НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

МАТЕРІАЛИ
ІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

12 червня 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 № 05 від 29 травня 2025 р.)

Р-34 **Резильєнтність динамічних** систем, науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 12 червня 2025 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2025. 183 с.

R-34 **Resilience of** dynamic systems, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials (Kyiv, June 12, 2025). Kyiv: PIMEE NAS of Ukraine, 2025. 183 p.

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

МАТЕРІАЛИ
ІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

12 червня 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

В.Ф. Залужний

ЗАБЕЗПЕЧЕННЯ ЕНЕРГЕТИЧНОЇ РЕЗИЛЬЄНТНОСТІ МОРСЬКИХ ПОРТІВ УКРАЇНИ В СУЧАСНИХ УМОВАХ ВЕДЕННЯ ЗБРОЙНОЇ БОРОТЬБИ

Визначенні проблемні питання функціонування морських портів в сучасних умовах ведення збройної боротьби.

Розкриті особливості забезпечення енергетичної резильєнтності морських портів України.

Обговорюються шляхи підвищення цифрової та операційної резильєнтності морських портів в енергетичному домені.

Ключові слова: морські порти, енергетика, резильєнтність, кібербезпека.

Вступ

В умовах ведення війни на “виснаження” швидкість і безперервність логістичних процесів формують спроможність будь-якої держави до відбиття агресії та її стабільного функціонування [1-3].

Особливого значення у цьому процесі відіграють морські порти, які виступають у ролі стратегічних платформ для постачання зброї, гуманітарної допомоги, експорту товарів і імпорту енергоресурсів. Морські порти – це об’єкти критичної інфраструктури, які забезпечують економічну та воєнну безпеку держави.

Знищення або тимчасове виведення з ладу портової інфраструктури має глибокі економічні і воєнні наслідки, що підтверджується численними прикладами кінетичних та кібернетичних атак на українські та міжнародні порти.

З початком повномасштабного вторгнення росії у 2022 році українські морські в Азовському та Чорному морях стали об’єктами кінетичних та кібератак, які постійно удосконалюються [1-3].Окремі їх логістичні вузли зазнали атак, спрямованих на дестабілізацію вантажних перевезень. Блокада та зупинка портів, навіть часткова, мала значний вплив на експорт аграрної продукції, обмежила морські коридори та стала елементом гібридної війни проти економіки України.

Кожна година простою ключового морського порту завдає відчутних економічних збитків державі, та підтверджує, що безпека портів – це не лише питання бізнесу, а безпеки держави загалом [4].

Особливу роль у забезпеченні надійного функціонування морських портів відіграє енергетичний компонент. Без енергопостачання сучасний порт перестає функціонувати: зупиняються крани, митні процедури, навігація, охорона, зв’язок.

У таких умовах, значно зростають вимоги до забезпечення енергетичної резильєнтності морських портів України в сучасних умовах ведення збройної боротьби, як складової частини комплексної системи забезпечення їх живучості, що і обумовлює актуальність даної теми.

Основна частина

Сучасні морські порти з їх розвинутою інфраструктурою, системами навігації, управління морським рухом, моніторингу та контролю процесів, завантаження/розвантаження суден, роботи кранів, руху матеріалів та перевірка безпеки SCADA (Supervisory Control and Data Acquisition) суттєво залежать від спроможностей їх систем енергозабезпечення.

Системи енергозабезпечення морських портів – це складні, відкриті, нелінійні системи, які зазнають постійних внутрішніх та зовнішніх змін та перебувають під постійним впливом деструктивних (дестабілізуючих) факторів.

Підтвердженням цьому є досвід російсько-української війни, який переконливо свідчить, що системи енергозабезпечення морських портів є об'єктами широкомасштабних атак та впливів із застосування усіх можливих сил та засобів від космічного домену до інформаційного простору [1-3, 5].

Порушення умов нормального функціонування систем енергозабезпечення морських портів призводить до затримки обробки вантажів, порушує мережі постачання, впливає на вартість товарів, стримує експорт та імпорт.

Виведення з ладу енергетичної інфраструктури морського порту автоматично паралізує митні процедури, зв'язок, освітлення, контроль температури, що створює ризики не лише економічного, а й техногенного характеру.

Кожна година простою ключового терміналу морського порту здатна генерувати мільйонні збитки, порушити ланцюги постачання, заморозити експорт або імпорт.

За таких умов, ефективне функціонування морських портів неможливе без проведення комплексу заходів щодо забезпечення їх енергетичної резильєнтності.

У ході російсько-української війни розроблено комплексні плани захисту об'єктів критичної інфраструктури, у тому числі морських портів. Такі плани передбачали, насамперед, посилення їх фізичного захисту від різного роду кінетичних атак (крилаті ракети, безпілотні літальні апарати повітряного та морського базування та ін.) [1, 2].

У свою чергу, сучасна цифрова трансформація портів передбачає широке впровадження технологій Інтернету речей (IoT) [6] , цифрових двійників (Digital Twins) [7], хмарних обчислень, штучного інтелекту, автоматизованих кранів і логістичних систем. Ці технології дозволяють з одного боку – підвищити продуктивність, зменшити вплив людського фактору, оптимізувати логістику, а з іншого – призводять до збільшення кількості взаємопов'язаних систем потенційно вразливих до кібератак.

У випадку кібератаки на енергосистему морського порту виводяться з ладу системи навантаження, митного оформлення, охорони, що унеможливлює або істотно ускладнює функціонування відповідних систем логістичного забезпечення.

Уразливість SCADA-систем, PLC (програмованих логічних контролерів) [8] та мереж OT [9] створює ризик багаторівневої зупинки роботи і переривання бізнеспроцесів. Для прикладу, згідно з ENISA, більшість портів Європейського Союзу не мають сегментованих або ізольованих OT-мереж, що дозволяє зловмисникам через IT-інтерфейси атакувати енергетику порту [10].

Кібератаки, спрямовані на порти, дедалі частіше мають не лише фінансову, але й стратегічну мету. Зокрема документ IMO MSC.428(98) вимагає включення кіберризиків до систем управління безпекою (ISM Code) [11]. ENISA Port Cybersecurity Guidelines рекомендує розділення мереж OT/IT, проведення тестування на проникнення [9]. IACS UR E27 визначає вимоги до кіберзахисту обладнання, зокрема SCADA та енергетичних систем у судноплавстві та портах [5].

У цьому контексті порти виступають найяскравішими прикладами об'єктів, де злиття фізичного і цифрового простору відбувається через енергетику.

Виведення з ладу систем енергозабезпечення через кібератаки стає причиною повної зупинки порту і зриву логістичних ланцюгів. Усе це робить питання спільної кіберенергетичної резильєнтності актуальним питанням національної безпеки держави.

Найбільш відомими прикладами є кібератака на порт Маєрск. Внаслідок атаки вірусу NotPetya, за допомогою уразливості бухгалтерського програмного забезпечення, було виведено з ладу понад 17 терміналів у 76 країнах. Збитки перевищили $300 млн. [12].

У порту Лісабону, APT LockBit заблокував доступ до внутрішніх систем. Виведення з ладу торкнулось і енергетичної системи [13].

У "DP World" Австралія кібератака призвела до зупинки 4 ключових портів. Було зафіксовано доступ до енергетичних SCADA через зламані VPN [14].

У порту Шахід Раджай, Іран ймовірна кібератака з боку ізраїльських служб призвела до зупинки енергосистем та навігаційного модуля, що створило багатоденні затори [15].

Досконалі технічні засоби захисту не є остаточним фактором кіберенергетичної резильєнтності морських портів. Людський фактор залишається одним із головних векторів атак. Значна частина успішних вторгнень відбувається через фішинг, соціальну інженерію, слабке управління паролями або помилки в конфігурації систем.

У багатьох випадках оператори SCADA-систем не проходять спеціалізованого навчання з кібербезпеки, а кіберзахист не є частиною культури безпеки на об'єктах критичної інфраструктури.

З урахуванням визначених проблемних питань, для забезпечення енергетичної резильєнтності морських портів України доцільно продовжити проведення таких заходів [16, 17]:

інтегрувати енергетичну безпеку як окремий рівень у системі морської

портової безпеки, розробити Національну програму енергетичної резильєнтності об'єктів критичної інфраструктури;

запровадити системи енергетичної резильєнтності морських портів у яких передбачити перехід від директивного управління енергетичною безпекою та жорсткої централізації процесів безпеки до створення належних умови для еволюціонування системи, внутрішньої самоорганізації та динамічної адаптації, колективна ефективність та зростання адаптаційного потенціалу системи;

впровадити у системі морської портової безпеки регулярні незалежні аудити безпеки систем енергетичного забезпечення, SCADA/OT систем та ін.;

продовжити виконання фундаментальних, пошукових та прикладних досліджень для створення технологічних виробів та новітніх, проривних технологій енергетики майбутнього;

передбачити створення в морських портах резильєнтних енергетичних резервів з впровадженими заходами кіберзахисту (дизель-генератори, накопичувачі енергії та ін.). З цією метою організувати закупівлю найкращих зразків обладнання автономної генерації, провести аналіз існуючих та перспективних технологій та на підставі зібраних даних забезпечити розвиток власного виробництва та створення інновацій у сфері енергетики;

продовжити заходи щодо розробки, впровадження та оновлення нормативних документів та стандартів з фізичної та кібербезпеки інфраструктури морських портів;

організувати дієву міжвідомчу та внутрішню систему підготовки персоналу, залученого до забезпечення енергетичної резильєнтності морських портів (сумісні навчання особового складу підрозділів енергетиків, кібербезпеки та фізичного захисту, міжвідомчі навчання та сценарні тренування для персоналу та ін.).

Висновки

Енергетична інфраструктура морських портів є визначальним фактором їх цифрової та операційної резильєнтності.

Ефективність комплексного захисту морських портів від кінетичних та кіберзагроз, насамперед, залежить від якості проведення заходів з самоорганізації та динамічної адаптації систем енергетичної резильєнтності морських портів.

Енергетичний домен стає основним елементом забезпечення живучості морських портів та їх автоматизованих систем організаційного управління.

1. Рік війни за свободу : Воєнно-історичний нарис першого року широкомасштабної війни – Київ: Центр досліджень воєнної історії Збройних Сил України, 2024. – 1064 с.
2. Другий рік війни. Випробування на міцність: Воєнно-історичний нарис другого року широкомасштабної війни (24.02.2023-24.02.2024)/ У двох книгах. Книга І. /

Центр досліджень воєнної історії Збройних Сил України. – Київ: Видавець Бихун В.Ю., 2024. – 672 с.
3. Удари по голодуючим у світі: Як Росія знищує морську інфраструктуру України. (n. d.). Слово і діло. https://www.slovoidilo.ua/2023/08/03/infografika/suspilstvo/udary-po-holoduyuchym-sviti-yak-rosiya-znyshhuye-morsku-infrastrukturu-ukrayiny.
4. Vallance, I. R.-J. &. C. (2025, 21 May). UK exposes Russian cyber campaign targeting support for Ukraine. BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio. https://www.bbc.com/news/articles/c17rrjdr79po.
5. UR E27 rev1 - safer and cleaner shipping - IACS. (n. d.). Safer and Cleaner Shipping - IACS. https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-rev1.
6. Internet of things - Glossary | CSRC. (n. d.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/internet_of_things.
7. Digital twin definition - Glossary | CSRC. (n. d.). NIST Computer Security Resource Center | SRC. https://csrc.nist.gov/glossary/term/digital_twin_definition.
8. Programmable logic controller (PLC) - glossary | CSRC. (n. d.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.rip/glossary/term/programmable_logic_controller#:~:text=3,NIST%20SP%20800-82%20Rev.
9. Operational technology - Glossary | CSRC. (n. d.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/operational_technology.
10. Guidelines - Cyber risk management for ports | ENISA. (n. d.). Home | ENISA. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports
11. Maritime cyber risk management in safety management systems. (n. d.). https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.
12. Greenberg, A., & Excerpt. (2018, 21 серпня). The untold story of Notpetya, the most devastating cyberattack in history. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
13. Lockbit claims port of Lisbon attack, puts ransom deadline. (n. d.). The Cyber Express. https://thecyberexpress.com/lockbit-claims-port-of-lisbon-attack-ransom/.
14. Порти під кібератаками: Зростаюча загроза для морської галузі. (б. д.). Центр транспортних стратегій. https://cfts.org.ua/articles/porti_pid_kiberatakami_zrostayucha_zagroza_dlya_morsko_galuzi_2021/140318.15. Al Jazeera. (2020, 19 May). Israel cyberattack caused 'total disarray' at Iran port: Report. https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total-disarray-at-iran-port-report.
15. В.В. Мохор В.В., Коробейніков Ф.О. Стійкість і резильєнтність у безпековому домені // Реєстрація, зберігання і обробка даних. – 2024. – Т. 26. – № 1 – С. 113-120.
16. Залужний В.Ф. Система управління військами та зброєю: тенденції розвитку в умовах сучасної збройної боротьби // Електронне моделювання. – 2025. – Т. 47. – № 2. – С. 67-80.

