, 2014-16, 2020, and 2022. Integrating these metrics into a composite resilience score would enable systematic comparison of WTI vs. Brent and supports decision-making in risk management and policy.

1. Eckmann, J.-P., Kamphorst, S. O., & Ruelle, D. (1987). Recurrence plots of dynamical systems. *Europhysics Letters, 4*(9), 973–977. https://doi.org/10.1209/0295-5075/4/9/004.
2. Marwan, N., Romano, M. C., Thiel, M., & Kurths, J. (2007). Recurrence plots for the analysis of complex systems. *Physics Reports, 438*(5–6), 237–329. https://doi.org/10.1016/j.physrep.2006.11.001.
3. Takens, F. (1981). Detecting strange attractors in turbulence. In D. A. Rand & L.-S. Young (Eds.), *Dynamical Systems and Turbulence, Warwick 1980* (Lecture Notes in Mathematics, Vol. 898, pp. 366–381). Springer. https://doi.org/10.1007/BFb0091924.

4. Allain, C., & Cloitre, M. (1991). Characterizing the lacunarity of random and deterministic fractal sets. *Physical Review A, 44*(6), 3552–3558. https://doi.org/10.1103/PhysRevA.44.3552.
5. Plotnick, R. E., Gardner, R. H., Hargrove, W. W., Prestegaard, K. L., & Perlmutter, M. (1996). Lacunarity analysis: A general technique for the analysis of spatial patterns. *Physical Review E, 53*(5), 5461–5468. https://doi.org/10.1103/PhysRevE.53.5461.
6. Braun, T., Unni, V. R., Sujith, R. I., Kurths, J., & Marwan, N. (2021). Detection of dynamical regime transitions with lacunarity as a multiscale recurrence quantification measure. *Nonlinear Dynamics, 104*(4), 3955–3973. https://doi.org/10.1007/s11071-021-06457-5.
7. Bielinskyi, A., Soloviev, V., Solovieva, V., Semerikov, S., & Radin, M. (2023). Recurrence quantification analysis of energy market crises: a nonlinear approach to risk management. *CEUR Workshop Proceedings*, 3465, 110-131. https://ceur-ws.org/Vol-3465/paper14.pdf.
8. Bielinskyi, A., Serdyuk, O., Semerikov, S., & Soloviev, V. (2021). Econophysics of cryptocurrency crashes: a systematic review. *CEUR Workshop Proceedings*, 3048, 31-133. https://ceur-ws.org/Vol-3048/paper03.pdf.

Д.А. Гнатюк

КОНТЕКСТНО-ЗАЛЕЖНА LSTM-XGBOOST АРХІТЕКТУРА ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У ЖУРНАЛАХ ПОДІЙ БАГАТОСЕРВІСНИХ СЕРВЕРНИХ ПРОГРАМНИХ СИСТЕМ

Сучасні розподілені системи генерують величезні обсяги журналів подій, що містять критичну інформацію про стан системи та аномалії. Більшість існуючих рішень на базі глибокого навчання вимагають GPU інфраструктури, що створює бар'єри для розгортання на периферійних пристроях, промислових системах та в ресурсообмежених середовищах. Водночас, традиційні CPU-based методи демонструють недостатню точність для промислового застосування.

У роботі досліджується можливість створення системи виявлення аномалій, яка працює виключно на CPU, зберігаючи при цьому контекстну точність. Запропонований підхід поєднує контрольоване навчання LSTM вкладень з XGBoost класифікатором та спеціалізованою обробкою багато сервісних контекстів середовищ.

ПРОБЛЕМАТИКА ТА ЗАПРОПОНОВАНІ РІШЕННЯ

Традиційні підходи використовують глобальні ковзні вікна, що змішують журнали подій з різних сервісів в один потік. Це призводить до втрати часових залежностей, оскільки помилка в базі даних має інший контекст та наслідки, ніж помилка в сервісі API. Попередні експерименти показують, що таке змішування призводить до серйозної деградації метрик та сприяє появі хибних висновків.

У роботі запропоновано контекстно-залежну архітектуру з окремими буферами для кожної пари (хост, сервіс). Система підтримує незалежні контексти з ковзними вікнами для збереження часових залежностей. Паралельне керування реалізоване через блокування-на-контекст, що забезпечує ефективну складність операцій. Попередні експерименти демонструють покращення метрик класифікації. Однак залишаються відкритими питання масштабованості при збільшенні кількості контекстів та можливої конкуренції блокувань при високому навантаженні.

LSTM мережі ефективно захоплюють семантичні патерни в текстових журналах подій, проте втрачають важливу структурну інформацію, таку як часові аномалії (сплески активності, затримки між подіями). Експерименти показують, що використання тільки LSTM підходу демонструє певний рівень точності, тоді як використання тільки ручних статистичних ознак показує нижчі результати.

Запропоноване гібридне рішення об'єднує LSTM вкладення (семантичні ознаки) зі статистичними ознаками (часові патерни), формуючи розширене представлення для XGBoost класифікатора. Це дозволило досягти

покращення метрик порівняно з LSTM-only підходом. Планується дослідити оптимальність розмірності представлення та альтернативні механізми об'єднання, з механізмом уваги.

Класичний підхід передбачає двоетапне навчання: попереднє навчання вкладень без нагляду (зазвичай через автоенкодер) з подальшим заморожуванням та навчанням класифікатора [1]. Така схема має фундаментальну проблему: відсутність потоку градієнтів від задачі класифікації до вкладень призводить до того, що вкладення оптимізовані для реконструкції, а не для дискримінації аномалій. Базовий експеримент з неконтрольованим автоенкодером показав обмежені результати.

У даній роботі запропоновано архітектуру подвійного призначення, де LSTM одночасно виконує дві задачі: генерацію вкладень для XGBoost та бінарну класифікацію. Спільна оптимізація через бінарну крос-ентропійну втрату забезпечує зворотне поширення градієнтів до вкладень, що дозволяє їм адаптуватися безпосередньо під задачу виявлення аномалій. Попередні результати демонструють суттєве покращення метрик, а між класова відстань у просторі вкладень значно збільшується порівняно з неконтрольованим підходом. Критичними питаннями для подальшого дослідження залишаються мінімальна кількість позначених зразків та механізми адаптації до нових типів аномалій у режимі безперервного навчання.

Різні сервіси мають суттєво різні базові рівні аномалій: деякі сервіси демонструють низький відсоток аномалій, тоді як інші генерують значно більше попереджень. Використання глобального порогового значення призводить до дилеми: або висока кількість хибних спрацювань, або велика кількість пропущених аномалій [2].

Запропоноване рішення полягає в адаптивному калібруванні порогових значень для кожного контексту окремо. Для кожного сервісу будується крива точність-повнота, і обирається поріг, що максимізує F1-метрику. На тестовій вибірці це дозволило досягти високої точності класифікації. Однак існує ризик перенавчання під валідаційну вибірку, а також відкритим залишається питання калібрування порогів для нових сервісів без історичних даних.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

Досліджується гіпотеза, що інтеграція PyTorch з Intel Math Kernel Library забезпечує значне прискорення на CPU. Попередні вимірювання показують потенційне прискорення матричних операцій та прямого проходу LSTM завдяки векторизації SIMD інструкцій. Однак ці результати потребують верифікації через контрольовані бенчмарки з порівнянням MKL-оптимізованої версії з базовою реалізацією. Додатково планується тестування на ARM архітектурах.

Для прискорення навчання XGBoost використовується метод гістограмних розбиттів (tree_method='hist') замість точного методу. Гіпотеза

полягає в тому, що робота з обмеженою кількістю зразків замість повного набору зразків дає кращу алгоритмічну складність. Попередні експерименти показують суттєве прискорення навчання та зменшення використання пам'яті.

Критичним питанням залишається можлива втрата точності через гістограмну апроксимацію та поведінка методу при масштабуванні до великих наборів даних.

Профілювання виявило основні вузькі місця в конвеєрі обробки: LSTM та XGBoost виведення займають більшість часу обчислень. Попередня обробка та групування контекстів становлять меншу частину від загальної затримки. Для мінімізації затримки використовується підхід без пакування, що створює компроміс між затримкою та пропускною здатністю.

ПОПЕРЕДНІ РЕЗУЛЬТАТИ ТА ВАЛІДАЦІЯ

Експерименти проводилися на синтетичному наборі даних, що імітує журнали подій багатосервісної платформи. Навчальна вибірка містить декілька десятків тисяч запитів журналів подій з множини контекстів різних хостів та сервісів. Валідаційна вибірка включає достатню кількість зразків для оцінки продуктивності. Критичним обмеженням є синтетична природа даних, що вимагає валідації на реальних промислових журналах подій.

Порівняльний аналіз з базовими методами показує наступне. LogBERT, згідно з літературними джерелами [3, 4], демонструє високі показники точності, однак вимагає GPU та має значну затримку. Запропонований підхід досягає конкурентних результатів з низькою затримкою на CPU. Неконтрольований LSTM автоенкодер, XGBoost з ручними ознаками та випадковий ліс показують нижчі результати.

Важливо відзначити, що результати LogBERT екстрапольовані з літературних джерел та не тестувалися безпосередньо на даному наборі даних, що є обмеженням для прямого порівняння.

Запропонований підхід демонструє незначне зниження точності порівняно з заявленими показниками LogBERT, однак забезпечує суттєве покращення затримки, значне зменшення операційних витрат, повністю усуває залежність від GPU та дозволяє розгортання на периферійних пристроях. Робоча гіпотеза полягає в тому, що така втрата точності є прийнятною для широкого класу застосувань, що потребують ресурсообмеженого розгортання.

ВИСНОВКИ

Це дослідження розглядає питання: чи можна досягти промислового рівня виявлення аномалій у журналах подій на апаратурі з CPU без значної втрати якості. Попередня відповідь, базована на синтетичному наборі даних, є позитивною: продемонстровано конкурентні метрики класифікації, низьку затримку та високу точність. Однак ця відповідь потребує підтвердження

через валідацію на реальних даних, тестування масштабованості та пряме порівняння з сучасними методами.

Потенційний вплив успішної валідації є значним: можливість периферійного розгортання на IoT пристроях, промислових або захищених системах. Суттєве зменшення вартості порівняно з GPU рішеннями; демократизація доступу до машинного навчання без необхідності дорогої апаратури.

1. Ocansey, I. T., Bhattacharya, R., & Sen, T. (2025). LogTinyLLM: Tiny Large Language Models Based Contextual Log Anomaly Detection. arXiv https://arxiv.org/abs/2507.11071.
2. Zhu, J., He, S., & Lyu, M. R. (2016). SLHE: A Log-based Anomaly Detection Framework for Cloud Systems. In Proceedings of the 27th International Symposium on Software Reliability Engineering (ISSRE), pp. 207–218.
3. Van den Bergh, T., Doerr, C., & van Eeten, M., "DEEPCASE: Semi-Supervised Contextual Analysis of Security Events," 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022, pp. 522-539, doi: 10.1109/SP46214.2022.9833671.
4. Zhang, Y., Li, Y., & Wang, X. (2021). LogBERT: Log Anomaly Detection via BERT. arXiv preprint arXiv:2103.04475.

УДК 004.6:004.82

В.Р. Герасимов, В.В. Душеба

СУЧАСНІ МЕТОДИ ОПТИМІЗАЦІЇ СТРУКТУРИ NOSQL-БАЗ ТИПУ «КЛЮЧ–ДОКУМЕНТ»

Ключові слова: NoSQL, документно-орієнтовані бази даних, оптимізація структури даних, денормалізація, міграція з реляційних баз, локальний пошук, жадібний алгоритм, генетичний алгоритм.

Сучасні інформаційні системи дедалі частіше поєднують реляційні та NoSQL бази даних через потребу в обробці великих обсягів інформації, високій частоті запитів і масштабованості. Реляційні бази забезпечують цілісність даних, але мають жорстку схему, що ускладнює горизонтальне масштабування [1]. Документно-орієнтовані NoSQL-бази типу «ключ–документ» натомість підтримують гнучкі структури, забезпечують високу продуктивність читання і запису та здатність зберігати працездатність при зміні навантаження чи структури даних. Оптимізація їхньої схеми безпосередньо пов’язана з резильєнтністю системи — здатністю адаптуватися без втрати ефективності [2].

Процес міграції даних із реляційних баз у документні сховища потребує уважного планування структури документів. Невдалий вибір схеми може призводити до дублювання даних, збільшення часу доступу та ускладнення оновлень [3]. Для підвищення продуктивності та оптимального використання ресурсів застосовують різні методи оптимізації структури документів, кожен з яких має свої особливості, переваги та обмеження.

Локальний пошук (Local Search) використовується для поступового покращення структури даних на основі локальних критеріїв продуктивності. Метод передбачає ітеративні зміни окремих документів або колекцій, спрямовані на зменшення часу читання та підвищення швидкості доступу. Основною перевагою є простота реалізації та швидка адаптація до змін навантаження. Водночас локальний пошук може застрягати у локальних оптимумах, що обмежує досягнення глобально найефективнішої структури бази [2].

Жадібний алгоритм (Greedy Algorithm) дозволяє обирати найкращу конфігурацію на кожному кроці оптимізації, орієнтуючись на конкретний критерій продуктивності. Цей підхід добре підходить для систем, де потрібне швидке прийняття рішень і обмежений час на планування. Його переваги включають швидкість та простоту впровадження, проте метод не гарантує досягнення глобального оптимуму і може пропустити більш ефективні комбінації [2].

Генетичний алгоритм (Genetic Algorithm) застосовується для пошуку оптимальної структури документів із використанням принципів еволюційного відбору та комбінування різних варіантів. Він ефективний для

великих і складних баз даних, де важливо одночасно враховувати кілька критеріїв продуктивності. Перевагами є здатність знаходити високоефективні конфігурації і гнучкість при багатокритеріальних задачах. Недоліками є значні обчислювальні ресурси та складність налаштування параметрів [4].

Адаптивна денормалізація (Adaptive Denormalization) дозволяє змінювати структуру документів залежно від характеру запитів та навантаження. Метод забезпечує оптимізацію продуктивності читання і дозволяє ефективно масштабувати систему при змінних умовах. Переваги включають гнучкість і підвищення швидкості обробки запитів. Обмеження пов'язані зі складністю автоматизації та потенційним надмірним дублюванням даних при некоректних налаштуваннях [4].

Оптимізація структури та запитів у NoSQL-сховищах безпосередньо сприяє підвищенню резильєнтності системи, оскільки забезпечує стабільну продуктивність за змінних навантажень і еволюції даних. Локальний пошук і жадібні алгоритми дозволяють швидко адаптуватися до короткочасних коливань, тоді як генетичні підходи й адаптивна денормалізація підвищують стійкість до довготривалих структурних змін. Завдяки цьому система зберігає ефективність навіть у динамічних умовах.

Висновки

Ефективність методів оптимізації залежить від обсягу даних, характеру навантажень і цільових пріоритетів системи. Локальний пошук і жадібні алгоритми доцільні для систем середнього масштабу з частими оновленнями, тоді як генетичні алгоритми та адаптивна денормалізація забезпечують стабільну роботу при складній структурі та великій взаємозалежності даних. Огляд підтверджує необхідність системного підходу до оптимізації NoSQL-сховищ і створює підґрунтя для подальшої автоматизації процесів міграції SQL-даних. Оптимізаційні стратегії не лише підвищують продуктивність, а й зміцнюють резильєнтність інформаційних систем, забезпечуючи їхню адаптивність до змін у структурі даних і навантаженнях.

1. Герасимов В. Р., Душеба В. В. Аналіз методів оптимізації роботи баз даних // Електронне моделювання. — 2024. — Т. 46, № 6. — С. 43–54.
2. Saravanan Subramanian, Subhash Saravanan. Modern Trends in NoSQL Data Bases // *International Journal of Computer Trends and Technology (IJCTT)*. — 2024. — Vol. 72, no. 9. — Pp. 126-130.
3. Khan W. SQL and NoSQL Database Software Architecture: A Systematic Literature Review // Journal of Computer Science and Technology. — 2023. — Vol. 38, no. 2. — Pp. 1–15.
4. Chen Y., Zhang X. Adaptive Denormalization in Document Databases Using Query Prediction Models // Journal of Big Data. — 2023. — Vol. 10, no. 1. — Pp. 12–28.

О.Г. Клименко

МОДЕЛІ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ УЗЕ ДЛЯ ЗМЕНШЕННЯ ТЕРМІНУ ОКУПНОСТІ В УМОВАХ РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ УКРАЇНИ

Одним із важливих напрямків сучасного розвитку електроенергетики є децентралізація генерації і розподілу електроенергії шляхом впровадження локальних енергетичних ресурсів та засобів управління їх режимами за технологіями «розумних мереж». Проєкт спрямований на вирішення проблеми оптимізації роботи мікромережі саме на українському ринку електроенергії за рахунок систем зберігання енергії. Рішення полягає в охопленні трьох ключових перспектив: створення стандартизованих процедур приєднання, впровадження локалізованих мереж і надання можливості керування активами в реальному часі.

Основні завдання проєкту наступні: аналіз перспектив впровадження мікромереж в Україні (від наявності основних компонентів на місцевому ринку до міжнародних регуляторних стандартів); розробка математичних моделей мікромереж із врахуванням вимог Правил улаштування електроустановок та Кодексу систем розподілу України. Математичні моделі призначені для оцінки доцільності впровадження енергетичних ресурсів у складі мікромереж для різних типів споживачів, а також оцінки ефекту від їх експлуатації як в режимі підключення до системи розподілу, так і в острівному режимі.

За IEC TS 62898 визначення «Microgrid» (мікромережа) – це група приєднаних до мережі навантажень та розподілених енергоресурсів з визначеними електричними границями, що формують місцеву електричну енергосистему на розподільчих рівнях напруги (0,4 кВ, 10 кВ, 35 кВ), що діє як єдиний керований організм та здатна працювати з будь-якою іншою (групою) зв’язано чи в острівному режимі [1].

Автономний або острівний режим - наразі це найважливіша функція. Коли у загальній мережі стається аварія (наприклад, блекаут), мікромережа автоматично від'єднується від неї у "точці загального підключення" (POC). Після від'єднання вона продовжує живити своїх місцевих споживачів, використовуючи власну генерацію (наприклад, сонячні панелі + генератор) та накопичену енергію (з акумуляторів). Це забезпечує безперебійне живлення для критично важливих об'єктів.

За роботу мікромережі відповідає зовнішня система енергоменеджменту (EMS). У режимі реального часу EMS відстежує генерацію, споживання та наявність живлення від системи розподілу. У складі мікромережі EMS є основним засобом контролю та управління режимами як мікромережі загалом, так і окремих енергетичних ресурсів [2].

Економічно доцільним наразі є впровадження складових мікромереж – установок зберігання електроенергії (УЗЕ – ESS). Кількість саме таких

установок на території України безупинно збільшується. Інтерес інвесторів пояснюється їх здатністю створення бізнес-процесів. Така УЗЕ володіє наступними експлуатаційними характеристиками:

- віддалене управління, низькі витрати на утримання;
- маневреність (швидкодія в поєднанні з високою потужністю);
- компактність та відносно малі габарити всієї установки, відносно легке та швидке розгортання;
- високий коефіцієнт корисної дії (близько 90%), відповідність європейським екологічним вимогам;
- «пільгове» ввезення обладнання на територію України (без ПДВ);
- відповідність вимогам енергосистеми до балансування потужності.

За "Кодексом систем розподілу" УЗЕ класифікуються відповідно до рівня напруги в точці приєднання та їхньої максимальної потужності відпуску за типами: 1) тип А1 - точка приєднання з напругою нижче 110 кВ і максимальна потужність відпуску до 0,15 МВт включно; 2) тип А2 - точка приєднання з напругою нижче 110 кВ і максимальна потужність відпуску до 1 МВт включно, крім тих, що відносяться до класу А1; 3) тип В - точка приєднання з напругою нижче 110 кВ і максимальна потужність відпуску від 1 МВт до 20 МВт включно; 4) тип С - точка приєднання з напругою нижче 110 кВ і максимальна потужність відпуску від 20 МВт до 75 МВт включно; 5) тип D - точка приєднання з напругою 110 кВ або вище та/або максимальна потужність відпуску становить вище 75 МВт [3].

В роботі використано досвід участі у створенні об’єкту енергетики, що набула статусу «Постачальник допоміжних послуг» НЕК «Укренерго» - УЗЕ типу «В» виробництва HUAWEI, зі встановленою потужністю 8 МВт, ємністю 10 МВт/год (на основі акумуляторних комірок LiFePO4).

Якісну оцінку ефективності роботи цієї установки зберігання електроенергії можна здійснити на основі добових графіків (рис. 1, рис. 3) та за погодинних (рис. 2, рис. 4) обсягів накопичення та відпуску електричної енергії (ЕЕ) УЗЕ (з системи моніторингу). [10]

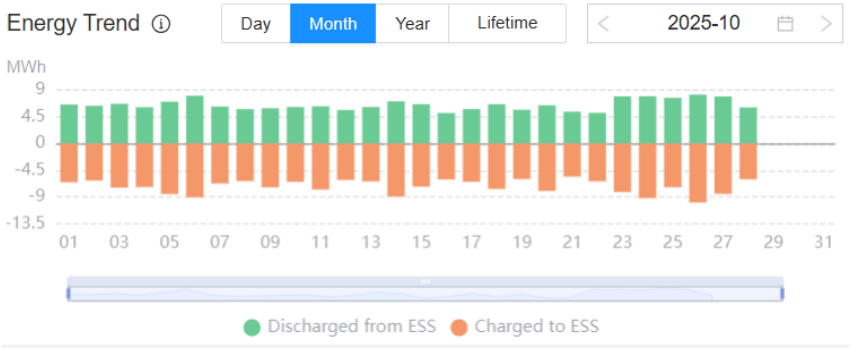


Рисунок 1. – Графік накопичення та відпуску ЕЕ УЗЕ добовий в режимі РПЧ

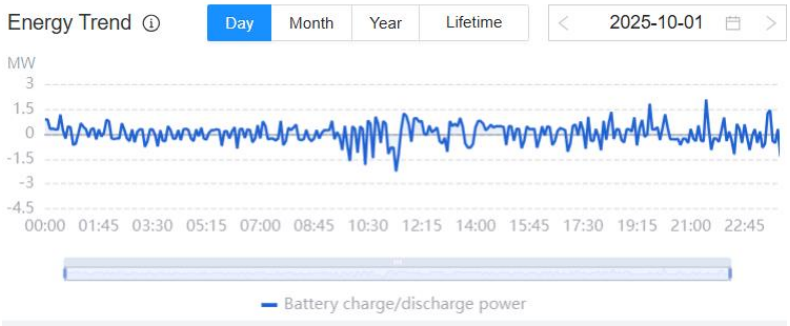


Рисунок 2. – Графік накопичення та відпуску ЕЕ УЗЕ погодинний в режимі РПЧ

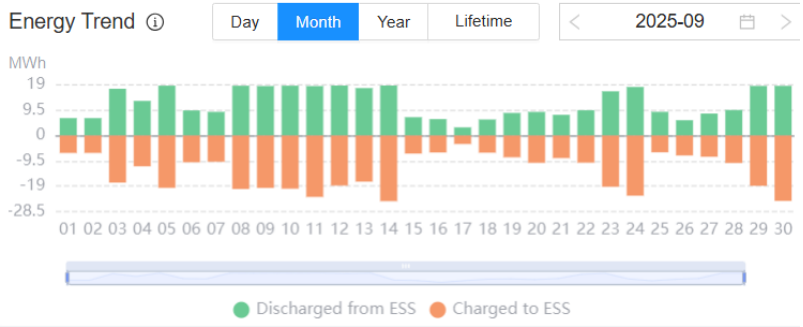


Рисунок 3. – Графік накопичення та відпуску ЕЕ УЗЕ добовий в заданому режимі, за механізмом «самовиробництво»

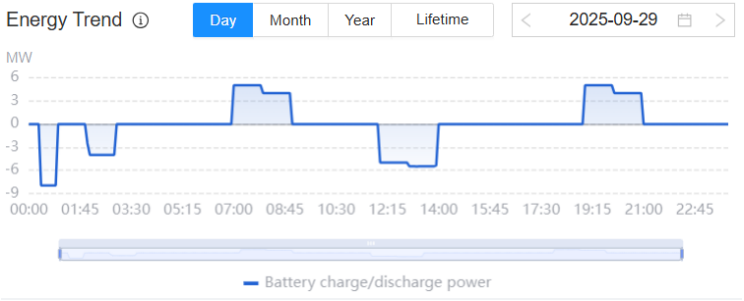


Рисунок 4. – Графік накопичення та відпуску ЕЕ УЗЕ погодинний в заданому режимі, за механізмом «самовиробництво»

На рис. 2 показано роботу УЗЕ в режимі «резерв підтримки частоти» (РПЧ - FCR), УЗЕ здійснює первинне регулювання частоти, автоматично, зі швидкістю реакції 0,1-2 с з моменту відхилення частоти від номінального значення. Суттєво на стабільність енергосистеми системи впливає потужність кількість УЗЕ. Потреба Оператора системи передачі (НЕК «Укренерго») в РПЧ була закрита Спеціальним аукціоном від 15 серпня 2024 р. на наступні п’ять років. Тому решта УЗЕ може бути встановлено та підключено до мережі завдяки іншим сценаріям використання в комерційній діяльності. [4]

За результатами аналізу економічного ефекту від експлуатації УЗЕ визначено наступні вимоги до проєктування локальних об’єктів з УЗЕ:

1) слід використовувати один або більше з таких принципів розрахунку: чиста приведена вартість; дохід на інвестиції; норма прибутку; час, необхідний для досягнення беззбитковості;

2) кількісно оцінити соціально-економічні вигоди з точки зору підвищення надійності електропостачання, включаючи, зокрема: пов’язане зменшення ймовірності втрати електропостачання протягом усього терміну проведення реконструкції/переоснащення; ймовірну ступінь і тривалість такої втрати електропостачання; соціальну годинну вартість такої втрати електропостачання;

3) кількісно оцінити вигоди для внутрішнього ринку електричної енергії, транскордонної торгівлі та інтеграції генеруючих потужностей, що здійснюють виробництво електричної енергії з відновлюваних джерел енергії, включаючи, зокрема: реакцію активної потужності на відхилення частоти; резерви балансування; забезпечення реактивною потужністю; ведення режиму перевантаження; захисні заходи [3].

Попередньо, ця УЗЕ проходила випробування в різних режимах роботи. На рис. 4 відображено графік накопичення та відпуску електроенергії від УЗЕ погодинний в заданому режимі, за механізмом самовиробництва. При цьому власник УЗЕ може продавати надлишки виробленої та/або збереженої електричної енергії в енергосистему за ринковими цінами [5].

Основною частиною досліджень є розробка моделей оптимізації. Ці моделі дозволяють визначити оптимальний графік керування компонентами мікромережі, залежно від коливання вартості електроенергії на роздрібному ринку. Імітаційне моделювання з використанням Gurobi Optimizer виконується при розв’язанні завдань розробки та тестування графіків управління режимами мікромережі на основі даних прогнозу споживання та вартості електроенергії з метою раціонального використання наявних локальних енергетичних ресурсів [7].

Мета досліджень полягає у розробці формалізмів для визначення оптимальної (за критерієм мінімізації строку окупності) архітектури мікромережі та планування графіків оптимального використання наявних енергетичних ресурсів. Розроблені за результатами досліджень математичні і

імітаційні моделі надаватимуть інструментарій для вибору оптимальних рішень як на етапах проєктування, так і у процесі експлуатації мікромережі. Розроблені формалізми також можуть бути використані при підготовці нормативно-правових актів, а також для імітації режимів як окремої онлайн-послуги для планування діяльності операторів мікромереж.

1. Microgrids – Part 4: Use cases, IEC TS 62898-4.
2. Microgrids – Part 2: Guidelines for operation, IEC TS 62898-2.
3. Code of transmission systems. NERC Resolution 14.03.2018 №309. URL: https://zakon.rada.gov.ua/laws/show/v0309874-18#Text (Accessed at 02.08.2025) (Ukr).
4. Ancillary services market. ULR: https://ua.energy/dopomizhni-poslugy/#1724134294973-419ecfbb-7d12.
5. On Alternative Energy Sources. Law of Ukraine 20.02.2003 № 555-IV ULR: https://zakon.rada.gov.ua/rada/show/555-15#Text (Accessed at 01.04.2025) (Ukr.)
6. Concept of implementation of “smart grids” in Ukraine by 2035. Order of the Cabinet of Ministers of Ukraine 14.10.2022 № 908-р. URL: https://zakon.rada.gov.ua/laws/show/908-2022-%D1%80#Text (Accessed at 01.04.2025) (Ukr).
7. Gurobi Optimizer. Copyright © 2025, Gurobi Optimization, LLC ULR: https://docs.gurobi.com/projects/optimizer/en/current/index.html.
8. I.V. Blinov, Ye.V. Parus, P.V. Shymaniuk and A.O. Vorushylo. 2024. Optimization model of microgrid functioning with solar power plant and energy storage system. Tekhnichna Elektrodynamika. 2024. No 5. Pp. 69–78. (Ukr) DOI: https://doi.org/10.15407/techned2024.05.069.
9. Kyrylenko O., Denysiuk S., Blinov I. Energy management: new priorities of the 21st century. Power engineering: economics, technique, ecology. 2024. No 1. Pp. 7–27. DOI: https://doi.org/10.20535/1813-5420.1.2024.297508 (Ukr).
10. © Huawei Digital Power Technologies Co., Ltd., ULR: https://eu5.fusionsolar.huawei.com/unisso/login.action.

О.С.Ткаченко, А.В. Ільєнко

МАТЕМАТИЧНА МОДЕЛЬ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Вступ

Сучасні соціальні мережі критично впливають на національну безпеку та свободу слова, створюючи дилему для правового регулювання. Вони є майданчиком для демократичного обміну думками, але водночас слугують каналом для поширення дезінформації та пропаганди. Ця подвійність вимагає розробки нових юридичних механізмів, здатних збалансувати захист суспільних інтересів від загроз і гарантування фундаментальних прав громадян.

Для вирішення цієї задачі пропонується створити математичну модель, яка кількісно оцінить вплив різного рівня регулювання на ключові індекси: свободу слова, безпеку та національні інтереси. Математичних підходів до створення моделей існує багато різних варіантів, адже всі моделі так чи інакше використовують різні змінні для розрахунків відповідних вагових коефіцієнтів та параметрів. Як один із варіантів математичної моделі, що описує компроміс між свободою слова та забезпеченням громадської безпеки й національних інтересів при регулюванні інформаційних впливів у соціальних мережах [1-6].

Опишемо математичну модель для кількісної оцінки та оптимізації правового регулювання поширення інформаційних впливів у соціальних мережах. Модель спрямована на досягнення балансу між свободою слова (FR) та забезпеченням громадської безпеки (SR) і захисту національних інтересів (NR).

1. Ключові Компоненти Моделі

Модель сформульована як оптимізаційна задача з єдиною змінною — рівнем регулювання (R).

1.1. Змінна регулювання (R)

$R \in [0,1]$: параметр, що характеризує інтенсивність застосування правових заходів.

$R = 0$: відсутність регулювання.

$R = 1$: максимальне регулювання.

1.2. Функції індексів

Основні індекси, що залежать від R наведено у таблиці 1:

Таблиця 1. — Основні індекси, що залежать від R

Індекс	Формула	Опис та Вплив R
Свобода Слова (FR)	$FR = 1 - R^{\gamma}$	Зі збільшенням R індекс зменшується. $\gamma > 0$ визначає швидкість втрати свободи.
Громадська Безпека (SR)	$SR = S_0 + (S_{\max} - S_0) \cdot (1 - e^{-k_S R})$	Зі збільшенням R індекс зростає. S_0 — базовий рівень безпеки. k_S — швидкість зростання індексу.
Захист Націнтересів (NR)	$NR = N_0 + (N_{\max} - N_0) \cdot (1 - e^{-k_N R})$	Зі збільшенням R індекс зростає. N_0 — базовий рівень захисту. k_N — коефіцієнт зростання.

1.3. Ефективний Рівень Інформаційної Загрози

Початковий рівень шкідливого інформаційного впливу ($I \in [0,1]$) зменшується регулюванням (1) або з урахуванням тексту загрози - x (2):

$$I_{\text{еф}}(R) = I \cdot (1 - R) \quad (1)$$

$$I_{\text{еф}}(R) = I_x \cdot (1 - R) \quad (2)$$

$I_{\text{еф}}(R)$ може коригуватися для врахування додаткових факторів, що підвищують ризик:

— історія користувача (H_u): $I_{\text{еф}}(R,u) = I_x \cdot (1 - R) \cdot (1 + H_u)$, де H_u — історія порушень, нормована до $[0,1]$;

— дезінформованість тексту (D_x): $I_{\text{еф}}(R) = I_x \cdot (1 - R) \cdot (1 + D_x)$, де D_x — рівень викривлення інформації;

— геолокація (G_l): ризик від розташування контенту в зоні конфлікту (може бути бінарним $0/1$ або градієнтною шкалою $G_l = e^{-k_d \cdot d(l,l_c)}$);

— контекст подій (C_t): ризик під час критичних подій ($C_t = e^{-k_C(t-t_0)}$).

1.4. Індекс Національної Безпеки

Загальний рівень національної безпеки ($NSLR$) враховує позитивні ефекти регулювання та негативний вплив залишкової загрози:

$$NSLR = SR + NR - \delta \cdot I_{\text{еф}}(R) \quad (3)$$

$\delta > 0$ — коефіцієнт ваги впливу інформаційної загрози.

Велике δ (наприклад, $\delta \approx 1$ або більше) означає критичний вплив загрози на безпеку.

1.5. Індекс Балансу (BR)

BR — зважена сума індексів, що відображає пріоритети суспільства/уряду:

$$BR = w_F FR + w_S SR + w_N NR \quad (4)$$

w_F, w_S, w_N — вагові коефіцієнти, причому $w_F + w_S + w_N = 1$.

Приклади вагових моделей:

— демократія: $w_F = 0.6, w_S = 0.2, w_N = 0.2$ (пріоритет свободи слова);

— національна безпека: $w_F = 0.3, w_S = 0.4, w_N = 0.3$ (збалансований контроль);

— авторитарний контроль: $w_F = 0.1, w_S = 0.4, w_N = 0.5$ (пріоритет державних інтересів).

2. Оптимізаційна задача та приклад розрахунку

2.1. Постановка задачі

Знайти оптимальний рівень регулювання $R^* \in [0,1]$, що максимізує BR за умов:

Максимізувати: BR, при умові: $FR \geq F_{\min}$ та $NSLR \geq NSL_{\min}$

2.2. Ілюстративний приклад (дані взято аналітично для наприклад України)

Вихідні дані: $\gamma = 1$; $S_0 = 0.5, S_{\max} = 1, k_S = 2$; $N_0 = 0.5, N_{\max} = 1, k_N = 2$; $I = 0.8$; $\delta = 0.5$. Вагові коефіцієнти: $w_F = 0.4, w_S = 0.3, w_N = 0.3$. Пороги: $F_{\min} = 0.7$; $NSL_{\min} = 0.9$.

Всі розрахунки для різних R наведено у таблиці 2:

Таблиця 2. – Розрахунки за різних вхідних R

R	FR	$NSLR$	BR	Допустимий
0.0	1.00	0.60	0.700	Ні ($NSLR < 0.9$)
0.2	0.80	≈ 1.01	≈ 0.719	Так (Максимум BR)
0.3	0.70	≈ 1.17	≈ 0.715	Так (FR на межі)

Згідно з моделлю та заданими параметрами, оптимальний рівень регулювання для досягнення балансу становить $R^* \approx 0.2$ (20% інтенсивності).

Висновки

Запропонована математична модель дозволяє кількісно прогнозувати зміни в показниках свободи слова, громадської безпеки та національної безпеки залежно від рівня регулювання R. Вона слугує інструментом для

аналізу та оптимізації правового регулювання, допомагаючи законодавцям визначити оптимальний рівень контролю для досягнення балансу між фундаментальними правами та безпекою.

1. Tkachenko, O., Ilyenko, A., Meleshko, Y., Ulichev, O., &Noga, H. (2025, June 20–22). Mathematical model of legalregulation of the spreadof information influencesin social networks. In *CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene&Conflict Management in Global Information Networks* (Kyiv, Ukraine). CEUR-WS. https://ceur-ws.org/Vol-4024/paper32.pdf.
2. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., &Смірнов, О. (2024). Правові засади поширення інформаційних впливів в соціальних мережах. *Кібербезпека: освіта, наука, техніка*, *2*(26), 170–188. https://doi.org/10.28925/2663-4023.2024.26.685.
3. Улічев, О. С. (2021). Модель і методи поширення інформаційних впливів у соціальних мережах в умовах інформаційного протиборства (Дисертація кандидата технічних наук, Національний авіаційний університет). Київ.
4. Dhar, J., Jain, A., &Gupta, V. K. (2016). A mathematical model of news propagation on onlinesocial networkand a control strategy forrumorspreading. *Social Network Analysis and Mining*, *6*(1), 57. https://doi.org/10.1007/s13278-016-0366-5.
5. Muhlmeyer, M., &Agarwal, S. (2021). Information spreadin a socialmediaage: Modelingandcontrol (1st ed.). CRC Press. https://doi.org/10.1201/9780429263842.
6. Наконечна, Ю. В. (2019). Математичні моделі динаміки поширення випадків приховування інформації в соціальних мережах. *The oretical and Applied Cybersecurity*, *1*(1), 41–47. https://doi.org/10.20535/tacs.2664-29132019.1.169082.

І.О. Сергієнко

АКТУАЛЬНІСТЬ ВПРОВАДЖЕННЯ ШІ В ОБЛАСТІ РОЗПІЗНАВАННЯ МОВНИХ ДІПФЕЙКІВ

Останнім часом стрімке зростання та удосконалення технік глибинного навчання породили нові випробовування у сфері безпеки, зокрема в маніпуляції цифровими медіа даними. З кожним роком стає все складніше відрізнити згенерований контент від оригінального, разом з тим зростає ризик у системах безпеки, що використовують ідентифікацію особи за обличчям, голосом та іншими біометричними характеристиками.

Стрімкий розвиток технік таких як Text-to-Speech (TTS) та Voice Conversion (VC) робить сферу розпізнавання діпфейків критичною для визначення оригінальності контенту [4]. В цьому досліджені розглядаються переваги та недоліки сучасних систем розпізнавання, ризики аудіо діпфейків.

Історичний контекст та вразливості. Перше змагання з виявлення підробки голосу було організоване ще в 2015 році та зосереджувалося на атаках TTS та VC [2]. Як результат було випущено набір даних підробного аудіо і запропоновано певний прийнятний рівень помилки EER (Equal Error Rate), який використовувався для розрахунку продуктивності методів виявлення [2]. Саме ж поняття діпфейк виникло на Reddit у 2017 році, коли користувач з таким самим іменем завантажив сфальсифіковане відео на веб-сайт, підмінивши обличчя актора [3].

Класифікація голосових діпфейків. Діпфейк — це тип контенту, створений у цифровому форматі, в якому оригінальні людські обличчя на фото, відео чи голоси у записах замінені на згенеровані комп'ютером [3]. Розпізнаваність є досить складною в глибинному навчанні через постійне вдосконалення генеративних моделей. Відтак, ознаки що вилучаються можуть суттєво вплинути на точність та потужність передбачення моделі.

Аудіо діпфейки класифікуються наступним чином:

• Атаки відповіді (Replay attacks). Бувають двох форм: виявлення далекого поля та виявлення копі-пасту. Такі атаки повністю розпізнаються глибинними згортковими мережами.

• Синтез мови (Speech Synthesis). Відтворює людську мову в цифровому форматі, зазвичай використовуючи комп'ютерне програмне або апаратне забезпечення. TTS є компонентом синтезу мови, що приймає написаний матеріал і генерує мовлення на основі тексту за попередньо визначеними лінгвістичними правилами.