С.О. Романенко

ОПТИМІЗАЦІЯ АЛГОРИТМІВ ОБРОБКИ ВЕЛИКИХ ДАНИХ ДЛЯ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ХМАРНИХ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Сучасні хмарні системи управління інформаційною безпекою (СУІБ) відіграють ключову роль у забезпеченні кіберстійкості та резильєнтності критичної інфраструктури, що вимагає високої продуктивності та адаптивності в умовах зростаючих обсягів даних. Оптимізація алгоритмів обробки великих даних є ефективним шляхом підвищення ефективності таких систем, дозволяючи оперативно виявляти, прогнозувати та реагувати на кіберзагрози, мінімізуючи затримки та ресурсні витрати. Метою дослідження є розробка та впровадження шляхів покращення резильєнтності хмарних СУІБ за допомогою оптимізації алгоритмів обробки великих даних, включаючи застосування штучного інтелекту та предиктивної аналітики.

Проведено аналіз теоретичних засад резильєнтності динамічних систем у контексті кібербезпеки, зокрема, механізмів самовідновлення, адаптивного управління та здатності до відновлення функціональності після деструктивних впливів. Виявлено ключові виклики для забезпечення резильєнтності хмарних СУІБ, серед яких: низька швидкість реагування на кібератаки в реальному часі, значні обчислювальні витрати при аналізі аномалій та складність прогнозування майбутніх загроз. Для подолання цих проблем запропоновано комплексний підхід, що поєднує потокову обробку даних, машинне навчання для предиктивної аналітики та розподілені обчислення.

Запроваджено архітектуру потокової обробки подій безпеки з використанням Apache Kafka, що забезпечує швидкий збір та аналіз даних для оперативної ідентифікації інцидентів та прогнозування можливих збоїв. Розроблено оптимізовані алгоритми машинного навчання для виявлення аномалій та прогнозування кібератак, що дозволяє СУІБ адаптивно реагувати на нові загрози та запобігати їх поширенню. Для забезпечення масштабованості та адаптивності до динамічних навантажень використано розподілені обчислення на базі Apache Spark. Впроваджено систему безперервного моніторингу резильєнтності алгоритмів, яка відстежує їх ефективність та генерує рекомендації для автоматичного коригування параметрів. Для підвищення адаптивних властивостей системи створено централізовану платформу управління даними безпеки, що дозволяє уніфікувати процеси аналізу та забезпечувати узгодженість дій.

Експериментальна апробація на прикладі хмарної СУІБ для моніторингу розподілених мережевих атак продемонструвала скорочення часу виявлення загроз на 15% та зменшення навантаження на обчислювальні ресурси на 10%. Перевагами запропонованого підходу є підвищення швидкості аналізу, автоматизація превентивних заходів та покращення

здатності систем до самовідновлення. Для забезпечення конфіденційності та цілісності даних застосовано сучасні криптографічні протоколи та IAM-політики. Розроблено інструменти для автоматичного тестування адаптивності та стріс-тестування алгоритмів у хмарних середовищах.

Додатково впроваджено механізм автоматичного кешування результатів аналізу, що суттєво знижує час відповіді системи під час пікових навантажень та підвищує її операційну стійкість. Для підвищення кваліфікації фахівців у галузі резильєнтності кіберсистем організовано спеціалізовані тренінги з використання технологій обробки великих даних та ШІ-інструментів. Розроблено інтуїтивно зрозумілий візуальний інтерфейс для управління та візуалізації роботи алгоритмів аналізу безпеки, що спрощує їх інтеграцію в операційні процеси.

Для підвищення ефективності обробки даних, що є критично важливим для резильєнтності, застосовано алгоритми стиснення логів безпеки, що мінімізують обсяг передачі та зберігання даних у хмарі. Впроваджено базу знань з шаблонами оптимізованих алгоритмів, які можуть бути адаптовані до різних архітектур СУІБ та різноманітних типів загроз, забезпечуючи їх швидке розгортання та адаптацію. Для підтримки еластичності та масштабованості інтегровано хмарні платформи з підтримкою автоматичного масштабування обчислювальних ресурсів. Розроблено інструменти автоматичного виявлення аномалій у потоках даних на основі машинного навчання, що значно підвищує точність прогнозування інцидентів безпеки.

Для підтримки командної роботи та оперативної взаємодії створено централізовану систему управління версіями алгоритмів, що забезпечує синхронізацію змін між хмарними та локальними компонентами та сприяє безперервному розвитку системи. Впроваджено механізм автоматичного тестування алгоритмів перед розгортанням, що мінімізує ризик помилок та підвищує надійність системи. Для спрощення аудиту безпеки та відповідності стандартам розроблено модуль автоматичного генерування звітів, сумісних з ISO/IEC 27001, що сприяє прозорості та звітності. Організовано вебінари для адміністраторів із використання оптимізованих алгоритмів, що сприяє їх швидкому впровадженню та підвищенню операційної готовності.

Додатково впроваджено систему прогнозування пікових навантажень на основі аналізу історичних даних за допомогою алгоритмів машинного навчання, що дозволяє превентивно розподіляти ресурси та забезпечувати безперебійну роботу СУІБ. Для забезпечення безперервності роботи та швидкого відновлення розроблено механізм автоматичного відновлення конфігурацій алгоритмів після збоїв. Впроваджено стандартизовані шаблони для документування процесів аналізу даних, що полегшує сертифікацію та підвищує керованість системи. Для інтеграції з зовнішніми системами та обміну аналітичними даними створено API-інтерфейси, що сприяє формуванню комплексної екосистеми безпеки.

Для підвищення адаптивності СУІБ розроблено програмний модуль для автоматичного оновлення алгоритмів відповідно до нових типів загроз та векторів атак, забезпечуючи актуальність захисту. Впроваджено систему оцінки ефективності алгоритмів обробки даних, яка дозволяє оптимізувати їх конфігурацію та підвищувати загальну продуктивність. Для підтримки аналітиків створено інтерактивну платформу з прикладами найкращих практик обробки великих даних, що сприяє швидкому освоєнню технологій та підвищенню їхньої компетентності.

Таким чином, оптимізація алгоритмів обробки великих даних є ключовим інструментом для підвищення резильєнтності хмарних СУІБ. Реалізація запропонованих заходів, таких як потокова обробка, моніторинг продуктивності, предиктивна аналітика, автоматизоване тестування та інтеграція штучного інтелекту, сприяє створенню швидких, масштабованих та адаптивних систем безпеки. Подальші дослідження передбачають розробку самонавчальних ШІ-алгоритмів для адаптивної оптимізації обробки даних та інтеграцію з блокчейн-технологіями для забезпечення прозорості та незмінності аналізу. Впровадження таких рішень у навчальні програми сприятиме підготовці фахівців, здатних створювати ефективні та безпечні хмарні системи нового покоління.

1. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum.
2. Smart Contracts. В Principles of Security and Trust (с. 164-186).
3. Huang, Z., & Benyoucef, M. (2013). From e-commerce to social commerce: A close look at design features. Electronic Commerce Research and Applications, 12(1), 4-12. https://doi.org/10.1016/j.elerap.2012.12.003.
4. Marr, B. (2021). Artificial Intelligence in Practice: How 50 Successful Companies Used AI and Machine Learning to Solve Problems. Wiley.

С.Ф. Гончар, М.Ю. Комаров

ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНЮВАННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ

Дослідження показують різні підходи до оцінювання кіберрезильєнтності. Зокрема, підходи до оцінювання кіберрезильєнтності із застосуванням аналізу ризиків приводяться у [1]. Разом з тим, для дуже складних систем, та для систем із взаємопов'язаними компонентами стає надзвичайно важко провести оцінювання ризику, яке б адекватно враховувало взаємозв'язки між компонентами системи, а також потенційні каскадні ефекти, які можуть виникнути у системі [2].

У роботах [3, 4] запропоновано оцінювання кіберрезильєнтності на основі визначення площі під кривою функціональності системи.

Так у [3] зазначається, що кіберрезильєнтність залежить від таких аспектів системи, як її дизайн, елементи керування, підготовка, запобігання, навчання тощо, які відбуваються перед деструктивною дією. Однак, остаточна оцінка кіберрезильєнтності починається з визнання неминучості деструктивних дій: коли система зазнає впливу, її функціональність погіршується, і основна увага приділяється швидкості відновлення. При цьому, більш стійка система демонструватиме більшу площу під кривою функціональності S_F – інтеграл збереження функціональності системи $F(t)$ за загальний час місії T_M, рис. 1. Тоді автори пропонують визначати величину кіберрезильєнтності системи, як $CR = S_F / (F(0) \cdot T_M)$ [3].

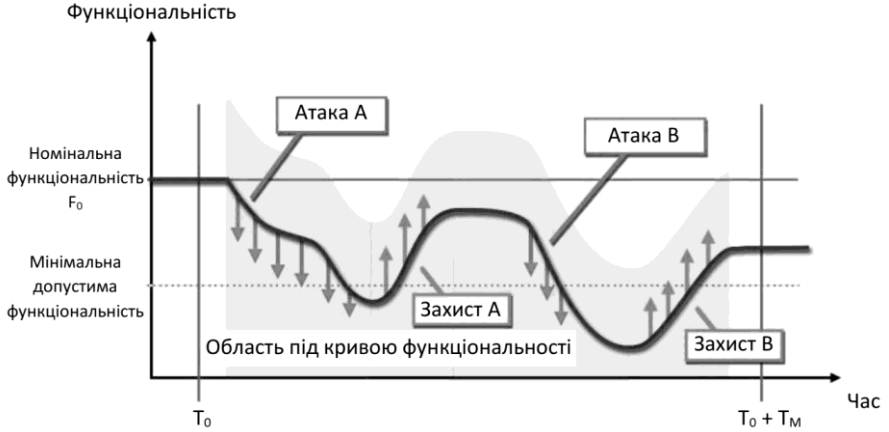

Рисунок 1 – Резильєнтність як площа під кривою функціональності [3]

Ще один підхід до оцінювання кіберрезильєнтності на основі визначення площі під кривою функціональності приводиться у [4], де

приводяться метрики резильєнтності, які включають міри часу та метрики, які включають показники функціональності, рис. 2. Наприклад, мірою часу може бути часовий інтервал між моментом, коли функціональність системи знижується нижче допустимого порогу, і моментом, коли вона відновлюється принаймні до цього порогу, а показником функціональності може бути площа під кривою функціональності від моменту її погіршення до завершення її відновлення.

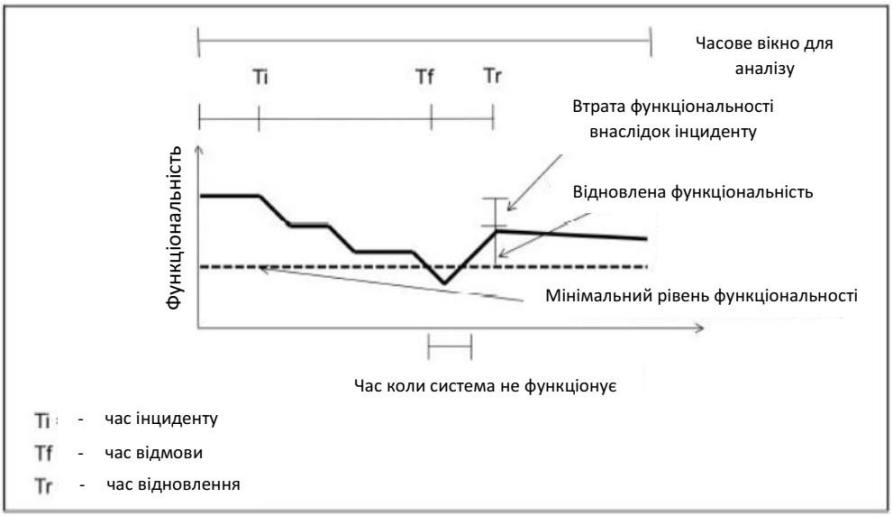

Рисунок 2 – Метрики резильєнтності [4]

Розглянуті підходи до оцінювання кіберрезильєнтності можливо застосовувати у випадку складних систем, а також систем із взаємопов'язаними компонентами.