• Перетворення голосу (Voice Conversion). Технологія зміни характеристик одного голосу для імітації іншого при збереженні лінгвістичного змісту.

Сучасний стан досліджень. Виявлення діпфейків, що базується лише на аудіо, менш досліджене порівняно з підходами по виявленню діпфейк

зображень та відео [3]. Більшість досліджень базується на одночасному аналізі аудіо та просторово-часової інформації, яка видобувається з відеоконтенту при навчанні моделей глибинного навчання [3].

Дослідники пропонують підходи, що базуються на множині алгоритмів машинного навчання для покращення точності класифікаційних моделей, використовуючи алгоритми Random Forest, Decision Tree та SVM. Модель SVM перевершує інші моделі машинного навчання на більшості піднаборів даних, за винятком набору даних for-original [3].

У проаналізованих дослідженнях можна виділити чотири сучасні глибинні моделі, які навчають задля вилучення ознак з мовних сигналів: X-vector, ECAPA-TDNN, ResNet-TDNN та WavLM [3, 4].

Поєднання залишкової мережі (ResNet) з нейронними мережами з часовою затримкою (TDNN) дає змогу ефективно вилучати ознаки з мовних сигналів [1]. Ця гібридна архітектура дозволяє моделі фіксувати як короткострокові, так і довгострокові часові залежності, критичні для створення дискримінативних вбудовувань мовців.

MLP з ResNet досягла найвищої точності (92,25%) та найкращого середнього балу F1 (92,24%) [1]. Логістична регресія з X-vector продемонструвала високу продуктивність з точністю 89,26% та збалансованими балами F1 для пародійних (89,06%) та справжніх (89,45%) класів [1]. Логістична регресія з ECAPA-TDNN показала точність 85,55% та середній бал F1 85,50% [1].

Автори дослідження [1] запропонували фреймворк для виявлення підробленої мови з використанням попередньо навченої моделі XLS-R. Замість точного налаштування всієї моделі, впроваджено авторами внутрішньоблокові адаптери (IBA) та міжблокові адаптери (CBA) для забезпечення адаптації до конкретних завдань.

Обмеження та виклики. Хоча рішення для виявлення пропонують певну стійкість до ефектів стиснення аудіо, їм бракує узагальнення для різних вихідних наборів даних. Це означає, що модель, навчена на одному датасеті, може погано працювати на іншому.

Моделі машинного навчання демонструють погані результати перевірки продуктивності та виявлення аудіо діпфейків без застосування покращених методів на основі ознак [3]. Для покращення результатів необхідні більш складні техніки вилучення ознак.

Підходи глибинного навчання, незважаючи на кращі результати, вимагають [3]:

значно більшого часу на навчання;

потужніших обчислювальних ресурсів;

великих обсягів якісних навчальних даних.

WavLM постійно показував низькі результати в усіх моделях без додаткового налаштування, що свідчить про більшу потребу моделей у адаптації до конкретних завдань виявлення діпфейків [1].

Перспективи розвитку. На основі аналізу найефективніших систем, виклад основних обмежень та дорожньої карти майбутнього ASVspoof виділяються наступні пріоритети [5]:

Покращення узагальнення моделей на різних датасетах;

Розробка більш ефективних методів вилучення ознак;

Створення легших архітектур для практичного застосування.

Перспективним є підхід на основі трансферного навчання для виявлення діпфейків, який дозволяє використовувати знання, отримані на одних завданнях, для вирішення інших подібних задач з меншими витратами ресурсів.

Необхідне розширення роботи з виявлення діпфейкового аудіо шляхом проведення детальних експериментів на різних наборах даних з використанням підходів на основі машинного та глибокого навчання, що дозволить створити більш універсальні та надійні системи виявлення.

Висновки. Отже, впровадження ШІ в області розпізнавання мовних діпфейків є критично важливим напрямком досліджень у сфері кібербезпеки. Сучасні підходи, що поєднують традиційне машинне навчання з глибинними нейронними мережами, демонструють непогані результати, досягаючи точності понад 92% на окремих завданнях.

Проте залишаються значні виклики, пов'язані з узагальненням моделей, обчислювальними вимогами та необхідністю постійного вдосконалення методів у відповідь на еволюцію генеративних технологій. Подальший розвиток цієї галузі вимагає інтеграції різних підходів до вилучення ознак, застосування інноваційних архітектур та створення більш репрезентативних датасетів для навчання та тестування систем виявлення діпфейків.

1. Alsalihi M. H., Sztahó D. Spoof speech classification using deep speaker embeddings and machine learning models. Array. 2025. Vol. 27. P. 100494. URL: https://doi.org/10.1016/j.array.2025.100494.
2. Deepfake audio detection with spectral features and ResNeXt-based architecture / G. Tahaoglu et al. Knowledge-Based systems. 2025. Vol. 323. P. 113726. URL: https://doi.org/10.1016/j.knosys.2025.113726.
3. Hamza A., Others. Deepfake audio detection via MFCC features using machine learning. IEEE access. 2022. Vol. 10. P. 134018–134028. URL: https://doi.org/10.1109/ACCESS.2022.3231480.
4. Liu R., Zhang J., Li H. Hierarchical multi-source cues fusion for mono-to-binaural based Audio Deepfake Detection. Information fusion. 2025. Vol. 120. P. 103097. URL: https://doi.org/10.1016/j.inffus.2025.103097.
5. Liu X., Others. ASVspoof 2021: towards spoofed and deepfake speech detection in the wild. IEEE/ACM transactions on audio, speech, and language processing. 2023. Vol. 31. P. 2507–2522. URL: https://doi.org/10.1109/TASLP.2023.3285283.

М.Л. Дранік, Д.В. Кулида

МЕТОДИ ІНТЕГРАЦІЇ ВІДНОВЛЮВАНИХ ДЖЕРЕЛ ЕНЕРГІЇ У СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО ТЕПЛОПОСТАЧАННЯ СОЦІАЛЬНОЇ ІНФРАСТРУКТУРИ

Вступ

Сучасна система централізованого теплопостачання України перебуває в критичному стані через значний знос обладнання та інфраструктури. Тепломережі в містах зношені на 70-80%, а втрати тепла сягають 20-30%. Централізоване теплопостачання охоплює 35-40% населення країни (за іншими оцінками — до 50%), а обсяг виробництва теплової енергії становить близько 6,2 млн т н.е.. Витрати закладів соціальної інфраструктури на опалення зростають щорічно: якщо у 2013 році на опалення однієї школи витрачали 570 тисяч грн, то у 2023 році ця цифра зросла до 1,8 млн грн. Житловий фонд та бюджетні установи України споживають приблизно 32% енергії країни, що вдвічі-втричі більше за споживання в провідних європейських країнах [1].

Відповідно до Енергетичної стратегії України на період до 2035 року, передбачено зростання частки відновлюваної енергетики до рівня не менше 25% від загального постачання первинної енергії. Згідно з Директивою ЄС 2012/27/EU про енергоефективність, ефективне централізоване теплопостачання має використовувати мінімум 50% відновлюваної енергії, 50% відпрацьованого тепла, 75% тепла від когенерації або 50% комбінації такої енергії та тепла [2,3].

У європейських країнах централізоване теплопостачання активно інтегрує відновлювані джерела енергії: частка ВДЕ у секторі ЦТ ЄС становить 23%, де біомаса забезпечує значну частку виробництва. В Україні біомаса вже замістила близько 5,2 млрд м³ природного газу у 2020 році, що становить приблизно 15% від загального довоєнного споживання. Потенціал заміщення газу у сфері централізованого теплопостачання сягає 3 млрд м³ на рік. Успішні приклади впровадження відновлюваних технологій демонструють міста Житомир, Жовква та Дубно, де частка теплопостачання з біомаси становить 40-70% [4].

Мета і завдання дослідження

1. Систематизація існуючих технологій інтеграції ВДЕ у системи централізованого теплопостачання.Важливим аспектом є визначення особливостей застосування кожної технології для об'єктів соціальної інфраструктури з урахуванням їх специфічних вимог до безперебійності та стабільності теплопостачання [5].

2. Формування системи критеріїв для оцінки ефективності різних схем інтеграції ВДЕ, включаючи енергетичну ефективність, економічну доцільність, екологічний ефект та технічну можливість реалізації [6].

Основні результати

Дослідження систематизувало чотири основні методи інтеграції ВДЕ у системи централізованого теплопостачання соціальної інфраструктури:

Біомаса як джерело тепла. Аналіз реалізованих проєктів показав, що використання біомаси (пелет, брикети) у котельнях централізованих мереж може заміщувати до 40–70% потреби в теплі, що продемонстровано в містах Житомир, Жовква та Дубно. Перевагами є наявність локальних ресурсів і низька вартість палива, серед обмежень — потреба в модернізації котелень і логістика постачання палива [7].

Сонячні теплові колектори та PVT-модулі. Реальні кейси впровадження гібридних СЕС із сонячними колекторами у школах і лікарнях свідчать про потенційне покриття до 20–30% річного попиту на гарячу воду. Рекомендовано інтегрувати колектори у буферні ємності тепломережі з використанням теплообмінників для оптимального розподілу тепла. [8]

Геотермальні джерела та теплові насоси. Використання низькопотенційного геотермального тепла через теплові насоси забезпечує стабільну температуру подачі тепла незалежно від погодних умов. У деяких комунах ЄС показано, що такі системи можуть заміщувати до 50% потреби в енергії централізованих мереж [9].

Комбіновані гібридні схеми. Найбільш ефективними визнано гібридні схеми, які поєднують декілька ВДЕ (біомаса + сонячні колектори або теплові насоси + сонячні колектори). Такі рішення забезпечують більш рівномірний розподіл навантаження та зменшують залежність від одного виду джерела [10].

Оцінка ефективності інтеграції за критеріями:

Енергетична ефективність: очікуване зниження витрат тепла на 15–40% залежно від схеми інтеграції.

Економічна доцільність: термін окупності комплектних рішень за даними міжнародних оглядів становить 5–8 років.

Екологічний ефект: зменшення викидів CO_2 до 35–60% порівняно з викопним паливом.

Оцінка ефективності інтеграції за критеріями базується на даних світових оглядів і пілотних проєктів:

Енергетична ефективність: пілотні впровадження низькотемпературних систем із інтеграцією теплових насосів та сонячних колекторів продемонстрували зниження теплового навантаження на мережу до 38% завдяки оптимізації робочих температур і відновлюваним джерелам енергії [11].

Економічна доцільність: аналіз термінів окупності комерційних теплових насосів у низькотемпературних системах вказує на середній період від 5 до 8 років залежно від типу установки (ґрунт/вода, повітря/вода) та фінансових умов проєкту [12].

Екологічний ефект: результати пілотного проєкту WEDISTRICT у Бухаресті свідчать про зменшення викидів CO_2 на 67% після переходу з

газових котлів на геотермальні теплові насоси у поєднанні з сонячними панелями [13].

Виявлено, що ключовими чинниками успішної інтеграції є доступність технічної інфраструктури, фінансова підтримка на державному та місцевому рівнях, а також наявність кваліфікованих фахівців для обслуговування гібридних систем [3].

Висновки та перспективи подальших досліджень

У результаті проведеного аналізу виявлено, що інтеграція відновлюваних джерел енергії (ВДЕ) у системи централізованого теплопостачання соціальної інфраструктури здатна суттєво підвищити енергоефективність мереж, зменшити витрати на тепло та скоротити викиди парникових газів. Класифікація технологій інтеграції (біомаса, сонячні колектори, геотермальні теплові насоси) дозволила виокремити їхні переваги й обмеження в умовах українських міст.

Оцінка ефективності показала потенційне зниження теплового навантаження мережі до 38% завдяки впровадженню низькотемпературних систем з тепловими насосами та сонячними колекторами, терміни окупності технологій становлять в середньому 5–8 років, а комбіновані гібридні схеми можуть забезпечити скорочення викидів CO_2 на понад 60%. Вітчизняні проєкти з використання біомаси в Житомирі, Жовкві та Дубно продемонстрували заміщення до 70% теплової енергії викопного палива.

Найважливішими факторами успішної імплементації ВДЕ є модернізація технічної інфраструктури, фінансова підтримка на державному й місцевому рівнях та наявність кваліфікованих фахівців для обслуговування гібридних систем.

1. Гуч-Денисенко В. «Де взяти кошти на термомодернізацію шкіл, садочків та лікарень: рішення для громад у 2024 році», 13 Лют 2024 https://rubryka.com/article/termomodernizatsiya-u-gromadah/.
2. Енергетична стратегія україни до 2035 року «безпека, енергоефективність, конкурентоспроможність», 20 сер 2021, Https://www.gpee.com.ua/news_item/732.
3. USAID. Нормативно-правова база для систем централізованого теплопостачання в Україні: Уроки ЄС та Великої Британії, https://internews.ua/storage/app/media/rang/Materials/2024/EUUKlessons.pdf.
4. Желєзна Т.А. «Досвід функціонування конкурентних ринків теплової енергії в країнах ЄС», https://uabio.org/wp-content/uploads/2016/01/zheliezna-competitive-heat-market.pdf.
5. USAID. Навчальний семінар «Розробка схем теплопостачання населених пунктів України», https://energysecurityua.org/wp-content/uploads/2021/02/dh-traning-feb-18-19-2021-ukr.pdf.
6. Клопов І.О. «Оцінка ефективності політики підтримки відновлювальних джерел енергії», Науковий вісник херсонського державного університету, випуск 22. Частина 2. 2017, с.60-62, http://www.ej.kherson.ua/journal/economic_22/2/14.pdf.
7. Гелетуха Г. «Не газом єдиним», 12 травня 2025р., https://epravda.com.ua/energetika/ne-gazom-yedinim-806497/.

8. Білозерова Л. «Гібридні СЕС для шкіл та лікарень: як потрапити у проєкт», 24 травня 2023, https://ua-energy.org/uk/posts/avtonomni-ses-dlia-shkil-ta-likaren-iak-potrapyty-u-proiekt%2011.
9. Павленко О. «Геотермальні рішення та теплові насоси дозволять забезпечити україну теплом на 50 років та знизити його вартість для населення», https://dixigroup.org/21960-2/.
10. Волошин В. Від пари до штучного інтелекту: еволюція централізованого опалення», 05.05.2025, https://city-institute.org/blog/vid-pari-do-shtuchnogo-intelektu-evolyucziya-czentralizovanogo-opalennya-na-shlyahu-do-stalogo-majbutnogo-mist.
11. Sarbu, I.; Mirza, M.; Muntean, D. Integration of Renewable Energy Sources into Low-Temperature District Heating Systems: A Review. *Energies* 2022, *15*, 6523. https://doi.org/10.3390/en15186523.
12. What are the pay back periods for commercial heat pumps?, https://mirkinstallatie.nl/en/smart-cooling-heat-pumps/What-are-the-payback-periods-for-commercial-heat-pumps/.
13. Renewable-powered district heating systems undergo testing in Europe, 02.10.2025, https://globalenergyprize.org/en/2025/10/02/renewable-powered-district-heating-systems-undergo-testing-in-europe/.

С.В. Матвєєв, І.В. Івченко

СУЧАСНИЙ СТАН ЕНЕРГОСПОЖИВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація Швидке масштабування систем штучного інтелекту (ШІ), зокрема великих мовних моделей (LLM), трансформує попит на обчислювальні ресурси й ставить на порядок денний питання енергоспоживання дата-центрів, вуглецевого сліду й стійкості енергосистем. У доповіді узагальнено сучасні оцінки енергоспоживання навчання й інференції, роль апаратних архітектур і показників інфраструктури, а також ключові напрями оптимізації. На основі останніх джерел зроблено висновки щодо ризиків масштабування та практичних кроків для зниження енергетичних та екологічних витрат [1].

Індивідуальне зростання потужності моделей штучного інтелекту у поєднанні з їх масовим використанням призводить до подвійного навантаження на енергосистеми: по-перше, великі одномоментні витрати під час тренування (training), по-друге, постійні витрати під час інтенсивної інференції (serving). Міжнародне енергетичне агентство (IEA) вказує, що попит енергії від дата-центрів, орієнтованих на ШІ, зростає швидше за загальне споживання електроенергії й у базовому сценарії може суттєво збільшити частку сектору в глобальному балансі до кінця десятиліття. Це створює виклики для планування інфраструктури та досягнення кліматичних цілей [1].

Класичні дослідження вказують, що тренування великих нейронних мереж споживає сотні мегават-годин і породжує суттєві викиди CO_2, якщо використовувати енергію з вуглецевими джерелами. Дослідники підкреслюють, що вибір архітектури, дата-центру та процесора може змінювати вуглецевий слід у десятки або сотні разів (Patterson et al., 2021). Тренування великої LLM (порядку сотень мільярдів параметрів) - разова, але дуже енергомістка операція; інференція - множинні, але відносно менш затратні одиничні операції, які в сумі можуть домінувати у річному енергобалансі системи за інтенсивного використання (наприклад, комерційні чат-боти з сотнями мільйонів запитів щомісяця). Це означає: оптимізація має йти по двох напрямах - зменшення витрат навчання (через ефективні алгоритми і розумний вибір ресурсів) та масштабна оптимізація інференції (алгоритмічна і апаратна).

Апаратні прискорювачі (GPU, TPU, нові чипи AMD) і конфігурація дата-центрів визначають базову енергоефективність. Виробничі гіганти повідомляють про значні поліпшення: наприклад, архітектури нового покоління (GPU H100 / очікувані Blackwell, Google Trillium TPU) підвищують продуктивність на ват у кілька разів у порівнянні з попередниками, що безпосередньо знижує енерговитрати на одиницю

корисної роботи (NVIDIA, DGX H100 design guide; Google, Trillium release) [2].

Інфраструктурний показник PUE (Power Usage Effectiveness) відображає, скільки енергії витрачається на інфраструктуру (охолодження, UPS, освітлення) відносно енергії, спожитої IT-обладнанням. Сучасні гіпермасштабні оператори досягають PUE близько 1.10–1.20 у найефективніших локаціях; середні значення по галузі вищі. Зниження PUE навіть на декілька десятих дає суттєву економію загальних витрат і викидів (приблизно пропорційну частці інфраструктури).

Google оголосив, що шосте покоління їхніх TPU (Trillium) дає значний приріст енергоефективності — заявлено +67% порівняно з TPU v5e, що означає значне зменшення витрат під час тренування та інференції при однакових робочих навантаженнях. Це приклад, коли інвестиції у нові архітектури прямо знижують енергетичну інтенситетність задач [3].

Технічні гіди DGX SuperPOD показують, що щільні конфігурації H100 вимагають продуманих рішень живлення й охолодження (приклад: 10.2 кВт на систему в типових конфігураціях), що підкреслює важливість сумісної інфраструктури для досягнення заявленої енергоефективності [2].

Ці факти вказують: безпосередній ефект від сучасних прискорювачів реалізується лише за умови відповідної інфраструктури (правильна подача потужності, охолодження, мережеві з'єднання).

IEA і регіональні новинні розслідування показують, що скупчення дата-центрів у деяких країнах (приклад — Ірландія) може призвести до локальних енергетичних напружень і конфліктів із національною енергетичною політикою. IEA прогнозує значне збільшення споживання дата-центрів до 2030 року у базовому сценарії, що підсилює необхідність інтеграції відновлюваних джерел та планування розміщення центрів з урахуванням енергетичного міксу.

Географічне планування має значення також з точки зору вуглецевого відбитку: суттєво менше CO_2e виникає при розгортанні інтенсивних робочих навантажень у регіонах з високою часткою ВДЕ або в періоди надлишку «зеленої» генерації.

Для забезпечення зниження енергоспоживання використовують такі алгоритмічні оптимізації: квантизація (Quantization) - зниження розрядності обчислень; Pruning (відсікання) — видалення нерелевантних ваг/нейронів, що зменшує FLOP і пам'ять; Knowledge distillation — створення компактних «студентських» моделей, що зберігають якості «вчителя», але потребують значно менше ресурсів на інференцію. Окремі дослідження та практичні кейси показують, що комбінація квантизації і pruning може знизити витрати на інференцію на 30–60% без суттєвого погіршення результатів.

Перехід на більш енергоефективні чипи (TPU Trillium, нові GPU серій H100/Blackwell, AMD MI300X) здатен знизити споживання енергії на операцію [3].

Переходи до рідинного або занурювального охолодження, використання free-cooling (охолодження зовнішнім середовищем), підвищення температури холодних коридорів - все це знижує частку енергії, що витрачається на інфраструктуру, і, відповідно, загальний PUE.

Сучасний стан енергоспоживання систем штучного інтелекту відображає баланс між швидким технологічним прогресом (який підвищує продуктивність на ват) та стрімким масштабуванням застосувань (яке підвищує загальний попит на енергію). У найближче десятиліття результат залежатиме від того, наскільки швидко індустрія зможе втілити апаратні інновації, алгоритмічні оптимізації та інфраструктурні покращення у поєднанні з переходом на відновлювані джерела енергії. Регулювання, прозорість та системне планування розміщення дата-центрів - критично необхідні для забезпечення енергетичної та кліматичної стійкості [1].

1. International Energy Agency. (2024). *Energy demand from AI (Energy and AI report). IEA.* https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai.
2. NVIDIA. (2023). *NVIDIA DGX SuperPOD data center design (DGX H100 guide)*. NVIDIA. https://docs.nvidia.com/nvidia-dgx-superpod/design-guides/dgx-superpod-data-center-design-dgx-h100.pdf.
3. Google Cloud. (2024). *Introducing Trillium — sixth-generation TPUs* (blog). Google Cloud. https://cloud.google.com/blog/products/compute/introducing-trillium-6th-gen-tpus. Google Cloud.

О.С. Кобус, С.Ю. Бондаренко

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙНУ ДЛЯ ПІДВИЩЕННЯ ІНСТИТУЦІЙНОЇ РЕЗИЛЬЄНТНОСТІ ПРАВООХОРОННИХ СТРУКТУР

Використання технологій блокчейну для підвищення інституційної резильєнтності правоохоронних структур сьогодні стає одним із найперспективніших напрямів цифрової трансформації безпекового сектору. У сучасних умовах зростаючої кіберзагрози, гібридних інформаційних атак, корупційних ризиків і падіння рівня суспільної довіри до державних інституцій правоохоронні органи стикаються з потребою забезпечення прозорості, незмінності та відтворюваності даних у процесах своєї діяльності. Блокчейн, як розподілений реєстр, що базується на принципі децентралізованого зберігання інформації, здатен забезпечити фундаментально нову архітектуру безпеки та довіри між суб'єктами кримінального правосуддя, а також сприяти формуванню стійкості (резильєнтності) інституцій до внутрішніх і зовнішніх дестабілізуючих факторів.

Технологія блокчейну передбачає створення ланцюга блоків, у якому кожен блок містить інформацію, зашифровану криптографічними методами, і є незмінним після верифікації в мережі. Для правоохоронних органів це означає можливість зберігати докази, службові документи, відеозаписи з бодікамер, протоколи обшуків, логи службових дій чи внутрішніх перевірок у такий спосіб, щоб жоден суб'єкт не міг їх підробити або знищити без залишення цифрового сліду. Це радикально підвищує інституційну резильєнтність, адже довіра до системи стає не продуктом людського фактору, а технологічно гарантованою властивістю.

Наприклад, блокчейн можна застосувати у створенні «ланцюга доказів» (chain of custody) – системи простежуваності матеріальних і цифрових доказів від моменту їх отримання до передачі до суду. Кожна дія з доказом (огляд, пакування, транспортування, експертиза) фіксується у блокчейні як окремий запис із часовою міткою. Це виключає можливість маніпуляцій із доказами, підробки підписів чи втрати даних. У такій системі навіть спроба несанкціонованої зміни залишає криптографічний слід, що автоматично підвищує рівень процесуальної справедливості й зміцнює довіру суспільства до органів правопорядку.

Водночас блокчейн може бути використаний для оптимізації внутрішніх адміністративних процесів; наприклад, для забезпечення прозорості закупівель, контролю за службовими перевірками чи обліку використання ресурсів. Розподілений характер бази даних унеможливлює централізоване маніпулювання записами, що робить систему більш стійкою до корупційних впливів і адміністративного зловживання. Інституційна резильєнтність у цьому контексті полягає у здатності системи самостійно

відновлювати баланс між контролем і довірою, реагувати на внутрішні відхилення, зберігаючи при цьому прозорість та підзвітність.

Інший аспект полягає у використанні смарт-контрактів, таких собі алгоритмічних угод, що автоматично виконують визначені умови. Для правоохоронних структур це може означати створення автоматизованих процедур реагування на певні події, наприклад, активацію розслідування після фіксації певного інциденту в інформаційній системі чи контроль за дотриманням термінів службових перевірок. Таким чином зменшується вплив людського фактору, прискорюється обіг інформації та забезпечується адаптивність організаційної структури до нових викликів.

У міжнародній практиці вже з'являються приклади використання блокчейну у сфері безпеки. Наприклад, Департамент поліції Дубая впровадив блокчейн-платформу для фіксації доказів і управління запитами громадян, що дозволило скоротити час на обробку справ і знизити рівень бюрократичних зловживань [5]. Аналогічно, у США розглядаються пілотні проєкти з використання блокчейну для зберігання відео з бодікамер, щоб гарантувати неможливість їх редагування або видалення [2]. Такі приклади демонструють, що технологія не лише підвищує ефективність управління, але й формує новий тип довіри між поліцією, судом і суспільством, тобто довіру, засновану на алгоритмічній прозорості.

Інституційна резильєнтність правоохоронних структур у контексті блокчейн-технологій полягає не лише у технічній стабільності системи, а й у формуванні нової організаційної культури – культури децентралізації, підзвітності й відповідального використання даних. Це створює передумови для зменшення ризиків корупції, посилення правових гарантій громадян і формування адаптивної цифрової екосистеми, здатної витримувати кризи. У підсумку блокчейн стає не просто інструментом збереження даних, а концептуально новою парадигмою управління довірою, яка формує стійкість інституцій на технологічному, правовому та соціальному рівнях.

З технічного погляду, використання технології блокчейну для підвищення інституційної резильєнтності правоохоронних структур базується на принципах розподіленого зберігання, криптографічного захисту, консенсусу та незмінності записів. Це не просто база даних, а самоверифікуюча екосистема, у якій кожен учасник є одночасно і користувачем, і контролером цілісності даних. Основна ідея полягає в тому, що інформація не зберігається в одному центральному сервері, а дублюється на безлічі вузлів (комп'ютерів або серверів), об'єднаних у спільну мережу. Це робить систему надзвичайно стійкою до збоїв, атак або спроб маніпуляції з боку окремих осіб чи груп.

Технічна архітектура блокчейну складається з ланцюга блоків, кожен з яких містить набір транзакцій або записів. Кожен блок має хеш, тобто криптографічний відбиток даних у ньому, який залежить від вмісту попереднього блоку. Завдяки цьому створюється ланцюг, у якому будь-яка спроба змінити дані в одному блоці автоматично змінює всі наступні хеші,

що миттєво виявляється мережею. У системах правоохоронного моніторингу це гарантує незмінність доказової бази, тобто якщо, наприклад, службове відео або протокол обшуку було записано в блокчейн, жоден користувач не зможе його видалити або змінити без цифрового сліду.

Кожен запис у блокчейні проходить процедуру верифікації: перевірку достовірності та законності додавання нового блоку. Цей процес забезпечується механізмом консенсусу, який визначає, як мережа узгоджує, які дані є істинними. У контексті правоохоронної діяльності можуть застосовуватися безенергетичні алгоритми типу Proof of Authority (скор. PoA) або Practical Byzantine Fault Tolerance (скор. PBFT), які не потребують великих обчислювальних потужностей, але гарантують швидкість і достовірність підтверджень [3]. Наприклад, лише авторизовані вузли (представники суду, прокуратури, поліції та експертних підрозділів) мають право верифікувати блоки. Це дозволяє зберегти контрольований, але прозорий характер системи.

З точки зору безпеки, блокчейн забезпечує криптографічну автентифікацію кожного користувача. Кожен працівник правоохоронного органу має унікальний криптографічний ключ: приватний (для підпису) і публічний (для перевірки підпису). Будь-яка дія, виконана користувачем, фіксується з цифровим підписом, який не може бути підроблений без знання приватного ключа. Наприклад, коли слідчий завантажує файл із доказом, система створює унікальний підпис транзакції, що підтверджує його авторство й час дії. Це забезпечує юридичну доказовість цифрових даних і формує довіру до системи навіть у судовому процесі.

Для зберігання великих обсягів інформації, таких як відео чи аудіо, блокчейн зазвичай поєднується з технологією Off-chain Storage, тобто самі файли зберігаються у хмарних або локальних зашифрованих сховищах, а у блокчейні фіксується лише їх хеш. Такий підхід забезпечує масштабованість системи й ефективне використання ресурсів, водночас зберігаючи принцип незмінності даних.

Технічна резильєнтність системи полягає також у розподіленій архітектурі, навіть якщо один вузол (наприклад, сервер поліції) буде знищено або зламано, повна копія реєстру зберігатиметься на інших вузлах (наприклад, у серверів судів або прокуратури). Це унеможливлює знищення доказів чи протоколів навіть у випадку масштабних кіберінцидентів або фізичного знищення дата-центрів. Таким чином, система набуває властивостей самовідновлення, що є ключовим чинником інституційної резильєнтності.

Важливою технічною складовою є механізми шифрування даних. У блокчейні використовуються алгоритми симетричного та асиметричного шифрування (наприклад, AES та RSA), які гарантують, що дані можуть бути прочитані лише уповноваженими користувачами [4]. Додатково можуть застосовуватись Zero-Knowledge Proofs (криптографічні протоколи, які дозволяють підтвердити істинність інформації без її розкриття). Це критично

важливо для роботи з конфіденційними або оперативними даними, коли необхідно перевірити факт дії без розкриття деталей.

Інтеграція блокчейну у правоохоронні системи також передбачає API-рівень взаємодії з іншими базами даних, наприклад, реєстрами судових рішень, кримінальними базами чи системами моніторингу. Це створює єдиний цифровий ланцюг, де дані синхронізуються автоматично, без дублювання і ручного введення. Результатом стає цифрова екосистема довіри, у якій усі транзакції між підрозділами, громадянами та іншими органами влади є прозорими, відтворюваними і технічно захищеними.

Отже, з технічного боку блокчейн у правоохоронній діяльності функціонує як криптографічно захищена, розподілена система управління інформацією, що забезпечує незмінність даних, верифікацію учасників, автоматизацію процесів і стійкість до зовнішніх впливів. Саме ці властивості роблять його інструментом технологічної та організаційної резильєнтності, що дозволяє правоохоронним структурам не лише ефективно реагувати на кризи, а й запобігати їм шляхом побудови безпечної, прозорої та саморегульованої цифрової інфраструктури.

Зрештою, головна цінність блокчейну у правоохоронній діяльності полягає у створенні умов, за яких будь-яка інформаційна взаємодія (від внутрішньої документації до публічного звіту) набуває властивості довготривалої достовірності. Це означає, що правоохоронні органи можуть діяти у середовищі, де ризики спотворення, витоку чи втрати інформації мінімізовані, а сама система здатна самостійно підтримувати баланс між безпекою, ефективністю та довірою. Таким чином, інтеграція блокчейну у діяльність правоохоронних структур не є лише технічним нововведенням, а стає стратегічним кроком до формування нової моделі інституційної резильєнтності у цифрову епоху.

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. 9 p. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 16.10.2025).
2. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. Blockchain Technology: Beyond Bitcoin // Applied Innovation Review. 2016. № 2. P. 6–10.
3. Underwood S. Blockchain Beyond Bitcoin // Communications of the ACM. 2016. Vol. 59, № 11. P. 15–17.
4. Zyskind G., Nathan O., Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data // Proceedings of the IEEE Security and Privacy Workshops. 2015. P. 180–184.

В.В. Микитенко

КОГНІТИВНО-АДАПТИВНА РЕЗИСТЕНТНІСТЬ СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМ: СТРАТЕГІЧНІ ОРІЄНТИРИ РОЗВИТКУ У ДОБУ ПОЛІКРИЗИ

Найбільш актуальним напрямом забезпечення резильєнтності динамічних систем є реалізація домінант концепції їх когнітивно-адаптивної резистентності [1] як нової форми синергетичної стійкості в умовах полікризи. Резистентність у дослідженні трактується як інтегрована властивість, що поєднує когнітивні, управлінські, соціальні, економічні та інституційні механізми адаптації систем до багатовимірних загроз і ризиків різної природи. Тому, доцільним є обґрунтування методологічних підходів до ідентифікації когнітивно-адаптивних резервів системи, здатних забезпечити не лише відновлення, а й розвиток через внутрішню мобілізацію ресурсів, самонавчання та стратегічне прогнозування. З огляду на це, маємо визначити структурні параметри нового формату управління («Resilience+ Governance» [2]), орієнтованого на інтеграцію галузевих стратегій у єдину модель соціо-еколого-економічної безпеки і сталого господарювання. Практична значущість дослідження полягає у формуванні підґрунтя для створення національної системи управління резистентністю, здатної підтримувати сталий розвиток, соціальну згуртованість і відновлення когнітивного потенціалу суспільства в умовах тривалої невизначеності.

Визнаємо, що в умовах полікризи, коли *соціально-економічні системи* (СЕС) стикаються із низкою взаємопов'язаних викликів (воєнних, енергетичних, екологічних, демографічних і когнітивних) зростає значення пошуку внутрішніх джерел відновлення і саморегуляції, які формують когнітивно-адаптивні резерви СЕС. Ідентифікація таких резервів спирається на інтеграцію системного, когнітивного, синергетичного та інституційного підходів, які дозволяють поєднати кількісне вимірювання стійкості з якісним аналізом здатності СЕС до навчання, передбачення і самозміни. Тож, першим методологічним орієнтиром – є когнітивний підхід, який розглядає СЕС як суб'єкт, здатний до самопізнання та рефлексивного управління власними станами. У цьому контексті – ключовим є аналіз когнітивних структур (моделей сприйняття ризиків, довіри до інституцій, соціальної пам'яті та навичок колективного навчання). При цьому, оцінка когнітивно-адаптивних резервів передбачає застосування інструментів когнітивного картування, індексного аналізу рівня когнітивної мобілізації населення та моніторингу соціальних наративів як маркерів колективної здатності до відновлення.

Другим методологічним виміром – є синергетичний підхід, що акцентує на нелінійній природі СЕС. З позицій синергетики, розвиток можливий лише у станах динамічної нерівноваги, коли система переходить через точки біфуркації та генерує нові структури. Відповідно, когнітивно-адаптивні резерви – ідентифікуються через виявлення зон самоорганізації (соціальних, територіальних або інституційних кластерів), здатних продукувати

інноваційні управлінські рішення навіть у кризових умовах (що потребує застосування кластерного аналізу, просторового моделювання стійкості, аналізу соціальних мереж для виявлення точок інституційної синергії).

Третій напрям – це системно-інституційний підхід, який дозволяє визначити ступінь інтеграції когнітивних і організаційних елементів у процес прийняття рішень. У цьому контексті ідентифікація резервів полягає у вимірюванні ефективності управлінських контурів зворотного зв'язку, здатних коригувати поведінку системи відповідно до зовнішніх змін. Використовуються методи функціонального моделювання управління (так називані DFD-моделі), індексації адаптивності управлінських структур, а також аналіз ступеня когнітивної взаємодії між суб'єктами прийняття рішень.

І, нарешті, четвертий методологічний орієнтир – це прогностично-аналітичний підхід, що фокусується на поєднанні стратегічного передбачення («foresight») з когнітивною аналітикою. Ідентифікація когнітивно-адаптивних резервів у цій площині здійснюється через формування сценарних моделей майбутнього розвитку СЕС та оцінку готовності суб'єктів управління до прогнозно-орієнтованих дій. За цим аспектом рекомендовано використовувати методи експертного оцінювання, динамічного сценарного аналізу, а також моделювання за принципами прийняття рішень в умовах глибокої невизначеності. Таким чином, когнітивно-адаптивні резерви постають не лише як ресурс стабілізації, а й в якості інтелектуального потенціалу розвитку, який забезпечує еволюцію СЕС шляхом самонавчання, інституційної рефлексії та про-активного управління. Їх виявлення дозволяє перейти від стратегії пасивного реагування до випереджальної стійкості (так називаної «*Strategies anticipatory resilience+*»), у якій резистентність перетворюється на основу довгострокової соціально-економічної безпеки.

З огляду на вказане, структурні параметри формату «Resilience+ Governance» матимуть наступний структурно-функціональний склад:

1) інтегративність стратегічного бачення. *«Resilience+ Governance»* («R+G») ґрунтується на інтеграції галузевих, територіальних і секторальних стратегій у єдину рамку соціо-еколого-економічної безпеки. Цей параметр передбачає: узгодження цілей сталого розвитку, безпеки, енергетики, транспорту, екології, цифровізації; розроблення мета-стратегії розвитку, у якій кожен сектор виконує функцію системного елемента єдиної резильєнтної еко-сфери; встановлення когнітивно-аналітичних зв'язків між стратегічними документами (від громади – до макрорівня держави). «Інтегративність» - стає рамковою функцією «R+G», перетворюючи множинність політик на єдину логіку соціально-економічного відновлення;

2) когнітивно-аналітична координація. У центрі нового управлінського формату – лежить когнітивна аналітика, що забезпечує зворотний зв'язок між даними, знаннями та рішеннями. Її параметри включають: а) створення національних і регіональних когнітивних хабів – для моніторингу ризиків, загроз і вразливостей; б) застосування систем штучного інтелекту (ШІ),

великих даних, сценарного моделювання – для передбачення соціо-економічних кризових реакцій; в) формування культури аналітичного мислення в управлінні – тобто, від реактивного реагування до про-активного прогнозування. А, когнітивна координація стає «нервовою системою» R+G»;
3) адаптивність управлінських контурів. Формат «R+G» працює як динамічна, а не статична модель. Ключовим у цій площині є принцип гнучкого реагування на зміну контекстів: перехід від лінійного планування до адаптивного стратегування; децентралізація управління з розширенням автономії регіонально-місцевих структур; введення механізмів експериментального управління (лабораторії, пілотні проєкти з низьким ризиком зворотного ефекту). А, адаптивність є управлінською здатністю не лише змінювати цілі, а й переосмислювати інструменти їх досягнення;
4) соціально-комунікативна інклюзивність. Управління за принципами «R+G» передбачає залучення суспільства як співтворця управлінських рішень. Його параметр включає: а) розвиток платформ громадського діалогу, соціального консенсусу і довіри; б) формування системи когнітивної взаємодії між державою, бізнесом, громадами і наукою; в) підтримку мережевої співпраці як базового інструменту підвищення соціального капіталу. З цього, «інклюзивність» переформовується у соціальну «енергетику» резистентності, що живить виміри адаптивності СЕС;
5) еколого-інноваційна спрямованість. Формат «R+G» органічно поєднує екологічну безпеку та технологічну модернізацію. Параметр охоплює: а) використання принципів циркулярної економіки, «зелених» фінансів та еко-системного управління; б) впровадження енергоефективних технологій, смарт-рішень, автоматизованого моніторингу екологічних ризиків; в) оцінку рівня сталості інфраструктурних рішень за критерієм «еколого-технологічна резистентність». А, «інноваційність» репрезентує не лише технологію, а нову філософію розвитку, засновану на поєднанні екологічної відповідальності та управлінської передбачуваності;
6) когнітивно-прогностичний зворотний зв'язок. Завершальним параметром – є побудова циклу когнітивного зворотного зв'язку (системи, у де кожне управлінське рішення породжує дані для навчання СЕС), шо передбачає: створення єдиної бази знань з оцінювання резистентності секторів і територій; аналітичне моделювання ефектів рішень за новим форматом «*ex ante – in process – ex post*»; використання управлінських моделей, які й передбачають майбутнє. Тож, «когнітивно-прогностичний контур» - стає інтелектуальним ядром «Resilience+ Governance».