1. 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.
2. A. Kott and I. Linkov, eds., Cyber Resilience of Systems and Networks. Cham, Switzerland: Springer, 2019.
3. Kott, A. and Linkov, I., 2021. To Improve Cyber Resilience, Measure It. IEEE Computer, 54(2), Feb.2021, pp.80-85.
4. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods / Deborah J. Bodeau et al. Mitre technical report. September 2018, 119 p.

Г.П. Костенко

ЦИРКУЛЯРНА МОДЕЛЬ УПРАВЛІННЯ БАТАРЕЯМИ ЕЛЕКТРОТРАНСПОРТУ В УМОВАХ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ РЕЗИЛЬЄНТНОСТІ

В умовах глобальної енергетичної трансформації, значного зростання частки відновлюваних джерел енергії (ВДЕ) та загроз, пов'язаних із порушенням логістичних ланцюгів, збройними конфліктами та зміною клімату, енергосистеми країн потребують нових підходів до побудови стійких та адаптивних структур [1-3]. Особливої актуальності набуває стратегія резильєнтності – здатність системи протистояти та відновлюватися після екстремальних впливів [4-5]. Одним із напрямів формування резильєнтної енергетичної інфраструктури є впровадження принципів циркулярної економіки в управлінні ресурсами.

Повторне використання відпрацьованих літій-іонних батарей електротранспорту (second-life batteries, SLB) у стаціонарних енергетичних застосуваннях є прикладом реалізації циркулярної моделі [6-8]. Це дозволяє поєднати екологічну доцільність з підвищенням енергетичної гнучкості та зменшенням залежності від імпорту ПММ. Представлено структуру циркулярної моделі управління SLB, яка дозволяє сформувати адаптивну систему резервування та підтримки критичної інфраструктури.

Реалізація концепції циркулярної економіки у сфері енергетики передбачає повторне використання ресурсів із максимальною ефективністю протягом усього їх життєвого циклу. Вторинні батареї електротранспорту — один із ключових об'єктів такої моделі, здатний водночас підвищити енергетичну резильєнтність критичної інфраструктури та зменшити негативний екологічний слід. Представлена нижче у Табл. 1 структура відображає інтегрований підхід до управління батареями, який охоплює технічну, економічну та екологічну оцінку.

Кожен етап не лише послідовно відображає логіку прийняття рішень, а й враховує взаємозв'язок між залишковим технічним потенціалом батарей, актуальними потребами об'єктів-споживачів та цілями сталого розвитку. Такий підхід дозволяє знизити витрати на створення нових резервних систем, продовжити термін корисного використання батарей і забезпечити адаптивне реагування в умовах нестабільного середовища.

Особливу увагу в моделі приділено цифровому моніторингу технічного стану батарей і відстеженню ефективності їх використання протягом часу. Завдяки впровадженню алгоритмів зворотного зв'язку та коригування дій, система здатна адаптуватися до зміни навантаження, погіршення характеристик або змін у конфігурації мережі.

Таблиця 1 - Структура циркулярної моделі для літій-іонних батарей електротранспорту

Етап	Зміст
1. Ідентифікація	Виявлення доступних батарей, класифікація за типом і станом
2. Оцінка ресурсу	Оцінека деградації батарей для прогнозу залишкового ресурсу
3. Визначення потреб	Аналіз потреб об'єктів критичної інфраструктури в енергоємності та потужності
4. Аналіз життєвого циклу	Розрахунок економічної доцільності (ІЕД, LCOS), оцінка викидів CO_2 та матеріального впливу, сценарний аналіз повторного використання
5. Оптимальний розподіл	Алгоритмічний розподіл батарей з урахуванням технічних, просторових та економічних обмежень
6. Управління циклом	Адаптивне керування експлуатацією на основі PDCA-циклу

Включення життєвого циклу до процесу управління дозволяє поєднати технічні рішення з довгостроковою економічною ефективністю. Замість традиційної оцінки лише на основі початкової вартості впроваджується аналіз витрат на зберігання, обслуговування, деградацію та утилізацію — що забезпечує прозорість при прийнятті рішень. Розрахунок індексу економічної доцільності або LCOS дозволяє порівнювати варіанти використання батарей з іншими технологіями резервного живлення.

Крім економіки, модель включає екологічну відповідальність. Продовження терміну служби батарей зменшує потребу у видобутку сировини, викиди CO_2, навантаження на системи утилізації та ризики екологічної шкоди. Таким чином, циркулярна модель управління перетворює вторинні батареї на стратегічний ресурс енергетичної резильєнтності — з гнучкістю, масштабованістю та відповідальністю перед довкіллям.

У традиційній практиці резервного живлення критичних об'єктів найчастіше використовуються дизельні генератори, що створює залежність від постачання паливно-мастильних матеріалів (ПММ), супроводжується високими викидами CO_2 та потребує постійного технічного обслуговування [9-10]. SLB є альтернативою, що має переваги, представлені у Табл. 2.

Таблиця 2 – SLB як сталий екологічний замінник дизель-генераторів для критичної інфраструктури

Параметр	Дизель-генератори	Вторинні батареї (SLB)
Джерело енергії	ПММ (дизель)	Електроенергія з ВДЕ або мережі
Час запуску	5–30 сек	<1 сек
Рівень шуму	Високий	Низький
Викиди CO_2	Високі	Нульові під час роботи
Потреба в обслуговуванні	Постійна	Мінімальна

Запропонована циркулярна модель дозволяє формувати систему адаптивного резервування, яка водночас підвищує стійкість до відключень, знижує залежність від викопного палива, забезпечує ефективніше використання наявних енергетичних ресурсів та сприяє розвитку локальних енергетичних кластерів. Такий підхід поєднує екологічні та енергетичні пріоритети, створюючи основу для стійкого функціонування критичної інфраструктури в умовах зростаючої нестабільності.

Для впровадження моделі на практиці необхідна координація між секторами: створення нормативної бази, реєстрів SLB, інструментів для моніторингу та прогнозування. У перспективі — це напрям інтеграції екологічної та енергетичної політики в єдину рамку стійкого розвитку.

Таким чином, циркулярна модель управління батареями електротранспорту є ефективним інструментом реалізації стратегії енергетичної резильєнтності. Вона дозволяє поєднати інновації в управлінні ресурсами з потребами критичної інфраструктури, а також забезпечує гнучкість, адаптивність і стійкість енергетичних систем в умовах зростаючих ризиків. Упровадження моделі сприятиме не лише енергетичній безпеці, а й переходу до сталого розвитку та зміцнення національної автономії.

Очікуваним результатом впровадження такого підходу є зниження техногенної вразливості об'єктів критичної інфраструктури, підвищення стабільності резервного живлення, оптимізація розподілу енергетичних ресурсів та адаптація систем до кризових ситуацій. Створення багаторівневої моделі — з урахуванням технічного, економічного, екологічного та просторового контекстів — дає змогу формувати гнучкі сценарії управління, що реагують як на зміну параметрів батарей, так і на зовнішні виклики.

Вторинні батареї у цій моделі виступають не просто об’єктами повторного використання, а як динамічні активи, що потребують спеціалізованої оцінки стану, прогнозу деградації та адаптивної експлуатації. Інтеграція моделей моніторингу, ризик-аналізу та цифрового управління забезпечує можливість безпечного залучення таких батарей до об'єктів з

підвищеною відповідальністю. Це формує підґрунтя для розвитку нової парадигми в управлінні енергетичними активами — цифрово контрольованої, стійкої до ризиків і орієнтованої на повний життєвий цикл ресурсу.

1. UNDP Resilience Building and Recovery Programme. (2023). URL: https://www.undp.org/ukraine/undp-resilience-building-and-recovery-programme (Last accessed: 02.06.2025).
2. On approval of the Energy Strategy of Ukraine for the period until 2050: Resolution of the Cabinet of Ministers of Ukraine dated April 21, 2023 No. 373-r. URL: https://zakon.rada.gov.ua/laws/show/373-2023-%D1%80#Textoku](https://zakon.rada.gov.ua/laws/show/373-2023-%D1%80#Textoku (Last accessed: 02.06.2025).
3. Babak, V., Nikitin, Y., & Teslenko, O. (2024). Holistic Approach To The Systemic Transformation of the Electric Power Industry, District Heating And Municipal Infrastructure. System Research in Energy, (4 (80), 6-25. https://doi.org/10.15407/srenergy2024.04.006.
4. Denysov, V., Kostenko, G., Babak, V., Shulzhenko, S., & Zaporozhets, A. (2023). Accounting the Forecasting Stochasticity at the Power System Modes Optimization. In A. Zaporozhets (Ed.), Systems, Decision and Control in Energy V. Studies in Systems, Decision and Control, 481 (pp. 43–55). Springer, Cham. https://doi.org/10.1007/978-3-031-35088-7_3.
5. Zaporozhets, A., Babak, V., Kostenko, G., Zgurovets, O., Denisov, V., Nechaieva, T. (2024). Power System Resilience: An Overview of Current Metrics and Assessment Criteria. In: Babak, V., Zaporozhets, A. (eds) 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.
6. Kostenko, G., & Zaporozhets, A. (2024). World experience of legislative regulation for lithium-ion electric vehicle batteries considering their second-life application in power sector. System Research in Energy, 2(77), 97–114. https://doi.org/10.15407/srenergy2024.02.097.
7. Kostenko, G. (2024). Accounting Calendar and Cyclic Ageing Factors In Diagnostic and Prognostic Models Of Second-Life EV Batteries Application In Energy Storage Systems. System Research in Energy, 3(79), 21–34. https://doi.org/10.15407/srenergy2024.03.021.
8. Kostenko, G., & Zaporozhets, A. (2024). Transition from Electric Vehicles to Energy Storage: Review on Targeted Lithium-Ion Battery Diagnostics. Energies, 17(20), 5132. https://doi.org/10.3390/en17205132.
9. Kostenko, G. (2025). Cluster Based Deployment Of Second Life Ev Batteries For Reliable And Sustainable Backup Power Solution In Power Systems. System Research in Energy, (1 (81), 40-60. https://doi.org/10.15407/srenergy2025.01.040.
10. Lytvyn, V. (2023). Ensuring Backup Power Supply Considering Wartime and Peacetime in Ukraine. Friedrich Ebert Foundation (40 p.).