Таким чином, формат «R+G» є не лише моделлю управління, а архітектурою соціально-економічного мислення, де знання, гнучкість, екологічна відповідальність і когнітивна мобілізація формують основу державної та регіональної безпеки. Відтак, дослідження засвідчує: в умовах полікризи категорія когнітивно-адаптивної резистентності є центральним концептом сучасної парадигми управління СЕС. Її сутність полягає у здатності СЕС не лише витримувати зовнішні деструктивні впливи, а й трансформувати кризові виклики у можливості для розвитку, забезпечуючи еволюційний перехід від реактивної до проактивної моделі державного,

інституційного та суспільного управління. Пропонований концепт «R+G» формує методологічне підґрунтя для інтеграції соціо-еколого-економічних і когнітивно-комунікаційних стратегій у єдиний простір соціо-еколого-економічної безпеки, що переорієнтовує управлінську систему від секторного адміністрування до системної взаємодії, у якій ключову роль відіграють знання, аналітика, адаптивність і соціальна участь. У межах цієї архітектури інтегративність, когнітивна координація, адаптивність, соціально-комунікативна інклюзивність, еколого-інноваційна спрямованість та когнітивно-прогностичний зворотний зв'язок – є базовими структурними параметрами стійкого управління. А, розроблена методологія ідентифікації когнітивно-адаптивних резервів доводить: основою резистентності є внутрішні джерела саморегуляції (когнітивний потенціал, інституційна пам'ять, соціальний капітал і здатність системи до навчання). Використання інструментів когнітивного картування, сценарного моделювання, системно-інституційного аналізу й аналітики невизначеності дозволяє формувати динамічну картину ризиків і можливостей розвитку у часовій перспективі.

Особливістю нового управлінського формату є його самонавчальний і прогностичний характер: система «R+G» сприймає кожну кризу як інформаційний імпульс для корекції управлінських стратегій, забезпечуючи оновлення управлінського знання й підвищення когнітивної спроможності суспільства. Це сприяє переходу від політики стабільності до парадигми випереджальної стійкості, у якій СЕС не просто виживають, а зростають, розвиваючи здатність до само-підтримуваної еволюції. У практичному вимірі – результати розробки є основою для: формування національної системи управління резистентністю, здатної узгоджувати дії держави, бізнесу, громад і науки; створення інтелектуальних платформ моніторингу стійкості, що поєднують когнітивну аналітику і ШІ; розроблення індикативних моделей прогнозування соціо-еколого-економічної безпеки територій і секторів. Загалом, «R+G» постає не лише як модель управління, а як новий формат соціального мислення, де знання, гнучкість, екологічна відповідальність і когнітивна мобілізація формують основу соціальної безпеки, державотворчої стійкості та стратегічного розвитку України в епоху невизначеності.

1. Mykytenko, V.V. The concept of resistance in ensuring adaptability and stability of spatial systems in conditions of polycrisis. Collection of Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Global Trends in Science: Research, Innovation and Development» (September 29 – October 1, 2025, Varna, Bulgaria). European Open Science Space, 2025. pp. 39-44. ISBN 979-8-89704-966-0 (series) DOI 10.70286/EOSS-29.09.2025.
2. Mykytenko, V.V. Resilience+ for Ukraine: socio-economic resilience and multifunctional development. Collection of Scientific Papers with the Proceedings of the 3rd International Scientific and Practical Conference «Modern Problems of Science and Technology» (September 22-24, 2025, Tallinn, Estonia). European Open Science Space, 2025. pp. 23-28. ISBN 979-8-89704-951-6 (series). DOI 10.70286/EOSS-22.09.2025.

Є.В. Котух

QUANTUM-RESISTANT CRYPTOGRAPHY FOR PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER THREATS

Critical infrastructure (CI) which is power, water, transportation, telecom, healthcare, and financial systems relies on public-key cryptography that will be broken by sufficiently capable quantum computers. Even before that point, "harvest-now, decrypt-later" (HNDL) adversaries can capture encrypted traffic today and decrypt it in the future. In 2024, the U.S. National Institute of Standards and Technology (NIST) finalized the first post-quantum cryptography (PQC) standards—ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205)—and in March 2025 selected HQC as an additional KEM to diversify assumptions. Adoption in Internet protocols has begun (e.g., TLS 1.3 hybrid X25519MLKEM768, OpenSSH hybrid KEX, DNSSEC algorithm modernizations and SMTP DANE deployments), but deployment in CI remains nascent and faces performance, interoperability, and lifecycle challenges.

Public-key cryptosystems used across CI (RSA, ECC, Diffie–Hellman) are vulnerable to quantum attacks such as Shor's algorithm. While timelines for "cryptographically relevant" quantum computers remain uncertain, multiple national security communities advise planning complete migrations by the early-to-mid-2030s. Meanwhile, HNDL adversaries can capture sensitive telemetry, command traffic, and archived backups now for later decryption, raising urgent confidentiality risks for long-lived CI data. Agencies have issued migration roadmaps (e.g., NSA CNSA 2.0), and NIST has published transition guidance to coordinate public and private stakeholders.

In August 2024, NIST published FIPS 203 (ML-KEM) with three parameter sets ML-KEM-512/768/1024—intended primarily for key establishment; FIPS 204 (ML-DSA, based on Dilithium) as a general-purpose signature; and FIPS 205 (SLH-DSA, based on SPHINCS+) as a conservative, stateless hash-based backup. A draft FIPS 206 (FN-DSA, based on Falcon) is advancing to finalize a compact lattice signature option. On March 11, 2025, NIST selected HQC (code-based) for standardization as a secondary KEM to diversify cryptographic assumptions alongside ML-KEM. NIST and partners continue to release implementation notes (e.g., ML-DSA FAQs), while U.S. federal guidance (CNSA 2.0) sets timelines for National Security Systems and influences broader CI suppliers. Procurement and deployment advice is also emerging.

Protocol Readiness and Internet-Scale Indicators

TLS/HTTPS and QUIC. Browser and library support for hybrid TLS 1.3 has moved from X25519Kyber768Draft00 to the standardized X25519MLKEM768 nomenclature following the ML-KEM FIPS publication and IETF draft updates. As of mid-/late-2025, Chrome and Firefox offer X25519MLKEM768 by default, while broader ecosystem work continues (Go 1.24 enabled support; Safari lagging

as of August 2025). Cloudflare and others report measurable PQ-hybrid traffic share growth since early 2024. For CI web portals, APIs, and control-plane services, this enables low-risk pilots using hybrid KEMs while maintaining backward compatibility.

SSH. OpenSSH pioneered PQ-hybrid KEX and later introduced ML-KEM-based options. However, observed adoption is still extremely low. A 2024 University of Illinois/NCSA measurement found only 0.029% of ~20.6 M observed SSH connections used PQC-hybrid KEX, underscoring the deployment gap in server and client fleets common in CI operations.

DNSSEC and DANE/SMTP. DNSSEC has progressed toward smaller and more performant ECDSA (Algorithm 13) signatures in major TLDs; Verisign completed .com/.net/.edu migrations in 2023, which reduces amplification and improves resilience—important for CI zones. Microsoft Exchange Online made inbound SMTP DANE with DNSSEC generally available in Oct 2024 and moved to mandate outbound DANE in 2025, indicating maturing support for authenticated, downgrade-resistant MTA-to-MTA TLS that CI organizations can adopt.

Baseline HTTPS Security Posture. HTTPS deployment is now ubiquitous: W3Techs reports ~88–89% of websites default to HTTPS, and Google's Transparency Report shows the majority of Chrome browsing time on HTTPS. While not PQ-specific, this penetration facilitates a broad TLS 1.3 hybrid upgrade path for CI web-facing services.

Protocol caveats. Early PQ integrations increase handshake sizes (particularly with PQ signatures), can stress middleboxes, and may expose implementation side-channels. Hybrid designs mitigate downgrade risks and offer continuity during migration, but they require thorough performance and compatibility testing in CI networks. (For example, IETF's TLS hybrid design notes duplication pitfalls and key-share considerations.)

Telecom (5G/6G) and CI Interdependencies

Key requirements in telecom—low latency, high session churn, multi-vendor interoperability, and exposure to ossified middleboxes—mirror challenges across CI control-planes. Hybrid KEMs in TLS/QUIC, careful certificate profile updates, and hardware offload planning (future PQ accelerators) are central to keeping 5G/6G control interfaces, MEC/edge workloads, and inter-operator links resilient during transition. 5G/6G networks are both CI and critical dependencies for other CI sectors. Standards bodies have begun PQC transition studies: 3GPP SA3 maintains TR 33.703 "Study on transitioning to PQC" and related security study items; GSMA has issued migration and use-case guidance for telecom operators (PQC in IoT, roaming, and core interfaces). Industry groups (ATIS, ETSI) and national programs have surveyed architectural impacts and transition pathways, while government-led technical reports outline PQC hardening of 5G Core interfaces—lessons that generalize to other CI backbones. Here is some important directions to pay attention:

Governance and risk framing. Establish a PQC program board, define HNDL risk tolerances, and align to national timelines (e.g., CNSA 2.0 milestones to 2030–2035).

Asset & crypto inventory. Enumerate where asymmetric crypto is used: TLS/QUIC, SSH, IPsec, messaging, PKI, firmware signing, backups, and third-party APIs. NIST's transition materials provide structure for this assessment.

Crypto-agility by design. Upgrade stacks to support hybrid KEMs and multiple signature schemes without forklift replacement (APIs, configuration flags, certificate profiles, and automated certificate management). Target TLS 1.3 + X25519MLKEM768 for Internet-facing endpoints.

Pilot hybrid PQ in low-risk paths. Start with external portals and brokered APIs; use major CDNs and clouds that already offer PQC; validate middlebox compatibility; monitor handshake sizes, latencies, and error modes. (Examples: Akamai and Cloudflare PQC rollouts; Go and browser defaults.)

Secure the naming & email planes. Sign critical zones with DNSSEC using modern algorithms; evaluate PQ-ready signing roadmaps; deploy SMTP DANE to harden inter-domain email, especially for incident response channels.

Code- and firmware-signing. Prioritize migration to ML-DSA (and/or SLH-DSA where conservative assumptions are required) for long-lived artifacts; align with CNSA 2.0 signature timelines; validate toolchains and HSM support.

Testbeds & red-team exercises. Build PQ-aware integration labs; replay operational traffic; measure loss/latency impacts; include downgrade and HNDL scenarios; rehearse key rollover and incident processes.

Procurement & supply chain. Require PQC roadmaps, FIPS validation plans, and crypto-agility from vendors; leverage buyer's-guide checklists and certification programs as they mature.

Conclusion

The PQC transition has moved from theory to standards and early large-scale deployments. For CI, the path forward is a hybrid, crypto-agile, risk-based migration: inventory cryptography, enable hybrid TLS on Internet-facing systems, modernize DNSSEC and MTA security, migrate signing to ML-DSA/SLH-DSA, and design testbeds that reflect real operational constraints. Aligning to national timelines (CNSA 2.0), leveraging maturing vendor ecosystems, and prioritizing HNDL-sensitive assets will reduce risk while maintaining availability and interoperability. All these activities should be a core CI objectives.

1. NIST. (2025, March 11). NIST selects HQC as fifth algorithm for post-quantum encryption. https://www.nist.gov/ NIST.
2. NSA. (2025). Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) timelines. https://media.defense.gov/.
3. Котух, Є. В. (2022). Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі: дис. д-ра наук з держ. упр.: 25.00.02. Харків, 2022. 479 с. Національний університет цивільного захисту України.

В.С. Волошин, О.В. Клєнін

АЛЬТЕРАНТИВНИЙ ВАРІАНТ АРГУМЕНТАЦІЇ ПРО ТЕРМОДИНАМІЧНО-КЛАСТЕРНУ СТРУКТУРУ ВОДИ

Аналіз останніх досліджень в області інтерпретації орієнтаційного порядку води, наприклад, на гідрофільних поверхнях [1], всередині білкових порожнин [2], та ін. дозволяє розглядати кластерну структуровану воду як предмет наших досліджень відносно підтвердження або спростування наявності мобільних, але локально обмежених асоціацій молекул води іншими методами дослідження. Як випливає з досліджень [3, 4], на кордонах власної межі розділу вода здатна організувати орієнтовані впорядковані шари, про що свідчить, наприклад, зміна провідності її русла або деякі інші якості, що дозволяють стверджувати про існування локальної структури води.Незважаючи на скептичну аргументацію щодо предмета дослідження, в даній роботі ми будемо оцінювати кластерну структуру води з позицій її ентропії, розуміючи зростання цього показника, як стан невпорядкованості системи і її дезорганізації.

Приймемо за відправну точку наступне. Вода складається з окремих молекул H_2O і численних скупчень подібних комбінованих молекул. Розрахунку підлягають системи, в яких послідовно та умовно: 100% води складається з окремих молекул; 50% води складається з окремих молекул, а решта – структуровані молекулярні системи; вода на 100% складається зі структурованих молекулярних систем. Тривалість життя кластерів становить $10^{-12} \div 10^{-14}$ с [2]. Тобто кластери здатні моментально з’являтися, а також миттєво розпадатися, але в той же час молекули, що розпалися, готові відразу ж перейти до іншої конфігурації об'єднання в нові кластери. І так до нескінченності. Такі кластери не можуть не брати участь у формуванні унікальних властивостей води, яка при дуже простій власній формулі проявляє різноманітні вкрай аномальні та інші цікаві здібності. За деякими даними, у зв'язаному стані в кластері можуть перебувати до кількох сотень молекул води. Якщо прийняти цю гіпотезу, то звідси випливає висновок: ступінь структурування води можна оцінити по її ентропії. Ентропія однієї молекули H_2O може значно відрізнятися від ентропії молекулярного кластера об'єднаних молекул.

Ми звернемося до загального правила термодинаміки, згідно з яким завжди структурована і впорядкована система має нижчу ентропію, ніж невпорядкована і менш організована система. Це правило повинно поширюватися як на воду, що складається з окремих і не пов'язаних між собою молекул H_2O, так і на кластери, що складаються з об'єднаних молекул води і миттєво виникають і розпадаються.

За базову точку відліку візьмемо стандартну молярну ентропію молекули реальної рідкої води $S^0_{H_2O,l} = 69.95 \pm 0.03$ ДЖ/(моль·К) з її

миттєво виникаючими і такими, що розпадаються, *H*-пов'язаними агрегатами при 298 К і 1 бар.

Розглянемо умовні «типи» стану води: мономери (з одних молекул) і кластери фіксованих розмірів *n* молекул. Доля молекул, що входить до складу кластера означимо, як $f \in [0,1]$. Тоді число кластерів на 1 моль молекул: $N_c = (fN_A)/n$. Число мономерів: $N_m = (1-f)N_A$. Кластери будуть розглядатися як взаємно нерозрізнені комплекси з внутрішнім коливним/обертальним спіновим внеском у модель.

Використовуючи в розрахунках комбінаторний (перестановочний) метод «склеювання» *n* молекул в нерозрізнені кластери, ми дещо «втрачаємо» в змісті від незнання характеру перестановок всередині кожного кластера. Але, в той же час, по Стірлінгу, ми отримуємо дуже просту оцінку втрати ентропії на кожен 1 моль впорядкованих молекул

$$\Delta S_{perm} \approx -R \cdot f \cdot [\ln(n) - 1] \quad (1)$$

з урахуванням ділення числа мікро станів на n! на кожний кластер. Тут R - постійна газу. Параметр ΔS_{perm} лінійний по *f* і зростає по модулю з розміром кластеру *n* (згідно правилам статистичної механіки $\ln(n!) \approx n\ln(n)$).

Розглядаючи ентропію змішування «видів» (мономерів↔кластерів), звернемо увагу на невеликий позитивний внесок, який виникає при змішуванні двох «видів» незалежних рухомих сутностей - мономерів і кластерів. Кількість «сутностей» (entities) на 1 моль молекул в даному випадку:

$$e_c = (1-f) + f/n. \quad (2)$$

Мольні частки «сутностей» серед *entities*:

$$x_m = \frac{1-f}{e_c}, x_c = \frac{f/n}{e_c}. \quad (3)$$

Тоді ідеальна ентропія змішування на 1 моль *entities*:

$$S_{mix,entities} = -R \cdot [x_m \ln(x_m) + x_c \ln(x_c)] \quad (4)$$

а в перерахунку на 1 моль молекул:

$$\Delta S_{mix} = e_c \cdot S_{mix,entities}. \quad (5)$$

Цей внесок дуже малий, при великому *n* число «сутностей» майже не змінюється (тут кластери зустрічаються рідко), а при $f \to 1$ суміш стає «консутентною» (тут тільки кластери), і змішування зникає. Остаточна оцінка молярної ентропії (при 298 К, 1 бар):

$$S(f,n) \approx S^0_{H_2O,l} + \Delta S_{perm}(f,n) + \Delta S_{mix}(f,n) \quad (6)$$

Слід зазначити, що це ідеалізована верхнерівнева оцінка впливу кластеризації. Результати розрахунків наведені в таблиці 1.

Припускаючи базовий розмір одного умовного кластера *n=200* і показуючи чутливість при *n=100* и *n=300* з вихідними константами *R*=8.3144626 Дж/(моль·К), $S^0_{H_2O,l} = 69{,}91$ Дж/(моль·К), (NIST), ускладнимо наступну задачу і розглянемо її з урахуванням тонкої динаміки структурних з'єднань.

1. Динамічна факторизація (фактор часу) забезпечується введенням коефіцієнта φ(τ) (частка «ефективного» впорядкування в межах кластера), який показує, яку частку часу насправді проводять молекули в кластерному стані відносно релевантної до ентропії/кореляції шкали $\varphi(\tau) = \frac{\tau}{\tau+\tau_{rel}}$. Тут τ — термін існування кластера ($10^{-14} - 10^{-12}$ с); τ_{rel} — характерний час релаксації/переорієнтації молекулярної водної зв'язки (оцінково приймаємо τ_{rel}=1· 10^{-12} с у відповідності до поняттів динаміки *H*-зв'язків і «jump» механізму). Ця форма дає $\varphi \to 0$ для дуже швидких розпадів і $\varphi \to 1$ для стабільних кластерів. Функціональна форма, це розумний приблизний вибір, і, як показує аналіз, інші гладкі ваги дадуть аналогічні якісні висновки.

2.Оскільки умови створення кластерів пов'язують з низькочастотними колективними модами, коли втрачається частина незалежності локальних librational/rotational ступенів стану молекули, то молярну «внутрішню» корекцію ми апроксимуємо у вигляді

$$\Delta S_{unt}(f,n) = f \cdot s_{cl}. \quad (7)$$

Тут: s_{cl} — ентропія (Дж/(моль·К)), що відноситься до «молекули», пов'язаної зі створенням кластеру (модельно прийнята, як пропорційна ($-R \cdot \gamma \cdot ln(n)$). У цій додатковій частині параметр $\gamma \ll 1$ кодує невеликий відносний ефект зміни локальної динаміки що надходить до однієї молекули. При розрахунках беремо умовно $\gamma=0.02$, τ_{rel}=1×10^{-12} с., рахунковий час існування кластера: $1 \times 10^{-12}, 1 \times 10^{-13}, 1 \times 10^{-14}$ с. Внутрішня динаміка кластерів (корекція моделі через $\gamma=0,02$), як показали подальші розрахунки, дає невеликий додатковий внесок у зміну ентропії (0.4–0.9 Дж/(моль·К), при $f=0.5–1,0$), тобто базисна величина визначається домінуючою комбінаторною перестановкою, а внутрішня "м'яка" динаміка - коригує порядок одиниць Дж/(моль·К).

3. Загальна скоригована молярна ентропія (див. табл. 1):

$$S(f,n,t) = S^0 + \varphi(\tau)[\Delta S_{perm}(f,n) + \Delta S_{int}(f,n) + \Delta S_{mix}(f,n)]. \quad (8)$$

Початкові суми (без ваги φ) для $n=200$:

— при $f=0.5$: $\Delta S_{perm} + \Delta S_{mix} + \Delta S_{int} \approx -18{,}1786$ Дж/(моль · К);

— при $f=1.0$: сумарно ≈−36.6191 Дж/(моль·К).

Наступний розрахунок проводиться з уточненням розподілу розмірів кластерів $P(n)$, щоб сума з сумою n з ваговими коефіцієнтами $\varphi(\tau(n))$ і $f(n)$ дала більш точні результати для зміни загальної ентропії води (табл. 1). Відзначимо досить високу чутливість ентропії до розмірів кластера:

—при n=100: $S_{f=0,5} \approx 55,16$; $S_{f=1} \approx 39,93$ Дж/(моль · К);

— при n=300: : $S_{f=0,5} \approx 50,45$; $S_{f=1} \approx 30,80$ Дж/(моль · К) – до 30%.

Таблиця 1. – Варіанти розрахунку термодинамічного стану води при різних комбінаціях молекул мономерів і кластерних угруповань

Варіант	**Доля в кластерах, f**	$\Delta S_{perm}(f,n)$, *Дж/моль·К*	$\Delta S_{mix}(f,n)$, *Дж/моль·К*	$S(f,n)$, *Дж/моль·К*
100% мономери	0,0	0,000	0,000	69,91
50% молекул у кластерах	0,5	-17,869	+0,131	52,17
100% молекул у кластерах	1,0	-35,738	0,000	34,17

З урахуванням тонкої динаміки всередині кластерів.

Доля в кластерах, f	$\tau(c)$	$\varphi(\tau)$	**Сума (без φ) ΔS,** Дж/моль · К)	**Скорегований $\Delta S_{eff} = \varphi \cdot \Delta S$, Дж/(моль·К)**	$S(f,n,\tau) = S^0 + \Delta S_{eff}$, **Дж/моль·К**
0,5	1×10^{-12}	0,50	-18,1786	-9,08	60,86
0,5	1×10^{-13}	0,0909	-18,1786	-1,65	68,30
0,5	1×10^{-14}	0,00990	-18,1786	-0,17	69,77
1,0	1×10^{-12}	0,50	-36,6191	-18,3	51,64
1,0	1×10^{-13}	0,0909	-36,6191	-3,32	66,62
1,0	1×10^{-14}	0,00990	-36,6191	-0,36	69,59

З урахуванням розподілу по розмірам кластерів.

Total f	Моном f_{mono}, с	E, с/моль	φ_{mix}	$\Delta S_{perm_{eff}}$ Дж/(моль·К)	$\Delta S_{int_{eff}}$, Дж/(моль·К)	$\Delta S_{mix_{eff}}$ Дж/(мольК)	$\Delta S_{total_{eff}}$ Дж/мольК	S_{final} Дж/мольК
0,0	1,0	1,000	0,00	0,0000	0,0000	0,0000	0,0000	69,91
0,5	0,5	0,504	0,04	-1,5721	-0,2544	-0,1140	-1,9405	68,01
1,0	0,0	0,005	0,1	-16,4444	-1,4534	-0,8745	-18,7722	51,18

Тобто, чим більше n, тим сильніше «штраф» $-R \cdot f \cdot [\ln(n) - 1]$ і тим нижче кінцева ентропія.

Наприклад, для гіпотетичного і невизнаного 912-молекулярного кластера С. Зєніна, розрахункове значення ентропії мало б бути в діапазоні від $S_{912,f=0,5} = 31,85$ Дж/(моль · К) до $S_{912,f=0,8} = 24,33$ Дж/(моль · К), тобто майже в три рази менше, ніж стандартна ентропія води.

Таким чином, навіть чисто комбінаторна стратифікація (що включає динаміку тонких зв'язків і з урахуванням розподілу розмірів кластерів) може дати певне зниження S при збільшенні f і n. Це узгоджується з основним принципом термодинаміки «більш впорядкована система пов’язана з меншою ентропією». Вклад від ідеального змішування ΔS_{mix} – десятичні частки Дж/(моль · К) і вона не компенсує комбінаторну втрату за рахунок «склеювання». В реальній воді кластери живуть піко секунди, а «структура» є сильно динамічною завдяки миттєвим перезборкам H-зв'язків і «*jump-reorientation*», що відповідає саме миттєву впорядкованість.

При тривалості життя кластерів порядку 1×10^{-12} с, що можна порівняти з часом релаксації локальної сітки водних з'єднань [5], динамічна

поправка для внутрішньо кластерних з'єднань залишається значною: при *f=0,5* сумарна молярна ентропія знижується до ≈60,9 Дж/(моль·К) (14,7%), а при повній «склейці» *(f=1)* — до ≈51,6 Дж/(моль·К) (35%). Це помітне зниження в порівнянні зі стандартним $S^0_{H_2O(1)} = 69{,}91$ Дж/(моль · К). При дуже коротких інтервалах життєвого циклу кластера (10^{-13}–10^{-14} с) ефект термодинамічного впорядкування практично зникає. Системи швидко перемішуються, впорядкованість «усереднюється», а ентропія близька до $S^0_{H_2O(1)}$.

Тому прийнято, що для зниження ентропії необхідно: або а) - кластери з тривалістю ≥10^{-12} с, або б) - велика частка молекул у кластерах [6] (*f≈0,5–1*). Якщо кластери надзвичайно флуктуаційні ($\tau \ll 10^{-13}$ с), термодинамічна різниця з неізольованими молекулами буде невеликою і важко реалізованою для вимірювань стандартними методами.

При обраній моделі розподілу молекул в кластері (лонг нормальне *P(n)* з медіаною 200 і $\sigma_{ln=0,5}$) і вибраними динамічними параметрами ($\tau(n) = 10^{-12}(n/200)^{0,5}$, $\tau_{rel} \geq 10^{-12}$, $\gamma = 0{,}02$) підсумкова молярна ентропія (див. таблицю 1) для:

- *f=0.0* (всі молекули — мономірні) залишається на рівні S_0 =69.91 Дж/(моль·К);

- *f=0.5* (половина молекул приймає участь у кластерах, що розподілені по *P(n)*) — S≈68.01 Дж/(моль·К) із зменшенням ≈1.90 Дж/(моль·К) відносно $S^0_{H_2O(1)}$). Більша частина маси кластерів припадає на великі *n* (близько сотень), але при *f=0,5* ефективна φ_{mix} (зважена за внеском entities) виявилася малою (~0,039), тому внески $\Delta S_{perm_{eff}}$ і $\Delta S_{int_{eff}}$ сильно редуцировані в порівнянні з «загальним» (статичним) випадком, який ми раніше розглядали без розподілу в динаміці;

- *f=1.0* (всі молекули в кластерах за розподілом) — S≈51.18 Дж/(моль·К) (велика знижка ≈ −18.73 Дж/(моль·К)). Доля entities сильно падає (e_c≈0.005), φ_{mix} вище (~0.098) і сумарний ефект стає крупнішим S_{final} ≈51.2 Дж/(моль·К)), аналогічно попередній оцінці для повного склеювання, але з відмінностями через розподіл розмірів і φ(n).

Бенчмаркінг. Доказом відомих молекулярних і квантово-механічних експериментальних досліджень варіантів стану води, в яких передбачається існування кластерів, можуть бути розрахункові значення ентропії різних кластерних структур у складі води, які не збігаються зі стандартними значеннями. Це може стати аргументом для актуалізації гіпотези про кластеризацію води як об'єктивної форми її існування. У якості такої роботи розглянемо статтю А. Токмачева, А. Хонгрева та Р. Дронковського [7], де на

основі квантово-хімічного аналізу можливих конфігурацій водневих мереж у кластері $(H_2O)_{20}$ були отримані статистичні дані щодо квантово-механічних та термодинамічних властивостей просторової та електронної структури молекулярних кластерів, виходячи з характеру кооперативності водневих зв'язків та співвідношення структура-властивість. Тим більш, як показує практика, що пограничні режими в будь-яких системах завжди дають цікаві і завжди обґрунтовані результати.

Звернемося до граничного режиму інтерфейсу стану води на межі розділу між фазного поля з орієнтацією молекул води (див. таблицю 1) [2]. За основу взяті авторські параметри, що вказують на наявність сильного такого між фазного поля (0,1–1 V·nm^{-1}), що спостерігається через фазовий кут $\chi^{(2)}$ і C_{dl} (табл. 2). Оцінка ступеня зниження орієнтаційної ентропії води в при поверхневому впорядкованому шарі води, яка пов'язана зі зміною електропровідності каналу, може бути підтвердженням існування локального структурування води. Але цей ефект обмежений тільки експериментальним інтерфейсом і не поширюється на весь обсяг.

Таблиця 2. – Дані спектроскопії та термодинаміки на межі розділу PS-SFG ↔провідність (з урахуванням даних [2]

Параметр	Контроль $\chi^{(2)}$	Контроль $\chi^{(2)}$	Очікуваний зсув, 0V	Ефект розміру (d)	$S(f,n,t)$, Дж/(моль)	Примітка
Фазовий кут, $\chi^{(2)}$	0 V	0 V	5-15%	0,6-1,0	$S_{\xi^{(2)}} = 66{,}87$	Зв'язок із зарядом інтерфейсу
Провідність каналу	pH 7,4	pH 7,4	+10-40%	0,7-1,1	$S_\rho = 60{,}11$	Зі збереженням іонної сили
EIS C_{dl}	0 V	$\pm 0{,}4\ V$	+10-30%	0,6-0,9	$S_{c_{dl}} = 64{,}55$	Ємність подвійного шару

Індекс впорядкованості гідратації білків (wNOE/wROE, T_1/T_2), визначений за допомогою NMR-спектроскопії, також підтверджує існування структурних доменів води, пов'язаних з макромолекулами (табл. 3). В основу покладено різний поздовжній (T_1) і поперечний (T_2) час релаксації доменів H_2O і кореляції в гідратних оболонках білків в порівнянні з водою за об'ємом. При цьому структурованість носить динамічний характер, а структурована, таким чином, вода в гідратному шарі швидко обмінюється молекулами з «вільною» водою.

Спостережувані авторами, і такі, що відрізняються у часі релаксації і кореляції, в гідратних оболонках білків в порівнянні з водою в об'ємі, підтверджують існування структурних доменів води, пов'язаних із макромолекулярними об'єднаннями. Засвоюване розрахункове значення ентропії для таких структурних доменів в прикордонному шарі $S(f,n,t) \approx 64{,}3 \div 68{,}0$ Дж/(моль·К), яке не значно відрізняється від стандартного значення (2,8÷ 8,7%).

Таблиця 3. – Систематизація результатів експерименту з NMR гідратацією ↔ каталітичного агента (за даними робіт [1, 2]

Параметр	WT	Варіант	Очікуваний зсув, %	D	Примітка
Локальна метрика wNOE(ROI)	-	Гідрофільність	+10-30	0,6-1,0	Уповільнення гідратації
Число оборотів ферменту, k_{cat}	-	Гідрофільність	+5-20	0,5-0,8	Спрямована кореляція
Константа Міхаеліса, K_M	-	Гідрофільність	-5-15	0,4-0,7	Зі збереженням структури білка
Каталітична ефективність ферменту, k_{cat}/K_M	-	Гідрофільність	+10-40	0,7-1,1	Цільова функціональна метрика

Мезоскопічну впорядкованість молекул води в проміжних масштабах, коли передбачувані стійкі молекулярні кластери з розмірами більшими за випадкові флуктуації, але не вищими за розмір кристала, підтверджують дослідження з роботи [5]. Тим не менш, структурована вода - це далеко не «четвертий стан речовини», а сукупність коротко існуючих локальних скупчень і доменів з підвищеною впорядкованістю мережі водневих зв'язків, що виникають в конкретних умовах, а саме, на межах розділу, в гідратних шарах, в сильних полях, на що натікає спектрометрія (NMR, FTIR, фемтосекундна динаміка), у поверхні білків, мембран, нуклеїнових кислот. Далеко неточні вихідні дані, представлені в паліативних дослідженнях EZ-зон Поллака [6] дають декілька перебільшені результати про зміну ентропії для води $S(f) \approx 39{,}8 \div 49{,}1$ Дж/(моль·К). Тим не менш, тенденцію до зниження ентропії для структурних об'єднань в таких EZ-зонах можна вважати обґрунтованою, тому що навіть при n_{var} і τ_{var}, значення розрахункової ентропії такої суміші $S(f,n,t) \leq 66{,}8 \cdot$ (4,3% від S^0).

Таким чином, систематизація лише таких окремих досліджень може надати можливості для більш ґрунтовного аналізу ефекта кластерного структурування води.

Висновки і перспективи подальших досліджень:

1. У сучасних наукових дослідженнях структурована вода представлена мікросередовищем, в якій молекули води в сукупності своїх взаємодій демонструють короткочасний і нестійкий просторовий порядок, який відрізняється від статистично ізотропного розподілу молекул H_2O у звичайній рідкій фазі. Ця впорядкованість може проявлятися спрямовано, поступально і динамічно.

2. Термодинамічна інтерпретація властивостей структурованої води показує, як в розрахунковому, так і в експериментальному варіантах здатність до її кластерної самоорганізації, але це явище виражено слабо і може претендувати на критеріальні якості по відношенню до цієї властивості, як це обґрунтовано, тільки в граничних областях окремих біологічних систем.

3. При часі життя кластера більше 1×10^{-12} с динамічна поправка на внутрішньо кластерні зв'язки залишається значною: при 50% агрегації кластерів сумарна молярна ентропія знижується до ≈60,9 Дж/(моль·К) (14,7%), а при гіпотетично повній агрегації – до ≈51,6 Дж/(моль·К) (35%). Це помітне зниження в порівнянні з $S^0_{H_2O(1)}$. З дуже короткими інтервалами життєвого циклу кластера ($\leq 10^{-13} \div 10^{-14}$ с.) ефект термодинамічного впорядкування практично зникає. Системи швидко перемішуються, впорядкованість «осереднюється», а ентропія близька до $S^0_{H_2O(1)}$.

4. Показано, що структурована вода на межі з біологічними системами являє собою більш термодинамічно впорядковане середовище, для якого існують короткоживучі молекулярні кластери, які є стабільними поблизу біомолекул і впливають на біохімію, електричні процеси та механіку органічних взаємодій.

1. Jurema M. J., Kirschner K. N., Shields G. C. Modeling of magic water clusters $(H_2O)_n$ and $(H_2O)_{21}H^+$ with the PM3 quantum-mechanical method. Journal of Computational Chemistry. New-Work, 1993. pp. 1326–1332.
2. Konovalov A. I., Ryzhkina I. S. Highly diluted aqueous solutions: formation of nanoassociates and their properties. Journal of Solution Chemistry. New-Work, 2014. Vol. 43, No. 3. pp. 1207-1226.
3. Laage D., Hynes J. T. A molecular jump mechanism of water reorientation. Science. Washington, 2006. Vol. 311. pp. 832–835.
4. Montagnier L., Aïssa J., Ferris S., Montagnier J.-L., Lavallée C. Electromagnetic signals are produced by aqueous nanostructures derived from bacterial DNA sequences. Interdisciplinary Sciences: Computational Life Sciences. Beijing,2009. Vol. 1, No. 2. pp. 81–90.
5. Xu X., Shen Y. R., Tian C. Phase-sensitive sum frequency vibrational spectroscopic study of air/water interfaces: H_2O, D_2O, and diluted isotopic mixtures // *The Journal of Chemical Physics*, Vol. 150, New York, 2019. PDF: 12 p.
6. Pollack G. H. The Fourth Phase of Water: Beyond Solid, Liquid, and Vapor. Olympia Publishing, Seattle,2013. pp. 1–256.
7. Tokmachev A. M., Tchougréeff A. L., Dronskowski R. Hydrogen-bond networks in water clusters $(H_2O)_{20}$: an exhaustive quantum-chemical analysis. ChemPhysChem. Weinheim,2010. Vol. 11. pp. 384–388.

Я.Ю. Дорогий, А.М. Піскун, В.В. Цуркан

МОДЕРНІЗАЦІЯ ГІДУ З ДЕРЖАВНИХ ПОСЛУГ УКРАЇНИ

Анотація. У тезах розглянуто підходи до модернізації Гіду з державних послуг України як елемента цифрової трансформації державного управління. Описано адаптацію європейських стандартів інтероперабельності та впровадження Національного інтероперабельного каталогу державних послуг. Визначено технічні та організаційні аспекти створення сучасної цифрової екосистеми для громадян, бізнесу та державних органів.

Вступ. Модернізація системи надання публічних послуг є одним із ключових напрямів цифровізації публічного управління в Україні. Гід з державних послуг забезпечує громадянам централізований доступ до інформації про сервіси, проте його архітектура потребує оновлення для відповідності європейським стандартам та принципам інтероперабельності.

Метою модернізації є створення уніфікованої структури даних, гармонізованої з моделями CPSV-AP та DCAT-AP, що використовуються в Європейському Союзі для опису державних послуг і наборів даних.

Аналіз літературних джерел. Розвиток сучасних цифрових інструментів управління публічними послугами є одним із ключових напрямків цифрової трансформації державного сектору в Україні. Актуальність теми модернізації Гіду з державних послуг обумовлена необхідністю забезпечення інтероперабельності державних систем, уніфікації даних та інтеграції з європейським цифровим простором. У цьому контексті важливим є аналіз міжнародних підходів, що визначають архітектуру, стандарти та технологічні засади побудови електронних сервісів.

У статті [1] представлено концептуальну модель Core Public Service Vocabulary Application Profile (CPSV-AP), яка використовується Європейською комісією для стандартизації опису державних послуг. У роботі наведено структуру метаданих для моделювання адміністративних процедур, документів і юридичних підстав. Цей підхід забезпечує сумісність між національними каталогами послуг різних країн ЄС і слугує основою для створення українського Національного іноперабельного каталогу державних послуг.

У регламенті [2] встановлено правові засади функціонування Єдиного цифрового шлюзу (Single Digital Gateway – SDG), який забезпечує транскордонний доступ громадян та бізнесу до адміністративних сервісів у межах Європейського Союзу. Документ визначає вимоги до уніфікації державних порталів, обміну інформацією між країнами-членами та впровадження принципу одноразового подання даних (Once Only Principle).

У технічному документі [3] Once-Only Technical System (OOTS) описано архітектуру та функціональні принципи реалізації системи обміну даними між державними органами ЄС. Автори розглядають механізми ідентифікації

користувачів, передачі даних та валідації документів у межах міждержавних транзакцій. Ця модель є технічним еталоном для побудови української інфраструктури сумісності та зменшення адміністративного навантаження на користувачів.

У дослідженні [4] представлено уніфікований огляд щодо застосування штучного інтелекту в державному управлінні, а також запропоновано класифікацію типів систем AI-GOV (operational fitness, epistemic alignment, normative divergence). Ця праця має практичне значення для проєктів цифрової трансформації державних сервісів, серед яких модернізація Гіду з державних послуг в Україні.

Таким чином, аналіз наявних джерел показує, що розвиток державних цифрових сервісів у Європейському Союзі базується на уніфікованих стандартах даних, семантичній інтероперабельності та використанні інтелектуальних технологій. Ці підходи створюють методологічну основу для модернізації Гіду з державних послуг України, що дозволить забезпечити сумісність із європейськими платформами, спростити доступ до сервісів та підвищити якість державного управління.

Концептуальні засади. Реформування Гіду ґрунтується на впровадженні моделі Національного інтероперабельного каталогу, який забезпечує семантичну сумісність між державними реєстрами та порталами послуг.

Основними завданнями є:

– уніфікація описів державних послуг на основі CPSV-AP;

– забезпечення багатомовності та адаптації до транскордонних сервісів ЄС;

– інтеграція з технічними системами SDG та OOTS відповідно до регламентів ЄС [2-3];

– впровадження AI-сервісів для інтелектуального пошуку, автоматичної класифікації та формування рекомендацій у каталозі державних послуг, що підвищить точність і персоналізацію результатів для користувачів.

Архітектурне рішення. Каталог реалізується як RDF-сумісна база знань із відкритим API, що підтримує SPARQL-запити. Така модель дає змогу формувати зв’язки між послугами, документами та життєвими ситуаціями користувача, а також використовувати елементи штучного інтелекту для рекомендаційних сервісів.

Очікувані результати. Модернізований Гід забезпечить структурованість, відкритість і машинну оброблюваність даних, що дозволить створити умови для транскордонного обміну інформацією та впровадження принципу одноразовості (Once Only Principle).

Висновки. Модернізація Гіду з державних послуг України є ключовим кроком до інтеграції в європейський цифровий простір. Вона забезпечує перехід до інтероперабельної архітектури, підвищує ефективність управління послугами та сприяє формуванню інтелектуальної екосистеми публічного сектору.

Реалізація проєкту створює передумови для впровадження транскордонних цифрових сервісів та підвищення рівня довіри громадян до держави.

1. European Commission. Introduction to the Core Public Service Vocabulary Application Profile (CPSV-AP). – 2024. – URL: https://surli.cc/djzjdb.
2. Regulation (EU) 2018/1724 establishing a single digital gateway (SDG). – EUR-Lex, 2018. – URL: https://surl.li/loelws.
3. European Commission. Once-Only Technical System (OOTS). – 2024. – URL: https://surl.lu/dkqpuo.
4. Straub, V. J., Morgan, D., Bright, J., & Margetts, H. Artificial intelligence in government: Concepts, standards and a unified framework. – arXiv. https://doi.org/10.48550/arXiv.2210.17218, 2022.

К.В. Кармазін

ІНТЕЛЕКТУАЛЬНІ АЛГОРИТМИ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ АДАПТИВНИХ СИСТЕМ ПОТОКОВОГО ВІДЕО

Сучасні системи потокового відео є складними динамічними структурами, які функціонують у мінливому середовищі мережевого трафіку, обмежених ресурсів і різнорідних користувацьких умов. Класичні алгоритми адаптивної потокової передачі Adaptive Bitrate Streaming (ABR), що базуються на евристичних або статистичних правилах, не здатні повною мірою забезпечити стійкість якості користувацького досвіду Quality of Experience (QoE) [1] при різких змінах пропускної здатності каналів чи затримках передачі. Унаслідок цього система стає резильєнтно нестійкою: навіть незначні флуктуації мережевих параметрів призводять до буферизації, втрат кадрів або зниження роздільної здатності, що погіршує сприйняття контенту користувачем. Крім того, у контексті сучасних цифрових екосистем (освіта, телемедицина, безпека, «розумні міста», керування техно-екологічними подіями [2]) стабільність мультимедійних сервісів є критичною для забезпечення інформаційної резильєнтності суспільства загалом. Лімітованість пропускної здатності в мобільних мережах, енергетичні обмеження на пристроях користувачів, а також варіативність мережевого середовища створюють умови, за яких традиційні підходи до управління якістю потокового відео стають неефективними. Наявна проблема полягає у відсутності інтегрованих інтелектуальних механізмів, здатних адаптувати поведінку системи до непередбачуваних змін зовнішнього середовища, підтримуючи при цьому баланс між якістю, стабільністю та ефективністю використання ресурсів.

У цій роботі пропонується розробити інтелектуальну модель адаптивної потокової передачі відео, здатну підвищувати резильєнтність системи за рахунок прогнозування мережевих умов, гнучкого управління бітрейтом та координації між агентами в децентралізованому середовищі. Завдання полягає у формуванні формальних основ для оцінювання QoE у контексті резильєнтності системи, коли важливо не лише досягнути високого середнього рівня якості, а й мінімізувати її коливання при зовнішніх збуреннях. Необхідно розробити нову метрику, – Resilient Quality of Experience (RQE), яка відображатиме стабільність сприйняття користувачем відеопотоку у часі. Також постає завдання розробити інтелектуальні алгоритми прийняття рішень, які використовуватимуть методи машинного навчання та навчання з підкріпленням Reinforcement Learning (RL) для оптимізації параметрів передавання. Додатковим аспектом постановки задачі є забезпечення кооперативної стійкості системи в умовах одночасного доступу багатьох користувачів. Це передбачає моделювання мультиагентної взаємодії, коли кожен агент (наприклад, клієнтський пристрій) діє

автономно, але координує свої дії із сервером або edge-вузлом, забезпечуючи спільну резильєнтність мережі.

Для вирішення поставленої задачі пропонується багаторівневий інтелектуальний підхід, який поєднує аналітичне моделювання, машинне навчання та мультиагентну координацію. На першому рівні реалізується прогнозування динаміки мережевих параметрів із використанням глибинних рекурентних нейронних мереж (LSTM, GRU). На другому рівні впроваджується адаптивний модуль прийняття рішень, який використовує RL-алгоритми для вибору оптимальної якості відео. На третьому рівні формується мультиагентна архітектура, у якій кожен вузол системи може обмінюватися інформацією для координації дій. Додатково пропонується використання методів генеративного штучного інтелекту [3] для реконструкції втраченої або спотвореної відеоінформації. Ефективність алгоритмів перевірятиметься у середовищах Mininet та NS-3, порівняно з класичними ABR-підходами за метриками QoE, QoS, енергоспоживання та стабільності.

Робота пропонує нову концепцію резильєнтності адаптивних систем потокового відео на основі інтелектуальних алгоритмів прогнозування, навчання з підкріпленням і мультиагентної координації. Застосовано поняття Resilient Quality of Experience (RQE), що відображає стабільність сприйняття користувачем у динамічних мережевих умовах. Запропоновано багаторівневу архітектуру адаптивної передачі, яка поєднує прогнозування пропускної здатності, оптимізацію бітрейту та реконструкцію відео за допомогою генеративних моделей штучного інтелекту.

Отримані результати можуть мати практичне застосування у мультимедійних платформах, державних онлайн-сервісах і мобільних мережах 4G/5G, де вони підвищують стабільність і якість відеопередачі. Запропоновані алгоритми можуть використовуватись у комерційних (YouTube, Netflix, Megogo) та освітніх системах для зменшення буферизації й оптимізації трафіку. Реалізація підходу забезпечує створення самоадаптивних і стійких відеосистем, здатних підтримувати високу якість користувацького досвіду навіть за умов нестабільних мереж.

1. Ajeyprasaath K. B., Vetrivelan P. A Hybrid Machine Learning Approach for Improvised QoE in Video Services over 5G Wireless Networks // Computers, Materials & Continua. – 2024. – Vol. 78. – P. 3195–3213. [DOI: 10.32604/cmc.2023.046911].
2. Kateryna Melkumian, Julia Pisarenko, Alexander Koval. Organization of Regional Situational Centers of the Intelligent System “Control_TEA” using UAVs // Proceedings of the 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD-2021).- PP.37-40. [DOI: 10.1109/APUAVD53804.2021.9615416].
3. Artioli, E. Generative AI for HTTP Adaptive Streaming // Proceedings of the 15th ACM Multimedia Systems Conference (MMSys ‘24). – New York: Association for Computing Machinery, 2024. – P. 516–519. [DOI: 10.1145/3625468.3652912].

Я.Ю. Дорогий, А.М. Піскун, В.В. Цуркан

ВИКОРИСТАННЯ ШІ ДЛЯ МОДЕРНІЗАЦІЇ ГІДУ З ДЕРЖАВНИХ ПОСЛУГ УКРАЇНИ

Анотація. У статті розглянуто застосування технологій штучного інтелекту (ШІ) у процесі модернізації Гіду з державних послуг України. Підкреслюється роль інтелектуальних сервісів у підвищенні ефективності пошуку, персоналізації рекомендацій, підтримці адміністраторів і забезпеченні сумісності з європейськими цифровими стандартами. Описано ключові напрями впровадження ШІ, такі як NLP-пошук, reasoning, рекомендаційні системи та AI-асистенти.

Вступ. Сучасний етап цифрової трансформації державного управління вимагає створення інноваційних сервісів, орієнтованих на потреби громадян та бізнесу. Гід з державних послуг є ключовим елементом електронного урядування України, що забезпечує централізований доступ до публічних сервісів. Проте наявні проблеми – дублювання інформації, різні формати описів та обмежені можливості пошуку – зумовлюють потребу у впровадженні інтелектуальних технологій. Застосування ШІ сприятиме автоматизації обробки даних, підвищенню якості сервісів і гармонізації з європейськими стандартами CPSV-AP та DCAT-AP.

Аналіз літературних джерел. Розвиток цифрових публічних сервісів із використанням ШІ є предметом досліджень провідних науковців і практиків.

У статті [1] розглянуто принципи побудови європейських каталогів державних послуг, які базуються на відкритих стандартах та забезпечують міжкраїнову інтероперабельність. Підкреслюється важливість семантичної уніфікації для інтеграції України у спільний цифровий простір ЄС.

У дослідженні [2] акцент зроблено на впровадженні моделей обробки природної мови (NLP) для побудови інтелектуальних пошукових систем у державних порталах. Автори демонструють ефективність гібридних моделей, які поєднують семантичний пошук із рекомендаційними механізмами.

У роботі [3] розкрито можливості reasoning-технологій (SPARQL, OWL, SHACL) у побудові зв'язків між публічними послугами, що дозволяє формувати автоматизовані ланцюжки дій користувачів.

У статті [4] проаналізовано застосування Retrieval-Augmented Generation (RAG) для формування пояснень та підказок користувачам державних платформ, що сприяє підвищенню рівня довіри та прозорості ШІ-рішень.

Таким чином, огляд показує, що інтеграція ШІ у публічні сервіси поєднує технічні та організаційні аспекти, спрямовані на забезпечення людиноцентричності, автоматизації та прозорості державного управління.

Основна частина. Впровадження ШІ в архітектуру Гіду з державних послуг спрямоване на створення системи нового покоління – Національного інтероперабельного каталогу. Основні напрями застосування ШІ:

– Інтелектуальний пошук – використання NLP-моделей для розуміння запитів природною мовою, семантичної інтерпретації намірів користувача та формування релевантних результатів [2].

– рекомендаційні механізми – система пропонує пов'язані або комплексні послуги, підказки адміністраторам щодо дублювань і можливих помилок.

– reasoning-модуль – використання онтологічних правил (SHACL, OWL RL, SPARQL) для автоматичного формування ланцюжків дій – від цільової послуги до необхідних документів і супутніх процедур [3].

– AI-асистенти – автоматичне класифікування звернень громадян, створення чернеток відповідей, аналітика частотності запитів.

– персоналізація досвіду – використання механізмів RAG для генерації пояснень, рекомендацій та підтримки користувачів.

Реалізація цих функцій відповідає принципам європейської стратегії цифровізації (SDG, OOTS) та концепції "людина в центрі", де рішення ШІ є прозорими, контрольованими і перевіряються людиною [1].

Висновки. Інтеграція технологій ШІ у Гід з державних послуг є стратегічним напрямом розвитку цифрової держави. Вона забезпечує не лише зручність та швидкість взаємодії, але й підвищує якість даних, автоматизує процеси адміністрування та сприяє інтеграції України до європейського цифрового простору. Подальші дослідження мають бути спрямовані на стандартизацію AI-моделей, формування метрик якості ШІ-сервісів і розробку етичних протоколів використання інтелектуальних агентів у державному секторі.

1. European Commission. Introduction to the Core Public Service Vocabulary Application Profile (CPSV-AP). – 2024. – URL: https://surli.cc/djzjdb.
2. Park, J.; Kim, C. Natural Language Processing Adoption in Governments and Future Research Directions: A Systematic Review. – Applied Sciences, 2023, 13, 12346. – URL: https://surl.li/vjcklz.
3. Shadbolt, N.; Berners-Lee, T.; Hall, W.; O'Hara, K.; Tiropanis, T.; Hendler, J. Linked Open Government Data: Lessons from Data.gov.uk. – IEEE Intelligent Systems, 2012, 27(3), 16-24. – URL: https://surl.li/tdupen.
4. Lewis, P.; Perez, E.; Piktus, A.; Petroni, F.; Karpukhin, V.; Goyal, N.; Küttler, H.; Lewis, M.; Yih, W.; Rocktäschel, T.; Riedel, S.; Kiela, D. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. – Advances in Neural Information Processing Systems, 2020, 33, 9459-9474. – URL: https://surl.lu/bosyyy.

Я.Ю. Дорогий, А.М. Піскун, В.В. Цуркан

КІБЕРБЕЗПЕКА НАЦІОНАЛЬНОГО ІНТЕРОПЕРАБЕЛЬНОГО КАТАЛОГУ ДЕРЖАВНИХ ПУБЛІЧНИХ ПОСЛУГ

Анотація. Доповідь присвячена аналізу кібербезпеки в контексті розвитку державних публічних послуг, з акцентом на вимоги до національного інтероперабельного каталогу державних послуг в Україні. На базі технічного плану модернізації Гіду державних послуг розглядаються ключові загрози, стандарти захисту та рекомендації для інтеграції з європейськими системами. Мета – висвітлити необхідність комплексного підходу до забезпечення безпеки даних, автентифікації та моніторингу для підвищення стійкості публічних сервісів до кіберзагроз..

Вступ. Державні публічні послуги стають дедалі залежнішими від інформаційних технологій, що робить їх особливо вразливими до різноманітних кіберзагроз, таких як хакерські атаки, витоки даних чи порушення цілісності систем. Це особливо актуально для України в умовах геополітичних викликів, де зростання кількості кібератак на державну інфраструктуру вимагає посиленого захисту та впровадження проактивних заходів. Кібербезпека є ключовим елементом для забезпечення надійності, конфіденційності та доступності сервісів, що підкреслює необхідність відповідності міжнародним стандартам, таким як ISO/IEC 27001 для управління інформаційною безпекою, OWASP для протидії веб-вразливостям та eIDAS для електронної ідентифікації. Такий підхід не лише мінімізує ризики, але й сприяє ефективній інтеграції з європейськими платформами SDG (Single Digital Gateway) та OOTS (Once-Only Technical System), дозволяючи забезпечити транскордонну взаємодію, спростити адміністративні процеси та підвищити довіру громадян до цифрових послуг.

Аналіз літературних джерел. Розвиток кібербезпеки державних публічних послуг є предметом досліджень провідних експертів та організацій.

У дослідженні [1] проаналізовано ключові кібервиклики для урядового та публічного секторів у 2024 році, включаючи загрози від кібератак, які можуть призвести до економічних, соціальних та політичних наслідків. Автори наголошують на необхідності посилення захисту критичних сервісів через впровадження комплексних стратегій.

У статті [2] розглянуто топ-5 кіберзагроз для публічного сектору, таких як компрометація даних та порушення роботи державних послуг. Підкреслюється важливість розуміння цих загроз для запобігання втратам у сфері електронного урядування.

У роботі [3] розкрито вплив кібератак на сектор публічного адміністрування, включаючи загрози для електронних урядових активностей та захисту чутливих даних. Автори демонструють, як атаки можуть порушити державні процеси та підірвати довіру громадян.

У статті [4] проаналізовано найкращі практики кібербезпеки в публічному секторі, включаючи впровадження комплексних фреймворків, регулярні оцінки ризиків та управління вразливостями. Це сприяє підвищенню стійкості державних систем до кіберзагроз.

Як підсумок, огляд літератури показує, що кібербезпека державних послуг поєднує технічні заходи з організаційними аспектами, спрямованими на мінімізацію ризиків та забезпечення стійкості.

Основна частина. Вимоги до кібербезпеки в технічному плані модернізації Гіду державних послуг передбачають багаторівневий підхід до захисту, що охоплює архітектурний, програмний, інфраструктурний та організаційний рівні.

Система забезпечує надійну багаторівневу автентифікацію з використанням кваліфікованого електронного підпису (КЕП), Дія.Підпис чи BankID. Розмежування доступу базується на моделі RBAC (Role-Based Access Control), де права надаються за принципом найменших привілеїв. Це інтегрується з європейськими стандартами eIDAS для транскордонної ідентифікації.

Трафік має захищатися протоколом TLS версії не нижче 1.2 з сильними шифрами (наприклад, AES-256). Чутливі дані в базах шифруються в стані спокою. Модернізований гід має відповідати вимогам протидії типовим вразливостям за OWASP Top 10, включаючи XSS, CSRF та SQL-ін'єкції.

Вимогами також передбачається детальне логування подій, захищене від модифікацій, з регулярним архівуванням. Моніторинг включає збір логів у реальному часі, аудит дій користувачів та адміністраторів. Для відмовостійкості впроваджуються резервне копіювання (повні, інкрементальні) та тестування відновлення.

Безпека враховує сумісність з SDG та OOTS, де принцип Once-Only вимагає захищеного обміну даними без повторного подання. Документ підкреслює необхідність відповідності ДСТУ ISO/IEC 27001 та 27002 для загального захисту.

Ці заходи забезпечують стійкість каталогу до кібератак, мінімізуючи ризики для громадян та бізнесу.

Висновки. Кібербезпека державних публічних послуг є критичною для розвитку цифрової держави, особливо в контексті інтеграції України з ЄС. На базі аналізу технічного плану Гіду державних послуг можна зробити висновок, що комплексний підхід до автентифікації, шифрування, моніторингу та відповідності стандартам (ISO, OWASP, eIDAS) дозволить мінімізувати загрози та підвищити довіру до сервісів.

1. Cybersecurity considerations 2024: Government and public sector. – KPMG, 2024. – URL: https://surl.lt/sbulop.
2. The Top 5 Cyber Threats Facing the Public Sector | IDB. – 2025. - URL: https://surl.li/xexjja.
3. Cyberattacks Impact and Harm on the Public administration sector. – Cyberpeace Institute, 2025. – URL: https://surl.li/hwyjje.
4. Guarding Governance: Cybersecurity in the Public Sector | UpGuard. – 2025. – URL: https://surl.li/kipilk.

О. І. Васильєва, С. В. Нараєвський

РОЛЬ ФАРМАЦЕВТИЧНОЇ ПРОМИСЛОВОСТІ У ЗАБЕЗПЕЧЕННІ РЕЗИЛЬЄНТНОСТІ ЄВРОПЕЙСЬКИХ ЕКОНОМІК

Фармацевтична промисловість відіграє ключову роль у забезпеченні економічної та соціальної резильєнтності багатьох країн світу, зокрема, європейських.

По-перше, сектор забезпечує безпосередньо стійкість системи охорони здоров'я через виробництво життєво необхідних лікарських засобів, інновації у медицині та готовність до криз. Для ілюстрації масштабів інтеграції фармацевтики у національні економіки у таблиці 1 розраховано частки фармацевтичної галузі у загальному обсязі промислового виробництва окремих країн Європи.

Таблиця 1.. – Частка фармацевтики у обсягах промислового виробництва у 2023 році, %

Країна	Частка фармацевтики у промисловому виробництві, %
Швейцарія	34,0
Франція	10,5
Ірландія	46,3
Німеччина	5,0
Іспанія	14,6

Фармацевтична промисловість Ірландії демонструє надзвичайну важливість для країни, оскільки на неї припадає майже половина усього промислового виробництва, тобто кожен другий промисловий товар, вироблений у Ірландії, так чи інакше, пов'язаний з фармацевтикою (табл. 1). У Швейцарії також спостерігається вагома частка фармацевтики у промисловості, що свідчить про стійкість економіки країни у період криз. Відомо, що фармацевтична промисловість не піддається циклічним коливанням, що робить її однією з найбільш стабільних галузей у структурі національних економік. На відміну від інших промислових секторів, що реагують на зміни у глобальній кон'юнктурі, споживчому попиті чи фінансових ринках, фармацевтика зберігає високий рівень виробництва навіть у періоди економічної нестабільності. Це пояснюється потребою у лікарських засобах, незалежно від фаз економічного циклу. Таким чином, економіки Ірландії та Швейцарії є резильєнтними у кризових умовах, демонструючи здатність адаптуватися та підтримувати стабільність навіть за несприятливих зовнішніх обставин. Серед аналізованих країн Іспанія займає проміжне положення, оскільки фармацевтика у даній країні є важливою галуззю, про що свідчать 14,6% у промисловому виробництві, проте

не домінуючою. Незважаючи на міжнародну присутність французьких та німецьких потужних фармацевтичних компаній, країни мають нижчі частки галузі у загальному промисловому виробництві. Структура промисловості Франції та Німеччини є більш диверсифікованою, де провідними галузями є машинобудування, енергетична та хімічна промисловості. Фармацевтичне виробництво у цих країнах часто інтегрується у ширші промислові комплекси, де воно виконує підтримуючу функцію, сприяючи розвитку суміжних галузей.

Фармацевтика є важливим експортним сектором та джерелом робочих місць, що робить її значущим чинником макроекономічної стабільності. Аналіз структури експорту та імпорту фармацевтичної продукції дає можливість не лише оцінити роль галузі в економіці країн, а й виявити рівень технологічного розвитку, інтеграції у глобальні ринки та здатність країн забезпечувати власні потреби у лікарських засобах.

Таблиця 2. – Частка фармацевтичної продукції у структурі зовнішньої торгівлі у 2023 році, %

Країна	Частка експорту фармацевтики у загальному обсязі експорту, %	Частка імпорту фармацевтики у загальному обсязі імпорту, %
Швейцарія	25,5	16,1
Франція	6,3	4,9
Ірландія	40,2	9,3
Німеччина	7,1	5,3
Іспанія	5,4	5,2

Ірландія та Швейцарія демонструють високу орієнтованість на експорт фармацевтичної продукції, оскільки мають найвищі частки серед аналізованих країн (табл. 2) Ірландія має потужну внутрішню виробничу базу, що здатна забезпечити як зовнішні, так і внутрішні потреби країни, підтримуючи значну частку експорту продукції і відносно низький рівень імпорту. Фармацевтичні товари характеризуються високою доданою вартістю, сформованою завдяки інтенсивним науково-дослідним розробкам, складним технологічним процесам і високим кваліфікаційним вимогам до праці. Таким чином, країни з потужною фармацевтичною промисловістю мають вищу стійкість до зовнішніх шоків і кращі умови економічного зростання. Незважаючи на значні обсяги експорту, Швейцарія є лідером серед п’яти країн за часткою імпорту фармацевтичної продукції. Франція, Німеччина та Іспанія мають значно нижчі частки фармацевтики у експорті та імпорті завдяки більш диверсифікованій структурі зовнішньої торгівлі та орієнтованість галузі переважно на внутрішній ринок.

Отже, фармацевтична промисловість відіграє ключову роль у забезпеченні резильєнтності європейських економік. Її розвиток сприяє зміцненню

макроекономічної стабільності, підвищенню конкурентоспроможності та збереженню стійкості у кризовий період. Проаналізувавши фармацевтичну галузь у п’яти європейських країнах, зокрема, Швейцарії, Ірландії, Франції, Німеччині та Іспанії, визначено, що для другої вона є найважливішою, забезпечуючи 44,8% загального промислового виробництва, а також формує основу експорту, забезпечуючи високий рівень доданої вартості й інноваційності. Для інших країн галузь є не менш важливою, проте орієнтованою на забезпечення власних потреб, притому залишаючись одним із ключових елементів технологічного розвитку. Зміцнення фармацевтичного сектору є важливою умовою економічної стійкості, адаптивності та довгострокового зростання європейських економік.

1. The Pharmaceutical Industryin Figures. (2025). European Federation of Pharmaceutical Industriesand Associations. https://www.efpia.eu/media/uj0popel/the-pharmaceutical-industry-in-figures-2025.pdf.
2. MerchandiseTrade – TradeDashboard. (б. д.). WTO Stats. https://stats.wto.org/dashboard/merchandise_en.html
3. WorldBankOpenData. (б. д.). WorldBankOpenData. https://data.worldbank.org/indicator/NV.IND.MANF.CD.

І.П. Каменева

РЕЗИЛЬЄНТНІСТЬ ТА ЗАСОБИ АДАПТАЦІЇ ЕКОЛОГІЧНИХ СИСТЕМ В УМОВАХ ВИСОКОГО РИЗИКУ

Вступ. В останні роки в світі відбувається занадто багато нетипових і надзвичайних події, суттєво відмінних від минулого досвіду. Перш за все це неочікувані кліматичні явища або катастрофічні події (землетруси, цунамі, вулканічні виверження, жахливі посухи або масштабні зливи, нетипові для окремих регіонів, що відрізняються суттєво нелінійним характером), Також сюди можна віднести численні техногенні аварії, вибухи та інші небезпечні інциденти, що виникають на фоні військових конфліктів. Такі події мають вкрай негативний вплив на природне середовище, особливо, на екологічні системи, розташовані поруч з критичної інфраструктури.

З метою прогнозування поведінки екологічних систем, що перебувають під впливом природних лих, техногенних аварій, вибухів та інших аномалій, традиційно використовують різноманітні методи та засоби математичного моделювання складних динамічних систем, побудовані на основі відомих закономірностей та накопиченого досвіду. Насамперед це роботи, спрямовані на дослідження особливостей складних систем, зокрема, методи нелінійної динаміки, різноманітні міждисциплінарні дослідження, в тому числі, засоби оцінювання майбутніх подій за допомогою евристичних методів, експертних знань та експертних систем [1 - 5 тощо].

Серед найбільш актуальних задач екологічного моделювання необхідно виділити прогнозування стійкості та резильєнтності на системному рівні, ідентифікацію критичних параметрів, визначення адаптаційних можливостей на системному рівні та дослідження механізмів гомеостазу, який забезпечує резильєнтність та відновлення екологічних систем.

Моделі екологічних систем. Математичне моделювання в природних науках включає побудову статичних і динамічних моделей взаємозв'язків між окремими блоками в складних системах [2, 3]. В статичних моделях аналізується окремий стан досліджуваної системи для заданого моменту часу. Такі моделі мають переважно описовий характер. Динамічні моделі відображують розвиток системи у часі. При коректній постановці задачі такі моделі використовують для прогнозування поведінки системи в майбутньому та вибору оптимальних рішень щодо управління цією системою.

Найбільш поширеним способом математичного моделювання в екології є представлення природної системи як системи диференціальних рівнянь, де швидкість зміни стану можна задати як функцію чинників, які впливають на екосистему. За допомогою сучасних методів обчислень знаходяться чисельні рішення системи рівнянь на заданих інтервалах часу, що, власне, відтворює динаміку реальних екологічних процесів. На основі чисельних рішень такої

системи рівнянь можна визначити поведінку системи в майбутньому та її можливі реакції на ті чи інші зміни вихідних параметрів.

Останнім часом зростає увага до імовірнісних схем моделювання, що включають випадкові компоненти, що здатні відобразити та передбачити мінливість і адаптивні можливості екологічних систем. Математична природа стохастичних моделей значно складніша, але багато в чому аналогічна до детермінованих моделей.

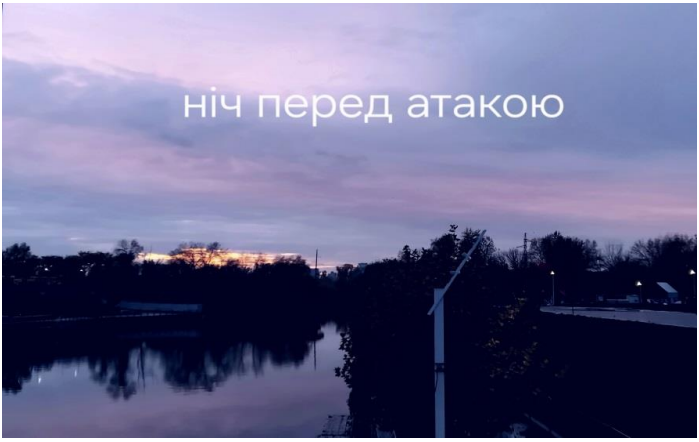


Рисунок 1. – Природа завмирає в очікуванні нічної атаки

Для побудови імітаційних моделей детермінованого або ймовірнісного типу необхідно одержати певну вихідну інформацію (дані моніторингу), отриману в результаті експериментів або спостережень. Етапи, пов'язані з підготовкою інформації, мають складати істотну частину єдиної програми досліджень. Якщо певних даних не вистачає, залишається можливість додатково скористатися експертними оцінками, одержаними за допомогою компетентних фахівців із відповідної галузі.

Уточнюючи параметри моделі і рівняння, зіставляючи їх із емпіричними даними, можна побудувати стійку динамічну модель, що досить точно відображує реальний природний процес. Така модель дозволяє визначати тенденції розвитку або руйнівних змін досліджуваної системи для заданого інтервалу часу. Результати моделювання традиційно представляють в вигляді графіків, що відображують динаміку значень окремих параметрів.

Для якісного дослідження динамічних моделей запропоновано методи якісної теорії диференціальних рівнянь [5], де поведінка складної системи представлена як динаміка траєкторій у фазовому просторі. Візуальні образи досліджуваних траєкторій (фазові портрети) на площині або в тривимірному просторі забезпечують можливості для аналізу і прийняття рішень на основі спостережень за динамікою стану системи на екрані в реальному часі.

Якщо методи якісної теорії диференціальних рівнянь обмежується лише дослідженням системи двох рівнянь, то фазовий портрет екологічної системи для більшого числа вимірів можемо одержати за допомогою переходу до факторного простору, який можна побудувати на основі невеликої кількості найбільш інформативних параметрів [6, 7].

Особливості аналізу резильєнтності природних систем

Для природних систем поняття резильєнтності має більш широкий діапазон застосування, ніж стійкість. Нагадаємо, що *стійкость* можна розглядати як природну здатність екологічної системи поглинати негативні впливи або протистояти збуренням та шкідливим чинникам, залишаючись у межах певного режиму, тобто зберігаючи свою структуру і функції.

З іншого боку, поняття *резильєнтності* на екологічному рівні включає додаткові можливості для переходу на інші режими, або енергетичні рівні існування, що дозволяє підтримувати життєдіяльність і виконувати свої основні функції. Тобто резильєнтність визначає більше можливостей для адаптації екологічних систем. З позицій математичного моделювання це здатність за рахунок певних механізмів підтримувати стан рівноваги (баланс всіх складових) на відповідному рівні для даного діапазону значень.

Адаптацію до нових умов можна визначити як особливий механізм пристосування, або налаштування, що забезпечує екологічній системі певну стабільність відповідно змінам умов зовнішнього середовища. Якщо відомі характеристики щодо змін середовища, можна передбачити тенденції у зміні параметрів такої системи. Її динаміка буде обмежена тим «коридором» значень, що відповідають коливанням зовнішніх факторів.

Зокрема, для дослідження процесу адаптації системи в умовах високого ризику слід визначити значення параметрів, що відповідають імовірним максимальним навантаженням на цю систему. Якщо у встановлених межах система зберігає стабільне положення або рухається у напрямку стабілізації, то можна говорити про стійкість до заданих навантажень. Резильєнтна система природного походження може активувати особливі засоби адаптації, які відрізняють живі організми від технічних систем. Відповідні механізми багато віків удосконалювались в процесі еволюції живої матерії.

Але головною особливістю живих організмів і природних систем є здатність до створення нових механізмів адаптації, які виникають на фоні неочікуваних небезпечних подій. Зокрема, ми знаємо приклади виживання і навіть появи нових видів в зоні аварії на Чорнобильській АЕС.

Засоби оцінювання резильєнтності природних систем.

В екологічних системах важливу роль відіграє поняття *гомеостáз*у, що характеризує певну здатність відкритої системи забезпечувати стабільність свого внутрішнього стану за допомогою відповідних реакцій (зворотних зв'язків), спрямованих на підтримку стану динамічної рівноваги [4, 6].

На формальному рівні стабільний (або стійкий) стан можна уявити як досить малу імовірність порушень гомеостазу протягом певного проміжку часу. Але можна визначити певне критичне значення зовнішнього впливу

(граничний стан), перехід через яке призводить до різкої якісної зміни структури системи – *біфуркації* (стрибкоподібного процесу). В такій ситуації перехід у новий стан вже не буде однозначним, тому що біфуркації утворюють розгалуження, тобто декілька можливих шляхів для подальшого функціонування. Вибір одного з них залежить від випадкових впливів, які породжуються флуктуаціями довкілля в момент біфуркаційного переходу.

Математичне моделювання подібних процесів детально досліджується в теорії катастроф, яка включає математичні засоби для аналізу особливостей та біфуркацій в поведінці динамічних систем різної природи [8].

На перших етапах аналізу необхідно визначити основні параметри, які характеризують поточний стан, їх критичні значення а також зовнішні навантаження внаслідок вибухів, пожеж, руйнувань або інших катаклізмів, що утворюють найбільші ризики для природних ресурсів в зоні враження.

В [5] представлено ряд математичних моделей водних та аграрних екосистем, що потрапили під вплив аварійних викидів внаслідок катастрофи на ЧАЕС. В результаті моделювання було показано, що окремі системи після біфуркації можуть досить швидко відновлювати свої функції за рахунок внутрішніх механізмів адаптації до нових навантажень

Для аналізу і оцінювання резильєнтності природних систем на основі математичного моделювання можна адаптувати імовірнісні моделі подання знань, розроблені для задач екологічної безпеки (зокрема, задач оцінювання рівня забруднення повітря). Розроблений підхід включає універсальні засоби аналізу та візуалізації екологічної інформації з різних джерел.

1. Николис Дж. Динамика иерархических систем: Эволюционное представление. – Мир, 1989. – 488 с.
2. Nikolis, G., Prigogine, I. Exploring complexity: An introduction. W.H. Freeman and Company, New York, 1989. – 328 с.
3. Николис Дж. Динамика иерархических систем: Эволюционное представление. – Мир, 1989. – 488 с.
4. Джефферс Дж, Системный анализ и стратегии моделирования в экологии // Математические модели контроля загрязнения воды. – Мир, 1981. С. 439- 463.
5. Эрроусмит Д., Плейс К. Обыкновенные дифференциальные уравнения. Качественная теория с приложениями. – Мир, 1986. – 243 с.
6. Сердюцкая Л. Ф., Каменева И. П. Системный анализ и математическое моделирование медико-экологических последствий аварии на ЧАЭС и других техногенных воздействий. – "Медэкол", 2000. – 173 с.
7. Каменева І.П., Артемчук В.О. Проблема інформативності та визначення інформативних структур для підтримки прийняття рішень в галузі екологічної безпеки // Електронне моделювання, 2022, 44, № 3, с. 50-64.
8. Gilmore R. Catastrophe Theory for Scientists and Engineers. John Wiley & Sons Inc., 1981. – 686 с.

Ye. Chychykalo, V. Shendryk, Yu. Parfenenko

A USE CASE OF DIGITAL TWIN TECHNOLOGY FOR PROACTIVE ENERGY SUPPLY MANAGEMENT FOR ACTIVE ELECTRICITY CONSUMERS FROM RENEWABLE SOURCES

Recently, a trend towards decentralized energy systems keeps growing. It drives the need in new technologies that have capabilities to provide effective energy management. Digital Twin is an important tool for improving the adaptability and sustainability of modern energy infrastructure. It implements a dynamic virtual copy of a real physical energy system and provides system status monitoring in real time, conducts data-based analysis and makes proactive decisions [1]. This solution is quite relevant for active users of electricity, who produce electricity using alternative energy sources, such as solar and (or) wind.

Proactive management of energy distribution for such users creates both new opportunities and certain challenges. Among which, the instability of renewable energy production, demand fluctuations and limitations of traditional forecasting methods require new digital tools capable of integrating data flow analysis and proactive decision-making algorithms [2]. Digital Twin technology provides a single framework that integrates monitoring, simulation models, artificial intelligence algorithms for forecasting energy inputs and outputs, optimizing the use of stored energy, decision support during autonomous system management.

This study focuses on developing conceptual and experimental models, their optimization for low power computers. These models will show modeling, prediction and optimization capabilities of Digital Twin in an autonomous energy system with alternative energy sources. This will demonstrate how a virtual copy of the system, constant feedback between the physical and digital environments ensures high stability and efficiency of energy supply processes.

The Digital Twin will be developed based on a typical assembly including solar panel, LiFePo4 batteries and MPPT solar charge controller and will be responsible for proactive control of this autonomous power system. The simulation model will partially run on an energy-efficient microcomputer and will be integrated into a test energy system using a set of sensors for monitoring key indicators. Those sensors will be main suppliers of real time data for Digital Twin computing, analytics and decision-making models. Experiments will be conducted to simulate various environmental conditions and to test system behavior in predictable and extreme scenarios.

1. Song, Z.et al. (2023). Digital Twins for the Future Power System: An Overview and a Future Perspective.
2. David, I. et al. (2024). Digital Twin Evolution for Sustainable Smart Ecosystems. ACM/IEEE International Conference on Model Driven Engineering Languages and Systems.

О.А. Снєосіков, О.П. Нарєжній

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ КІБЕРАТАКАМ ТИПУ GPS SPOOFING І GPS JAMMING З ВИКОРИСТАННЯМ AI ДЛЯ АВТОНОМНОЇ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ

Надійність глобальних навігаційних супутникових систем є критично важливою для критичної інфраструктури. Проте, такі кіберзагрози на GNSS, як GPS spoofing та GPS jamming, становлять серйозну небезпеку, здатну спричинити порушення працездатності навігації, що несе певний ризик для авіації, морського транспорту, геодезії тощо [1, 2, 3]. Ця проблема є особливо актуальною для автономних систем диференційної корекції (АСДК), де безпека користувачів безпосередньо залежить від точності GNSS сигналів.

Традиційні підходи до захисту від кіберзагроз, включно зі статистичними та геометричними методами, не завжди здатні забезпечити необхідну швидкість та гнучкість для протидії кібератакам [2, 4]. На сьогоднішній день технології штучного інтелекту відкривають нові можливості для розробки інтелектуальних систем захисту, здатних аналізувати дані GNSS, виявляти аномалії та прогнозувати загрози в динамічних середовищах [5, 6]. Ця робота призначена для заповнення прогалин в існуючих рішеннях [7-10] шляхом створення прототипу гібридного методу захисту.

Для перевірки ефективності запропонованої системи було розроблено багатокомпонентний підхід, протестований на програмно згенерованому синтетичному наборі даних. Набір даних імітував три сценарії: нормальне функціонування, атаку типу GPS spoofing та атаку GPS jamming, з рівним представленням класів (по 500 записів). Кожен запис містить вісім значущих параметрів, таких як: потужність сигналу (power), затримка сигналу (delay), прискорення (accel), кількість видимих супутників (satellites), частота сигналу (frequency), рівень шуму (noise_level), допплерівське зміщення (doppler_shift) і кут приходу сигналу (angle_of_arrival).

На початковому етапі для виявлення аномалій у даних застосовано алгоритм K-Means з розділенням даних на три кластери. Метод успішно згрупував дані, виділивши кластер зі 100 аномальних сигналів, що відповідає 66.7% від загальної кількості очікуваних аномалій.

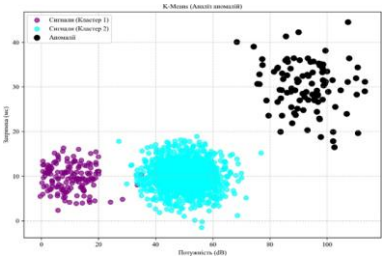


Рисунок 1. – Результати кластеризації K-Means

Для імітації умов реального часу, де дані надходять потоково, було використано модифікацію Онлайн K-Means. Цей алгоритм продемонстрував вищу адаптивність, ідентифікувавши 204 аномалії, що свідчить про його ефективність для систем реального часу.

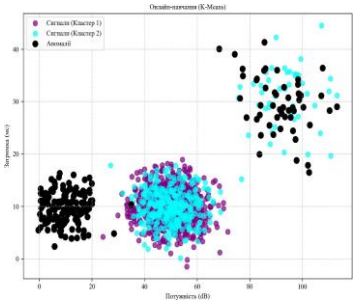


Рисунок 2. – Результати Онлайн K-Means

На наступному рівні захисту було застосовано класифікатор Random Forest. Навчена модель (70% навчання, 30% тестування) виконувала роль фільтра, точно розділяючи сигнали на легітимні та спотворені. Це дозволило значно підвищити загальну надійність системи.