В.В. Микитенко

ГІБРИДНА МОДЕЛЬ РЕГІОНАЛЬНОЇ РЕАБІЛІТАЦІЇ

Маємо визнати, що уповільнення просторового відновлення, зростання міжрегіональної нерівності та поширення *синдрому набутої безпорадності* (СНБ) серед населення постраждалих територій України потребують невідкладного запровадження адаптивної, міждисциплінарної та економічно доцільної моделі реабілітації. З огляду на критичний стан національної інфраструктури, екології, соціальної мобільності й економічної активності у макрорегіональних зонах, постала необхідність створення *Гібридної моделі регіональної реабілітації монофункціональних міст і ресурсних громад* (ГМРР) як багатовекторного рішення, що поєднує індустріальну трансформацію, когнітивну реабілітацію та соціо-еколого-економічну стабілізацію. Звіди, метою ініціативи ГМРР – є забезпечення багаторівневого, адаптивного та інноваційно орієнтованого повоєнного відновлення семи типологізованих *макрорегіональних зон України* (МРЗ) [1] шляхом впровадження гібридних моделей реабілітації, які інтегрують індустріальні, соціальні, когнітивні та просторові пріоритети, узгоджені з принципами європейського зеленого курсу, циркулярної економіки та соціальної згуртованості. Запропонована до впровадження ініціатива ГМРР - базується на ключових обставинах: а) наявність структурної просторової асиметрії в умовах відновлення, що вимагає сценарного підходу до кожної МРЗ; б) когнітивна та соціальна дезорієнтація громад у монофункціональних містах, що супроводжується деградацією трудового та інтелектуального потенціалу; в) необхідність реінтеграції постіндустріальних територій у нові європейські ланцюги вартості з урахуванням принципів «зеленої трансформації» та соціальної справедливості; г) потреба у фінансовій раціоналізації реабілітаційних заходів через запровадження інструментарію сценарно-програмного планування; д) міжнародні зобов'язання України у сфері регіонального розвитку, стійкості та декарбонізації, які потребують територіально адаптованої стратегії. З цього, задля вирішення і розвязання поставленого стратегічного завдання було:

- обґрунтовано методологічну основу і визначено стратегічні компоненти оригінальних ГМРР: сценарно-прогнозне моделювання відновлення із врахуванням ступеня руйнування, економічного профілю та соціо-генетичних ризиків; формування інтегрованих регіональних платформ (сценарних модулів) для кожної МРЗ; синтез механізмів: когнітивної ресоціалізації, індустріальної конверсії, вахтової мобільності, фінансового планування, екологічної адаптації; впровадження картографованих стратегій дорожніх карт на рівні макрозон;
- виконано розбудову й обґрунтування прогнозних гібридних моделей реабілітації семи МРЗ (рис. 1) в якості інструментально-концептуальних багаторівневих конструкцій, які поєднують сценарні механізми

індустріальної відбудови, когнітивної ре-соціалізації та соціо-еколого-економічного перезапуску територій із урахуванням типологічної специфіки семи повоєнних макрозон [1] держави (табл. 1).

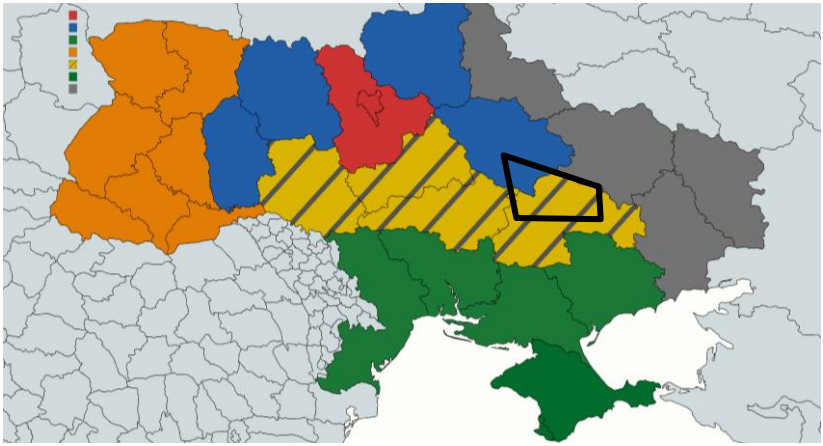

Рисунок 1 – Семи-зонна модельна карто-схема гібридної просторової регіональної реабілітації України за сімома (авторська розробка і візуаліація)

Таблиця 1 – Типізація макрорегіональних зон та гібридні рішення ГМРР

Макрорегіональна зона	Просторова специфіка	Гібридне модельне рішення
1. Зона стратегічного мобілізаційного відновлення – зона активізації (м. Київ, Київська обл.)	Стратегічна адміністративно-координаційна функція	Модель інноваційно-інституційної стабіліза-ції з акцентом на пілот-ні управлінські рішення
2. Транзитно-координаційна зона (центрально-північний пояс:Житомирська, Вінницька, Чернігівська і Хмельницька обл.)	Мережеве розташування та логістична транзитність	Модель логістично-інфраструктурної модернізації з когнітивною мобільністю
3. Східна лінія декомпресії (Харківська, Донецька, Луганська і Сумська обл.)	Зона критичних руйнувань та соціального згортання	Модель когнітивно-медичної реабілітації з пріоритетом елімінування СНБ

Кінець таблиці 1

4. Південна лінія декомпресії (Херсонська, Миколаївська, Одеська і Запорізька обл. та АР Крим і м. Севастополь)	Узбережна вразливість, логістика, агроіндустрія	Модель морсько-логістичної та агроекономічної стабілізації
5. Західна зона економічного збудження (Закарпатська, Львівська, Рівненська, Терно-пільська, Івано-Франківська, Чернівецька, Волинська обл.)	Підвищена транскордонна динаміка	Модель прикордонно-туристичної конверсії та агроінновацій.
6. Центральна зона модернізації (Черкаська, Дніпропетровська, Полтавська та Кіровоградська обл.)	Промислово-аграрна база, центр тяжіння	Модель смарт-індустріального оновлення та кластеризації.
7. Південно-Східний індустріальний пояс (географічний ромб: «Кривий Ріг – Кременчук –Запоріжжя – Дніпро»)	Постіндустріальні монотериторії	Модель важкоіндуст-ріальної конверсії з когнітивною підтримкою та ротаційною зайнятістю

Джерело* Визначено, сформульовано та систематизовано автором за [1].

Реалізація на практиці семи типів моделей ГМРР спрямовано на забезпечення адаптивного, інклюзивного та ресурсно-ефективного відновлення в умовах посткризового розвитку та євроінтеграційних викликів. Ці рішення дозволяють суб'єктам управління застосовувати адаптивні сценарно-програмні стратегії залежно від профілю території, ступеня руйнування, рівня СНБ ресурсних громад і монофункціональних міст, потенціалу індустріального відновлення та соціо-еколого-економічної структури певної громади. Специфічні особливості за кожною МРЗ набувають наступних ознак: 1) Зона стратегічного мобілізаційного відновлення: орієнтація на інституційно-когнітивний перезапуск; мультиінфраструктурна адаптація, синтез критичної інфраструктури з інноваційними хабами; 2) ранзитно-координаційна зона: логістична індустріалізація з просторовим балансуванням; концентрація на регіональній координації потоків, мережеве управління; 3) Східна лінія декомпресії: акцент на елімінації СНБ, медико-соціальній реабілітації, когнітивному супроводі, індустріально-енергетичному відновленні; 4) Південна лінія декомпресії: агро-морська реабілітація та розвиток портової логістики; інтеграція агроекономіки, логістики та медичного консультування; 5) Західна зона економічного збудження: орієнтація на туристично-креативну економіку та інноваційно-когнітивні ініціативи; низький рівень СНБ — висока мобілізаційна готовність; 6) Центральна зона модернізації – це

індустріально-когнітивна трансформація; впровадження смарт-моделей зайнятості та технологічного апгрейду; 7) Південно-Східний індустріальний пояс (географічний ромб) – важко-індустріальна конверсія з когнітивною підтримкою; сценарії відновлення залучають ротаційну зайнятість, цифрову реконструкцію та соціо-еколого-економічну декомпресію.

Поряд із цим, визначено сферу застосування ГМРР - при: розробленні регіональних стратегій повоєнного відновлення; оцінці інвестиційної та соціальної доцільності проєктів реабілітації; формуванні типових рішень для реінтеграції монофункціональних територій; побудові фінансових траєкторій регіонального розвитку в умовах асиметрії джерел фінансування. Їх запровадження передбачає алгоритмізацію управлінських дій за п'ятьма етапами за урахування принципів побудови полівекторних сценарно-прогнозних моделей реконструктивно-просторового розвитку [2] (табл. 2).

Таблиця 2 – Алгоритм управлінських дій щодо запровадження у практику ініціативи ГМРР

Етап	Зміст заходу	Координаційний орган	Результат
I	Оцінка потенціалу МРЗ і визначення обмежень	Мінрегіон, Державна служба статистики та ОВА	Картографована діагностика параметрів відновлення МРЗ.
II	Розроблення типових гібридних моделей	Міністерство економіки України, Мінреінтеграції	Сім модельних сценаріїв відновлення за типовими гібридними моделями.
III	Інституціоналізація моделі в регіонах	Рада з відновлення, ОМС	Створення управлінських і локальних платформ управління.
IV	Формування фінансово-програмних сценаріїв	Мінфін та Міністерство економіки України, міжнародні партнери	Розробка сценарно-програмних бюджетів із урахуванням специфіки.
V	Моніторинг, адаптація, масштабування	Агенція з відновлення, Мінцифри	Верифікація, оновлення, модельна корекція, тиражування і розширення.

Джерело* Визначено, сформульовано та систематизовано автором за [1].

За результати реалізації ініціативи ГМРР (див., табл. 2) імовірним стає: а) зменшення проявів СНБ та когнітивної інерції; б) формування інноваційних індустріальних кластерів в межах кожної із семи макрорегіональних зон; в) створення передумов для інтеграції до європейських ланцюгів вартості; г) раціоналізація інфраструктурних витрат із урахуванням соціо-генетичних ризиків; д) забезпечення стійкого просторового перезапуску країни. А, очікуваний вплив від реалізації ГМРР:

інституційне перезавантаження політик просторового розвитку на засадах прогнозно-сценарного підходу; зменшення проявів когнітивної втоми та синдрому набутої безпорадності у депресивних громадах; формування регіональних систем індустріального перезапуску з новою логікою зайнятості; впровадження фінансових сценаріїв із урахуванням ризиків та можливостей кожної МРЗ; укріплення адаптивного потенціалу регіонів до стратегій ЄС у сфері «зеленої» резилієнтної трансформації.

1. Микитенко В.В., Микитенко Д.О., Чупріна М.О. Сценарне моделювання просторового відновлення макрорегіональних зон України: соціо-еколого-економічні пріоритети реконструкції. *Демографія та соціальна економіка.* 2025. №1 (59). С. 109 – 132. https://doi.org/10.15407/dse2025.01.109.
2. Микитенко, В.В., Чупріна, М.О. (2025). Полівекторна сценарно-прогнозна модель реконструктивно-просторового розвитку України у повоєнному періоді. *Науковий вісник Міжнародної асоціації науковців. Серія: економіка, управління, безпека, технології*, 4(1) https://doi.org/10.56197/2786-5827/2025-4-1-1.

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

ОЦІНЮВАННЯ КІБЕРРЕЗИЛЬЄНТНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПІДХОДИ, ІНТЕГРАЦІЯ МЕТОДІВ ТА МОДЕЛЮВАННЯ

Кіберстійкість, а зокрема кіберрезильєнтність об'єктів критичної інфраструктури (ОКІ), стає дедалі важливішим аспектом національної та економічної безпеки. З огляду на зростання складності кіберзагроз, необхідно застосовувати ефективні підходи для оцінювання здатності ОКІ протистояти атакам, як внутрішнім, так і зовнішнім, вчасно виявляти загрози, мінімізувати наслідки інцидентів та швидко відновлювати функціонування ОКІ.

Оцінювання кіберрезильєнтності включає різні методи, які допомагають аналізувати ризики, вразливості та здатність системи відновлюватися після кіберінцидентів [1]. Ось кілька популярних підходів:

1. CyberResilienceReview (CRR) – методика, яка оцінює здатність організації підтримувати критичні функції під час кіберзагроз.
2. CyberRiskIndex (CRI) – індекс, що вимірює рівень ризику для організації, враховуючи її вразливості та потенційні загрози.
3. FrameworkforImprovingCriticalInfrastructureCybersecurity (NIST) – стандарт, який допомагає організаціям оцінювати та покращувати свою кіберстійкість.
4. Метод FMEA (FailureModeandEffectsAnalysis) – аналіз можливих збоїв та їх впливу на систему.
5. Метод HAZOP (HazardandOperabilityStudy) – виявлення потенційних ризиків та проблем у функціонуванні системи.

Ці методи дозволяють організаціям ідентифікувати слабкі місця, розробляти стратегії захисту та підвищувати загальну стійкість до кіберзагроз.

Для створення ефективного комплексного підходу до оцінювання кіберрезильєнтності об'єктів критичної інфраструктури доцільно інтегрувати переваги вже наявних методів, охоплюючи як технічні, так і організаційні аспекти [2]. Такий підхід має бути багаторівневим, динамічним і адаптивним до контексту конкретної галузі чи інфраструктури.