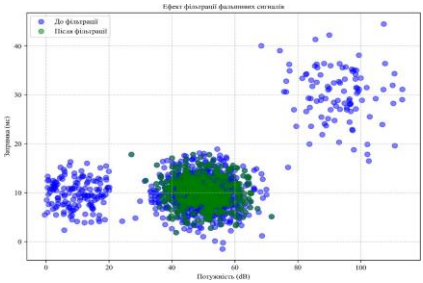


Рисунок 3. – Ефект фільтрації фальшивих сигналів

Прогностичний компонент системи був реалізований за допомогою рекурентної нейронної мережі з GRU-архітектурою (на основі трьох шарів по 128 нейронів кожен). Хоча точність моделі на валідаційному наборі склала 0.51, що є скромним результатом, вона підтвердила концептуальну можливість прогнозування майбутніх атак.

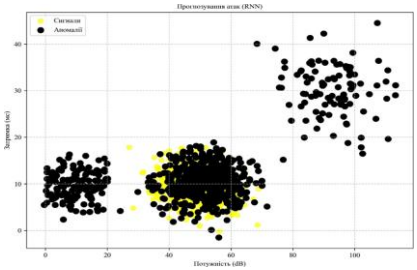


Рисунок 4. – Прогнозування атак за допомогою RNN

У роботі розроблено прототип методів штучного інтелекту для виявлення та протидії кібератакам типу GPS spoofing і GPS jamming для автономної системи диференціальної корекції. Прототип передбачає автоматичне залучення контрзаходів при виявленні загроз. До них належать: адаптивна корекція часу для компенсації затримок (змодельована корекція - 0.14 мс) та перемикання на інерційну навігаційну систему як резервний механізм. Також було змодельоване використання постквантової криптографії для забезпечення довгострокового захисту даних.

Дане дослідження підтверджує життєздатність гібридної AI-моделі для захисту GNSS від атак типу GPS spoofing та GPS jamming. Було продемонстровано, що Онлайн K-Means є ефективним інструментом для виявлення аномалій у потокових даних. Random Forest успішно виконує функцію класифікатора для фільтрації загроз. Результати RNN вказують на необхідність подальшого вдосконалення прогностичної моделі, зокрема шляхом її навчання на реальних даних GNSS.

Запропонований підхід є важливим та перспективним кроком на шляху до створення надійних та адаптивних систем кіберзахисту для автономних систем диференціальної корекції на основі AI-моделей. Майбутні дослідження мають бути спрямовані на роботу з реальними даними та вдосконалення архітектур нейронних мереж.

1. Зоря, І. С., & Марущак, А. В. (2023). Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf?sequence=3&isAllowed=y.
2. Нетаврована, А. (2023). Геометричний метод визначення GPS spoof атак на безпілотні літальні апарати. У Матеріали конференцій МЦНД (22.12.2023,

Одеса, Україна) (с. 316–321). https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/954.

3. Петровський, А. В. (2019). Алгоритм виявлення впливу спуфінгу під час виконавчої прокладки програмними засобами електронної картографічної навігаційно-інформаційної системи. Проблеми інформаційних технологій, 25, 30–38. https://doi.org/10.35546/2313-0687.2019.25.30-38.
4. Волошин, Д. Г., & Бульба, С. С. (2022). Інтелектуальний метод виявлення спуфінгу БПЛА. Сучасні інформаційні системи, 6(1), 88–96. https://doi.org/10.20998/2522-9052.2022.1.15.
5. Мустафаєв, О. В. (2024). Сучасні технології захисту від GPS спуфінгу у системах навігації. Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки, 35(74), №5, 58–61. https://doi.org/10.32782/2663-5941/2024.5.1/10.
6. Сусукайло, В. А. (2024). Розроблення моделі системи дослідження кіберзлочинів для складових інфраструктури інформаційних систем (Дисертація на здобуття ступеня доктора філософії, Національний університет «Львівська політехніка»). https://lpnu.ua/sites/default/files/2024/radaphd/27650/disertaciya-susukailo-va-1.pdf.
7. Radoš, K., Brkić, M., & Begušić, D. (2024). Recent advances on jamming and spoofing detection in GNSS. Sensors, 24(13), 4210. https://doi.org/10.3390/s24134210.
8. Siavash, J., & Ping, W. (2024). Intelligent anti-jamming based on deep reinforcement learning and transfer learning. IEEE Transactions on Vehicular Technology, 1–10. https://doi.org/10.1109/TVT.2024.3359426.
9. Alkhatib, M., McCormick, M., Williams, L., Leon, A., Camerano, L., Al, K., Devabhaktuni, V. K., Kaabouch, N., Svm, D., & Regularization, L. (2024). Classification and source location indication of jamming attacks targeting UAVs via multi-output multiclass machine learning modeling. У 2024 IEEE International Conference on Consumer Electronics (ICCE) (с. 1–5). https://ieeexplore.ieee.org/document/10444388.
10. Mohanty, A., & Gao, G. (2024). A survey of machine learning techniques for improving global navigation satellite systems. EURASIP Journal on Advances in Signal Processing, 1–40. https://asp-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13634-024-01167-7.pdf.

С.Б. Бурченко, І.І. Сватовський

МОДЕЛЬ УПРАВЛІННЯ РЕЗИЛЬЄНТНІСТЮ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ЕПОХУ КВАНТОВИХ ТЕХНОЛОГІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ

У сучасному світіпоняття резильєнтності змінюється, відходячи від традиційної концепції "відновлення" до більш динамічної та проактивної моделі. Також сучасна критична інфраструктура повинна розглядатися не як ізольовані фізичні системи, а як складні адаптивні системи (CAC), де цифрова трансформація створила безпрецедентний рівень взаємозв'язків і, як наслідок, нові вектори системних ризиків.Основою для розуміння сучасної резильєнтності є визначення Національного інституту стандартів і технологій США (NIST)[1-3].Резильєнтність визначається як здатність системи підтримувати необхідний функціонал в умовах несприятливих впливів, навіть у деградованому стані, та відновлюватися до ефективного операційного стану в часових рамках, що відповідають місійним потребам.[1] Це обумовлює ключовий принцип: резильєнтність — це не про запобігання збоям, а про їх адекватне управління.

Загальна концепція резильєнтності розширюється чотирма стратегічними принципами кіберрезильєнтності, визначеними NIST: Передбачати (Anticipate), Витримувати (Withstand), Відновлювати (Recover) та Адаптуватися (Adapt).[3] Цей фреймворк забезпечує структурований підхід до резильєнтності як до безперервного життєвого циклу, а не статичного стану. Він включає превентивні заходи, такі як планування загроз, створення систем, здатних витримувати пошкодження, стратегії швидкого відновлення та, що найважливіше, адаптацію шляхом усунення вразливостей та перегляду архітектури.

Для повного розуміння необхідно розглядати критичну інфраструктуру через призму складних адаптивних систем. З цієї точки зору, складність є необхідною умовою для резильєнтності, оскільки вона дозволяє складовим агентам системи володіти адаптивною спроможністю.[4] Резильєнтна система не просто повертається до початкового стану; вона навчається на основі збоїв, щоб краще справлятися з подібними подіями в майбутньому, змінюючи свою функцію, залишаючись при цьому тим самим *типом* системи.[4] Ця здатність до навчання та еволюції є ядром проактивної резильєнтності.

Цифрова трансформація є значущим глобальним фактором для критичної інфраструктури.[7] З одного боку, такі технології, як Інтернет речей (IoT), аналітика великих даних та хмарні обчислення, значно підвищують операційну ефективність. Вони уможливлюють предиктивне обслуговування, оптимізують прийняття рішень та покращують надійність послуг у таких секторах, як енергетика та водопостачання.[7] Інтеграція

цифрових технологій фундаментально змінює спосіб функціонування організацій та їх взаємодії зі стейкхолдерами.

З іншого боку, ця гіперзв'язаність кардинально змінює ландшафт ризиків. Вона розмиває традиційні периметри безпеки, створюючи величезну, розгалужену цифрову поверхню атаки, де єдина вразливість у бібліотеці з відкритим кодом або скомпрометований постачальник може мати каскадні, системні наслідки.[7] Застарілі системи SCADA замінюються на взаємопов'язані кіберфізичні системи, що додає нові вектори ризику, яких раніше не існувало. Цей парадокс полягає в тому, що самі інструменти, які використовуються для підвищення ефективності та резильєнтності, одночасно створюють нові, часто непередбачувані, вразливості. Тобто досягнення резильєнтності не може бути кінцевою метою; це має бути безперервний процес адаптації та ребалансування між операційною ефективністю, технологічними інноваціями та ризиками, що еволюціонують. Мета операторів критичної інфраструктури повинна полягати не в досягненні фінального "резильєнтного стану", а в розбудові організаційної та технічної спроможності для управління *динамічною рівновагою*.

Для управління цією новою реальністю пропонується фреймворк динамічних спроможностей (Dynamic Capabilities, DCs), який складається з трьох основних процесів: Відчуття (Sensing) — ідентифікація загроз та можливостей, Захоплення (Seizing) — мобілізація ресурсів для їх вирішення, та Трансформація (Transforming) — постійне оновлення та реконфігурація ресурсів.[12] Ця модель надає операційний план для організацій, що дозволяє розбудовувати адаптивну спроможність, необхідну для справжньої резильєнтності в середовищі, що постійно змінюється. "Відчуття" дозволяє установам критичної інфраструктури виявляти кіберзагрози, "захоплення" — швидко реагувати на них, а "трансформація" — постійно оновлювати свої ресурси та стратегії для відповіді на нові виклики.

Далі наведено результати аналізу двох найбільш значущих загроз для критичної інфраструктури, що змінюють її парадигму:

1. безпосередня та зростаюча небезпека кібератак, керованих штучним інтелектом;
2. довгострокова загроза повномасштабних квантових комп'ютерів.

По-перше у кіберпросторі супротивники все частіше використовують штучний інтелект для подолання традиційних засобів захисту. ШІ дозволяє автоматизувати весь життєвий цикл атаки, від ефективної розвідки та збору даних для гіперперсоналізованих фішингових кампаній до створення адаптивного шкідливого програмного забезпечення, яке еволюціонує для ухилення від виявлення.[13] За оцінками, до 40% усіх кібератак вже керуються ШІ, що дозволяє створювати більш правдоподібні спам-повідомлення та інфільтративне шкідливе ПЗ.[13]

Загроза виходить за межі крадіжки даних і поширюється на маніпуляцію самими моделями ШІ через атаки отруєння (poisoning) та ухилення (evasion), що може скомпрометувати ті самі системи, які

призначені для захисту інфраструктури.[14] Це створює сценарій "війни машин проти машин", де тактичні рішення приймаються з машинною швидкістю, роблячи застарілими захисні механізми з участю людини.[13] Економічний та соціальний вплив є приголомшливим: за прогнозами, глобальні збитки від кіберзагроз сягнуть 20 трильйонів доларів США щорічно до 2030 року.[10] Критичні сектори, такі як нафтогазовий, є основними цілями через їх економічну важливість та потенціал для фізичних руйнувань.[11]

По-друге безпека більшості сучасних цифрових комунікацій, включаючи криптографію з відкритим ключем (public-key cryptography, PKC), базується на математичних задачах, які є нерозв'язними для класичних комп'ютерів, але стають досяжними для майбутніх повномасштабних квантових комп'ютерів.[15]Основна небезпека полягає у сутності атаки "Збирай зараз, розшифровуй пізніше" (Harvest Now, Decrypt Later, HNDL). Супротивники активно збирають та зберігають зашифровані дані сьогодні, знаючи, що зможуть їх розшифрувати, коли з'явиться повномасштабні квантові комп'ютери.[15] Для критичної інфраструктури це означає, що будь-які чутливі дані з тривалим терміном зберігання (наприклад, інтелектуальна власність, інформація про національну безпеку, креслення інфраструктури) вже перебувають під загрозою.

Терміни появи повномасштабних квантових комп'ютерів є невизначеними, з оцінками від кількох років до десятиліття.[17] Однак тривалий час, необхідний для міграції складних криптографічних систем (10-20 років), означає, що перехід на квантово-стійкі рішення має розпочатися негайно.[17]

Таким чином ці дві загрози не є окремими; вони діють синергетично. ШІ робить фазу "збору" в атаці HNDL експоненціально ефективнішою та масштабнішою. Сучасний зловмисник може використовувати ШІ *сьогодні* для ефективного збору величезних обсягів зашифрованих даних з об'єктів критичної інфраструктури. ШІ може ідентифікувати потоки даних високої цінності та автоматизувати їх викрадення та зберігання. Зібрані дані потім утримуються до появи повномасштабних квантових комп'ютерів для розшифрування, реалізуючи загрозу HNDL у безпрецедентному масштабі. Це означає, що квантова загроза — це не просто майбутня проблема для криптографів, а нагальна проблема безпеки даних для всіх операторів критичної інфраструктури. Таким чином, нагальність міграції на постквантову криптографію посилюється поточними можливостями ШІ.

Для захисту від таких та других, також важливих загроз, пропонується Інтегрована модель управління резильєнтністю.Данабагатошарова модель управління резильєнтністю побудована на життєвому циклі CISA/NIST: Встановити цілі -> Оцінити ризики -> Планувати та тренуватися -> Постійно вдосконалюватися.[29] Технологічні та архітектурні напрямки, обговорені раніше, інтегруються в життєвий цикл.

- **Шар 1: Фундаментальна архітектура (гібридна мультихмара):** Базовий шар, що забезпечує географічну надлишковість, високу доступність та мобільність робочих навантажень.
- **Шар 2: Філософія безпеки (архітектура нульової довіри):** Рівень управління, що регулює весь доступ на основі динамічних, орієнтованих на ідентичність політик.
- **Шар 3: Двигун проактивного захисту (ШІ/МН та великі дані):** Інтелектуальний шар, що забезпечує предиктивне виявлення загроз, автоматизоване реагування (SOAR) та безперервну валідацію (цифрові двійники).
- **Шар 4: Захист на майбутнє (постквантова криптографія):** Криптографічний шар, що забезпечує довгострокову цілісність та конфіденційність усієї системи проти квантової загрози.

Чотири напрямки є взаємозалежними та створюють позитивний цикл. Перехід до гібридної мультихмарної архітектури (напрямок 1) робить необхідним підхід нульової довіри (напрямок 2). Впровадження нульової довіри генерує величезну кількість телеметричних даних (журнали доступу, стан пристроїв тощо). Такі дані є необхідним "паливом" для двигуна захисту на основі ШІ/МН (напрямок 3), який, у свою чергу, робить можливим динамічне застосування політик нульової довіри в масштабі. Довгострокова життєздатність усієї системи залежить від цілісності її даних та комунікацій, що може бути гарантовано лише шляхом переходу на PQC (напрямок 4). Таким чином, не чотири окремі ініціативи, а взаємопідсилюючий цикл. Нездатність інвестувати в будь-який з цих напрямків фундаментально послаблює інші, не дозволяючи організації досягти справді проактивної та резильєнтної позиції.

1. Resilience - Glossary | CSRC - NIST ComputerSecurityResourceCenter. веб-сайт. URL:https://csrc.nist.gov/glossary/term/resilience (дата звернення: 20.10.2025).
2. Information system resilience - Glossary | CSRC - NIST Computer Security Resource Center. веб-сайт. URL:https://csrc.nist.gov/glossary/term/information_system_resilience (дата звернення: 20.10.2025).
3. Cyber Resilience | PNNL. веб-сайт. URL:https://www.pnnl.gov/explainer-articles/cyber-resilience (дата звернення: 20.10.2025).
4. The need for general adaptivecapacity—Discussing resilience with complex adaptive systems theory - PMC - PubMedCentral.веб-сайт.URL:https://pmc.ncbi.nlm.nih.gov/articles/PMC12369295/ (дата звернення: 20.10.2025).
5. Engineering Resilient Complex Systems: TheNecessaryShiftTowardComplexityScience.веб-сайт. URL:https://www.researchgate.net/publication/337918662_Engineering_Resilient_Complex_Systems_The_Necessary_Shift_Toward_Complexity_Science. (дата звернення: 20.10.2025).

6. Digital Transformation of Infrastructure Systems: Convergence of Digital Innovation and Cyber-physicalResilience – Research Gate. веб-сайт.URL:https://www.researchgate.net/publication/389717035_Digital_Transformation_of_Infrastructure_Systems_Convergence_of_Digital_Innovation_and_Cyber-physical_Resilience (дата звернення: 20.10.2025).
7. The Impact Of Digitalization On Critical Infrastructure Security – Mirror Review.веб-сайт.URL:https://www.mirrorreview.com/impact-of-digitalization/(дата звернення: 20.10.2025).
8. The Impact of Digital Transformation on Organizational Resilience: The Role of Innovation Capability and AgileResponse – MDPI.веб-сайт.URL:https://www.mdpi.com/2079-8954/13/2/75 (дата звернення: 20.10.2025).
9. Securing the digital future: Cyber resilience and trust in the AI age | World Economic Forum.веб-сайт.URL:https://www.weforum.org/stories/2025/10/securing-digital-future-cyber-resilience-trust-ai-age-gfc-amgfcc/ (дата звернення: 20.10.2025).
10. Rock well research flags cyber threats as a top driver of technology in vestment across oil and gas.веб-сайт.URL:https://industrialcyber.co/reports/rockwell-research-flags-cyber-threats-as-a-top-driver-of-technology-investment-across-oil-and-gas/(дата звернення: 20.10.2025).
11. Full article: Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach.веб-сайт.URL:https://www.tandfonline.com/doi/full/10.1080/12460125.2025.2479546 (дата звернення: 20.10.2025).
12. Emerging Threatsto Critical Infrastructure: AI Driven Cybersecurity Trendsfor 2025.веб-сайт.URL:https://www.captechu.edu/blog/ai-driven-cybersecurity-trends-2025 (дата звернення: 20.10.2025).
13. Most Common AI-Powered Cyber attacks | Crowd Strike. веб-сайт. URL:https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/ (дата звернення: 20.10.2025).
14. National Security Agency | Frequently Asked Questions Quantum Computing and Post-Quantum Cryptography–DoD. URL: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF (дата звернення: 20.10.2025).
15. Quantum Computing, Cyber Security and Cryptography: Issues, Technologies, Algorithms, Programming and Strategie/ S.B. Goyal and al. Springer, 2025. 506 p. URL: https://link.springer.com/book/10.1007/978-981-96-4948-8 (дата звернення: 20.10.2025).
16. The NIST standards for quantum-safe cryptography | DigiCert.веб-сайт.URL:https://www.digicert.com/blog/nist-standards-for-quantum-safe-cryptography (дата звернення: 20.10.2025).
17. Post Quantum Cryptography algorithm sexplained – Quside.веб-сайт.URL:https://quside.com/post-quantum-cryptography-algorithms-explained/ (дата звернення: 20.10.2025).
18. Post-Quantum Cryptography Initiative | CISA. веб-сайт.URL:https://www.cisa.gov/quantum (дата звернення: 20.10.2025)
19. NIST Releases First 3 Finalized Post-Quantum Encryption Standards.веб-сайт.URL:https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (дата звернення: 20.10.2025).
20. AnIn-Depth Look at NIST's Post-Quantum Algorithms – EntropiQ.веб-сайт.URL:https://entropiq.com/nist-post-quantum-algorithms/ (дата звернення: 20.10.2025).

21. Artificial Intelligence (AI) in Cybersecurity: The Future of Thre at Defense – Fortinet.веб-сайт.URL:https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity (дата звернення: 20.10.2025)
22. Emerging Technology and Risk Analysis: Artificial Intelligence and Critical Infrastructure– RAND. URL:https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2800/RRA2873-1/RAND_RRA2873-1.pdf (дата звернення: 20.10.2025).
23. Transforming Cybersecurity in to Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence – MDPI.веб-сайт.URL:https://www.mdpi.com/2079-8954/12/5/165 (дата звернення: 20.10.2025).
24. Artificial Intelligence (AI) Cybersecurity – IBM.веб-сайт.URL:https://www.ibm.com/solutions/ai-cybersecurity (дата звернення: 20.10.2025).
25. North western Security and AI Lab Releases New Terrorism Early Warning System Forecasts. веб-сайт.URL:https://www.mccormick.northwestern.edu/news/articles/2024/11/northwestern-security-and-ai-lab-releases-new-terrorism-early-warning-system-forecasts/ (дата звернення: 20.10.2025).
26. CISA Artificial Intelligence Use Cases. веб-сайт.URL:https://www.cisa.gov/ai/cisa-use-cases (дата звернення: 20.10.2025).
27. Cybersecurity and Infrastructure SecurityAgency – AI Us eCases. веб-сайт.URL:https://www.dhs.gov/ai/use-case-inventory/cisa (дата звернення: 20.10.2025).
28. The NIST Cybersecurity Framework (CSF) 2.0 . URL:https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 20.10.2025).
29. NIPP Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach - CISA . URL:https://www.cisa.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf (дата звернення: 20.10.2025).
30. Whatisthe ENISA framework? | Answers - 6clicks. веб-сайт.URL:https://www.6clicks.com/resources/answers/what-is-the-enisa-framework (дата звернення: 20.10.2025).
31. ENISA NIS360: IsEurope Protecting the Right Sectors? - IndustrialCyber . веб-сайт.URL:https://industrialcyber.co/analysis/enisa-nis360-is-europe-protecting-the-right-sectors/ (дата звернення: 20.10.2025).

А.В. Ільєнко, В.А. Телющенко

МЕТОДИКА РАНЖУВАННЯ ПІДХОДІВ ДО ОЦІНКИ КІБЕРРИЗИКІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЦИВІЛЬНОЇ АВІАЦІЇ

Цивільна авіація (ЦА) належить до критичної інфраструктури, чиє функціонування залежить від складних інформаційно-комунікаційних систем (ІКС), що забезпечують планування, управління та моніторинг у реальному часі. До них належать системи аеропортових операцій, корпоративні мережі, операційні сервіси підтримки, а також керуючі підсистеми інфраструктури, тощо. Одночасно загрози стають більш системними (відмови сервісів, програм-вимагачів, експлуатації вразливостей у ланцюгах постачання), що вже призводить до затримок рейсів, перебоїв у наземному обслуговуванні та фінансових втрат. Операторам критичної інфраструктури ЦА необхідно не просто формально оцінити кіберризики, а й забезпечити абсолютну прозорість та обґрунтованість процесу вибору релевантного методологічного інструменту оцінки ризиків ІКС.

Мета

Проаналізувати наявні методи розрахунку кіберризиків ІКС та сформувати аргументований підхід до вибору методики оцінювання кіберризиків в ІКС цивільної авіації.

Виклад основного матеріалу

Для авіаційної галузі сформувалося узгоджене поле обов'язкових вимог до кібербезпеки. Держави ЄС мають виконувати Директиву NIS2 [1], яка підвищує планку управління ризиками та звітності для «важливих» і «суттєвих» суб'єктів, в тому числі у транспорті.

EASA Part-IS встановлює конкретні строки дотримання вимог, фактично зобов'язуючи аеропорти, організації та інфраструктуру, залучені до забезпечення авіаційних перевезень і наземного обслуговування, будувати систему управління інформаційною безпекою (СУІБ) на ризик-орієнтованих засадах. [2]

Всі ці фактори підводять до того, що галузі потрібен чіткий, прозорий і придатний до аудиту підхід, який допомагає обирати методи оцінювання ризиків і визначати пріоритети заходів, узгоджуючи це з вимогами безпеки польотів та наявними ресурсами та регуляторними вимогами.

Численні міжнародні стандарти та методології пропонують підходи до оцінювання кіберризиків. Серед них:

- Концептуальні стандарти (ISO/IEC 27005, ISO 31000): Встановлюють уніфікований процес управління ризиками (встановлення контексту, оцінка, обробка, моніторинг), але є методологічно гнучкими і прямо не визначають конкретний інструментарій оцінки.

- Деталізовані фреймворки (NIST SP 800-30, CRAMM, EBIOS, OCTAVE, TARA) надають конкретні кроки для ідентифікації загроз, вразливостей та обчислення ризику, але істотно різняться за ключовими параметрами.

Проблема полягає у відсутності універсального інструменту, який відповідав би потребам авіаційної галузі. Наявні методики не є універсальними і мають свої різні рівні деталізації процесу управління ризиками. Зокрема, одні вирізняються простотою впровадження та прийнятною ресурсоємністю, інші забезпечують глибший аналіз складних сценаріїв чи узгодження з міжнародними та галузевими вимогами.

Тому для СУІБ цивільної авіації потрібен узагальнений, прозорний і об'єктивний інструмент ранжування, що з урахуванням контексту організації дозволяє раціонально обирати чи поєднувати релевантні методики.

Доцільно застосувати багатокритеріальний підхід **(**Multi-Criteria Analysis**,** MCA) із моделлю зваженої суми (Weighted Sum Model, WSM), який зводить експертні оцінки за кількома критеріями до єдиного інтегрального показника та дозволяє ранжувати фреймворки за придатністю.

MCA узгоджує різні цілі, такі як відповідність стандартам, глибину та повноту аналізу, гнучкість застосування, операційні витрати та часові обмеження.

Пропонуємо розробити універсальний і «легкий» до впровадження метод WSM для ІКС цивільної авіації, який буде спиратеся на чітко визначений набір критеріїв, наприклад таких як відповідність, гнучкість, глибина, впроваджуваність, ресурси з уніфікованими шкалами та нормуванням. Ваги визначаємо за фіксованими правилами, використовуючи, наприклад, узгоджені оцінки експертів чи метод аналізу ієрархій, (MAI), щоб результат можна відтворити під час аудиту.

Метод аналізу ієрархій (MAI) - це формальна процедура попарних порівнянь, що перетворює експертні судження про відносну важливість критеріїв або альтернатив у числові ваги (пріоритети).

На рис. 1 показано узгоджену схему застосування WSM. Спочатку визначається контекс цілей та ідентифікуються системи, від яких залежить безперебійна робота організації, виділяють критерії та визначають важливість критерію, присвоєнням кожному певного вагового коефіцієнта. Далі, збираються дані для оцінки ризиків, отримані з різних джерел, таких як ENISA Threat Landscape (TL), бази даних CVE, тощо, приводятья до єдиних шкал для забезпечення їх порівнянності та обчислюється інтегральний бал WSM за формулою:

$$S_i := \sum_{j=1}^{m} W_j x_{ij} \tag{1}$$

де, S_i - інтегральний бал альтернативи

W_j - вага критерію;

x_{ij} - нормована оцінка за критерієм. Проводиться локальна перевірка чутливості для оцінки впливу зміни ваг критеріїв на результат.

Рисунок 1. – Схема застосування WSM при оцінці ризиків ІКС

На виході отримуємо вибір чи комбінацію методик, пороги прийнятності ризиків, план обробки ризиків. Далі проводиться аудит або впроваджується система управління інформаційною безпекою (СУІБ).

Застосування WSM забезпечує прозорість і простоту, так як підсумковий бал рахується як сума зважених оцінок за ключовими критеріями, тож логіка рішення зрозуміла керівникам. Ваги можна швидко змінювати під актуальні пріоритети, не перебудовуючи всю схему, тобто модель є гнучкою. І як результат, нормований інтегральний бал дає змогу коректно порівнювати методики та переводити числові значення у зрозумілі управлінські категорії для прийняття рішень («рекомендовано», «умовно рекомендовано», тощо).

Висновок.

Запропонований підхід встановлює чіткі й однакові правила вибору методик оцінювання кіберризиків для ІКС ЦА та забезпечує прозоре простеження всіх кроків рішення: від визначення критеріїв і ваг до нормованих оцінок і підсумкового бала. Застосування WSM дає практичні, обґрунтовані рекомендації для побудови ефективної СУІБ, узгодженої з вимогами EASA Part-IS і NIS2.

1. European Parliament, & Council of the European Union. (2022, December 14). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
2. European Commission. (2023, January 30). Commission Implementing Regulation (EU) 2023/203 laying down requirements for the management of information security risks with a potential impact on aviation safety (Part-IS). https://www.easa.europa.eu/en/document-library/regulations/commission-implementing-regulation-eu-2023203.
3. International Organization for Standardization. (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection—Guidance on information security risk management. https://www.iso.org/standard/80585.htm.

В.В. Шкарупило, В.В. Душеба

ЩОДО АСПЕКТІВ РОЗГЛЯДУ РЕЗИЛІЄНТНОСТІ З ПОЗИЦІЇ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ

Концепція резилієнтності розглядається в контексті кіберфізичних систем критичного призначення, у тому числі систем, призначених до застосування при вирішенні задач енергетики.

Означену концепцію пропонується опрацьовувати з точки зору інтерпретації поняття функційної безпечності, визначеного у стандарті ДСТУ EN 61508-5:2019 [1], що полягає у здатності системи реалізовувати власні функції в усіх передбачених проєктом режимах й умовах експлуатації [2].

Енергетичну інфраструктуру пропонується охоплювати з дотриманням наступних позицій: розгляд названої інфраструктури як кіберфізичної системи [3]; проведення стратифікації з метою уніфікації процесу зміщення від опрацювання резилієнтності на рівні системи до рівнів підсистем і навпаки [4–7].

У якості відмінної риси, притаманної саме енергосистемі України, розглядається деструктивний вплив, спричинений неспровокованим повномасштабним вторгненням країни-агресора зі Сходу [8].

Відповідно до згаданого визначення поняття функційної безпечності висувається припущення, що здатність кіберфізичної системи реалізовувати власні функції у передбачених режимах і умовах експлуатації залежить, у тому числі, від ступеню зазначеного деструктивного впливу, який поширюється на рівні і кібернетичний [9], і фізичний [10].

Пропонується оцінювати резилієнтність критичної енергетичної інфраструктури у частині відповідної складової – здатності до абсорбції небажаних впливів зовнішніх факторів – з урахуванням прояву означених впливів у контексті інтерпретації поняття функційної безпечності.

Дослідження проведено в 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»; 0125U002837 «Розвинення теоретичних засад забезпечення резильєнтності критичної енергетичної інфраструктури»; W911NF-22-2-0153 research work, funded by the US Army Engineer Research and Development Center (ERDC).

1. ДСТУ EN 61508-3:2019. (2019). Функційна безпечність електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT). [Чинний від 2019-09-01]. URL: https://zakon.rada.gov.ua/rada/show/v0249774-19#Text.

2. Про затвердження Вимог з ядерної та радіаційної безпеки до інформаційних та керуючих систем, важливих для безпеки атомних станцій: наказ Державної інспекції ядерного регулювання від 22.07.2015 № 140, із змінами, внесеними згідно з Наказом Державної інспекції ядерного регулювання № 508 від 25.11.2019. (2020). URL: https://zakon.rada.gov.ua/laws/show/z0954-15/ed20200109#n880.
3. Shkarupylo, V.V., Kudermetov, R.K., & Polska, O.V. (2018). On the approaches to cyber-physical systems simulation. *Advances in Cyber-Physical Systems (ACPS)*, 3(1), 51–54. https://doi.org/10.23939/acps2018.01.051.
4. Shkarupylo, V., Chemerys, O., Artemchuk, V., Alsayaydeh, J., Kudermetov, R., & Polska, O. (2024). Comprehensive stratified approach to energy resilience solutions taxonomy: a Ukraine scenario. Proc. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 1–8). IEEE. https://doi.org/10.1109/DESSERT65323.2024.11122234.
5. Шкарупило, В.В., Душеба, В.В., & Чемерис, О.А. (2024). Щодо тривимірної концепції опрацювання резилієнтності енергетичної інфраструктури. *Безпека енергетики в епоху цифрової трансформації: Шоста науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України*, (с. 176–177). ІПМЕ ім. Г.Є. Пухова НАН України. https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bevect-2024/.
6. Шкарупило, В.В., Чемерис, О.А., & Душеба, В.В. (2024). Стратифікований підхід до опрацювання резилієнтності у галузі енергетики. *Збірник матеріалів XLII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* (с. 54–55). ІПМЕ ім. Г.Є. Пухова НАН України. https://ipme.kiev.ua/konferencii/konferenciya-molodix-vchenix-2024/.
7. Шкарупило, В.В., Душеба, В.В., & Тіменко, А.В. (2023). Огляд рівнів забезпечення резилієнтності у галузі енергетики. *Survivability & Resilience – 2023: collection of materials of the international scientific and practical conference* (с. 33–34). ІПМЕ ім. Г.Є. Пухова НАН України. https://ipme.kiev.ua/konferencii/zhivuchist-ta-rezilyentnist-2023/.
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. Pricop, A.-I., Gavrilaş, M., Sălceanu, A., & Neagu, B.-C. (2023). Power systems resilience against cyber-attacks. A systematic analysis. Proc. *2023 10th International Conference on Modern Power Systems, MPS 2023*. IEEE. https://doi.org/10.1109/MPS58874.2023.10187420.
10. Nikolaieva, I., & Zwijnenburg, W. (2022). *Risks and impacts from attacks on energy infrastructure in Ukraine*. PAX report. https://paxforpeace.nl/wp-content/uploads/sites/2/import/2023-01/PAX_Ukraine_energy_infrastructure_FIN.pdf.

С.В. Кулик, А.В. Давидюк

БАГАТОРІВНЕВИЙ ПІДХІД ДО ВИБОРУ ХМАРНОГО ПРОВАЙДЕРА ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У дослідженні запропоновано підхід - набір методів вибору постачальника хмарних послуг для міграції даних об'єктів критичної інфраструктури (далі – ОКІ) в умовах воєнного стану та зовнішніх загроз. Показано, що традиційні підходи, орієнтовані на показники якості сервісу, вартість і масштабованість, не враховують критичних порогових вимог безпеки, суверенітету даних та стійкості до кінетичних і кіберзагроз. Це обумовлює застосування підходу, який полягає у поєднанні порогового фільтрування обов'язкових вимог, із прозоримбагатокритеріальним порівнянням допустимих варіантів та керування на основі подій. Підхід складається з трьох рівнів: (1) виключення варіантів за критеріями (юрисдикція і локалізація даних, наявність географічного резервування, механізми відновлення, сертифікації безпеки, операційна здійсненність); (2) зважене ранжування варіантів за економічними, технічними та організаційними показниками з аналізом чутливостірезультатів до зміни ваг, оцінок і припущень; (3) впровадження політик і збір телеметричних показників (затримки, доступність тощо) для швидкого реагування на критичні зміни затримок, відмови каналів зв'язку і зміни вартості послуг, з подальшою координацією розгортання інфраструктури та моніторингу за подіями. Новизна підходу полягає в інтеграції обов'язкових критеріїв безпеки, визначених умовами функціонування ОКІ в умовах військового стану, та суверенітету даних(Sierzputowski, 2019) з адаптивним прийняттям рішень у реальному часі. Це підвищитьстійкість ІТ-інфраструктури і прогнозованість витрат в умовах невизначеності. Запропонованийпідхід є відтворюваним, придатним для аудиту та масштабованим до використання декількох хмар і сервісних провайдерів одночасно, забезпечуючи обґрунтований вибір постачальника для ОКІ.

Міграція даних ОКІ до хмарних середовищ на сьогодні є актуальним завданням в умовах зростання кіберзагроз та фізичних руйнувань. Успішність цього процесу значною мірою залежить від правильно обраного провайдера хмарних послуг, який здатен забезпечити конфіденційність, цілісність та доступність інформації відповідно до вимог ISO/IEC 27001(*ISO/IEC 27001:2022, 2022*), NIST SP 800-53(*NIST SP 800-53, 2020*) та ЗУ «Про хмарні послуги»(Про хмарні послуги, 2024b).Класичні підходи до вибору хмарного провайдера, що зосереджені на показниках якості сервісу (QoS), вартості й масштабованості, часто не враховують кризових сценаріїв і обов'язкових обмежень безпеки, суверенітету даних(Sierzputowski, 2019) і стійкості до фізичних руйнувань. Отже, потрібен підхід, що поєднує обов'язкові пороги безпеки та юрисдикції, операційні тригери й прозорий

багатокритеріальний вибір у вигляді матриці, який можна виконувати швидко та повторювано.

Комплекс критеріїв вибору хмарної платформи може охоплювати технічні, фінансові та організаційні виміри (Kumar&Saini, 2024),(Sisodiaetal., 2024). Автори статей наголошують на необхідності порівняльного тестування, виваженого добору регіонів і зон доступності, а також на включенні механізмів відновлення після збоїв із заздалегідь визначеними цілями відновлення. Такі рекомендації є практично корисними, але здебільшого припускають стабільність середовища та доступність ресурсів для вимірювань, що в умовах війни може бути обмеженим.

Емпіричні дослідження систематизують сукупність визначальних чинників, серед яких експлуатаційні витрати (людські/часові), економічна ефективність, надійність, затримки та пропускна здатність, компетенції команди, безпека, ступінь прив'язки до постачальника, суверенітетданих, тривалість і вартість міграції, а також екологічні аспекти (Aubé&Polacsek, 2023). Окремо підкреслюється потреба підходу розв'язання компромісів між вартістю, строками та якістю, а також дефіцит процедур, що забезпечують підбір методів та інструментів міграції за заданими умовами. Для контексту війни цейпідхід корисний тим, що містить ознаки, які можуть трансформуватися у обов'язкові вимоги (наприклад, суверенітет даних) та в операційні обмеження (наприклад, час на виконання міграції).Паралельно описуються архітектурні рішення для мультихмарних середовищ, де передбачено окремі виміри: політик управління (вартість, безпека, продуктивність), постійного виявлення та профілювання постачальників (затримки, доступність ресурсів і сервісів, ціни, нормативно-правове регулювання), координація розгортання та спостереження за станом (Aubé&Polacsek, 2023). Ключовим є управління на основі подій (затримки, перебоъ у каналах зв'язкутощо), яке дає змогу оперативно реагувати на піки затримок, відмови каналів чи коливання цін. У воєнних умовах такий керованийвимір стає необхідним елементом стійкості.

Автор статті (Kumaretal., 2023) пропонує схеми ранжування альтернатив за допомогою процедури багатокритеріального прийняття рішень (аналіз ієрархій, близькість до ідеального рішення, тощо), а також їх нечіткі або комбіновані модифікації, що дають змогу враховувати лінгвістичні оцінки експертів та неповноту даних. Разом із тим, у дослідженні підкреслюється чутливість цих підходів до якості вхідної інформації та значні часові витрати на підготовку, що обмежує їх застосовність у кризових сценаріях, де час на ухвалення рішення вимірюється годинами або днями.

Мета дослідження — сформувати підхід вибору постачальника хмарних послуг для потреб ОКІ, яка:

– встановлює обов'язкові порогові умови безпеки, відповідності та стійкості;

– забезпечує прозоре багатокритеріальне порівняння лише серед альтернатив, що ці пороги пройшли;

– інтегрує оперативний вимір на основі подій, який підтримує корекцію рішень під час змін зовнішніх умов.

Наукова новизна полягає в інтеграції порогових критеріїв безпеки та суверенітету даних, релевантних функціонуванню ОКІ у воєнний період, із прозорим багатокритеріальним ранжуванням для обґрунтування компромісів та подієво орієнтованим операційним виміром, що забезпечує адаптивне прийняття рішень у реальному часі на підставі зовнішніх подій (мережеві відмови, енергетичні перебої, кінетичні та кібератаки) і внутрішніх метрик (перевитрати, деградація продуктивності), підвищуючи стійкість IT-інфраструктури та прогнозованість витрат в умовах невизначеності.Основні завдання: уточнити перелік критеріїв і розділити їх на обов'язкові та оптимізаційні, визначити процедури нормалізації та зважування критеріїв для ранжування допустимих альтернатив, окреслити механізми інтеграції з моніторингом і централізованим керуванням.

Комплексний аналіз сучасних підходів свідчить про необхідність відмови від універсальних методів вибору провайдерів хмарних ресурсів на користь композиційного підходу, у якому порогові вимоги гарантують мінімальний рівень безпеки та відповідності, багатокритеріальне порівняння забезпечує прозоре обґрунтування компромісів, а управління на основі подій підтримує життєздатність рішення в експлуатації. Запропонована методологія узгоджується з підходами до резервування (AmazonWebServices, 2021), вибору регіонів (GoogleCloud, n.d.) і управління витратами (FinOpsframeworkoverview, б. д.), а також з емпірично підтвердженими чинниками вибору (Aubé&Polacsek, 2023), і тому може бути до застосування в умовах сучасних воєн, коли доводиться поєднувати швидкість ухвалення рішень, суворі обмеження безпеки та вимоги до безперервності надання критичних послуг.

1. Amazon Web Services. (2021, February 12). *Disaster Recovery of Workloads on AWS: Recovery in the Cloud* (AWS Well-Architected Framework). https://docs.aws.amazon.com/pdfs/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-workloads-on-aws.pdf?utm.
2. Aubé, A., &Polacsek, T. (2023). Cloud migration high-level requirements. In *Lectur eNotesin Business Information Processing.* (pp. 19–34). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33080-3_2
3. *FinOps framework overview*. (б. д.). The Fin Ops Foundation. https://www.finops.org/framework/.
4. Google Cloud. (n.d.). *Best practices for Compute Engine regions selection*. Retrieved October 30, 2025, fromhttps://docs.cloud.google.com/solutions/best-practices-compute-engine-region-selection.
5. *ISO/IEC 27001:2022*. (б. д.). ISO. https://www.iso.org/standard/27001.
6. Kumar, A., Singh, A. K., &Garg, A. (2023). Applicationof MCDM methods incloud computing: A literature review. In *Artificial Intelligence, Blockchain, Computing and Security* (Vol. 1, pp. 868–873). CRC Press. https://doi.org/10.1201/9781003393580-129.

7. Kumar, N., &Saini, V. (2024). Choosing the rightcloud provider for limitless growthand maximize ROI. *2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit)* (pp. 906–911). IEEE. https://doi.org/10.1109/globalaisummit62156.2024.10947902.
8. *Security and privacy controls for information systems and organizations*. (2020). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r5
9. Sierzputowski, B. (2019). The data embassy under public international law. *International and Comparative Law Quarterly*, *68*(1), 225–242. https://doi.org/10.1017/s0020589318000428.
10. Sisodia, S., Sharma, S., Kumar, D., Biswas, L., &Aluvala, S. (2024). *Navigating the cloud: Choosing the right cloud computing services for your business*. In*2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)* (pp. 1–8). IEEE. https://doi.org/10.1109/KHI-HTC60760.2024.10481894.
11. Про хмарні послуги, Закон України № 2075-IX (2024b) (Україна). https://zakon.rada.gov.ua/laws/show/2075-20#Text.

А.І. Куляс, Т.Г. Голоцукова, Д.О. Рибачок

ОПТИМАЛЬНА ПОЛІТИКА НАДІЙНОСТІ ЕНЕРГОСИСТЕМ

Значні цінові стрибки стимулюють інвестиції у створення генеруючих потужностей, для підтримки надійності системи. У деяких ринкових моделях важливу роль відіграють вимоги до потужності. Основним чинником, що впливає на роботу оптових ринків, є дефіцит потужностей. Надійність включає: здатність системи витримувати раптові збурення – безпеку, та наявність достатніх потужностей для стабільної роботи – адекватність. Адекватність розглядається, за припущення, що безпека реалізується через планові резерви. Вимоги до операційних резервів (OR) важливі не лише для безпеки, а й через їхню роль у стимулюванні інвестицій, формуванні ціни та зміцненні адекватності. Оператор може закуповувати OR, але ринок має сам забезпечувати достатні планові резерви та бути стимульованим до цього [1].

Контингенція (Contingency) – фактична або потенційна відмова фізичного компонента енергосистеми, зазвичай генеруючого агрегату, що спричиняє дисбаланс між попитом і пропозицією. Унаслідок цього частота та напруга системи знижуються. Якщо наявні достатні оперативні резерви (OR), здатні компенсувати втрати протягом 5–10 хв, оператор зазвичай не вдається до відключення навантаження (LS). Після такого виходу частота та напруга в системі одразу починають знижуватися. Якщо вони падають надто сильно або надовго, відключення навантаження стає необхідним для відновлення балансу між попитом і зменшеною пропозицією. У перші миті після вимушеного відключення решта генераторів (G) автоматично збільшує свою потужність, використовуючи кінетичну енергію обертання, а не додаткове паливо. Коли ця енергія вичерпується, швидкість обертання падає, а разом із нею – частота та напруга системи. Зниження параметрів призводить до того, що споживачі починають брати менше потужності, і система тимчасово стабілізується на нижчому рівні частоти. Зниження частоти миттєво фіксується сенсорами частоти, і ті G, що мають надлишкову потужність, починають поступово збільшувати виробіток. Якщо їх недостатньою для відновлення частоти системи протягом 5–10 хв, оператор змушений відключити навантаження. Таким чином, резерв обертання та відключення навантаження є взаємозамінними механізмами відновлення системної частоти.

OR включають резерви обертання (Spinning Reserves, SP) та інші резерви з нижчою оперативністю. Зазвичай 10-хв SP є першою лінією захисту від контингенцій – їх забезпечують G, які працюють нижче максимальної потужності. Синхронізовані з системою, вони не потребують часу на запуск, хоча реагують поступово, нарощуючи потужність на 4 МВт за хв (40 МВт за 10 хв). Інші типи OR – це 10 та 30-хв неротаційні резерви (Nonspinning Reserves) – забезпечують G, які перебувають поза мережею, але можуть бути швидко введені в дію.

Адекватність характеризує достатність установленої потужності для покриття попиту й не змінюється миттєво. Безпека відображає здатність системи витримувати контингенції та може змінюватися щохвилини. Після виникнення контингенції, доки OR не відновлено, рівень безпеки суттєво знижується. OR підтримують короткострокову безпеку, а планові резерви забезпечують адекватність – здатність покривати пікові навантаження. Разом вони становлять основу генерувального аспекту надійності енергосистеми. Система, що має достатню встановлену потужність *K*, здатна підтримувати належний рівень безпеки, зводячи випадки примусового відключення навантаження до одного дня на десять років. Водночас система, яка може забезпечувати безпеку у всі дні, окрім одного на десять років, обов'язково має адекватну встановлену потужність.

Під безпекою розуміють здатність електроенергетичної (ЕЕ) системи витримувати раптові збурення. Адекватність – здатність системи забезпечувати сумарний попит в будь-який час, з урахуванням планових і очікуваних позапланових відмов. За неефективної політики управління OR система може бути адекватною, але небезпечною. Проте в адекватній системі утримання достатніх OR є відносно дешевим, тоді як забезпечення самої адекватності вимагає значних інвестицій. (Це припущення стосується ізольованої системи; у разі конкуренції двох сусідніх систем за одні й ті самі OR їхня вартість зростає). Отже, адекватність є ключовою економічною проблемою, а безпека – другорядною, але більш технічно складною. Для зосередження на проблемах інвестицій у генерацію та адекватність системи, приймається, що політика OR є ефективною, тобто забезпечує максимальну безпеку за наявної встановленої потужності. Усі варіанти такої політики мають гарантувати мінімальний рівень резервів.

Спрощена модель надійності (СМН). Потужність, виведена з експлуатації розглядається як додаткове навантаження системи. Якщо це збільшене навантаження *Lg* перевищує встановлену потужність *K*, то частину навантаження доводиться відключати. В інших випадках навантаження може відключатися з причин, не пов'язаних із *K*. У межах СМН передбачається, що, окрім таких зовнішніх причин, втрачене навантаження *LL* дорівнює *Lg* – *K* або нулю, якщо різниця від'ємна. Вартість *LL* вважається сталою і визначається у грошових одиницях за 1 МВт·год недопоставленої енергії. Оптимальний обсяг потужності визначається тоді, коли тривалість відключення навантаження дорівнює відношенню фіксованих витрат пікової установки до вартості втраченого навантаження. СМН ґрунтується на припущенні, що відключення навантаження не відбувається, якщо фактичне навантаження не перевищує обсяг придатної до експлуатації генеруючої потужності, тобто, що чітко визначений рівень *K* та втрати генерації *g*. Навантаження, *L*, визначається як економічний попит на ЕЕ – тобто обсяг потужності, який споживався б у разі нормальної роботи системи. Оскільки в моделі передбачається, що *OR* доступні завжди, коли це потрібно (у межах *K*), їх можна визначити як частину потужності, яка не виведена з експлуатації та не використовується для покриття навантаження. Відповідно:

$$OR = K - g\ - L \quad (1)$$

Оскільки L визначене як економічний попит, воно може перевищувати наявну пропозицію. У такому випадку виникає LL. Водночас частина попиту задовольняється, і сума цих двох величин дорівнює L. LL визначається тією мірою, OR є від'ємними, і дорівнює нулю, якщо OR додатне:

$$LL = max(\ -OR, 0) \quad (2)$$

Відключення навантаження може відбуватися навіть тоді, коли OR більше 0, а коли OR негативне, обсяг втраченого навантаження може бути більшим, ніж LL [2]. Такі надлишкові переривання постачання включають, зокрема, пошкодження у розподільних мережах і каскадні відмови [3]. СМН припускає, що ці надлишкові порушення не корелюють із OR. Якщо така кореляція справді відсутня, збільшення K не впливає на їхню частоту, а отже, вони розглядаються як постійні витрати, які можна не враховувати. Таким чином, LL у межах СМН не охоплює всі випадки втрат навантаження, але включає усі ті, що залежать від політики управління встановленою потужністю K. Відсутність кореляції між надлишковими LL та OR є ключовим припущенням СМН. За цієї умови номінальне LL можна легко обчислити, і саме воно має вирішальне значення для аналізу.

Для зручності вводиться поняття Lg, що визначається як: $L\_g=L+g$. Тоді рівняння для OR спрощується до: $OR= K-L\_g$. Виведення G з експлуатації еквівалентне додаванню до системи рівного за величиною навантаження у точці його підключення. Тобто відмова G функціонально дорівнює зростанню навантаження на відповідну потужність у його місці приєднання.

Припущення (П.1) – відключення навантаження здійснюється настільки, наскільки необхідно: LL=max(L_g-K,0) . Систематичне (номінальне) LL дорівнює величині, на яку Lg перевищує K. Lg включає економічний попит, L, та потужність, виведену з експлуатації, g. Термін «систематичне» вказує на ті втрати, що корелюють із різницею Lg – K.

LL, постійно змінюється, тому його неможливо використовувати для обчислення необхідного рівня K, яка змінюється лише поступово. Замість цього потрібно застосувати середнє значення LL. Вартість як миттєвих втрат навантаження LL, так і середніх втрат $\overline{LL}$, визначається множенням їхніх значень у МВт на вартість втраченого навантаження V_{LL}. Збільшення K на 1 МВт зменшує площу $\overline{LL}$ на величину D_{LS} (у МВт), де D_{LS} – тривалість часу, протягом якої Lg перевищує K. Це, своєю чергою, зменшує середню вартість втрат навантаження:

$$\Delta\text{Вартість} = \frac{(V_{LL} \times D_{LS})}{h} \quad (3)$$

Середня вартість додавання пікової потужності (додаткового 1 МВт):

$$FC_{peak}\ + D_{LS} \times VC_{peak} \quad (4)$$

де *FC_peak* – це фіксована вартість пікової установки, а *VC_peak* змінні витрати пікової установки. Оскільки D_{LS} дуже мале, домінує складова постійних витрат. Більшу частину витрат на забезпечення пікового навантаження становить саме фіксована вартість придбання пікової установки, тому вплив D_{LS} на вартість додавання 1 МВт можна знехтувати [2].

Із збільшенням *K* тривалість інтервалів, протягом яких ціна досягає максимального рівня зменшується. Для низьких значень *K*, величина $V_{LL} \times D_{LS}$, перевищує *FC_peak*, отже, збільшення *K* є економічно вигідним – додатковий МВт коштує менше, ніж заощадження, отримані від зменшення втрат навантаження. Для високих значень *K*: додаткове збільшення потужності стає дорожчим, ніж зменшення втрат, яке воно забезпечує. У точці оптимального значення *K* заощадження від скорочення втрат навантаження дорівнюють вартості встановлення ще одного МВт пікової потужності.

K набуває оптимального значення, коли:

$$V_{LL} \times D_{LS} = FC_{peak} \tag{5}$$

Політика управління не впливає на V_{LL} та *FC_peak*, регулювання має здійснюватися через D_{LS}. Отже, оптимальне значення тривалості відключення:

$$D_{LS}^{*} = \frac{FC_{peak}}{V_{LL}} \tag{6}$$

Оптимальна політика надійності – стимулює інвестиції тоді, коли $D_{LS} < FC_{peak}/V_{LL}$ і є оптимальною відповідно до СМН. Результат визначає оптимальну рівновагу між витратами та надійністю на основі мінімальної інформації. Залишається справедливим незалежно від розподілу ймовірностей відключень генерації, форми кривої тривалості навантаження чи характеру добових коливань попиту. У системі електропостачання, яка відповідає П.1, D_{LS}^{*} у розрахунку враховує лише те відключення, яке залежить від *K* [2]. Отже, ключовою характеристику оптимально надійної енергосистеми є оптимальна тривалість номінального відключення навантаження, яка залежить від вартості пікової установки та вартості втраченого навантаження.

Якщо припущення СМН не виконується в реальних умовах, таке ціноутворення може бути теоретично некоректним. Зі зростанням еластичності попиту форма кривої тривалості навантаження може істотно змінюватися, тому глибше розуміння механізмів надійності стає критично необхідним.

1. Golotsukova, T. (2025). The U.S. Energy Market: Structure, Regulation, And Industry Economics. In *Transfer Pricing In Ukraine: A System Of Analytical, Digital, And Control Management* (p. 1–28). Riga, Latvia. https://doi.org/10.30525/978-9934-26-553-2-1.
2. Stoft, S. (2002). *Power System Economics*. IEEE/Wiley.
3. Golotsukova, T., & Godliuk, V. (2025). Risks, resilience, and critical infrastructure management: digital, environmental, and social aspects. In *Innovation and digital transformation: education, economy and society dimensions* (p. 286–292). Katowice. https://doi.org/10.54264/M054.

О.А. Владимирський, В.М. Зварич, І.А. Владимирський, В.О. Артемчук

ВИКОРИСТАННЯ ДЕЯКИХ МЕТОДІВ СТАТИСТИЧНОГО ЗВ'ЯЗКУ ІНФОРМАЦІЙНИХ СИГНАЛІВ ДЛЯ ПОБУДОВИ СИСТЕМ ДІАГНОСТИКИ ЕЛЕМЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Побудова оцінки резильєнтності енергетичного обладнання залежить від побудови достовірних оцінок його технічного стану. Використання систем діагностування при побудові та експлуатації енергетичного обладнання може суттєво підвищити надійність такого обладнання та підвищити економічні показники його використання [1-3]. Особливо питання діагностування енергетичного обладнання виника в повоєнний період.

Показники надійності роботи енергообладнання визначаються результатом спільного впливу як факторів, що визначають умови експлуатації, так і внутрішніх чинників, що визначають властивості енергетичного обладнання. Поєднання таких факторів носить випадковий характер. Тому застосування статистичних методів для вирішення таких задач доцільно в багатьох практичних випадках.

Найбільш перспективними методами контролю і діагностики є неруйнівні методи, які, зазвичай, реалізуються за допомогою спеціалізованих комп'ютерних систем. Серед таких методів найбільш перспективним є метод вібродіагностики.

Розглянемо питання побудови системи вібродіагностики на прикладі побудови течешукача трубопроводів [4].

Поступове зростання загального зносу трубопровідних мереж та необхідність інтенсифікації робіт з оперативного усунення пошкоджень підвищує вимоги до точності та оперативності інструментального визначення прихованих під землею витоків. Цьому перешкоджають складні умови проведення робіт та обмеження існуючого інструментального діагностування трубопроводів.

Найбільш авторитетними розробниками і виробниками діагностичної апаратури для систем водо- та теплопостачання можна вважати фірми Великобританії (HWM-Water Ltd, Primayer Limited, Guided Ultrasonics Ltd), Німеччини (SebaKMT, Herman Sewerin GmbH), США (Fluid Conservation Systems) та Швейцарії (Gutermann).

Такі прилади та системи використовують найпростіші моделі трубопроводу. А це означає, що проблеми із забезпеченням необхідних показників оперативності, достовірності та точності в умовах сильного корозійного пошкодження, зношеності, що характерно для вітчизняних систем трубопроводів, є актуальними, особливо за наявності мілітарних загроз.

Існує два типи зв′язків між інформаційними сигналами, що описують технічний стан об′єкту, що досліджується [4]:

- Перший тип – лінійний зв′язок, який оцінюється взаємною коваріацією або кореляцією і, як правило, базується на багатовимірному нормальному рзподілі для моделювання структури залежності між інформаційними сигналами. Проблемою є те, що метод лінійної залежності ігнорує деякі флуктуації відносно асиметрії та ексцесу розподілів, є чутливим до ряду спотворень вихідних даних. Якщо вибірка реалізації інформаційного сигналу не достатньо велика, припущення про нормальність є сумнівним.
- Інший тип залежності вимірюється зв′язуючою функцією (яку іноді називають копулою, copula). Це функція, яка пов′язує між собою одновимірні функції розподілу та використовує гнучкий багатовимірний розподіл замість багатовимірного нормального апроксимуючого розподілу. Копула – це багатовимірна функція розподілу, яка враховує важкість хвостів розподілу та асиметрію розподілу інформаційного, здатна враховувати деякі інші спотворення вихідних даних.

Розглянемо більш детально обидва типи кореляційного зв’язку стосовно вирішення задач технічного діагностування

Розглянуто застосування лінійного кореляційного зв’язку**.** Цей тип зв’язку між даними про технічний стан обладнання є найбільш простим за обчисленням та поширеним. Як правило, він базується на використанні оцінки взаємної кореляційної функції (ВКФ) двох сигналів. Більш детально метод представлено в роботах [2-4].

В доповіді також використано поняття ентропії для опису залежностей інформаційних сигналів. Шеннон [5] ввів подібну міру інформації в своїй теорії комунікації, Джейнс [6] використав поняття ентропії в задачах статистичної механіки, Кульбак та Лейблер [7] використали це поняття для опису дивергенції (дистанції) між статистичними популяціями.

Взаємна інформація (ВІ) може бути використана для опису нелінійної кореляції між двома випадковими величинами [8]. Точне обчислення ВІ залишається складним завданням для неперервних випадкових величин. Розглядаючи неперервну випадкову величину X, її ентропію Шенона можна визначити як:

$$H(X) = -\int_{-\infty}^{\infty} f(x)\log f(x)dx \qquad \textbf{(1)}$$

де $f(x)$- гранична (маргінальна) функція розподілу ймовірностей від X. Далі, розглядаючи іншу неперервну змінну Y, ВІ між X та Y можна виразити як:

$$I(X,Y) = \int_{-\infty-\infty}^{\infty}\int^{\infty} f(x,y)\log\frac{f(x,y)}{f_1(x)f_2(y)}dxdy \qquad (2)$$

де *I(X;Y)* - це ВІ між *X* та *Y*; $f_1(x)$ та $f_2(y)$ - щільність розподілу ймовірностей для *X* та *Y*, відповідно; та *f(x, y)* – взаємна щільність розподілу ймовірностей для *X* та *Y*. Це дослідження вводить кумулятивну теорію для більш точної оцінки ВІ. Згідно [1], можна встановити функціональний зв'язок між взаємною функцією розподілу та кожною маргінальною функцією розподілу:

$$F(x,y) = C[F_1(x), F_2(y)] = C(u,v) \tag{3}$$

Щільність розподілу ймовірностей, що відповідає *C(u,v)*, можна представити як:

$$c(u,v) = \frac{d^2C(u,v)}{dudv} = \frac{d^2C(u,v)}{dF_1(u)dF_2(v)} = \frac{f(x,y)}{f_1(x)f_2(y)} \tag{4}$$

де *c(u,v)* – зв′язуюча (копула copula) щільність розподілу ймовірностей випадкових змінних *u* та *v*, а її опорний діапазон [0,1]. Крім того, підставимо рівняння (4) у рівняння (1), щоб знайти зв′язуючу (копула)-ентропію:

$$H_c(U,V) = -\int_0^1\int_0^1 c(u,v)\log c(u,v)dudv = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\log\frac{f(x,y)}{f_1(x)f_2(y)}dxdy \tag{5}$$

Використавши вирази (2) та (5) отримаємо:

$$I(X,Y) = -H_c(U,V)$$

Наведена вище формула означає, що ВІ випадкових змінних дорівнює від'ємній ентропії копули. Оцінюючи ВІ на основі копулової ентропії, необхідно лише оцінити відповідну копулову функцію за даними спостережень випадкових змінних, а потім підставити її в рівняння (5) для розв'язання.

Розглядаючи N змінних, отриманих із *складного процесу,* на основі параметричної копула ентропії, глобальну матрицю асоціацій можна записати як:

$$G_{obs} = \begin{pmatrix} 1 & -H_c(u_1,u_2) & \dots & -H_c(u_1,u_N) \\ -H_c(u_2,u_1) & 1 & \dots & -H_c(u_2,u_n) \\ \vdots & \vdots & \ddots & \dots \\ -H_c(u_N,u_1) & -H_c(u_N,u_2) & \dots & -H_c(u_N,u_N) \end{pmatrix} \tag{6}$$

де значення кожного елементу представляє нелінійну кореляцію між усіма змінними в цьому діагностичному процесі.

Для побудови розв′язувальних правил з діагностик и енергетичних об′єктів можна скористатись методом, викладеним в [9], який передбачає лінійне масштабування глобальної матриці асоціацій G_{obs}, декомпозиції G_{obs}, деконволюції матриці власних значень матриці G_{obs} та вибір відповідного порогу.

Висновки.

1. Використання методів оцінки нелінійного зв’язку, зокрема розглянутого методу на основі визначення взаємної інформації сигналів. Властивості та переваги подібних методів відносно традиційних потрібно визначати з врахуванням конкретних завдань та умов діагностування.

2. Необхідно відзначити, що викладені методи можуть бути використані при побудові інформаційно-вимірювальних систем діагностики різних типів енергетичного обладнання, що в своїх алгоритмах використовують аналіз зв′язків інформаційних сигналів.

Автори висловлюють щиру подяку Національному фонду досліджень України за грантову підтримку, завдяки якій були виконані та виконуються викладені дослідження в рамках проекту №2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів».

1. Ning Zhao, Winston T. Lin A copula entropy approach to correlation measurement at the country level Applied Mathematics and Computation 218 (2011) 628–642 doi:10.1016/j.amc.2011.05.115.
2. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. Електронне моделювання. 2021. Т. 43, № 3. С. 3—16. URL:https://doi.org/10.15407/emodel.43.03.003.
3. Владимирський О.А., Владимирський І.А. Просторовий і частотний Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. Електронне моделювання. 2021. 43 (4). С.22-36. URL: https://doi.org/10.15407/emodel.43.04.022.
4. О.А. Владимирський, В.М. Зварич, І.А. Владимирський, В.О. Артемчук Розвиток методів визначення кореляційного зв’язку між сигналами у системах технічного діагностування. Прийнята до публікації в журналі «Технічна електродинаміка», №6, 2025р.
5. C.E. Shannon, A Mathematical Theory of Communication, Bell. Syst. Tech. J. 27 (1948) 379–423.
6. E.T. Jaynes, Information theory and statistical mechanics, Phys. Rev. 106 (1957) 620–630.
7. S. Kullback, L.A. Leibler, On information and Sufficiency, The Annals of Mathematical Statistics, 1951, vol.22, pp.79-86.
8. Yan-NingSuna, Yun-JiePana, Li-LanLiua, -GuiGaoa, WeiQinc, Reconstructing causal networks from data for the analysis, prediction, and optimization of complex industrial processes. Engineering Applications of Artificial Intelligence 138, 2024, 109494.
9. Sun, Y., Qin, W., Zhuang, Z., 2022c. Nonparametric-copula-entropy and network deconvolution method for causal discovery in complex manufacturing systems. J. Intell. Manuf. 33, 1699–1713. https://doi.org/10.1007/s10845-021-01751-w.

С.А. Недосєка

АВТОМАТИЗОВАНА ОЦІНКА ПОШКОДЖЕНОСТІ ТА ЗАЛИШКОВОГО РЕСУРСУ МЕТАЛУ ТРУБОПРОВОДІВ

Одним з актуальних напрямків є забезпечення резильєнтності динамічних систем: математичні моделі, методи оцінювання та прогнозування стану резильєнтності, ідентифікація вразливостей, визначення резервів.

У рамках проекту 2023.04/0022 «Розроблення апаратно-програмного комплексу та методики оперативного виявлення пошкоджень систем тепло- та водопостачання з врахуванням їх зношеності та мілітарних впливів», запропоновано ряд технічних та методичних вдосконалень найбільш ефективних з існуючих на сьогодні, акустичних методів та приладів діагностування трубопроводів. Ці вдосконалення стосуються підвищення оперативності визначення витоків в умовах малого відношення сигнал-завада, подолання потужних акустичних завад, врахування спотворень сигналів від пошкоджень при їхньому поширенні, визначення параметрів цього поширення і т.і. [1-2]. Для практичного відпрацювання запропонованих нововведень розробляється випробувальний апаратно-програмний комплекс у складі трьох незалежних компонентів, включаючи систему акустико-емісійного (АЕ) діагностування ЕМА-4.

Дані, які отримує комплекс, дозволяють визначити поточний стан трубопроводів і отримати кількісні показники, які його характеризують.

Надалі постає питання, чи може об’єкт контролю працювати ще якийсь час, чи він потребує негайних заходів з ремонту або заміни. Одним з способів вирішити це питання є визначення пошкодженості та оціночного залишкового ресурсу.

Під пошкодженістю [3-4] розуміється інтегральна характеристика, що стосується, як правило, контрольованого виробу в цілому, а не окремих його вузлів або локальних ділянок. Пошкодженість, подана як скалярна величина, вказує, наскільки та чи інша характеристика матеріалу контрольованого об’єкта змінилася внаслідок експлуатаційного напрацювання, навантаження або впливу інших чинників.

Під залишковим ресурсом [5, 6] розуміють строк, протягом якого виріб можна безпечно експлуатувати без загрози його руйнування або втрати інших принципово важливих характеристик. Слід розрізняти плановий ресурс, реальний та оціночний. Плановий ресурс, як правило, задається на стадії проєктування конструкції. Реальний ресурс визначає термін від вводу виробу в експлуатацію до його руйнування або втрати характеристик, які дозволяють його подальшу експлуатацію. Реальний ресурс заздалегідь невідомий і систематично зменшується.

На відміну від реального ресурсу, оціночний, або, іншими словами, прогнозований ресурс [6] є величиною, яка може бути розрахована певним науково обгрунтованим способом, і в залежності від поточних умов

експлуатації, способу розрахунку та ряду додаткових факторів може змінюватися як в більший, так і в менший бік. Якщо потрібно подовжити експлуатацію виробу з гарантією безпеки на термін в один-два роки, а оціночний ресурс, з урахуванням обов'язкового запасу, який має бути встановлений для кожного типу виробу окремо, становитиме вдвічі-втричі більший термін, то прийняття рішення про можливість подальшої експлуатації при таких показниках буде в достатній мірі обгрунтованим.

Наразі накопичено значний досвід з визначення пошкодженості і оціночного залишкового ресурсу [7, 8], зокрема трубопроводів з різних регіонів України з різним експлуатаційним напрацюванням. Для визначення пошкодженості матеріалу труб було використано кілька сотень зразків. Дослідження стану зразків проводили п'ятьма інструментальними методами , а саме методом АЕ при випробуваннях зразків на статичний розтяг, скануванням призматичних зразків з використанням АЕ системи (активний АЕ метод), визначенням ударної в'язкості, визначенням розсіяння твердості (метод LM-твердості) і зважуванням малих проб у рідині з метою визначення зміни їх щільності внаслідок напрацювання.

В процесі виконання досліджень було запропоновано критерій оцінки залишкового ресурсу матеріалів з експлуатаційним напрацюванням, оснований на статистичній обробці та побудові логарифмічного тренду для результатів оцінки пошкодженості структурно-чутливими методами металу труб з різних газопроводів України з різним терміном напрацювання.

Отримані результати показали, що дані декількох інструментальних методів можуть бути успішно використані для визначення пошкодженості досліджених матеріалів, якщо їх узагальнити шляхом використання формального критерію пошкодженості, сформульованого як $\Delta W_П = 1- П_{ПОШК} / П_{ПЕРВ}$, де П - параметр, що відбиває зміни деякої властивості матеріалу у процесі накопичення пошкоджень, $П_{ПОШК}$, $П_{ПЕРВ}$ - значення параметру П відповідно для матеріалу у пошкодженому та первинному стані.

Осереднене значення пошкодженості ΔW може бути описане рівнянням $\Delta W = ae^{bt}$, де t - термін експлуатаційного напрацювання, a=0.1352, b=0.0333. Параметром пошкодженості ΔW можна скористуватися для визначення залишкового ресурсу випробуваних матеріалів, причому – за даними будь-якого з інструментальних методів.

Для цього побудуємо номограму у координатах "Пошкодженість - залишковий ресурс", скористувавшись рівнянням кривої ΔW і враховуючи, що у точці ΔW =1 залишковий ресурс повинен приймати значення 0.

Розмістимо дані на номограмі та опишемо їх логарифмічною залежністю, потім екстраполюємо її до значення пошкодженості ΔW =0. Отримане рівняння відповідної лінії тренду, що має вигляд $t_{ЗАЛ} = n \ln(\Delta W) + m$, де $t_{ЗАЛ}$ - залишковий ресурс, n = -30.03, m = -0.115, може бути використане для визначення залишкового ресурсу досліджених матеріалів за відомою пошкодженістю (рис. 1).

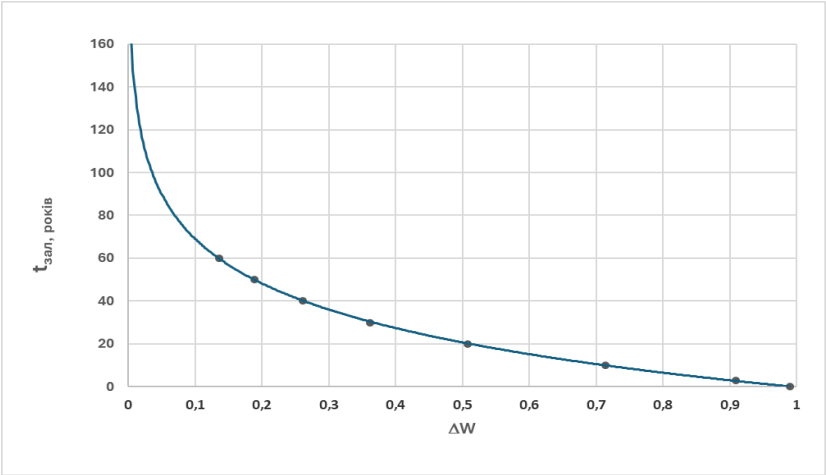


Рисунок 1. – Номограма для визначення залишкового ресурсу tзал за відомою пошкодженістю ΔW

В умовах, коли потрібно швидко визначити пошкодженість металу труб або інших елементів трубопроводів, зокрема системи тепло – та водопостачання, користування розрахунковими формулами для визначення пошкодженості та номограмою для визначення оціночного залишкового ресурсу може зайняти певний час, так само як і ознайомлення з інструктивними матеріалами з їх використання. Внаслідок цього виникло завдання автоматизації цих розрахунків і створення відповідної комп'ютерної програми. Така програма була створена, і під час її розробки реалізовані певні заходи з підвищення якості оцінки поточного стану матеріала, а саме можливість задати реальне напрацювання контрольованого виробу з метою корекції базової номограми.

Програма для MS Windows 32-бітних та 64-бітних версій дозволяє задати вже визначену або розрахувати пошкодженість матеріалу, отриману одним або декількома інструментальними методами, загалом до 10.

При цьому програма дозволяє коригувати номограму «Пошкодженість – залишковий ресурс» для умов, які відрізняються від типових. Можна задати власний коефіцієнт корекції діаграми, зокрема розрахувати його автоматично, якщо відомі пошкодженість і строк напрацювання конкретного об'єкта контролю. Інтерфейс програми (рис. 2) є інтуїтивно зрозумілим, а файли зберігаються у текстовому форматі, що дозволяє одразу використовувати їх для складання звітів.

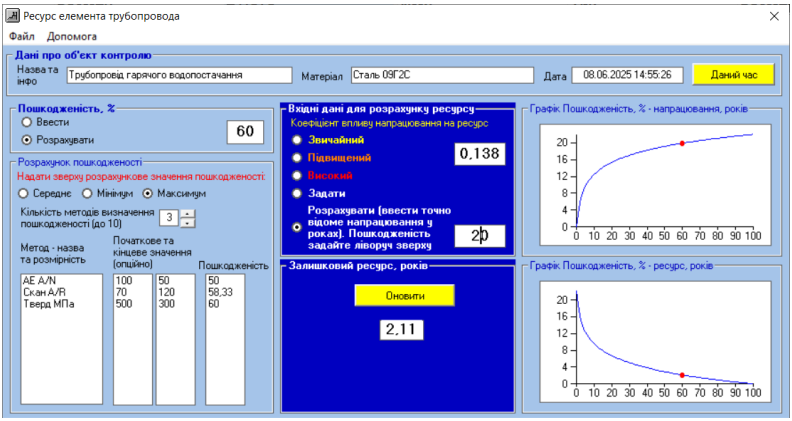


Рисунок 2. – Приклад екрану програми для трьох методів визначення пошкодженості та розрахунку залишкового ресурсу у разі відомого строку напрацювання 20 років

При розрахунку можна задати, яка саме пошкодженість буде використана у кінцевому варіанті – середня, мінімальна чи максимальна. Праворуч розташовані графіки у координатах «Пошкодженість – напрацювання» та «Пошкодженість – ресурс», які дозволяють аналізувати конкретну криву для вибраного випадку розрахунку. На графіках червоною точкою відмічені поточні значення напрацювання та ресурсу.

У наведеному на рис. 2 прикладі показаний варіант розрахунку залишкового ресурсу для труби з сталі 09Г2С, яка працює 20 років в системі гарячого водопостачання. Задіяні 3 методи визначення пошкодженості, а саме власне метод АЕ, сканування АЕ імітатором та визначення твердості.

В умовах проведення реальних обстежень об’єкта контролю автоматично, без задіяння ручних розрахунків за діаграмою ресурсу, отримано його оціночне значення, дещо більше ніж 2 роки. Можливість зберегти отримані дані у файлах дозволяє вести банк даних відносно визначеної пошкодженості та ресурсу різних об’єктів контролю.

Підготовлено заявку до Національного органу інтелектуальної власності ДО “Український національний офіс інтелектуальної власності та інновацій” на реєстрацію авторського права на службовий твір “Комп'ютерна програма “Ресурс елементу трубопровода”. Програма є універсальною і не прив’язаною до конкретних типів об’єктів або їх фізичних та геометричних характеристик, що дозволяє використовувати її максимально широко, легко інтегрувати в системи оцінки стану і ремонту трубопроводів.

Автор висловлює щиру подяку Національному фонду досліджень України за грантову підтримку, завдяки якій були виконані викладені дослідження в рамках проєкту №2023.04/0022.

1. Владимирський О.А., Владимирський І.А., Артемчук В.О., Криворучко І.П., Семенюк Д.М. Особливості і розвиток технологій виявлення витоків трубопроводів тепло- та водопостачання в умовах зношеності та мілітарних впливів. *Електронне моделювання.* 2024, 46(5), с. 64-73. URL: https://doi.org/10.15407/emodel.46.05.064.
2. Vladimirsky A.A., Vladimirsky I.A. Correlation parametric method for determining the velocity of acoustic wave propagation in a pipeline. *Електронне моделювання.* 2024, 46(6), с. 55. URL: https://doi.org/10.15407/emodel.46.06.055.
3. API 579-1/ASME FFS-1 (2016) "Fitness-for-Service." Comprehensive standard for damage assessment for metal structures.
4. 20. DIN 50113:2009 "Testing of metallic materials — Evaluation of damage."
5. ДСТУ 2860-94 «Надійність техніки. Терміни. Залишковий ресурс» .
6. ДСТУ 8646:2016 «Надійність техніки. Оцінювання та прогнозування залишкового ресурсу (строків служби) технічних систем».
7. Недосека С.А., Недосека А.Я. Комплексная оценка поврежденности и остаточного ресурса металлов с эксплуатационной наработкой // *Технічна діагностика та неруйнівний контроль,* 2010. №1, С. 9-16.
8. Недосека А. Я., Недосека С. А. Основы расчета и диагностики сварных конструкций: учебное пособие. 5-те изд., перераб. и доп. / под ред. Б. Е. Патона. Глава 7. Киев: Индпром, 2021. 94 с.

О.М. Джигун, В.В. Чьочь

ВИРІШЕННЯ ПРОБЛЕМИ АДЕКВАТНОСТІ ПОТУЖНОСТІ ТА ГНУЧКОСТІ ДЛЯ ПЛАНУВАННЯ ЕНЕРГЕТИЧНОЇ СИСТЕМИ

Електроенергетика України є базовою галуззю економіки держави. Виробництво електричних ресурсів засноване на атомній енергетиці, гідроенергетиці, процесах спалювання мазуту та вугілля, біопалива та природного газу, крім того, Україна використовує відновлювані джерела енергії (ВДЕ), такі як сонячна енергія (СЕС), вітряні турбіни (ВЕС) та гідростанції. Електроенергетика є пріоритетною для держави та формує значну частку національної економіки.

Російська агресія вплинула на енергетичну інфраструктуру України. Четвертий рік поспіль енергетична інфраструктура перебуває під прицільними атаками агресора. Енергетична система країни зазнала масштабних руйнувань від російських атак, що кардинально змінило підходи до розвитку енергетичної інфраструктури. Обслуговування та ремонт сонячних електростанцій набули особливої актуальності в умовах воєнного стану, а питання пожеж на сонячних електростанціях потребують особливої уваги через підвищені ризики [1].

Удари по електроенергетиці мають системний і комбінований характер, мета яких підірвати енергетичну безпеку країни. Ворогом окупувано 18 ГВт генерації, включно з ГЕС, ТЕС та найбільшою в Європі атомною електростанцією – Запорізькою АЕС. Найгірша ситуація у прифронтових регіонах, де регулярні обстріли знищують мережеву інфраструктуру і спричиняють перебої з енергопостачанням. Українська енергетика зустрілася з переліком загрозливих викликів, як то ядерний тероризм із захопленням Запорізької АЕС, численні пошкодження критичної інфраструктури – електричних і газових мереж, паливна криза. Але не дивлячись на бойові дії по всій території країни продовжено синхронізацію енергетичної системи України з енергосистемою Континентальної Європи. Стратегія енергетичного переходу була адаптована до воєнних умов з акцентом на розвиток розподіленої генерації та систем накопичення енергії. Енергетична система України почала активну інтеграцію з європейським ринком електроенергії, що забезпечило додаткові можливості для експорту та імпорту електричної енергії.

Українська енергосистема ще за декілька років до повномасштабного вторгнення рф потребувала будівництва високоманеврової генерації для посилення гнучкості. Це було необхідно для оптимізації режимів її роботи в умовах стрімкого збільшення потужності СЕС та ВЕС. А після перших ударів ворога по енергетичній інфраструктурі у 2022 році, розбудова нової генерації, зокрема, розподіленої, стала безальтернативним шляхом до енергетичної стійкості України [2, 3].