Для побудови ефективної системи оцінювання доцільно інтегрувати переваги різних методик та інноваційних технологій, які охоплюватимуть як технічні, так і організаційні аспекти. Така модель повинна бути багаторівневою, динамічною та адаптивною до специфіки кожного об'єкта або галузі [3]. Інтегрована багаторівнева модель оцінювання:

1. *Базова структура і стратегічне планування*

Основою системи кібербезпеки може слугувати NIST CybersecurityFramework, який структурує заходи за п'ятьма функціями: ідентифікація, захист, виявлення, реагування та відновлення. Цей фреймворк

задає логіку формування політик і процедур безпеки [4].

Для посилення стратегічного планування доцільно залучити індекс CyberRiskIndex (CRI), що забезпечує кількісну оцінку ризиків. Він враховує як внутрішні вразливості, так і зовнішні загрози, дозволяючи організаціям встановити пріоритети у розподілі ресурсів.

2. *Технічний аналіз уразливих точок*

Для глибшого аналізу технічних компонентів системи доцільно використати методику FMEA (FailureModeandEffectsAnalysis). Вона дозволяє виявити критичні точки відмов у компонентах або процесах і оцінити можливі наслідки для системи загалом.

Доповненням до FMEA виступає HAZOP (HazardandOperabilityStudy) — метод систематичного аналізу відхилень від нормального функціонування процесів. Поєднання цих підходів підвищує точність виявлення технічних і операційних ризиків.

3. *Оцінка стійкості до інцидентів*

На рівні організаційного управління доцільно застосовувати CyberResilienceReview (CRR). Цей метод оцінює спроможність організації зберігати виконання ключових функцій під час кібератак і в період відновлення після них.

CRR дозволяє не лише виявити прогалини в управлінських або операційних процесах, а й оцінити готовність організації до кризових ситуацій, зокрема з точки зору бізнес-неперервності та швидкості реагування [5].

4. *Інтеграція та автоматизація*

Досягнення цілісності системи оцінювання потребує об’єднання результатів усіх методів в єдиний цифровий інструмент. Це може бути дашборд, що в реальному часі відображає стан кіберрезильєнтності за показниками CRI, FMEA, HAZOP, CRR, NIST тощо.

Додатково, впровадження SIEM-систем (SecurityInformationandEventManagement) дозволяє автоматизувати збір та аналіз подій безпеки. А використання цифрових двійників ОКІ дає змогу моделювати гіпотетичні атаки та тестувати плани реагування у безпечному середовищі.

5. *Адаптація до галузевих умов*

Кожен об’єкт критичної інфраструктури має унікальні характеристики, що визначають його вразливість. Тому оцінювання має враховувати галузеву специфіку - наприклад, особливості ІТ-архітектури, регуляторні вимоги, критичність процесів.

Для цього доцільно використовувати модульні шаблони, адаптовані до типових сценаріїв у сферах енергетики, транспорту, охорони здоров’я, застосування БПЛА, тощо. Це забезпечує гнучкість і точність у проведенні оцінювання.

6. *Людський фактор та навчання*

Кіберрезильєнтність — це не лише технології. Вона значною мірою

залежить від готовності персоналу до дій в умовах інциденту. Регулярні тренування, симуляції атак, кібервправи та внутрішні навчальні програми відіграють вирішальну роль у зміцненні безпеки.

Також варто враховувати «соціальну резильєнтність» — здатність команд ефективно співпрацювати та приймати рішення в умовах стресу. Формування культури безпеки має стати складовою довгострокової стратегії кіберзахисту.

7. *Інноваційні технології з моніторингу*

Під час використання комплексного підходу до оцінювання кіберрезильєнтності об’єктів критичної інфраструктури важливу роль відіграє система моніторингу, за допомогою якої відбувається виявлення кіберзагроз та інших ІТ-інцидентів. Наприклад, збір даних та моніторинг за допомогою БПЛА може використовувати візуальне спостереження, алгоритми комп'ютерного зору і обробки зображень. Додаткове використання БПЛА для моніторингу може покривати безліч завдань, таких як екологічні інспекції на відповідність заданим нормам, аудит енергоефективності, допомога рятувальникам у ліквідації надзвичайних ситуацій, пошук людей та інші.

Передача цих даних з БПЛА до центральної системи моніторингу та аналітичного центру дозволяє виявляти аномалії, визначати візуальний стан конкретного об'єкта чи обладнання, вимірювати параметри навколишнього середовища, в якому знаходиться об’єкт критичної інфраструктури, тощо. Передані дані з БПЛА структуруються та постійно відстежуються в автоматичному режимі і у разі надходження сигналу про зміну показників від їх нормальних значень - інформує відповідальних осіб за допомогою повідомлення, дзвінка, або іншого виду зв`язку, а також відображає їх у дашборді на робочому місці відповідальної особи.

Щоб науково-практично довести покращення кіберрезильєнтності, доцільно застосовувати поетапну методику, що включає математичне моделювання, оцінку індексів ризику та імітаційне тестування [6-7].

При формулюванні задачі лінійного програмування (ЛП), яка дозволяє оптимізувати розподіл ресурсів (бюджет, час, людські ресурси) на заходи з кібербезпеки, треба врахувати змінні моделі, які представляють впровадження заходів безпеки, а обмеження враховують витрати [8]. Застосування імітаційного моделювання кіберінцидентів до і після впровадження покращень, дозволяє оцінити різницю в часі реагування, обсязі втрат, збереженні критичних функцій тощо. Кількісна оцінка за допомогою CRI (CyberRiskIndex) або RPN (RiskPriorityNumber у FMEA-аналізі) допоможе наочно показати, наскільки зменшився ризик (зниження RPN після впровадження заходів сигналізує про підвищення кіберстійкост).

Побудова лінійної моделі для підвищення кіберрезильєнтності об’єкта критичної інфраструктури (ОКІ). Модель розв’язується методами лінійного програмування, результатом чого буде оптимальний план впровадження заходів в межах ресурсів.

Мети моделі це максимізація рівня кіберрезильєнтності, яку можна представити у вигляді зваженої суми заходів безпеки. Кожен захід має свою ефективність (вагу) у посиленні стійкості системи. Нехай змінні $x_1 - x_5$ представляють рівень реалізації п'яти ключових заходів: сегментація мережі, автоматичний моніторинг, навчання персоналу, багатофакторна автентифікація та резервне копіювання. Кожна змінна приймає значення від 0 до 1, що означає частку впровадження заходу. При встановленні обмежень треба врахувати,що загальні витрати не повинні перевищувати наявний бюджет, та часові обмеження на людські ресурси або тривалість впровадження. Цільова функція формується сумою $x_1 - x_5$, що показує вплив кожного заходу на кіберрезильєнтність, що означають впровадження/рівень заходу (наприклад, SIEM-система, навчання персоналу, firewall, MFA тощо)

Формалізація через ЛП (лінійне програмування)

Задача: максимізувати кіберрезильєнтність організації за рахунок інвестування в певні заходи безпеки, враховуючи обмежений бюджет та людські ресурси.

Наприклад, нехай:

- x1- рівень впровадження сегментації мережі,
- x2- рівень автоматичного моніторингу,
- x3- рівень навчання персоналу,
- x4- рівень багатофакторної автентифікації,
- x5- рівень резервного копіювання,
- xi∈[0,1]- частка реалізації заходу.

Цільова функція, щодо максимізаціїкіберрезильєнтності:

$$F = a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3 + a_4 \cdot x_4 + a_5 \cdot x_5 \quad (1)$$

де a_1, a_2, a_3, a_4, a_5- коефіцієнти ефективності кожного заходу (оцінюються експертно або емпірично).

Обмеження:

1. **Бюджетне обмеження:**

$$B \geq b_1 \cdot x_1 + b_2 \cdot x_2 + b_3 \cdot x_3 + b_4 \cdot x_4 + b_5 \cdot x_5 \quad (2)$$

де b_1,b_2,b_3,b_4,b_5 - вартість реалізації заходу i, B — загальний бюджет.

2. **Обмеження часу чи ресурсів:**

$$T \geq t_1 \cdot x_1 + t_2 \cdot x_2 + t_3 \cdot x_3 + t_4 \cdot x_4 + t_5 \cdot x_5 \quad (3)$$

де t_1,t_2,t_3,t_4,t_5 - часові витрати, T — доступний ресурс часу/персоналу.

Таблиця 1 – приклад для дослідження

Заходи	Ефективність (a)	Вартість (b)	Час (t)	Змінна (xi)_
Сегментація мережі	10	5	2	x1
Автоматичний моніторинг	14	7	3	x2
Навчання персоналу	9	4	1	x3
Багатофакторна автентифікація	11	6	2	x4
Резервне копіювання	8	3	1	x5

Обмеження:

- **Бюджет:** ≤ 20
- **Час:** ≤ 7
- **x2 ≥ 0.5**

Цільова функція (максимізація):

$$F = 10 \cdot x_1 + 14 \cdot x_2 + 9 \cdot x_3 + 11 \cdot x_4 + 8 \cdot x_5 \quad (4)$$

Таким чином, комплексний підхід із використанням ЛП, імітаційного моделювання та ризик-метрик дозволяє не лише приймати обґрунтовані рішення, а й науково доводити їхню ефективність. Комбінуючи ці підходи, ми отримуємо гнучку, багатовимірну систему оцінки кіберрезильєнтності, яка не лише виявляє вразливості, але й стимулює розвиток здатності до адаптації, навчання та відновлення. Такий підхід особливо актуальний в умовах постійних змінсередовища кіберзагроз та зростаючої залежності критичної інфраструктури від цифрових технологій. Такий підхід дозволяє обґрунтовано довести покращення кіберстійкості через кількісні оцінки та моделювання, а також забезпечити стратегічне планування з урахуванням технологічних галузевих обмежень ОКІ.

1. Звіт про стан кібербезпеки в Євросоюзі за 2024 рік. URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union (дата звернення: 25.05.2025).
2. Сидоренко В.М., Максимець А.В. Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. *Кібербезпека: освіта, наука, техніка*. 2025.Т.3 №27.С. 560-571.
3. Гончаренко Є.О. Вибір підходу до оцінки ризиків інформаційної безпеки для підприємств роздрібної торгівлі: магістерська дисертація. Київ, 2019. 92 с.
4. NIST SpecialPublication 800-160.

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf (дата звернення: 27.05.2025).
5. Singer P. W., Friedman A. CybersecurityandCyberwar: WhatEveryoneNeedstoKnow. 2014. 306 с.
6. Комаров. М.Ю., Гончар С.Ф., Дімітрієва Д.О. Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури.*NuclearandRadiationSafety.* 2021. С. 59-65.
7. Качинський А.Б. Безпека, загрози та ризик: наукові концепції та математичні методи. Київ, 2003. 472 с.
8. Захист критичної інфраструктури в умовах надзвичайних ситуацій / за заг. ред. П. Б. Волянського. Київ : НІСД, 2021. 375 с.

Ю.І. Калюжна

ЦИФРОВИЙ СУВЕРЕНІТЕТ ЯК БАЗОВИЙ ЕЛЕМЕНТ АРХІТЕКТУРИ РЕЗИЛІЄНТНОСТІ: ВІДПОВІДЬ НА ВИКЛИКИ XXI СТОЛІТТЯ

Сучасна епоха характеризується формуванням принципово нової реальності, в якій ризики, виклики та шоки більше не є ізольованими інцидентами. Натомість, вони інтегруються у всеосяжні, багатовимірні та ланцюгові кризи, що пронизують усі сфери: від глобальної політики та економічних систем до екологічних змін і соціальних взаємодій. Така складна та перманентна динаміка кризових явищ вимагає від держави та її інституцій не просто пристосування, а докорінної реконфігурації та розбудови принципово нової архітектури політичного управління й національної безпеки. Метою цієї трансформації є забезпечення стійкої життєздатності держави в умовах постійного коливання та нестабільності. У цьому контексті, цифровий суверенітет виступає не як звичайне розширення сфери державного контролю, а як фундаментальний компонент архітектури резилієнтності держави, що є визначальною відповіддю на сукупність викликів, притаманних поточному століттю.

Глобальні цифрові трансформації докорінно змінили основи взаємодії між особистістю, соціумом та державою, а також суттєво вплинули на взаємодію між державами, розширивши традиційне розуміння суверенітету за межі його класичних атрибутів – території, населення та владних структур. В умовах зростаючої трансграничності інформаційних потоків та критичної залежності країн від всесвітньої цифрової інфраструктури, цифрова самостійність набуває статусу вирішального компонента національної безпеки. Більше того, цифрова самостійність та незалежність виступають фундаментальним стовпом стратегічної автономії сучасної держави, перетворюючись на критично важливий механізм зменшення вразливості не лише до впливу технологічно розвинених країн, а й до агресивних дій з боку держав-проксі (proxy state) та автократичних режимів, які активно застосовують цифровий простір для кібертероризму, гібридних війн та інших деструктивних операцій.

На тлі цих глибоких змін, концепція державної стійкості (резилієнтності) набуває особливої ваги. Резилієнтність держави трактується як її спроможність підтримувати та розширювати потенціал як у цивільній, так і у військовій сферах, аби значно ускладнювати ворожі дії та виступати як одна з передумов національної безпеки. Ця стійкість формується у відповідь на широкий спектр регіональних, гібридних та глобальних загроз. Для демократичних систем резилієнтність означає спроможність витримувати зовнішні та внутрішні потрясіння без насильства, запобігаючи або відновлюючись від тривалої деградації демократичних характеристик їхніх інститутів, процесів та практик. Вона охоплює не лише державні

структури, а й недержавні та суспільні актори. В академічному дискурсі розуміння резилієнтності еволюціонувало. Хоча традиційно розрізняють резилієнтність як «продуктивність» (resilience as performance) – наскільки стійкою є система, та «потенціал» (resilience as capacity) – здатність системи залишатися або стати стійкою [2; 10], сучасні дослідження вказують, що дуалізм «ознака-стан» є концептуальною помилкою, яка перешкоджає досягненню консенсусу у визначенні резилієнтності. Натомість, дедалі більшого поширення набуває трансакційний підхід, який розглядає резилієнтність не як статичну якість, а як динамічний процес, потенціал та результат взаємодії між системою (державою) та її мінливим середовищем. Цей підхід підкреслює, що резилієнтність не є вродженою чи фіксованою, а формується і змінюється з часом та в різних контекстах, будучи характеристикою середовища так само, як і властивістю суб'єкта. Саме цей трансакційний потенціал резилієнтності, невід'ємною частиною якого є цифровий суверенітет, визначає, наскільки політична система здатна впоратися зі стресовим впливом без суттєвих змін у демократичних якостях її структур і процесів [7].

У широкому трактуванні, цифровий суверенітет охоплює здатність держави самостійно визначати свою політику в кіберпросторі, ефективно здійснювати контроль над національною цифровою інфраструктурою, обробкою даних, технологічним розвитком та регуляторним середовищем. Це необхідно для надійного захисту її життєво важливих стратегічних інтересів, а також прав і свобод громадян. Ця концепція є ключовою, багатоаспектною стратегічною парадигмою, яка формує основи як державної політики, так і міжнародних відносин. Її центральним завданням є забезпечення національної безпеки та резилієнтності держави в умовах дедалі зростаючої залежності від цифрових технологій [1; 3; 4; 5; 9].

Цифрова самостійність виступає як наріжний камінь архітектури державної стійкості, оскільки вона надає державі можливість:

Надійно керувати критичними цифровими активами: Забезпечення захисту енергетичних систем, фінансових мереж, комунікацій та державних сервісів від кібератак є життєво важливим для збереження функціональності держави в період кризи. Зокрема, гібридна війна РФ проти України слугує яскравим прикладом, коли кібератаки на критичну інфраструктуру спрямовані не лише на завдання економічних збитків, а й на стратегічне послаблення національної резилієнтності.

Охороняти інформаційний простір: Контроль над потоками інформації та ефективна протидія кампаніям з дезінформації є абсолютно необхідними для підтримки суспільної довіри та єдності, що є основними компонентами стійкості.

Гарантувати стратегічну незалежність: Цифровий суверенітет мінімізує залежність від іноземних технологічних провайдерів, уможливлюючи для держави ухвалювати самостійні рішення та діяти автономно в умовах глобальної геополітичної турбулентності.

Особлива гострота взаємозв'язку між цифровим суверенітетом та резилієнтністю стала очевидною в умовах наростання гібридних загроз. Як відзначає Я. Кеплін [6], гібридні операції здатні істотно впливати на рівень державної безпеки, а послідовна розбудова резилієнтності слугує ефективним контрзаходом проти подібних видів загроз. У війні проти України кібернетичний простір набув статусу одного з вирішальних фронтів, де РФ систематично здійснює кібератаки на об'єкти критичної інфраструктури та розгортає широкомасштабні дезінформаційні операції. Систематичне втручання у цифрову інфраструктуру та спроби дестабілізації державних систем за допомогою кібернетичних атак є прямим посяганням на державний суверенітет.

Стійкість демократичних систем у XXI столітті прямо залежить від їхньої спроможності витримувати зовнішні та внутрішні шоки, запобігаючи або швидко долаючи тривалу втрату своїх демократичних якостей. У цьому контексті, цифровий суверенітет відіграє центральну роль, надаючи державі можливість ефективно протистояти зовнішнім впливам, що потенційно можуть підірвати демократичні інститути та процеси (як це було з кібератаками та дезінформацією, спрямованими на ЄС та Україну). Теоретичний підхід до демократичної резилієнтності розрізняє три ключові аспекти: здатність системи продовжувати функціонувати (continuation), чинити опір (resistance) деградації демократії, та «відновлюватися» (bounce back) після початкових пошкоджень [2; 8]. Розвинений цифровий суверенітет безпосередньо впливає на дієвість цих механізмів, дозволяючи державі оперативніше виявляти загрози, реагувати на них та мінімізувати їхній деструктивний вплив на демократичні процеси. Також, як показує досвід російської агресії проти України, резилієнтність до загроз критичній інфраструктурі є життєво важливою для виживання держави [10].

В контексті посилення глобальної геополітичної нестабільності та інтенсифікації технологічного суперництва, стратегічне значення цифрового суверенітету невпинно зростає, закріплюючи за ним статус вирішального чинника національної безпеки. Отже, цифровий суверенітет виходить за межі суто технічних чи правових категорій, перетворюючись на фундаментальний, наріжний компонент у загальній архітектурі державної резилієнтності. Ця спроможність дає змогу державам не лише успішно протистояти різноманітним шокам та стресовим впливам, а й ефективно пристосовуватися до них, відновлювати функціональність та динамічно розвиватися в умовах перманентної турбулентності XXI століття. Формування всебічної державної стійкості вимагає постійного вдосконалення цифрових можливостей, надійного захисту життєво важливої інфраструктури, ефективної протидії дезінформації та кібератакам, а також безумовного забезпечення цифрового суверенітету. Лише дотримуючись такого комплексного підходу, держави зможуть адекватно та ефективно реагувати на багатогранні виклики цифрової епохи, гарантуючи власну життєздатність у складному глобалізованому світі.

1. Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European security*, 31(3), 337-355. URL: https://www.tandfonline.com/doi/pdf/10.1080/09662839.2022.2101887.
2. Croissant, A., & Lott, L. (2024). *Democratic resilience in the twenty-first century: Search for an analytical framework and explorative analysis* (V-Dem Working Paper Series No. 2024:149). Varieties of Democracy Institute. https://www.v-dem.net/media/publications/WP_149.pdf.
3. Debating Europe. (2022). *How can Europe reach digital sovereignty?* [Video]. YouTube. https://www.youtube.com/watch?v=kBRsbW67sHY.
4. Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty-Rhetoric and reality. *Journal of european public policy*, *31*(8), 2099-2120. https://doi.org/10.1080/13501763.2024.2358984.
5. Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024, November 14). Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society*, 3(59). https://doi.org/10.1007/s44206-024-00146-7.
6. Keplin, J. (2023). Building state resilience against hybrid activities. *Przegląd Bezpieczeństwa Wewnętrznego*, 15(29), 241–266. https://doi.org/10.4467/20801335PBW.23.029.18771.
7. Kuldas, S., & Foody, M. (2021). Neither Resiliency-Trait nor Resilience-State: Transactional Resiliency/e. *Youth & Society*, *54*(8), 1352-1376. https://doi.org/10.1177/0044118X211029309.
8. Merkel, W., & Lührmann, A. (2021). Resilience of democracies: responses to illiberal and authoritarian challenges. *Democratization*, 28(5), 869–884. https://doi.org/10.1080/13510347.2021.1928081.
9. Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. *EU cyber direct, research in focus series.* URL: https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/khGGovSY/rif_timmersmoerel-final-for-publication.pdf.
10. Ostrowski, P., & Zych, R. (2024). State's resilience to critical infrastructure threats: The example of the Russian war on Ukraine. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, 17(2), 349–363. https://doi.org/10.32084/tkp.9050.

М.Б. Фесенко

ЩОДО ОДНІЄЇ ТЕНДЕНЦІЇ КОМПОНУВАННЯ ЕНЕРГЕТИЧНОЇ ВИБУХОВОЇ СУМІШІ

В останні роки у суспільстві виникло чимало інтересу щодо комплексу особо небезпечних засобів, зокрема до вибухових речовин. Деякі мешканці невеликих населених пунктів у сільської місцевості живуть буквально на пороховій бочці, хоча ніякої думки про це не мають та взагалі не розуміють масштабів прихованої біля них небезпеки. Стійкість, незламність та резильєнтність мають опиратися на знання та бути свідомими. Тому актуальною задачею є побудова бази знань особо небезпечних засобів. Люди бачать, що коїться навколо них. Жити у постійної небезпеці важко. Населення дуже цікавить, що може бути далі, чого ще можливо очікувати від використання особо небезпечних засобів. У однокомпонентних вибухових речовинах використовуються достатньо прости конструктивні схеми. Традиційно вибуховий контур складає ланцюг з підривника, детонатора та вибухової речовини, що спрацьовують по вказаній послідовності. Окремі компоненти цієї схеми можуть бути дубльовані та паралельні. Якщо ця конструкція не використовується стаціонарно, то деякі засоби її доставки містять ще додатково метальну вибухову речовину, зокрема порох. Тому традиційно вибухові речовини поділяли на ініціюючи (первинні), бризантні (вторинні) та метальні. Вибухова речовина звичайно містить вуглець, водень, кисень та азот. Кількість вибухової речовини визначається таким чином, щоб вибухова хімічна реакція відбулася як у відкритому середовищі, так й у ізольованому. Вже досягнути границі потужності та швидкості розповсюдження детонаційної хвилі. Зараз можливості зростання факторів ураження для однокомпонентних речовин майже вичерпано. Перспективу має лише модифікація вже відомих вибухових речовин та їх вдосконалення. Тому розповсюдження однокомпонентних речовин обмежується їх традиційним використанням. На їх доповнення та заміну використовуються вибухові суміші. Відомо, що слабким місцем вибухової речовини є її вага. Засоби транспортування та доставки вибухової речовини до цілі не в змозі подолати обмеження ваги, тому їх ефективність доки ще не велика. Міни важких мінометів, гармат великого калібру, головні частини ракет, авіаційні бомби та безпілотні летальні апарати працюють на границі своїх можливостей. Але використання щодо наведення та керування цими засобами комп'ютерних програм сумісно з даними від дистанційного зондування Землі та супутникової навігації значно підвисило точність улучання в ціль та вибір цієї цілі. Дистанційне зондування Землі дозволяє оперативно визначити місця розташування сховищ боєприпасів, пального, складів сільськогосподарських добрів, сховищ радіоактивних речовин, та тому подібне.

Ціллю даної роботи є виявлення тенденції щодо компонування вибухових речовин до енергетичної суміші та визначення можливих наслідків цього компонування. Протидія загрозам має ґрунтуватися на фундаментальних динамічних сучасних знаннях про них. Енергетична суміш уявляє собою складну комбінацію вибухових речовин. Кожен компонент підбирається у суміш зовсім не випадково. Кожен компонент вибухової суміші підготовлює умови для ефективного спрацювання її наступного компонента. Тому кожен попередній компонент (з послідовності підриву) є ініціюючим для послідуючого компонента вибухової суміші, що у даному випадку спрацьовує як вторинний. Але до послідуючого вже за ним компонента суміші він одночасно спрацьовує як ініціюючий компонент, тобто виконує подвійну функцію (вторинного до попереднього та первинного для послідуючого). Обов'язковою частиною суміші вибухових речовин є флегматизатори. Деякі компоненти додаються у вибухову суміш для надання додаткової бризантної дії. Якщо площа вибухонебезпечної частини добрів велика, то бризантна місцева дія вибуху здатна охопити ще удвічі, а то й у тричі більшу площу, тому що зовні добавиться ще ініціюючий заряд. Бризантна ударна дія хвилі детонації здатна подрібнювати на частки усе навколо себе. Такий ланцюг навіть нагадує схеми невипадкової послідовності спрацювання компонентів ядерної зброї, яка також починається зі використання звичайної хімічної вибухової речовини у якості ініціюючої.

Вибухові суміші готують як шляхом змішування у спеціальних умовах, так й у ізольованих варіантах. Технологій тут декілька. Основна тенденція розвитку цих технологій полягає у тому, щоб спростити технологічний процес та зробити його більш надійним, зменшити ціну та підвищити безпеку. Раніше уся суміш розташовувалася у одному корпусі (хоча й ізольовано), у однієї касеті, у однієї головної частині тощо. Зараз з'являється нова тенденція, коли частина суміші знаходиться у одному корпусі, а її додаткові компоненти знаходяться у іншому корпусі. Ці мобільні варіанти значно легше транспортувати, оскільки вага розподіляється на декілька засобів транспортування. Потім окремі частини суміші для досягнення максимального ефекту ураження послідовно або одночасно влучають у задану (обрану) ціль. Загальний вибух відбувається більш потужним, як й ураження цілі. Може бути задіяне декілька таких комбінацій одночасно. При цьому можуть бути задіяні різні засоби транспортування частин вибухової суміші.

Впродовж цієї тенденції додаткова частина вибухової суміші може стаціонарно розташовуватися у іншому місці на території супротивника. Сховища радіоактивних відходів, як правило, знаходяться поза межами населених пунктів. До того ж їх підрив у якості одного з можливих варіантів брудної бомби є не бажаним ні для кого, бо на багато років зробить забруднену радіацією територію непридатної до проживання. Вона може тоді використовуватися тільки у якості буферної зони або полігону щодо

випробувань сучасного озброєння та утилізації застарілої зброї та боєприпасів. Такий варіант найменш вірогідний, тому його не слід розглядати, щоб не втрачати дарма часу. Найбільш вірогідним є варіант ураження сховищ сільськогосподарських добрів з використанням саме їх компонентів у якості складових частин загальної вибухової суміші. Наприклад, це може бути сховище калієвої селітри на сільськогосподарському підприємстві або товарний потяг з добривами, та тому подібне. Добрива використовуються сезонно, а виробляються, транспортуються та накопичуються у продовж усього року. На жаль, накопичення та скупчене складування добрив, а це по декілька тонн разом, відбувається частіше у самих сільських поселеннях, де розташовані підприємства та мешкають їх співробітники. Тому підрив добрів може не тільки негативно впливати на населення, на екологію, але й знести у повітря частину поселення навколо сховища. Таке небезпечне положення треба негайно виправити та підвищити резильєнтність інфраструктури аграрного комплексу країни. Люди мають жити у безпеці.

Аграрний комплекс уявляє собою складну динамічну систему, де усе роками налагоджено та сезонно рухається. Ґрунт треба проорати, підготовити щодо посівної, внести своєчасно добрива. Потім у заданий термін провести посівну, зростити врожай з використанням підкормок. Вирощене зерно треба зібрати, просіяти, просушити та складувати у визначених умовах, потім транспортувати до користувачів. На увесь такий щорічний цикл існують логістика, енергетика, спеціалізована інфраструктура та відповідні технології, що не мають бути порушені. Якщо зі цього налагодженого ланцюгу випаде хоча би одна ланка, то одразу порушиться уся динамічна ланцюгова система. Підкреслимо, що при просіюванні та просушуванні зернових накопичується дуже багато пилу, що також вибухонебезпечне, особливо при зовнішньому втручанні. Зараз підприємства аграрного комплексу працюють у несприятливих умовах. Багато посівних площ забруднено з використанням особо небезпечних засобів та потребують розмінування. Не вистачає робітників, добрів, засобів захисту рослин, елеваторів, техніки, пального, транспорту. Але доки ще система аграрного комплексу стійка та здатна проявляти резильєнтність до деяких тимчасових природних негараздів. Для аграрного комплексу країни, що складає її економічну базу, сільськогосподарські добрива є критичний ресурс. На ньому будується економіка країни. Без добрів не буде гарного врожаю ні зернових, ні маличних культур, не буде що їсти ні населенню, ні військовим. Не буде їх врожаю, не буде що продавати та не за що буде купляти те, що потрібно державі. Військове протистояння завжди має економічну складову. Виведення економіки з ладу може призвести країну до кризи. Тому сховища добрів аграрного сектору економіки є однієї з важливих цілей для супротивника. Наведений можливий сценарій розвитку подій є одним з варіантів стратегії обрання цілей. Зараз відкривається багато інформації, що раніше була прихована. Не секрет, що деякі добрива містять у своєму складі

радіоактивні нукліди та випромінюють, зокрема: селітри, азотна та калієва, азотно-фосфорні, фосфорні та калієві добрива як окремо, так й у трійному поєднаному варіанті, у стані після диспергування чи у рідині. Відомо, що природна радіоактивність калієвих добрів порівнює з радіоактивністю збідненого урану. Крім того, мінеральні добрива ще й дуже токсичні. Особливо токсичні з'єднання саме азоту, кадмію, калію, ртуті, свинцю, фосфору, фтору та багатьох ізотопів, що накопичуються у організмі та отруюють його. Відомі професійні захворювання кожних покровів, дихальної системи, очей, нірок, печені та інших органів та систем у робітників, що працюють тривалий термін з мінеральними добривами. Тобто робітники сільськогосподарських підприємств працюють з вибухонебезпечними радіоактивними речовинами, не знаючи про це нічого. Тому надовго їх не вистачає. Мають бути спеціалізовані засоби захисту, умови праці та постійний дозиметричний контроль. Такі міри здатні підвищити резильєнтність співробітників.

Звернемо увагу на те, що деякі хімічні сполуки мають подвійне призначення. Вони можуть використовуватися як у якості сільськогосподарських добрів, так й у якості вибухових речовин. Тому, з військової точки зору, сховище сільськогосподарських добрів з високим ступенем вірогідності можливо розглядати як багатотонний склад деяких вибухових речовин пониженої потужності. Так, калієва селітра під назвою бертолетова сіль входить до складу димного пороху, де до неї після диспергування додається ще сіра та деревне вугілля. Ця суміш сполохає навіть від слабкого імпульсу, удару, тертя та полихає на декілька порядків скоріше, ніж інші вибухові речовини, та дуже легко детонує при звичайнісінькому атмосферному тиску. Саме тому у початку роботи було наведено порівняння небезпеки життя поруч зі добривами як з пороховою бочкою. Закладений пороховий заряд, як відомо, має фугасну дію, що уражує тим більше, чим більше використовується пороху. Відметімо, що назва добрів іноді співпадає зі назвою вибухових сумішей, зокрема аміачно-селітрові. Аміачна селітра окрім весняної підкормки злаків використовується у якості складової частини деяких сумішей вибухових речовин пониженої потужності, де до її сумішей входять вибухові або запальні доданки. Наприклад, амоніти містять у собі крім аміачної селітри ще від двадцяти до п’ятдесяти процентів тротилу. Підриваються вони звичайно за допомогою проміжного зовнішнього детонатору, чутливі до удару та тертя, сприятливі до детонації. Якщо аміачної селітри у вибухової суміші дуже багато, то вона має властивість дефлаграції з великою швидкістю при деяких визначених умовах. На теперішній час велика кількість вибухових речовин є нітросполуками або їх сумішами.

Якщо не уся маса вибухових компонентів добрів детонує після ініціюючого підриву, то вона доповнить собою невибухові компоненти добрів, що разом забруднять у наслідок вибуху навколишнє середовище у великої концентрації та кількості. Доповнімо, що добрива токсичні та

радіаційні тим більше, чим більше їх концентрація. Відомо, що передозування добрив шкідливе ще більше, ніж їх нестача. Так, якщо спилити величезну тополю з діаметром стовбура не менше метра та висотою тридцять п'ять або сорок метрів та висипати на зріз стовбура усього два кілограма калієвої селітри (стандартна розфасовка), а потім накрити селітру плівкою, то стовбур не дасть ні єдиної порослі, а дерево поступово загине на кореню. Постійне випромінювання, хоча й у невеликих дозах, поступово перетворюється у хронічне, оскільки з часом накопичується у організмі та діє до кінця життя. Звернемо увагу, що у даному випадку радіаційне забруднення навколишнього середовища є побічним ефектом знищення добрів. Але погіршення радіоекологічної ситуації та хімічне забруднення підірваними добривами не побічно, а напряму впливає на стан здоров'я людини. Як відомо, при пролонгованої дії на організм людини малих доз випромінювання виникає запальний процес імунної системи з порушенням ліпідного ґенезу з прогресуванням атеросклерозу, що приводить до прискореного старіння, тобто значному перевищенню біологічного віку над календарним.

Прогнозування подальшого розвитку динаміки та очікувані наслідки ситуації з можливим радіаційним та хімічним забрудненням територій сільськогосподарськими добривами у великої кількості та концентрації потребує моделювання, зокрема квантового, хімічного та еволюційного. Для більшості добрів відомо, які їх компоненти випромінюють, існують відповідні рівняння їх розпаду. Складніше передбачити, яки перетворення компонентів відбудуться у наслідок вибуху. Моделювання підкаже, які резильєнтні міри треба здійснити на упередження.

Н.Л. Кужель, О.В. Кужель, Д.М. Юрченко

СОЦІАЛЬНА РЕЗИЛЬЄНТНІСТЬ КОЛЕКТИВУ ОРГАНІЗАЦІЇ ЧЕРЕЗ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ УПРАВЛІННЯ КОНФЛІКТАМИ

У сучасних умовах динамічного розвитку організацій та постійних змін у соціально-економічному середовищі особливої актуальності набуває здатність трудових колективів ефективно протистояти стресам, адаптуватися до викликів і зберігати внутрішню стабільність. Ця здатність описується поняттям соціальна резильєнтність, яке вказує на рівень згуртованості, психологічної стійкості, адаптивності та конструктивної взаємодії в колективі.

Одним з ключових чинників формування соціальної резильєнтності в організаційному середовищі є впровадження технологій управління конфліктами. Такі технології охоплюють низку взаємопов'язаних напрямів, зокрема інформаційний, комунікативний, організаційний і соціально-психологічний,кожен із яких має власне наукове підґрунтя та практичну значущість у забезпеченні емоційного балансу, зменшенні напруження в колективі та підвищенні здатності організації до сталого розвитку.

У цьому контексті застосування сучасних технологій управління конфліктами розглядається як інструмент не лише для мінімізації деструктивних проявів, але й для підсилення соціальної резильєнтності, трансформуючи конфлікти у ресурс командного зростання та покращення корпоративного клімату.

Інформаційна технологія управління конфліктами спрямована на забезпечення повного, точного та своєчасного обміну інформацією в організації. Її теоретичним підґрунтям є когнітивна теорія конфліктів, відповідно до якої значна частина суперечностей виникає внаслідок дефіциту або викривлення інформації. Завдяки впровадженню ефективних каналів комунікації, використанню електронних інформаційних систем та прозорості управлінських процесів знижується ймовірність виникнення конфліктогенних ситуацій [1].

Комунікативна технологія базується на соціально-психологічних дослідженнях міжособистісної взаємодії, зокрема на принципах ефективного спілкування, активного слухання, емпатії та конструктивного зворотного зв'язку. Ця технологія дозволяє мінімізувати напругу у трудових відносинах через розвиток навичок ведення діалогу, подолання комунікативних бар'єрів та підтримання відкритого обговорення проблем, що виникають [1].

Організаційна технологія має за основу класичні управлінські концепції, які передбачають чітку регламентацію функціонування організації. Її метою є усунення конфліктів, спричинених неузгодженістю структури управління, розподілом обов'язків чи ресурсів. Шляхом удосконалення організаційної структури, оптимізації бізнес-процесів і

формалізації службових повноважень можна істотно знизити ймовірність виникнення структурних і ролевих конфліктів [3].

Соціально-психологічна технологія орієнтована на глибинну роботу з особистістю та колективом. Вона спирається на методи психодіагностики, медіації, соціальної підтримки та тренінгового навчання. Основна мета цієї технології - формування в працівників стресостійкості, емоційної саморегуляції, розвитку навичок конструктивної поведінки у конфліктних ситуаціях. Такий підхід сприяє стабілізації емоційного фону в колективі, зміцненню командного духу та зниженню частоти деструктивних проявів конфліктів [4].

Таким чином, кожна з технологій управління конфліктами має власну специфіку, однак найбільшої ефективності можна досягти лише шляхом їх комплексного та взаємодоповнюючого застосування. Впровадження технологій управління конфліктними ситуаціями на підприємстві сприяє не лише мінімізації деструктивних наслідків, але й трансформації конфліктів у ресурс розвитку організації.

1. Микиша, А. Д. (2022). Виникнення конфліктів в організаціях та стратегії їх вирішення. У *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: Збірник тез доповідей міжнародної наукової інтернет-конференції (м. Тернопіль, 7–8 червня 2022 р.)* (с. 55–57). Тернопіль.
2. Гавриш, О. М., & Зоргач, А. М. (2022). Вплив лідера на управління конфліктами в колективі підприємства. *Український журнал прикладної економіки та техніки*, (4), 239–244. http://ujae.org.ua/vplyv-lidera-na-upravlinnyakonfliktamy-v-kolektyvi-pidpryyemstva/ (Дата звернення: 28.05.2025).
3. Городняк, І. В. (2022). Методологічні засади дослідження управління конфліктами в організації. *Проблеми сучасних трансформацій. Серія: економіка та управління*, (6). https://doi.org/10.54929/2786-5738-2022-6-04-01 (Дата звернення: 28.05.2025).
4. Шаульська, Л. В., & Гринкевич, Р. І. (2022). Управління конфліктами компетентнісної та соціально-психологічної природи в інноваційно-активній організації. *Вісник економічної науки України*, 2(43), 132–139. https://doi.org/10.37405/1729-7206.2022.2(43).132-139 (Дата звернення: 28.05.2025).

Л.А. Рибалко-Рак, Р.В. Держій, В.В. Борисенко

КОРПОРАТИВНА СОЦІАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЯК ЧИННИК ФОРМУВАННЯ СОЦІАЛЬНОЇ РЕЗИЛЬЄНТНОСТІ У ВНУТРІШНЬОМУ СЕРЕДОВИЩІ ПІДПРИЄМСТВА

У сучасних умовах соціально-економічної нестабільності, цифрової трансформації та глобальних викликів, з якими стикаються організації, ключового значення набуває здатність підприємства адаптуватися, зберігати стабільність та відновлюватися після кризових ситуацій. Ця здатність охоплюється поняттям організаційної резильєнтності, а її основою є згуртованість персоналу, ефективна внутрішня комунікація, високий рівень довіри та залученості співробітників.

У цьому контексті корпоративна соціальна відповідальність, орієнтована на внутрішнє середовище підприємства, набуває стратегічного значення. Йдеться про відповідальність організації перед своїми працівниками через створення безпечних умов праці, підтримку психоемоційного благополуччя, розвиток професійних компетенцій, справедливу систему мотивації та участь персоналу в прийнятті управлінських рішень [1].Інтеграція корпоративної соціальної відповідальностіу внутрішню політику підприємства сприяє формуванню соціально резильєнтного колективу, який здатний не лише ефективно працювати в умовах змін, але й перетворювати виклики на можливості. Це, у свою чергу, забезпечує довгострокову стійкість, конкурентоспроможність і сталий розвиток підприємства в цілому.

У практичному вимірі реалізація корпоративної соціальної відповідальності у внутрішньому середовищі сучасних організацій здійснюється через низку стратегічно важливих напрямів, що сприяють зміцненню резильєнтності колективу та організаційної культури загалом.Одним із ключових напрямів є формування здорового та безпечного робочого середовища, що передбачає впровадження стандартів охорони праці, запобігання професійним ризикам, а також ініціатив із підтримки фізичного та ментального здоров’я працівників [2]. Це включає програми з емоційного вигорання, профілактичні заходи, гнучкий режим роботи та корпоративні ініціативи зі зниження рівня стресу.

Важливу роль відіграє розвиток системи внутрішніх комунікацій, яка забезпечує прозорість управлінських процесів, своєчасне інформування співробітників, двосторонній зворотний зв’язок та залучення персоналу до прийняття рішень [3]. Такий підхід сприяє формуванню довіри до керівництва, зниженню внутрішніх конфліктів і підвищенню рівня відповідальності кожного працівника за результати діяльності організації.

Не менш значущим напрямом є інвестування в розвиток людського капіталу шляхом організації систематичного навчання, професійного зростання та розвитку лідерського потенціалу. Це забезпечує не лише

підвищення кваліфікації працівників, але й формує внутрішню мотивацію до самореалізації та адаптації до нових умов, що є основою персональної та командної резильєнтності.

Крім того, практикою відповідальної організації є формування інклюзивного середовища, що враховує потреби різних соціальних груп, сприяє недискримінаційним підходам у кадровій політиці та підтримує принципи рівності й поваги до людської гідності. Такий підхід не лише знижує соціальну напруженість, але й зміцнює відчуття єдності та приналежності до організації.

Інтеграція цінностей корпоративної соціальної відповідальності у корпоративну культуру через соціальні ініціативи, етичні кодекси, програми внутрішнього волонтерства та підтримки соціально важливих проєктів сприяє формуванню високого рівня лояльності персоналу, що є важливим фактором довготривалої стійкості організації до криз і зовнішніх змін.

Таким чином, корпоративна соціальна відповідальність у внутрішньому середовищі підприємства постає не лише як етична чи соціальна ініціатива, а як інструмент стратегічного управління, що має безпосередній вплив на організаційну резильєнтність. Комплексна реалізація корпоративних соціально відповідальнихпрактик, орієнтованих на підтримку працівників, розвиток людського потенціалу та побудову інклюзивного корпоративного клімату, формує основу для адаптивності, згуртованості та стабільності колективу. У результаті, організація набуває здатності не лише протистояти кризам, а й трансформувати їх у джерело внутрішнього зростання, підвищуючи конкурентоспроможність та сталий розвиток у довгостроковій перспективі.

1. Букреєва, Д., & Денисенко, К. (2022). Соціальна відповідальність бізнесу як основа забезпечення ділової активності підприємств: євроінтеграційний аспект. *Економіка та суспільство*, (38). https://doi.org/10.32782/2524-0072/2022-38-.
2. Краузе, О. І., Піняк, І. Л., & Шпилик, С. В. (2022). Соціальна відповідальність в контексті діджиталізації бізнесу. *Міжнародний науковий журнал «Інтернаука». Серія: Економічні науки*, (11). https://doi.org/10.25313/2520-2294-2022-11-8381.
3. Євтушенко, Г. В., &Тимохова, Г. Б. (2022). Аналіз форм реалізації концепції соціальної відповідальності бізнесу в умовах бойових дій в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія: Економічна*, (103), 91–96.

Д.І. Симонов, Б.Ю. Заіка, Є.Д. Симонов, М.Б. Фесенко

ТОПОЛОГІЧНІ ІНВАРІАНТИ ЯК ІНСТРУМЕНТ ДІАГНОСТИКИ СТІЙКОСТІ СОЦІАЛЬНИХ СТРУКТУР

Вступ

У сучасному суспільстві соціальні структури, охоплюючи як онлайн-платформи, так і реальні соціальні структури, дедалі частіше перебувають під зростаючим впливом складних та динамічних чинників: соціальних, політичних, економічних та інформаційних. Зростання частоти криз, інформаційних атак і політичних потрясінь висуває нові вимоги до дослідження стійкості структур та здатності до їх оперативного відновлення й адаптації. У цьому контексті ключовим стає поняття резильєнтності, що визначає інтегративну здатність соціальної системи зберігати функціональність і цілісність, реагувати на зовнішні й внутрішні збурення, а також відновлювати структурні та інформаційні зв'язки [1-2].

Мета роботи – математичний аналіз еволюції резильєнтності соціальних мереж під впливом різноспрямованих динамічних факторів, а також виявлення закономірностей і механізмів підвищення соціальної стійкості в умовах змін. Новизна дослідження полягає у використанні сучасних математичних моделей і топологічного аналізу для формалізації, кількісної оцінки та прогнозування резильєнтності, що забезпечує можливість створення ефективних стратегій підвищення стійкості соціальних систем.

1. Топологічні інваріанти резильєнтності

У сучасних дослідженнях складних систем, зокрема соціальних, все більшого значення набувають інструменти топологічного аналізу, що дозволяють виявляти структурні властивості мережі, стійкі до деформацій та локальних змін. Зокрема, персистентна гомологія забезпечує формалізований підхід до ідентифікації й кількісної оцінки таких інваріантів, як компоненти зв'язності, цикли та порожнини в мережевій структурі на різних просторових та часових масштабах.

Нехай $G_t = (V_t, E_t)$ – динамічний граф, що моделює соціальну систему у момент часу *t*, де V_t – множина вершин (акторів), а E_t – множина ребер (соціальних зв'язків). На основі G_t будується сімейство вкладених комплексів $\{K_\tau(G_t)\}_{\tau \geq 0}$, що відповідають Vietoris–Rips комплексам для різних порогових значень τ, які визначають силу чи щільність зв'язків.

Для кожного τ розглядається гомологічна група $H_k(K_\tau(G_t)), k = 1, 2, \ldots$, яка характеризує *k*-вимірні топологічні структури: компоненти зв'язності $(k = 0)$, цикли $(k = 1)$, порожнини $(k = 2)$ тощо. Персистентна гомологія

дозволяє відстежити появу та зникнення цих структур у процесі зміни t, що описується персистентними діаграмами $D_k(G_t)$.

Для оцінки резильєнтності соціальної мережі вводимо наступний динамічний інваріант:

$$R_k\left(G_{[t_0,t_1]}\right) = \sup_{t\in[t_0,t_1]} \max_{\gamma\in D_k(G_t)} \left(\text{pers}(\gamma)\right), \quad (1)$$

де $\text{pers}(\gamma)$ – персистентність k-вимірного класу γ (тобто різниця між моментом народження (“birth”) та загибелі (“death”) структурної особливості).

Цей інваріант описує здатність мережі підтримувати стійкі багатовимірні топологічні структури у динаміці, що асоціюється з резильєнтністю до структурних та інформаційних атак. Крім того, розглядається середнє та кумулятивне значення персистентності всіх структур, що народжуються у заданому часовому інтервалі.

У цьому дослідженні ми висуваємо наступні гіпотези:

1. Гіпотеза структурної резильєнтності: соціальні мережі з високими значеннями R_0 (персистентність компонент зв’язності) виявляють вищу стійкість до фрагментації під впливом зовнішніх атак чи масових видалень вузлів.
2. Гіпотеза когерентної взаємодії: Значні значення R_1 (стійкі цикли) корелюють із наявністю альтернативних шляхів комунікації, що забезпечує збереження інформаційної цілісності навіть у разі деструкції окремих зв’язків.
3. Динамічна гіпотеза: Зниження R_k у динаміці свідчить про втрату резильєнтності мережі та перехід у критичний стан, тоді як стабільність або зростання цього інваріанту асоціюється зі здатністю мережі до самовідновлення.

Запропоновані динамічні топологічні інваріанти, обґрунтовані апаратом персистентної гомології, дають можливість формалізовано та кількісно оцінювати еволюцію резильєнтності соціальних систем. Вони є фундаментом для побудови моделей, що здатні виявляти критичні зміни у структурі соціальних систем та прогнозувати їхню здатність до відновлення в умовах динамічних зовнішніх впливів [3-4].

2. Математична модель адаптивності соціальних структур

Моделювання адаптивності соціальних структур вимагає розширення класичної концепції динамічного графа до врахування механізмів самонавчання та самоорганізації структури під впливом інформаційних і структурних викликів. Запропонована модель ґрунтується на описі соціальної структури як динамічного графа зі змінною топологією $G_t = (V_t, E_t, W_t)$, де V_t – множина вузлів (акторів) на момент часу t,

$E_t \subset V_t \times V_t$ – множина ребер (соціальних зв'язків), $W_t : E_t \to \mathbb{R}_+$ – функція ваги (сил