Повномасштабна війна кардинально змінила пріоритети енергетичного розвитку України, поставивши на перше місце питання безпеки та стійкості енергосистеми. Попри постійни удари українська енергосистема демонструє здатність оперативно реагувати. За час повномасштабної війни українські енергетики навчилися захищати об'єкти енергетики, швидко ліквідовувати наслідки атак, відновлювати потужності протягом короткого часу.

У більшості аналізів майбутньої європейської енергетичної системи робиться висновок про те, що для досягнення цілі політики в галузі енергетики та зміни клімату, значну увагу приділено збільшенню використання ВДЕ. У рамках цього очікується, що частка виробництва електроенергії з ВДЕ зросте з 20% у 2010 році до 44% у 2030 році та 52% у 2050 р. Гідрогенерація є найбільшим джерелом відновлюваної електроенергії в Європі, але її потенціал здебільшого вже використаний. Це означає, що розвиток значної частини ВДЕ в майбутньому буде базуватися на змінній генерації такої, як вітер і фотоелектричних систем. Ці енергії, однак, як і попит на електроенергію, мають змінну величину, яка не зовсім передбачувана. Як наслідок, коротко- та довгострокова мінливість і невизначеність у балансуванні електричного навантаження та виробництва, ймовірно, збільшиться в майбутньому [4].

Щоб впоратися з цією зростаючою мінливістю та невизначеністю, система електроенергії потребуватиме достатню гнучкість, тобто здатність системи адаптувати свою роботу як до передбачуваних, так і до непередбачуваних коливань, умов, або на стороні попиту, або на стороні генерації, у різних часових масштабах, в межах економічних кордонів), щоб постійно підтримувати баланс між генерацією попиту. Таким чином, планування енергетичної системи потребуватиме вирішення проблеми адекватності потужності та гнучкості. Адекватність пов'язана з питаннями інвестиційних рішень і використовується як міра довгостроковості, здатність системи відповідати попиту та пропозиції з прийнятним рівнем ризику. Це міра, яка інтерналізує стохастичні коливання сукупного попиту та пропозиції)

Система електроенергії завжди потребувала гнучкості, щоб справлятися з попитом, мінливістю і невизначеністю генерації річкової ГЕС, а також незапланованої генерації відключення. Однак додаткова мінливість і невизначеність, спричинені вітром і фотоелектричними параметрами, будуть збільшувати потреби та сприяти гнучкості енергосистеми.

Незважаючи на те, що гнучкість в основному потрібна в робочих масштабах часу від хвилини на добу наперед, це потрібно враховувати на етапі планування. Система, яка має достатню потужність для задоволення пікового навантаження може мати проблеми з обслуговуванням попиту і мінливістю покоління. Як наслідок, уявлення про гнучкість і етап планування енергосистем допоможе створити систему, яка зможе впоратися з цією варіативністю економічно ефективним способом.

Оцінка потреб у гнучкості та адекватності, ймовірно, постане новим завданням для планування енергетичних систем. На рисунку наведено приклад із загальною структурою енергії і процес планування системи електроенергії, включаючи моделювання виробничих витрат і оцінка гнучкісті.

Рисунок 1. – Концептуальна структура для інтеграції моделей енергетичної та електроенергетичної систем

Гнучкість української енергосистеми в умовах війни знизилася через руйнування критичної інфраструктури, але адаптується завдяки відновленню, модернізації та розвитку розподіленої генерації. Систему роблять більш стійкою шляхом ремонту пошкоджених об'єктів, встановлення нових, в тому числі малих за потужністю (наприклад, сонячних), а також шляхом впровадження альтернативних джерел енергії для зменшення залежності від централізованих станцій, які є більш вразливими до атак.

Основні виклики та проблеми, що виникли внаслідок агресії рф:

1. *Масштабні руйнування*: понад 1000 ударів по енергетичних об'єктах призвели до втрати значної частини генеруючих потужностей та пошкодження до 60% загальної інфраструктури.

2. *Вразливість централізованих об'єктів*: масовані ракетні атаки продемонстрували вразливість великих електростанцій, що підкреслило потребу в децентралізації генерації.

3. *Зниження частки зеленої енергетики*: значна частина вітрових та сонячних електростанцій була виведена з експлуатації до осені 2022 року, що негативно вплинуло на баланс енергосистеми.

Шляхи підвищення гнучкості та стійкості

1. *Розподілена генерація*: це ключовий фактор стійкості, який дозволяє зменшити залежність від централізованих об'єктів. Розвиток невеликих сонячних та інших малих об'єктів допомагає забезпечити енергією споживачів навіть при виведенні з ладу великих станцій.

2. *Модернізація та відновлення*: необхідне постійне відновлення та модернізація пошкодженої інфраструктури, а також впровадження сучасних технологій для підвищення її стійкості до атак.

3. *Розвиток альтернативної енергетики*: навіть в умовах війни, розвиток відновлюваних джерел енергії (сонячної, вітрової, гідроенергетики) є пріоритетом для забезпечення енергетичної незалежності та зниження ризиків.

1. Українська енергетика у час війни https://www.ecotech.ua/ukrayinska-energetyka-u-chas-vijny.
2. Оцінка стійкості енергетичної інфраструктури України. Аналітичний звіт. https://dixigroup.org/wp-content/uploads/2022/05/dixi-energy-resilience-str.pdf.
3. https://e-b.com.ua/energeticna-stiikist-ukrayini-vikliki-politika-texnologiyi-80.
4. Directorate-General for Energy; Directorate-General for Climate Action; Directorate General for Transport, “EU energy, transport and GHG emissions: trends to2050, reference scenario 2013 / European Union, 2013.

Т.П. Нечаєва, В.О. Дерій, О.В. Згуровець

МОДЕЛЮВАННЯ СТІЙКОСТІ ЛОКАЛЬНОЇ МУЛЬТИЕНЕРГЕТИЧНОЇ СИСТЕМИ В УМОВАХ ІНТЕГРАЦІЇ ВДЕ

Інтеграція значної частки вітрових (ВЕС) та сонячних (СЕС) електростанцій з мінливим (стохастичним) характером генерації спричинив ряд проблем для енергосистем, обумовлених їх недостатньої гнучкістю з виникненням надлишку електроенергії. Одним із можливих способів утилізації цієї надлишкової електроенергії та забезпечення стійкості енергосистем є використання технології Power-to-Heat (PtH) [1]. Технологія PtH за допомогою електричних теплогенераторів (ЕТГ) перетворює електричну енергію в теплову, яка передається системі централізованого теплопостачання (СЦТ), де вона споживається та /або акумулюється. В умовах декарбонізації енергосистеми при суттєвій частці потужностей ВЕС та СЕС системи централізованого теплопостачання можуть стати інструментом стабілізації її функціонування з утилізацією надлишку генерації ВЕС та СЕС.

Моделювання збалансованої роботи локальної мультиенергетичної системи при впровадженні значних обсягів ВЕС та СЕС спрямовано на забезпечення балансової надійності та стійкості її функціонування в умовах нерівномірності добового графіка споживання електроенергії, стохастичного характеру сонячної та вітрової генерації з використанням батарейних систем акумулювання електроенергії та технології Power-to-Heat за умови максимального залучення власних джерел генерації.

Основним принципом моделювання є забезпечення спільного покриття погодинного попиту на електричну енергію споживачів, під'єднаних до локальної мережі, та попиту на теплову енергії споживачів централізованого теплопостачання протягом календарного року.

В укрупненому вигляді баланс електричної потужності ЕС описується виразом:

$$P_t^{DS} + P_t^{VS} \pm P_t^{RS} \pm P_t^{ES} \pm P_t^{F} - Z_t^{L} - Z_t^{EHG} = 0\,, \qquad (1)$$

де t – час; P_t^{DS} – потужність диспетчеризованих джерел (ТЕЦ); P_t^{VS} – потужність мінливих джерел (ВЕС, СЕС); P_t^{RS} – потужність регулюючих джерел (газопоршневих, газотурбінних установок); P_t^{ES} – потужність електричних акумуляторних накопичувачів; P_t^{F} – потужність перетікання електроенергії; Z_t^{L} – потужність електричного навантаження; Z_t^{EHG} – потужність електричних теплогенераторів (електричні котли, теплові насоси).

Баланс теплової потужності ЦТ можна представити наступним виразом:

$$q_t^{B} + q_t^{CHP} + q_t^{EHG} - q_t^{L} \pm q_t^{TS} = 0\,, \qquad (2)$$

де q_t^{B} – потужність котелень; q_t^{CHP} – потужність відпуску теплової енергії від комбінованих установок (ТЕЦ, когенераційні установки); q_t^{EHG} – потужність електричних теплогенераторів; q_t^{L} – потужність теплового навантаження; q_t^{TS} – потужність теплових акумуляторів.

Стійкість енергосистеми забезпечується за умови:

$$P_t^{RS} \pm P_t^{ES} - Z_t^{EHG} \geq \Delta Z_t^{L} + \Delta P_t^{VS}, \quad (3)$$

де ΔZ_t^L – зміна електричного навантаження енергосистеми; ΔP_t^{CS} – зміна потужності ВЕС та СЕС.

Як видно із виразу (3), додаткові компоненти P_t^{ES} та Z_t^{EHG} можуть забезпечити більш широкі можливості щодо підтримки балансу потужностей та стійкості енергосистем (P_t^{ES} фактично є додатковим джерелом, яке може відпускати або споживати електроенергію у випадку різкого зменшення навантаження або сумарної потужності генерації).

Схема використання технології PtH в енергетичній системі (ЕС) та СЦТ [1] (рис. 1) передбачає споживання надлишкової енергії від ВЕС і СЕС для заряду батарейних акумуляційних системах з подальшим їх розряджанням у години підвищеного попиту або перетворенням технологіями PtH в теплову енергію для СЦТ з проміжним зберіганням її надлишку у теплових акумуляторах.

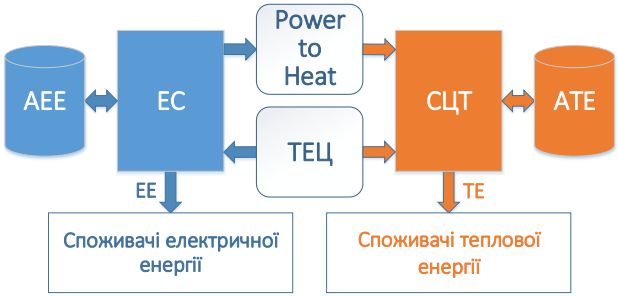


Рисунок 1. − Схема використання технології Power-to-Heat
(АЕЕ – акумулятори електроенергії, АТЕ – акумулятори теплової енергії, ТЕ – теплова енергія, ЕЕ – електроенергія)

Моделювання стійкого та збалансованого функціонування локальної мультиенергетичної системи базується на розвитку MILP моделі оптимального завантаження агрегатів локальної комбінованої системи енергопостачання системи для забезпечення попиту споживачів на електричну та теплову енергію [2] з залученням батарейних акумуляційних систем та ЕТГ для використання надлишкової електроенергії ВДЕ (ВЕС та СЕС).

Основними обмеженнями математичної моделі є баланси для кожного часового періоду доби між обсягами споживання і виробництва електричної та теплової енергії установками генерації електроенергії, теплової енергії, когенераційними та комбінованими установками, що розглядаються при моделюванні, з використанням акумуляційних систем накопичення електроенергії та електричних котлів.

Розроблену модель реалізовано на даних щодо споживання електричної та теплової енергії кінцевих споживачів громади міста Сміла [2], з

використанням програмно-інформаційного комплексу [3], розробленого з використанням комбінації стандартного програмного забезпечення Microsoft Excel і надбудови SolverStudio з використанням мови моделювання GMPL (GNU MathProg).

Покриття добового електричного та теплового навантаження локальної мультиенергетичної системи громади однієї доби опалювального сезону наведено на рис. 2.

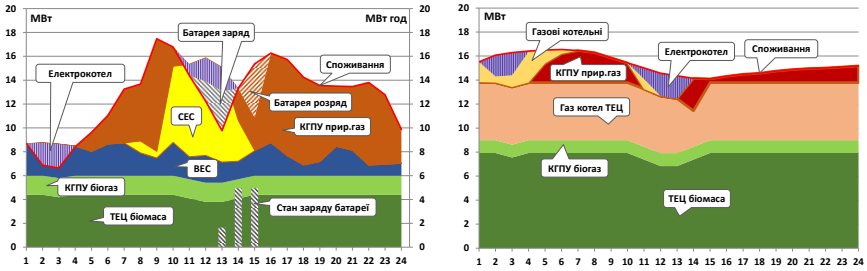


Рисунок 2. − Добові графіки покриття електричного (ліворуч) та теплового (праворуч) навантаження однієї доби опалювального сезону

Результати моделювання показали, що при виникненні надлишку потужності ВЕС у нічні години провалу попиту на електричну енергію та потужності СЕС у полуденні години зниження попиту на електричну енергію відбувається споживання електроенергії електроакумуляційними системами та електрокотлами, які перетворюють її в теплову енергію для покриття теплового навантаження СЦТ. Для підтримки теплового балансу відбувається зменшення відпуску теплової енергії котелень на природному газі.

Висновки

Моделювання застосування в локальній мультиенергетичній системі технології Power-to-Heat та накопичувачів енергії показало, що використання PtH технології забезпечує: гнучке регулювання енергетичного балансу; підвищення стійкості енергосистеми; зменшення споживання природного газу; зменшення викидів парникових газів; уникнення збитків від примусових обмежень вітрових та сонячних електростанцій.

1. Derii, O. V., Nechaieva, T. P., & Zgurovets, O. V. (2024). Technological possibilities of increasing the resilience of the power and district heating systems of Ukraine. *Energy Technologies & Resource Saving*, 81(4), 5–21. https://doi.org/10.33070/etars.4.2024.01.
2. Nechaieva, T., Teslenko, O., Trokhaniak, V., & Makarevych, S. (2025). Modelling the energy balances community under conditions increasing energy independence and reducing greenhouse gas emissions. *Machinery & Energetics*, 16(1), 104-116. DOI: 10.31548/machinery/1.2025.104.
3. Denysov, V., & Babak, V. (2023). Software and information simulation complex of multi-node integrated and autonomous power and heat supply systems. *System Research in Energy*, 2023 (3), 50–63. https://doi.org/10.15407/srenergy2023.03.050.

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

ДЕФІНІЦІЯ ПОНЯТТЯ РЕЗИЛЬЄНТНОСТІ ПРАЦІВНИКА ОРГАНІЗАЦІЇ ДО АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Атаки соціальної інженерії орієнтовані здебільшого на працівників організацій. Це пов'язано, по-перше, зі специфікою реалізування таких загроз; по-друге, зі зосередженістю на людині як найбільш уразливому складникові забезпечування кібербезпеки [1]. Діяльність працівника здійснюється у межах встановлених функцій з визначеними обов'язками та повноваженнями. Вони дозволяють йому взаємодіяти з іншими працівниками та завдяки цьому забезпечувати досягненість організацією поставленої мети [2]. Урахування зазначеної інформації важливе при організуванні атак соціальної інженерії. Насамперед про середовище, місце, роль і поведінку працівника в ньому. Цим обумовлюється спроможність зловмисника отримувати доступ до чутливої інформації [1, 3]. Тому визначання поняття резильєнтності працівника організації до атак соціальної інженерії є актуальним завданням.

Встановлені функції з визначеними обов'язками та повноваженнями виконуються працівником у конкретному середовищі організації. Таке виконання супроводжується наданням доступу до глобальної мережі Інтернет. Водночас дані фактори доповнюються активним упровадженням у діяльність працівників організацій технологій штучного інтелекту. Існування таких точок входу дозволяє зловмисникам реалізовувати загрози соціальної інженерії. Це проявляється шляхом представляння ними, наприклад, новим працівником, адміністратором, фахівцем служби технічної підтримки або керівником. Крім того, надсиланням повідомлень зі закликанням до виконання негайних дій – підтвердження даних, переходження за посиланням, відкривання вкладених файлів. Тож діяльність працівника в конкретному середовищі організації відбувається з існуванням небезпек, готовністю до яких можливе пом'якшення атак соціальної інженерії [1, 3, 4].

Діяльність працівника в конкретному середовищі організації пов'язана з необхідністю урахування факторів волатильності, невизначеності, складності та неоднозначності [1, 5]. Їхнє врахування важливе, зокрема, з погляду захищання від атак соціальної інженерії. Оскільки врахування першого фактору дозволяє зважати на мінливість середовища. Воно може бути пов'язане як з появою нових технологій, так і зміненням умов праці. Окрема увага приділяється наявності достатнього обсягу інформації про уразливості, загрози, наслідки, ризики, а також заходи та засоби їх обробляння. Існування факторів волатильності та невизначеності в організаційному середовищі призводить до появи інших. Наприклад [5], складності діяльності працівника асоціюється з існуванням нечітких взаємозв'язків, швидких і несталих змін. Разом з тим, до неоднозначних дій з його боку можуть призводити

відсутність, недостатність або суперечливість інформації про уразливості, загрози, наслідки, ризики.

Запобігання проявам факторів впливу на діяльність працівника в конкретному середовищі організації можливе шляхом віддавання переваги застосуванню знань, умінь, навиків і, як наслідок, досвіду для приймання рішень (наприклад, переходити за посиланням або відкривати підозрілий файл чи ні). Тож здоровий глузд і практичне мислення пропонуються як фундаментальні принципи концепції резильєнтної поведінки працівника [5]. Виокремлюванням цих принципів емоційність залишається другорядною. Для цього також важливо працівнику об'єктивно аналізувати, інтерпретувати, піддавати сумнівам і перевіряти інформацію. Цим визначаються наступні принципи критичного та скептичного мислень. Задоволеність даних принципів досягається завдяки обміну даними про уразливості, загрози, наслідки, ризики та готовністю до навчання і самонавчання, зокрема. Тому зазначене загалом узгоджується з поняттям резильєнтності та дозволяє визначати стосовно працівника організації з огляду на його здатність засвоювання і адаптування до мінливого середовища діяльності за умови невизначеності [1, 2, 6].

Отже, дефініція поняття резильєнтності працівника організації до атак соціальної інженерії формулюється через його здатність засвоювання і адаптування до мінливого середовища діяльності. В даному випадку умовою невизначеності, по-перше, враховується обсяг інформації (відсутність/ наявність) про вразливості, загрози, наслідки та ризики. По-друге, впливання на застосування працівником знань, умінь, навиків з огляду на здобутий досвід залежно від обставин діяльності. Водночас йому важливо уникати емоційності в проявах поведінки. В діях опиратися на застосовність критичного та скептичного підходів до мислення. І загалом бути обізнаним стосовно як атак соціальної інженерії, так і заходів і засобів обробляння.

1. Мохор В. В. , Цуркан О. В., Герасимов Р. П., Яшенков В. П., Демченко І. М., Михайлова О. О. Куб резильєнтності працівників організацій до атак соціальної інженерії. Резильєнтність динамічних систем : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (Київ, 27 грудня 2024 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2024. С. 216, 217.
2. ISO 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07; revised 2023-07-14]. URL: https://www.iso.org/standard/73906.html (accessed on: 24.10.2025).
3. Widdowson A. Humans and Cyber Security. How Organisations Can Enhance Resilience Through Human Factors? Boca Raton, Abingdon : CRC Press, 2025. 152 p.

4. Hausken K. Cyber resilience in firms, organizations and societies. Internet of Things. 2020. Vol. 11. Article ID 100204. DOI: https://doi.org/10.1016/j.iot.2020.100204.
5. Warzawa T., Härting R.-C. Cyber Resilient Employee – Determinants and Definition. Procedia Computer Science. 2025. Vol. 270, P. 4334–4342. DOI: https://doi.org/ 10.1016/j.procs.2025.09.558
6. ISO 22372:2025. Security and resilience. Community resilience. Guidelines for infrastructure resilience. [Valid from 2025-10-24]. URL: https://www.iso.org/ standard/50275.html (accessed on: 24.10.2025).

П.В. Шиманюк

РОЗРАХУНОК ВТРАТ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ ПРИ ЗМІНІ ТОПОЛОГІЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Для зменшення витрат на компенсації втрат електроенергії запропоновано використання сучасних методів прогнозування на основі штучних нейронних мереж. Дослідження охоплює розробку та порівняння трьох архітектур: Transformer, LSTM та eResNet, для оцінки точності прогнозуваня втрат у розподільних мережах [1-3].

На рисунках 1-3 наведено блок-схеми архітектури нейронних мереж.

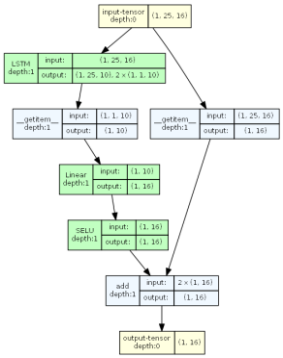


Рисунок 1. – Архітектура нейронної мережі LSTM для одночасного прогнозу вузлового навантаження

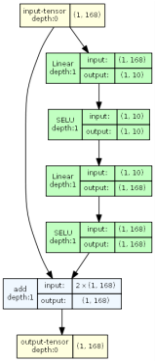


Рисунок 2. – Архітектура нейронної мережі eResNet з блоком автоенкодера та скороченим з’єднанням

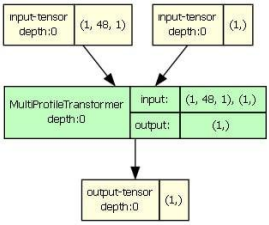


Рисунок 3. – Архітектура нейронної мережі Transformer для атаптивного прогнозу для кожного інтервалу часу

Основна увага приділялася архітектурі Transformer яка базується на механізмі самоуваги (self-attention) [4], і дозволяє ефективно виявляти залежності між елементами часових рядів незалежно від їх розташування. На відміну від рекурентних моделей, Transformer обробляє всю послідовність одночасно, що забезпечує високу швидкість обчислень та масштабованість.

Для прогнозування вузловоого навантаження було запропоновано модифіковану модель MultiProfileTransformer. Вона враховує добову зміну навантаження, формуючи окремі прогнози для кожного півгодинного інтервалу доби. Модель складається з вхідного шару розмірності 32, двох трансформерних кодерів з чотирма точками уваги та вихідного шару з 48 окремих лінійних блоків, рисунок 3.

Паралельно було протестовано модель eResNet, яка складається з трьох автоенкодерних блоків із SELU-активацією, та класичну рекурентну модель LSTM. Навчання моделей проводилось на процесорі Intel i3 10100 (3.6 ГГц, 16 ГБ ОЗП). Час навчання: LSTM — 15 хв, eResNet — 8 хв, Transformer — до 4 годин (для навантаження) та менше хвилини (для втрат).

Для навчання моделей використано ретроспективні дані ОСР України за період 2017–2019 років. Набір містить вимірювання з 16 вузлів навантаження з дискретністю 30 хвилин, загалом 48 048 значень. Для моделювання втрат застосовано еталонну мережу середньої напруги CIGRE [5], яка включає 15 вузлів та два трансформатори потужністю 25 МВА (110/20 кВ).

Було перевірено стійкість моделей до змін топології мережі шляхом розрахунку режимів при відключенні автоматичних вимикачів рисунок 4-8.

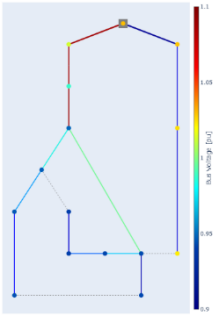


Рисунок 4. – Базова топологія (3 вимикачі вимкнено, пунктир)

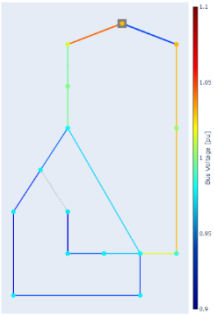


Рисунок 5. – Вимикач 1 вимкнуто

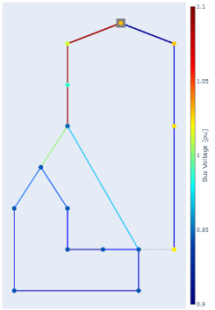


Рисунок 6. – Вимикач 2 вимкнуто

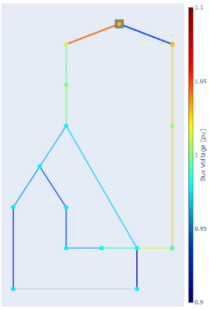


Рисунок 7. – Вимикач 3 вимкнуто

Результати показали, що зміна втрат не перевищує 2%, що свідчить про стабільність моделей, але також вказує на необхідність точнішого калібрування або вибору іншої тестової мережі.

В дослідженні було застосовано методи попередньої обробки даних — виявлення та заміна аномальних значень, що суттєво підвищило точність прогнозів [6-7].

Для оцінки точності моделей використано функцію середньої абсолютної похибки у відсотках (MAPE). Порівняльний аналіз представлено у таблиці 1.

Найменшу похибку забезпечує підхід з прогнозом навантаження, що підтверджує його перевагу над прямим прогнозом втрат.

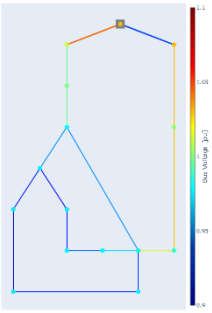


Рисунок 8. –. Всі вимикачі увімкнуто

Таблиця 1. − Результати розрахунку втрат на за допомогою різних методів прогнозування

Методи який застосовується	Величина похибки MAPE, %
Прогноз втрат без аномальних значень (Transformer)	14.56
Прогноз втрат без аномальних значень (eResNet)	20.24
Втрати за прогнозними значеннями без аномальних значень	8.4

Модель Transformer показала гарні результати при прямому прогнозуванні втрат, при тому прогноз вузлового навантаження з подальшим розрахунком втрат займає багато часу та обчислювальних ресурсів.

Запропоновані методи прогнозування демонструють високу ефективність в задачах короткострокового прогнозування втрат електроенергії. Інтеграція алгоритмів попередньої обробки дозволяє підвищити точність моделей. Найкращі результати досягаються при прогнозуванні навантаження з подальшим розрахунком втрат, що забезпечує більш надійне управління енергомережами. Дане дослідження є частиною спільного Українсько-Литовського науково-дослідного проєкту «Smart Grid модель для оперативного керування розподільними мережами на основі методів штучного інтелект»

1. Vaswani, A., Shazeer, N., Parmar, N., et al. (2017). Attention Is All You Need. In Advances in Neural Information Processing Systems (NeurIPS), 30. https://arxiv.org/abs/1706.03762.
2. Albeladi, K., Zafar, B., Mueen, A.: Time series forecasting using LSTM and ARIMA. Int. J. Adv. Comput. Sci. Appl. 14(1), 313–320 (2023).
3. V. Miroshnyk, P. Chernenko, P. Shymaniuk Univariable short-term forecast of nodal electrical loads of energy systems. Tekhn. elektr., (2), 67-73 (2020). DOI: https://doi.org/10.15407/techned2020.02.067.
4. G. Antonesi, T. Cioara, I. Anghel, V. Michalakopoulos, E. Sarmas, and L. Toderean, “A systematic review of transformers and large language models in the energy sector: towards agentic digital twins,” Applied Energy, vol. 401, p. 126670, Dec. 2025, doi: https://doi.org/10.1016/j.apenergy.2025.126670.
5. ELECTRA. (2014). Benchmark systems for network integration of renewable and distributed energy resources. https://e-ci-gre.org/publication/ELT_273_8-benchmark-systems-for-network-integration-of-renewable-and-distributed-energy-resources.
6. Блінов І.В., Мірошник В.О., Шиманюк П.В., Сичова В.В. Вплив аномальних значень наточність прогнозування втрат в розподільчих мережах. Енергетика: економіка,технології, екологія. 2024. №4 С.149-154. https://doi.org/10.20535/1813-5420.4.2024.316249.
7. Blinov, I.; Radziukynas, V.; Shymaniuk, P.; Dyczko, A.; Steculа, K.; Sychova, V.; Miroshnyk,V.; Dychkovskyi, R. Smart Management of Energy Losses in Distribution Networks UsingDeep Neural Networks. Energies 2025, 18, 3156. https://doi.org/10.3390/en18123156.

Є.В. Парус, І.В. Блінов

МОДЕЛІ ЕКОНОМІЧНОЇ ДИСПЕТЧЕРИЗАЦІЇ НА ДОБУ НАПЕРЕД ДЛЯ ВЛАСНОГО ЕЛЕКТРОСПОЖИВАННЯ МІКРОМЕРЕЖІ

Один із важливих напрямів розвитку електроенергетики України визначає впровадження технологій розподіленої генерації та засобів управління локальними електроенергетичними системами [1], зокрема створення мікромереж на принципах “розумних мереж” [2]. Основні вимоги до архітектури та функцій мікромереж наведені у міжнародних стандартів, зокрема у серії IEC TS 62898. Однією з важливих задач є побудова моделей економічної диспетчеризації енергетичного устаткування мікромережі на добу наперед з метою мінімізації вартості закупівлі електроенергії власником мікромережі у електропостачальника.

Математичні моделі імітують режими енергетичного устаткування мікромережі з двома основними цілями за класифікацією [3]:

– підвищення надійності та забезпечення енергопостачання для всіх навантажень або критичної їх частини в острівному режимі роботи мікромережі (ціль А по [3]);

– зниження вартості електроенергії, спожитої користувачами мікромережі, у режимі підключення до системи розподілу шляхом оптимізації функцій установки зберігання енергії (УЗЕ) (ціль С по [3]).

Дослідження актуальних для України цілей експлуатації мікромережі наведено в [4], а актуальних функцій енергоменеджменту – у [5].

Бізнес-модель функціонування мікромережі передбачає використання локальних енергетичних ресурсів виключно для забезпечення власних потреб електроспоживання. Експорт електроенергії із мікромережі у систему розподілу не допускається. Тому профіцит генерації СЕС, який неможливо використати для поточного електроспоживання чи для накопичення в УЗЕ, примусово обмежується.

Математичні моделі враховують такі основі енергетичні ресурси мікромережі, як: недиспетчеризоване навантаження в мікромережі з виділенням критичної його частини; інвертор (основний засіб оперативного управління режимами мікромережі); сонячна електростанція (локальна недиспетчеризована генерація); УЗЕ (основний засіб оптимізації балансів енергії в мікромережі) та приєднання до системи розподілу (балансуючий вузол для схеми електричних з’єднань та джерело електроенергії з ринковою вартістю).

Ціль задачі економічної диспетчеризації визначає мінімізацію вартості закупівлі електричної енергії:

$$Min(GF) = \sum_{h=1}^{24}\left(C_h^{\text{куп}} \cdot V_h^{\text{СР}}\right) + \sum_s PF_s$$

де: $C_h^{\text{куп}}$ – ціна купівлі електроенергії у електропостачальника в розрахунковий період *h*, (₴/кВт·год); $V_h^{\text{СР}}$ – змінна оптимізації, обсяги отриманої (імпортованої) із системи розподілу електроенергії в розрахунковий період *h*, (кВт·год); PF_s – штрафні функції для врахування додаткових не цінових критеріїв оптимізації.

Процедура оптимізації використовує наступні штрафні функції.

А) штраф за не використаний (обмежений) профіцит генерації СЕС:

$$PF_{\text{СЕС}} = K_{\text{СЕС}}^{\text{PF}} \cdot \sum_{h=1}^{24} C_h^{\text{куп}} \cdot V_{\text{R},h}^{\text{СЕС}}$$

де: $K_{\text{СЕС}}^{\text{PF}}$ – коефіцієнт штрафу, $V_{\text{R},h}^{\text{СЕС}}$ – змінна оптимізації, обсяги примусового обмеження генерації СЕС в розрахунковий період *h*, (кВт·год).

У процесі оптимізації штрафна функція стимулює накопичення в УЗЕ частини генерації СЕС, коли власне електроспоживання в мікромережі вже повністю забезпечується енергією від СЕС. Якщо значення профіциту генерації СЕС більше за максимум потужності заряджання УЗЕ, або ємність накопичувача УЗЕ вже заповнена, то такий залишок профіциту підлягає примусовому обмеженню і за результатами оптимізації означує відповідне значення змінної $V_{\text{R},h}^{\text{СЕС}}$.

Б) штраф за нерівномірний графік заряджання/розряджання УЗЕ в години з однаковими ринковими цінами:

$$PF_{\text{УЗЕ}} = K_{\text{УЗЕ}}^{\text{PF}} \cdot \sum_{h=1}^{24} C_h^{\text{куп}} \cdot \left(\frac{\Delta V_{\text{зар,max}}^{\text{УЗЕ}}}{\left(V_{\text{зар,max}}^{\text{УЗЕ}}\right)^2} \cdot \left(V_{\text{зар},h}^{\text{УЗЕ}}\right)^2 + \frac{\Delta V_{\text{роз,max}}^{\text{УЗЕ}}}{\left(V_{\text{роз,max}}^{\text{УЗЕ}}\right)^2} \cdot \left(V_{\text{роз},h}^{\text{УЗЕ}}\right)^2 \right)$$

де: $K_{\text{УЗЕ}}^{\text{PF}}$ – коефіцієнт штрафу; $V_{\text{зар},h}^{\text{УЗЕ}}$, $V_{\text{роз},h}^{\text{УЗЕ}}$ – змінні оптимізації, обсяги відповідно заряджання та розряджання енергії в УЗЕ за розрахунковий період h, (кВт·год); $V_{\text{зар,max}}^{\text{УЗЕ}}$, $V_{\text{роз,max}}^{\text{УЗЕ}}$ – обсяги енергії в УЗЕ в умовах максимальної потужності відповідно заряджання та розряджання протягом розрахункового періоду h, (кВт·год); $\Delta V_{\text{зар,max}}^{\text{УЗЕ}}$, $\Delta V_{\text{роз,max}}^{\text{УЗЕ}}$ – втрати електроенергії в умовах максимальної потужності відповідно заряджання та розряджання протягом розрахункового періоду *h*, (кВт·год).

Штрафна функція розраховує умовну вартість втрат енергії в УЗЕ у режимах заряджання і розряджання. Функція стимулює вирівнювання потужностей заряджання/розряджання УЗЕ у години з однаковими ринковими цінами незалежно від обсягів електроспоживання в мікромережі у ці періоди часу. Штрафна функція дорівнює нулю, коли УЗЕ знаходиться у стані очікування.

В) штраф за нерівномірний графік імпорту електроенергії заряджання/розряджання УЗЕ в години з однаковими ринковими цінами:

$$PF_{\text{СР}} = K_{\text{СР}}^{\text{PF}} \cdot \sum_{h=1}^{24} C_h^{\text{куп}} \cdot \left(V_h^{\text{СР}}\right)^2$$

де: $K_{\text{СР}}^{\text{PF}}$ – коефіцієнт штрафу.

Штрафна функція розраховує умовну вартість втрат енергії в мікромережі. Додатково штрафна функція може застосовуватися для контролю коректності станів УЗЕ, як наведено у [6]. Альтернативний спосіб контролю станів УЗЕ з використанням системи бінарних змінних представлений у [7].

Для оптимізації додатково використовується система обмежень, якою визначаються: баланси енергії в мікромережі, контроль потоків енергії від СЕС, контроль потоків енергії від УЗЕ, контроль рівня заповнення накопичувача УЗЕ та контроль рентабельної експлуатації УЗЕ. Детальний опис системи обмежень висвітлено у [6, 7].

Запропоновані моделі поєднують завдання підтримки стану готовності до ізольованого режиму мікромережі на основі використання УЗЕ та завдання раціонального використання доступних енергоресурсів для оптимізації за економічними критеріями графіків закупівлі електроенергії.

Підготовлено за результатами виконання наукової роботи «Забезпечення ефективного функціонування та розвитку розподіленої енергетики в Україні з використанням технологій мікромереж» (шифр: РЕЖИМ-3, КПКВК 6541230).

1. Про схвалення Стратегії розвитку розподіленої генерації на період до 2035 року і затвердження операційного плану заходів з її реалізації у 2024 - 2026 роках. Розпорядження Кабінету Міністрів України.18.07.2024 №713-р.
2. Концепція впровадження “розумних мереж” в Україні до 2035 року. Розпорядження Кабінету Міністрів України 14.10.2022 № 908-р.
3. IEC TS 62898-1: 2017+AMD 1: 2023 Microgrids – Part 1: Guidelines for microgrid projects planning and specification. 2023. 78 p.
4. Блінов, І.В., С.О. Палачов, Є.В. Парус, О.Г. Клименко. Сценарії використання мікромереж згідно з міжнародними стандартами. Праці Інституту електродинаміки Національної академії наук України, вип. 70, Квітень 2025, с. 014, https://doi.org/10.15407/publishing2025.70.014.
5. Блінов, І.В., С.О. Палачов, Є.В. Парус, О.Г. Клименко. Структура та функції систем енергоменеджменту мікромережі в умовах підключення до системи розподілу згідно до вимог міжнародних стандартів. Праці Інституту електродинаміки Національної академії наук України, вип. 71, Серпень 2025, с. 15 – 27, DOI: https://prc.ied.org.ua/index.php/proceedings/article/view/404.
6. Блінов І., Парус Є., Шиманюк П., Ворушило А. Модель оптимізації функціонування мікромережі з СЕС та установкою зберігання енергії. *Технічна електродинаміка*. 2024. № 5. С. 69-78 DOI: https://doi.org/10.15407/techned2024.05.069.
7. Парус Є.В., Блінов І.В. Оптимізація використання доступних енергоресурсів мікромережі за умов підтримки готовності до ізольованого режиму. *Технічна електродинаміка*. 2025. №5. С. 56-69. DOI: https://doi.org/10.15407/techned2025.05.056.

М.С. Дунаєвський, О.М. Хом'як, О.С. Шаталов

ВИКОРИСТАННЯ МЕТОДУ ВИРІВНЮВАНОЇ ВАРТОСТІ ДЛЯ ПОРІВНЯННЯ ТЕХНОЛОГІЙ ГЕНЕРАЦІЇ ЕЛЕКТРОЕНЕРГІЇ

Вступ. Підвищення енергобезпеки України забезпечується пришвидшеними темпами розвитку енергетики на основі відновлювальних джерел електроенергії (ВДЕ), будівництвом додаткових виробників електроенергії, нарощуванням кількості енергонакопичувачів у системі [1]. Серед завдань, що стоять перед цими процесами не тільки економічні цілі, але й цілі забезпечення резильєнтності критичної інфраструктури, якою є енергосистема [2]. Зокрема, збільшення кількості розподілених генераторів електроенергії, кількості активних учасників (prosumers) та агрегаторів на енергоринку забезпечують вищий рівень його децентралізації, а відтак і стійкості. Якщо короткострокова стійкість потребує, зокрема, застосування високооптимізованих методів балансування, то довгострокова стійкість передбачає методологічну порівняльну оцінку переліку довгострокових проектів з будівництва перспективних енергопотужностей, з подальшою реалізацією найбільш конкурентного проекту [3, 4].

Мета та завдання. Мета та завдання цієї роботи – продемонструвати приклад використання методу вирівнюваної вартості для порівняння витрат на генерацію електроенергії.

Виклад основного матеріалу. В методі вирівнюваної вартості (levelised cost) для порівняння різних технологій обчислюють вартість електроенергії на 1 кВт-год або річні витрати на володіння та функціонування електростанції [4].

Як прийнято у будь-якому аналізі проектів, спочатку визначається поточна приведена вартість (present value (PV)) інвестицій та регулярних витрат (recurring costs). Далі ця величина розподіляється на рівномірний еквівалентний ряд років життєвого циклу. В цьому полягає концепція вирівнювання, що відіграє важливу роль в аналізі проектів енергетики. Оскільки термін служби технологій генерації зазвичай є довготривалим (15–40 років), а деякі компоненти витрат з часом можуть істотно дорожчати, то порівнювати витрати простіше, якщо для кожної технології знаходити єдине постійне значення всіх витрат, еквівалентне їх поточній вартості. Щоб обчислити величину вирівнюваної вартості, потрібно перетворити ряд значень річних витрат у деяку величину, використовуючи коефіцієнт дисконтування i в часі.

Припустимо, що вартість електроенергії щороку зростає з певним темпом. Поточна приведена вартість цього зростаючого ряду визначається як $PV = A \times PVF$, де A – поточна річна (annual) вартість, а коефіцієнт поточної вартості (present value factor (PVF)) розраховується як

$PVF = \frac{\left[1 - \frac{(1+a)^n}{(1+i)^n}\right]}{(1-a)}$, де a – коефіцієнт річного зростання ціни палива (використовуваного для генерації електроенергії), n – кількість років інвестиційного горизонту.

Вирівнювана середньорічна вартість (levelised annual cost) визначається як $PV \times CRF$, де $CRF = \left[\frac{i(1+i)^n}{(1+i)^n - 1}\right]$ – коефіцієнт відновлення капіталу (Capital Recovery Factor (CRF)).

Оскільки виробництво електроенергії передбачає витрати на паливо, інші непаливні витрати на експлуатацію та технічне обслуговування (operation and maintenance costs), інвестиції (фіксовані витрати), то кожний з цих елементів використовується для обчислення вирівнюваної вартості. Загальні витрати за весь життєвий цикл визначаються на основі цих складових. Відношення цих витрат до загального обсягу електроенергії, виробленої протягом життєвого циклу (кВт-год), дає питомі витрати електроенергії ($/кВт-год).

Для обчислення вирівнюваної вартості достатньо таких послідовних кроків: 1) зібрати дані про електростанцію та сформулювати припущення щодо її характеристик, експлуатаційних і капітальних витрат, ставки дисконтування; 2) обчислити чисту поточну вартість (net present value (NPV)) NPV_c капітальних та експлуатаційних витрат; 3) розрахувати NPV_e виробленої електроенергії протягом життєвого циклу, враховуючи дисконтування; 4) обчислити вирівнювану вартість як відношення $\frac{NPV_c}{NPV_e}$.

Використовуючи обчислення вирівнюваної вартості, для прикладу порівняємо дві технології (електростанції) – вугільну та парогазову (combined cycle). Вихідні дані для розрахунку вирівнюваних витрат наступні: для кожної потужність становить 400 МВт, завантаженість 70%, припускаємо щорічний ріст цін на паливо на рівні 4%, вирівнювану ренту основних активів (levelized fixed charge rate) на рівні 15%, двадцятирічний горизонт інвестиційного проекту; вартість побудови вугільної електростанції в перерахунку на кіловати потужності 1100 $/кВт, парогазової 700 $/кВт, фіксована складова операційних витрат на рік (fixed O&M cost) 20 $/кВт та 9 $/кВт відповідно, змінна складова операційних витрат на рік (variable O&M cost) 5 $/кВт та 3 $/кВт відповідно, теплова потужність (heat rate) 2100 ккал/кВт-год та 1950 ккал/кВт-год, вартість палива 8 $/Гкал та 20 $/Гкал. Необхідно визначити, який варіант є кращим.

Розрахуємо спершу фактор вирівнювання (levelisation factor). Оскільки ставка дисконтування (10%), щорічний ріст цін на паливо (4%) та

інвестиційний горизонт (20 років) однаковий для двох технологій значення фактору вирівнювання буде одним і тим же.

$$U = PVF \times CRF == \frac{\left[1 - \frac{(1+0.04)^{20}}{(1+0.1)^{20}}\right]}{(1-0.04)} \left[\frac{0.1(1+0.1)^{20}}{(1+0.1)^{20}-1}\right] = 1.32 .$$

Щорічні витрати для вугільної електростанції становитимуть:

$$400 МВт \times 70\% \times 8760(год/р.) \times 2100(ккал/кВт \cdot год) \times 8(\$/Гкал) \times 1.32 \times \frac{1}{10^9} =$$

$= 54.4$ млн \$/рік. Щорічні витрати для електростанції з комбінованим парогазовим циклом становитимуть: $400 МВт \times 70\% \times 8760(год/р.) \times 1950(ккал/кВт \cdot год) \times 20(\$/Гкал) \times 1.32 \times$

$\times \frac{1}{10^9} = 126.28$ млн \$/рік. Змінна складова операційних витрат на рік для вугільної електростанції становитиме $400 МВт \times 70\% \times 8760(год/р.) \times$

$\times 5(\$/МВт \cdot год) \times 1.32 \times \frac{1}{10^6} = 16.19$ млн \$/рік. Змінна складова операційних витрат на рік для електростанції з комбінованим парогазовим циклом становитиме $400 МВт \times 70\% \times 8760(год/р.) \times 3(\$/МВт \cdot год) \times$

$\times 1.32 \times \frac{1}{10^6} = 9.71$ млн \$/рік. Фіксована складова операційних витрат на рік для вугільної електростанції становитиме: $400 МВт \times 20(\$/кВт/р.) \times 1.32 \times \frac{1}{10^3} = 10.56$ млн \$/рік. Фіксована складова операційних витрат на рік для електростанції з комбінованим циклом становитиме: $400 МВт \times 9(\$/кВт/р.) \times 1.32 \times \frac{1}{10^3} = 4.75$ млн \$/рік. Щорічні інвестиційні витрати для вугільної електростанції: $400 МВт \times 1100(\$/кВт) \times 0.15 \times \frac{1}{10^3} = 66$ млн \$/рік. Щорічні інвестиційні витрати для електростанції комбінованого циклу: $400 МВт \times 700(\$/кВт) \times 0.15 \times \frac{1}{10^3} = 42$ млн \$/рік.

Загальні вирівнювані витрати вугільної електростанції на рік таким чином становлять: $54.4 + 16.19 + 10.56 + 66 = 147.15$ млн \$/рік. Аналогічні витрати електростанції з комбінованим парогазовим циклом становлять $126.28 + 9.71 + 4.75 + 42 = 182.74$ млн \$/рік.

Чиста приведена вартість генерації електроенергії (NPV of electricity generation) кожної зі станій становить $\frac{(400\times 0.7\times 8760)}{\left(0.1\times 1.1^{20}\right)} = 3645930.9$.

Вирівнювана вартість електроенергії (levelized electricity cost) за кВт-год для вугільної електростанції становить $\frac{0.14715}{3645930.9} = \$\ 0.0404$, а для електростанції з комбінованим циклом $\frac{0.182.74}{3645930.9} = \$\ 0.0501$.

Отже, за наведених припущень вугільна технологія має дещо нижчі вирівнювані витрати й відповідно математично є кращим вибором. Водночас слід зауважити, що вартість залежить від припущень, зокрема щодо коефіцієнта використання потужності, темпів зростання витрат та технічної ефективності. В прикладі не враховано зовнішні витрати або витрати, пов'язані з викидами вуглецю. Результати можуть змінитися при включенні цих чинників до аналізу.

Висновки. Розглянутий метод вирівнюваної вартості дозволяє оцінювати та порівнювати вартості різних технологій електрогенерації. Його розширення задля врахування зовнішніх витрат, а також задля моделювання більш складних технологічних процесів, може стати основою методології інвестиційної оцінки довгострокових проектів будівництва електростанцій.

Дослідження здійснено в рамках проекту «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації», що виконується за напрямом використання бюджетних коштів «підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок» бюджетної програми КПКВК 6541230 в НАН України.

1. Горбачук В.М., Дунаєвський М.С., Сирку А.А. (2020). Сучасні питання генерування та накопичення енергії в енергосистемі України. Східна Європа: економіка, бізнес та управління. Випуск 1 (24). С. 260–268.
2. Горбачук В.М., Лупей М.І., Дунаєвський М.С. (2022) Підходи до резильєнтності критичних інфраструктур. Science and education for sustainable development. A.Ostenda, V.Smachylo (eds.) Katowice, Poland: University of Technology, Katowice. P. 87−95. DOI:10.54264/M005.
3. Каплун В., Войтенко В., Стецюк П., Хом'як О. (2025) Балансування мікроенергосистем з адресним потокорозподілом потужності та мінімізацією втрат електроенергії. Збірник тез доповідей за матеріалами III міжнародної науково-практичної конференції «Цифрові технології в енергетиці і автоматиці» (6 червня 2025 р., Київ, Україна). С. 23–25.
4. Bhattacharyya S.C. Energy Economics: Concepts, Issues, Markets and Governance (2019). 2nd ed. P. 699–734.

С.Ф. Гончар, М.Ю. Комаров, О.С. Потенко

МЕТОД ОЦІНЮВАННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ НА ОСНОВІ ВИЗНАЧЕННЯ КУТОВОГО КОЕФІЦІЄНТА

На сьогоднішній день не можна гарантувати повну захищеність будь-якої інформаційної системи, у тому числі об'єкта критичної інформаційної інфраструктури (далі – системи) [1]. Якщо раніше метою було забезпечення кібербезпеки системи, то поступово вона трансформується у забезпечення кіберрезильєнтності. Як зазначається в [2] кібербезпека зосереджена на зміцненні системи, щоб запобігти зменшенню її функціональності, увага приділяється ступеню зменшення функціональності, а кіберрезильєнтність зосереджена на відновленні функціональності системи. Відновлення може бути повним або частковим, та передбачає адаптацію системи, яка підвищить її стійкість до майбутніх деструктивних дій або, в деяких випадках, покращить її функціональність. При цьому, на перший план виходять задачі мінімізації часу відновлення функціональності системи, забезпечуючи захист життєво важливих її компонентів, тобто, забезпечення кіберрезильєнтності інформаційних систем об'єктів критичної інформаційної інфраструктури, як стану критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз [3].

Враховуючи викладене вище актуальною задачею являється оцінювання кіберрезильєнтності систем, що дасть змогу оцінити кіберрезильєнтність, порівняти з допустимим значенням, зробити висновок про її достатність чи необхідність підвищення тощо.

Підхід до оцінювання кіберрезильєнтності із застосуванням аналізу ризиків досліджено в [4], оцінювання кіберрезильєнтності на основі визначення площі під кривою функціональності системи досліджено в [5], методи оцінювання кіберрезильєнтності об'єктів критичної інфраструктури розглянуто в [6]. В даних дослідженнях, зокрема, зазначається, що для дуже складних і взаємопов'язаних систем оцінка ризику стає обмеженою у сфері кібербезпеки оскільки стає надзвичайно важко провести оцінку ризику, яка адекватно враховує потенційні каскадні ефекти, які можуть виникнути.

З урахуванням розглянутих підходів до оцінювання кіберрезильєнтності систем можна зазначити, що кіберрезильєнтність системи буде визначатися довжиною лінії поглинання та кутом її нахилу до осі абсцис, а також довжиною лінії відновлення та кутом її нахилу до осі ординат, рис. 1. Таким чином, кіберрезильєнтність пропонується оцінювати за виразом:

$$CR = \frac{T_2 - T_1}{F_0 - F_1} + \frac{F_2 - F_1}{T_3 - T_2}, \quad (1)$$

де F0 – номінальна функціональність системи;
F1 – функціональність системи після завершення фази поглинання;
F2 – функціональність системи після завершення фази відновлення;
T1 – час початку фази поглинання;
T2 – час завершення фази поглинання;
T3 – час завершення фази відновлення.

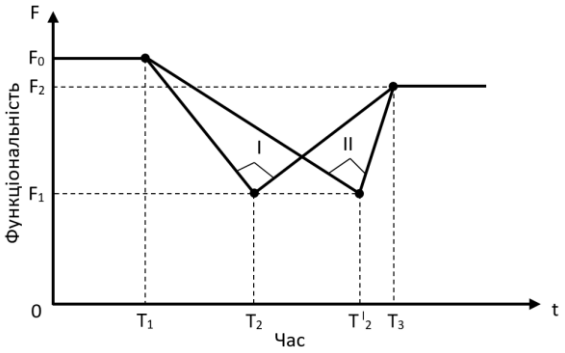


Рисунок 1. – Щодо методу оцінювання кіберрезильєнтності на основі визначення кутового коефіцієнта

Вираз для визначення кіберрезильєнтності (1) враховує кут нахилу лінії поглинання до осі абсцис, а також довжиною кут нахилу лінії відновлення до осі ординат.

1. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія / С.Ф. Гончар. – Київ : «Альфа реклама», 2019. – 176с.
2. Kott, A. and Linkov, I., 2021. To Improve Cyber Resilience, Measure It. IEEE Computer, 54(2), Feb.2021, pp.80-85.
3. Гончар С.Ф. Методологія оцінки ризиків кібербезпеки інформаційної системи об'єктів критичної інфраструктури // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. – 2019. – Т.30(69). Ч.1. – №4. – С. 40-44.
4. Гончар С.Ф., Комаров М.Ю. Підхід до оцінювання кіберрезильєнтності із застосуванням аналізу ризиків : Матеріали науково-практичної конференції «Кібербезпека енергетики», Київ, 2025. – С. 43-44.
5. Гончар С.Ф., Комаров М.Ю. Дослідження методів оцінювання кіберрезильєнтності : Матеріали науково-практичної конференції «Резильєнтність динамічних систем», Київ, 2025. – С. 13-14.
6. Комаров М.Ю., Гончар С.Ф. Огляд методів оцінювання кіберрезильєнтності об'єктів критичної інфраструктури : Матеріали науково-практичної конференції «Кібербезпека енергетики», Київ, 2025. – С. 22-24.

В.Р. Сенченко, А.В. Бойченко

ВИКОРИСТАННЯ ОНТОЛОГІЧНИХ МОДЕЛЕЙ ДЛЯ ДОСЛІДЖЕННЯ ВЗАЄМОПОВ'ЯЗАНИХ КРИТИЧНИХ ІНФРАСТРУКТУР

Дослідження поширення каскадного ефекту у ряді пов'язаних критичних інфраструктур є важливим для забезпечення їх надійності та безперервності функціонування. Каскадний ефект виникає через взаємозв'язки між окремими елементами інфраструктури, коли збої в одному елементі спричиняють послідовні порушення в інших. Аналіз таких явищ потребує пошуку нових підходів до моделювання складних системних взаємозв'язків із застосуванням формалізованих методів опису.

Сучасні дослідження підтверджують що комп'ютерні онтології, надають широкі можливості для моделювання складної природи критичної інфраструктури [1 -5]. Зокрема, заслуговує уваги використання можливостей логічного висновку при дослідженні гетерогенних даних для різних доменів [2] та розробка інтегрованої онтології, зосередженої на кібербезпеці аеропортів [3]. У роботі [4] запропонований підхід до онтологічного пошуку інформації з відкритих джерел географічних даних застосовний до захисту критичної інфраструктури що дозволяє дозволяє створити розуміння загроз і вразливостей без необхідності фізичного доступу чи використання закритих даних. Дослідження на прикладі взаємопов'язаних систем дренажу, транспорту та будівництва під впливом міських повеней показує, що використання онтологій ефективно сприяє виявленню взаємозалежностей між різними інфраструктурними системами [5].

Вивчення каскадного ефекту через поєднання онтологічного й графового аналізу є перспективним напрямом для дослідників і практиків. Використання онтологічних моделей для дослідження складних організаційно-технічних систем показало свою ефективність у ряді робіт [6, 7].

Процедура побудови онтологічної моделі критичної іфраструктури для подальшошого дослідження включає наступні кроки:

- розробка концептуальної моделі інфраструктурних систем;
- створення класів онтології та ієрархій властивостей;
- кодування взаємозалежностей через об'єктні властивості;
- додавання індивідів як конкретних втілень розроблених класів;
- застосування правил логіки для прихованих зв'язків;
- перевірка логіки онтології за допомогою засобів виведення;
- візуалізація структури онтології та шляхів залежностей;
- перевірка онтології експертами предметної області.

Початковим етапом семантичного моделювання є побудова концептуальної моделі ПрО. Семантичні (онтологічні) моделі взаємодії КІ

урбаністичного регіону використовують онтології для визначення сутностей інфраструктури та їх компонентів: об'єкти, класи основні концепти, визначення і значення властивостей, аксіоми. Для побудови коректної моделі взаємодії КІ сутності мають відображувати як фізичні властивості інфраструктури (генератор, лінія передачі, портовий кран, насос), так і сутності управлінських систем, які входять до складу кожної КІ (SCADA система, комунікаційна система, ERP системи, білінгова система тощо).

Формально модель онтології, яка описує взаємодію КІ в межах урбаністичного регіону при виникненні каскадного ефекту – $Ont(CI)_{ur}$, можна представити у вигляді математичного виразу

$$\boldsymbol{Ont(CI)_{ur} = < C^{(CI)}, Rel^{(CI)}, At^{(CI)}, Ex^{(C)}, Rul^{(S)}, Ad^{C(md)} >}$$

де: $C^{(CI)}$ – підмножина класів (<Classes>) основних концептів – семантичних понять (<Entities>), які визначають основні класи як фізичних, так і допоміжних об’єктів КІ;

$Rel^{(CI)}$ – підмножина відношень (<Relationship>) між класами C^((CI)) об’єктів КІ або екземплярами класів. Відношення описуються через <Object properties> та задаються предикатами – дієсловами через які описуються відношення (наприклад, «залежить від…», «зв’язн з…», «надає послуги…» тощо);

$At^{(CI)}$ – підмножина атрибутів (<Data properties>, що описує властивості класів C^((CI)) <Data properties> має включати достатньо повний перелік основних та додаткових властивостей об’єктив КІ, їх типи даних, області значень тощо;

$Ex^{(CI)}$ – множина екземплярів (<Instances>) класів C^((CI)), яка використовується для опису кожного конкретного об’єкту інфраструктури. Саме з окремих екземплярів створюється база знань, яка достатньо повно описує взаємодію між КІ;

$Rul^{(S)}$ – підмножина правил логічного виводу дозволяє виявляти приховані зв’язкі між об’єктами КІ через логічний вивід, який здійснюється за допомогою формування запитів до бази знань (Knowledge Graph) різними мовами <DL Query> або <SPARDL Query> та машини виводу – Reasoner. У формуванні правил виведення важливу роль відіграють з Restrictions (обмеження) на властивості.

$Ad^{C(md)}$ – додаткові метадані: кожен клас, відношення або атрибут можна доповнити додатковою метаінформацією та призначити правильні унікальні ідентифікатори. Метадані дають додаткові відомості про сутності, їх властивості та зв’язки, допомагають формалізувати структуру і значення даних у вигляді схем, словників, що допомагає краще зрозуміти і інтерпретувати основні дані в онтології.

Засоби Protégé дають змогу створювати, редагувати та візуалізувати відповідні онтології, що описують класи, властивості, та відношення між компонентами системи. (Рис. 1).

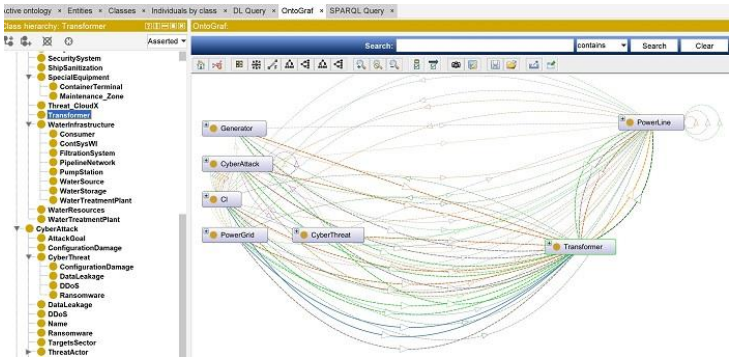


Рисунок 1. – Фрагмент графового представлення фрагменту моделі

Наступним кроком моделювання є визначення сценаріїв поширення каскадних збоїв. Для цього застосовуються запити до онтології за допомогою відповідних логічних формул, які дозволяють виявляти ланцюги впливів.

Запропонована методологія забезпечує структурований підхід до виявлення прихованих взаємозалежностей у системах критичної інфраструктури. Результати дослідження можуть бути застосовані для оптимізації управління критичними інфраструктурами шляхом проактивного виявлення вразливостей.

1. Masucci, V., Adinolfi, F., Servillo, P., Dipoppa, G., & Tofani, A. (2009). Critical infrastructures ontology based modelling and simulation. Proceedings of the Third Annual IFIP Working Group, 11, 22-25.
2. Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2018). On the use of ontology data for protecting critical infrastructures. Journal of Information Warfare, 17(4), 38-55.
3. Aleid, K. (2020). Development of an Integrated Ontology to Enhance Interoperability for Airports Security Solutions.
4. Galbusera, L., & Giannopoulos, G. (2017, March). Exploiting web ontologies for automated critical infrastructure data retrieval. In International Conference on Critical Infrastructure Protection (pp. 119-136). Cham: Springer International Publishing.
5. Dao, J., Ng, S. T., Yang, Y., Zhou, S., Xu, F. J., & Skitmore, M. (2021). Semantic framework for interdependent infrastructure resilience decision support. Automation in Construction, 130, 103852.
6. Сенченко В. Р., Бойченко А. В. Підхід до оцінки ризиків виникнення каскадних ефектів критичної інфраструктури. //Інформаційні технології та безпека. Зб. наук. праць. – В.24. – К.: ІПРІ НАНУ, 2024. С.110-118. ISBN: 978-617-8180-00-3.
7. Сенченко В.Р. Дослідження методів та технологій інтеграції онтологічної моделі з реляційними даними / Сенченко В.Р., Бойченко А.В. Бойченко О.А. // Реєстрація, зберігання і обробка даних. – 2018. – Т. 20, № 3. – с. 91 – 101.

G.P. Kostenko, A.O. Zaporozhets

VIRTUAL POWER PLANTS WITH INTEGRATED ELECTRIC VEHICLES FOR FREQUENCY REGULATION AND GRID RESILIENCE

The growing electrification of the transport sector and rapid expansion of renewable energy sources (RES) have fundamentally changed the dynamics of modern power systems. As variable solar and wind generation replaces conventional synchronous plants, maintaining system frequency and operational stability becomes an increasingly complex challenge. Electric vehicles (EVs), whose global stock is projected to exceed 250 million units by 2030, are emerging as one of the most promising distributed energy resources. Equipped with high-capacity lithium-ion batteries and bi-directional chargers, EVs can operate not only as energy consumers but also as controllable storage units capable of supplying power back to the grid [1-2].

The concept of Virtual Power Plants (VPPs) provides the technological and organizational foundation for integrating such assets. By aggregating thousands of EVs into a unified digital platform, a VPP can coordinate their charging and discharging to support frequency regulation, peak shaving, and local resilience enhancement. In this context, EVs become mobile, adaptive components of the power system - providing flexibility at multiple time scales, from sub-second frequency response to hourly load balancing. This paper explores the functional structure, control logic, and performance indicators of EV-based VPPs, with particular attention to their role in frequency regulation and grid resilience.

Functional Structure of EV-Based VPP

VPP is a software-driven aggregation system that unites diverse distributed energy resources - photovoltaic systems, small-scale generation, stationary batteries, and EVs - into a single controllable portfolio (Fig. 1) [3].

The VPP Control Center communicates with each EV via a cloud-based energy management system and real-time communication protocols (OCPP, IEC 61850, or ISO 15118). Each connected EV charger acts as an agent capable of executing control commands, reporting its State of Charge (SoC), charging power limits, and availability.

The architecture of an EV-based VPP includes the following core modules:

(a) Forecasting Module – predicts renewable generation, grid demand, and EV availability using data analytics and weather models.
(b) Optimization Engine – determines the optimal charging/discharging schedule to minimize frequency deviations and maximize revenue from ancillary services.
(c) Communication Interface – enables secure real-time data exchange between the aggregator, grid operator, and individual EVs.
(d) Control Module – executes commands at the charger or fleet level to regulate power flow within milliseconds.

(e) KPI Monitoring System – tracks performance metrics such as Frequency Stability Index, Response Time, Energy Efficiency Ratio and grid resilience indicators.

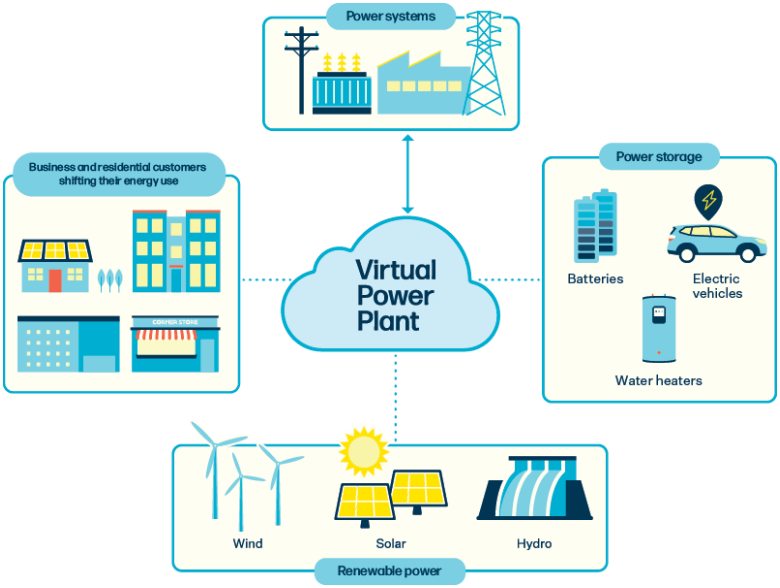


Figure 1. – Conceptual architecture of a Virtual Power Plant integrating electric vehicles and distributed energy resources [3]

In such architecture, EVs form a distributed adaptive layer of frequency regulation (FR): instead of relying solely on spinning reserves, the system dynamically activates thousands of small-capacity storage units to stabilize grid frequency.

Frequency Regulation Mechanisms

EV participation in FR can be realized in several control modes [4]:

- Primary frequency response (fast reaction): EVs immediately adjust charging or discharge power in response to frequency deviations (Δf).
- Secondary control (centralized dispatch): the VPP aggregator optimizes total EV power exchange to restore nominal frequency and schedule compliance.
- Tertiary control (market-based): VPP participates in balancing markets by offering aggregated flexibility bids.

Simulation studies and pilot projects in Europe and Japan demonstrate that aggregating just 5–10 % of the regional EV fleet can supply sufficient flexibility to compensate for typical short-term renewable fluctuations [4]. For example, a 100-MW aggregation of EVs with 40-kWh batteries can provide over 400 MWh of frequency control energy for several minutes without affecting user mobility.

Key Performance Indicators (KPI) for EV-VPP Operation

Efficient operation of EV-based VPPs requires continuous evaluation using technical and economic indicators. Table 1 summarizes a representative KPI framework. These indicators allow the VPP operator to maintain a dynamic balance between frequency quality, economic efficiency, and asset lifetime. In real-time operation, the KPI monitoring layer interacts with the optimization engine, enabling feedback-driven control — for example, reducing participation of low-SoC vehicles to prevent range anxiety.

Table 1. – KPI Framework for EV-VPP Operation

Category	Indicator	Purpose
Technical	Frequency Stability Index (FSI)	Quantifies reduction in frequency deviation amplitude
	Response Delay (ms)	Measures reaction speed to control signal
	Charging Efficiency (%)	Evaluates power losses during bidirectional conversion
	Availability Ratio (%)	Portion of time EVs remain grid-connected
Economic	Levelized Cost of Storage (LCOS)	Cost per unit of energy provided to the grid
	Flexibility Revenue (€/MWh)	Income from ancillary service markets
	ROI, Payback Period	Financial viability for fleet operators
Environmental	CO_2 Reduction (kg/kWh)	Avoided emissions via displaced peaking generation
Resilience	Reliability Index (RI)	Probability of service continuity during grid disturbances

Contribution to Grid Resilience

Beyond frequency control, EV integration significantly enhances grid resilience, defined as the system's ability to absorb, adapt, and recover from disturbances.

EV fleets provide both preventive and restorative functions [5]:

(i) During normal operation, the distributed flexibility of EVs prevents frequency excursions and voltage collapses, reducing the risk of cascading failures.

(ii) In emergency or post-fault conditions, aggregated EVs can act as localized mobile energy reservoirs, supplying critical loads such as hospitals or telecommunication centers through Vehicle-to-Load (V2L) or microgrid configurations.

(iii) After partial grid blackouts, the same EV fleets can support black-start procedures, supplying auxiliary power for restarting local generation units.

Assessment indicates that when 15–20 % of total EV capacity participates in VPP control, the average frequency deviation decreases by 30–35 %, and the system recovery time after a 0.5-Hz disturbance shortens by up to 25 %. These results demonstrate that EV-based VPPs can become a cornerstone of resilient energy systems with high shares of renewables.

Economic and Operational Aspects

The business model of EV integration into VPPs depends on incentive structures and energy market design. Three main frameworks are emerging:

- *Aggregator-based participation*: an energy service company aggregates EV fleets and participates in ancillary markets on behalf of vehicle owners, distributing profits proportionally.
- *Utility-driven control*: the distribution operator directly manages EV flexibility to support local grid stability.
- *Peer-to-peer VPPs:* decentralized control where EV owners trade flexibility via blockchain-enabled platforms.

Economic assessments show that annual revenue per EV from FR services ranges between €100–300, depending on market prices and participation frequency [4]. Although individual gains are modest, aggregated benefits at the fleet or city level become substantial, creating incentives for both operators and policymakers to integrate EVs into flexibility markets.

Operationally, maintaining user comfort is crucial. VPP algorithms must ensure that participation in FR never compromises mobility requirements [4]. Predictive models of trip patterns and smart-charging strategies enable synchronization between user schedules and grid needs.

Despite technological maturity, large-scale deployment of EV-based VPPs is constrained by regulatory gaps, fragmented communication standards, cybersecurity risks, potential battery degradation, and limited consumer acceptance, requiring unified standards, secure protocols, and adaptive market mechanisms to enable distributed flexibility [2].

Conclusions:

Virtual Power Plants with integrated Electric Vehicles represent a transformative paradigm in modern power system management. Through coordinated aggregation and real-time control, EV fleets can effectively participate in FR, voltage support, and resilience enhancement, offering a scalable alternative to conventional reserves.

The KPI-based management framework ensures optimal balance between technical performance, economic benefits, and user constraints. The development of such systems requires integrated policies combining regulatory frameworks, data standards, and financial incentives. For Ukraine and other emerging energy systems, EV-based VPPs can become a strategic instrument for strengthening grid stability, accelerating renewable integration, and fostering resilience under conditions of uncertainty and disruption.

1. Kostenko, G.P. Situation analysis of electric transport development prospects and its integration into Ukrainian power system. Power Eng. Econ. Tech. Ecol. 2023, 1, 71. https://doi.org/10.20535/1813-5420.1.2023.276185.
2. Bosak A., Kostenko G., Zaporozhets A. Electric Vehicle Battery Type Suitability in V2L Applications to Enhance Grid Load Flexibility: A Comparative Study // Power Engineering: economics, technique, ecology. – 2025. – No. 3 (2025). – P. 81. – DOI: https://doi.org/10.20535/1813-5420.3.2025.339751.
3. What is a Virtual Power Plant and why does it matter? Url: https://portlandgeneral.com/blog/virtual-power-plant-supports-grid-reliability.
4. Zaporozhets, A., Kostenko, G., & Zgurovets, O. (2023). Preconditions and Main Features of Electric Vehicles Application for Frequency Regulation in the Power System. ITTAP 2023. CEUR Workshop Proceedings, 3628, 43-54.
5. Zaporozhets, A. et al. (2024). Power System Resilience: An Overview of Current Metrics and Assessment Criteria. In: Systems, Decision and Control in Energy VI. Studies in Systems, Decision and Control, vol 561. Springer, Cham. https://doi.org/10.1007/978-3-031-68372-5_2.

В.О. Мірошник, В.В. Сичова

ВИЯВЛЕННЯ АНОМАЛЬНИХ ЗНАЧЕНЬ У ДАНИХ ОБСЯГІВ ТОРГІВ РИНКУ «НА ДОБУ НАПЕРЕД»

Вступ. Моделювання ринку електричної енергії України потребує високої точності вихідних даних, зокрема часових рядів фактичних та заявлених обсягів купівлі й продажу електроенергії. Реальні дані часто містять аномальні значення, спричинені технічними похибками, людським фактором або нестандартною поведінкою учасників ринку. Такі аномалії спотворюють результати моделювання, знижують адекватність прогнозів цін і порушують баланс попиту та пропозиції. Тому попереднє очищення та реконструкція часових рядів є необхідним етапом побудови достовірних моделей функціонування ринку електроенергії.

Метою дослідження є підвищення достовірності даних для моделювання роботи ринку електричної енергії шляхом виявлення та реконструкції аномалій у часових рядах фактичних і заявлених обсягів купівлі та продажу.

Для досягнення цієї мети реалізовано комплексний підхід, який поєднує кілька методів виявлення аномальних значень (Transformer-реконструкція, HMM, Matrix Profile, DBSCAN), оцінювання якості їх результатів за статистичними метриками (кількість виявлених аномалій, зміна дисперсії, коефіцієнт Jaccard), та формування очищених рядів для подальшого використання у моделях прогнозування цін і поведінки учасників ринку.

Моделі і методи

1. Transformer-based Reconstruction

Ця модель використовує архітектуру на основі механізму уваги (attention) для моделювання складних нелінійних залежностей у часових рядах. Виявлення аномалій відбувається за відхиленням між фактичними та реконструйованими значеннями, що відображає здатність моделі відтворювати нормальний патерн даних.

2. Модель на основі прихованих марковських процесів (Hidden Markov Model, HMM)

Побудована на статистичному підході, який представляє часовий ряд як послідовність прихованих станів із певними ймовірностями переходів. Аномалії визначаються як спостереження, що мають низьку ймовірність появи у межах заданої моделі станів.

3. Метод матричного профілю (Matrix Profile)

Невибірковий метод пошуку аномалій, що базується на обчисленні відстаней між усіма підпослідовностями часового ряду. Ділянки з найвищими значеннями матричного профілю вважаються аномальними, оскільки вони суттєво відрізняються від решти патернів.

4. Метод кластеризації DBSCAN (Density-Based Spatial Clustering of Applications with Noise)

Ґрунтується на щільності даних: точки, що не належать до жодного щільного кластера, класифікуються як аномальні. Метод дозволяє виявляти локальні аномалії без необхідності задавати кількість кластерів і добре працює для сезонних або циклічних даних після попереднього розкладання ряду.

Після виявлення аномалій кожен метод формує реконструйований ряд, у якому аномальні значення замінюються оціненими на основі поведінки сусідніх точок або статистичних закономірностей. Залежно від моделі:

- Transformer прогнозує очікуване значення на основі попередніх спостережень, зберігаючи часовий контекст;
- HMM замінює аномалії найімовірнішими значеннями, що відповідають поточному прихованому стану системи;
- Matrix Profile підбирає найближчий нормальний фрагмент і відновлює значення за його структурою;
- DBSCAN замінює аномальні значення за допомогою лінійної інтерполяції.

Такі реконструкції дозволяють зменшити вплив шуму, уникнути від'ємних або фізично неможливих значень і зберегти природну динаміку часових рядів.

Для оцінки якості реконструкції використано такі метрики:

1. Зміна дисперсії (ΔD) між вихідним і реконструйованим рядами дозволяє оцінити ступінь згладжування та збереження варіативності даних.

2. Кількість виявлених аномалій (N_a) – показує чутливість кожного методу до відхилень.

3. Коефіцієнт Jaccard – використовується для порівняння узгодженості результатів між різними методами виявлення аномалій.

Результати.

Випробування моделей проведено на даних щодо обсягу купівлі й продажу електроенергії та заявлених обсягів купівлі та продажу. Досліджуваний період березень 2022 – вересень 2025. Результати наведено в таблицях 1-2.

Таблиця 1. – Значення метрик оцінки результатів

	Обсяг купівлі/продажу		Заявлений обсяг продажу		Заявлений обсяг купівлі	
Модель	ΔD	N_a	ΔD	N_a	ΔD	N_a
Matrix	1850,5	1221	-5552,4	1222	684,2	1224
Transformer	81547,9	1224	108138,3	1224	99838,7	1224
HMM	0	0	0	0	0	0
DBSCAN	5117,6	73	7269,8	44	5400,6	87

Результати моделювання засвідчили суттєві відмінності між моделями у здатності відновлювати часові ряди після усунення аномалій.

Модель Matrix Profile продемонструвала стабільну роботу для всіх трьох типів рядів, забезпечивши помірне значення зміни дисперсії та найбільшу кількість виявлених аномалій, що свідчить про високу чутливість до локальних відхилень.

Transformer виявив найбільші значення ΔD, що свідчить про сильні коливання реконструйованих значень і можливу переоцінку динаміки при відновленні аномальних точок.

Модель HMM виявилася неефективною для аналізу ринкових часових рядів через низьку адаптивність до різких змін обсягів.

DBSCAN продемонстрував збалансовані результати: помірні значення ΔD і невелику кількість аномалій, що вказує на ефективне виділення лише справжніх аномалій без надмірного шуму.

Таблиця 2.– Значення коефіцієнта Jaccard

Обсяг купівлі/продажу				
	Matrix	Transformer	HMM	DBSCAN
Matrix	1	0,0222	0	0,0008
Transformer	0,0222	1	0	0,0253
HMM	0	0	0	0
DBSCAN	0,0008	0,0253	0	1
Заявлений обсяг продажу				
	Matrix	Transformer	HMM	DBSCAN
Matrix	1	0,0179	0	0
Transformer	0,0179	1	0	0,0226
HMM	0	0	0	0
DBSCAN	0	0,0226	0	1
Заявлений обсяг купівлі				
	Matrix	Transformer	HMM	DBSCAN
Matrix	1	0,0238	0	0,0015
Transformer	0,0238	1	0	0,025
HMM	0	0	0	0
DBSCAN	0,0015	0,025	0	1

За результатами порівняння коефіцієнтів Jaccard найвищу схожість у виявленні аномалій між моделями Matrix Profile та Transformer ($J \approx 0{,}02$–$0{,}025$), тоді як DBSCAN мав слабку, але стабільну кореляцію ($J \approx 0{,}001$–$0{,}025$).

Висновки. Проведене порівняння моделей показало, що найкращий баланс між точністю виявлення та стабільністю реконструкції забезпечує комбінація Matrix Profile (для первинного виявлення) і DBSCAN (для уточнення локальних аномалій).

Transformer виявляє широкий спектр відхилень, але може надмірно реагувати на короткострокові флуктуації, що знижує стабільність прогнозу.

HMM неефективна для аналізу ринкових часових рядів через слабку адаптацію до різких змін обсягів.

Отримані результати можуть бути використані для попередньої фільтрації даних у процесі моделювання цін на ринку електричної енергії, що підвищує достовірність прогнозних моделей.

Робота виконана в межах теми «Короткострокове прогнозування цін на оптовому ринку електроенергії для управління енергоресурсами мікромережі» (0125U002919).

1. Yeh, C. C. M., Der, A., Saini, U. S., Lai, V., Zheng, Y., Wang, J., ... & Keogh, E. (2024, December). Matrix Profile for Anomaly Detection on Multidimensional Time Series. In 2024 IEEE International Conference on Data Mining (ICDM) (pp. 911-916). IEEE.
2. Xu, J., Wu, H., Wang, J., & Long, M. (2021). Anomaly transformer: Time series anomaly detection with association discrepancy. arXiv preprint arXiv:2110.02642.
3. Leon-Lopez, K. M., Mouret, F., Arguello, H., & Tourneret, J. Y. (2021). Anomaly detection and classification in multispectral time series based on hidden Markov models. IEEE transactions on geoscience and remote sensing, 60, 1-11.
4. Мірошник, В. О., & Шиманюк, П. В. (2021). Аналіз методів достовіризації даних для задач короткострокового прогнозування вузлових електричних навантажень. Праці Інституту електродинаміки Національної академії наук України, (60), 51-57.

ЗМІСТ

МАТЕРІАЛИ
ІІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

06 листопада 2025 року
м. Київ

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Олега Мудрака
(колишня Генерала Наумова), 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua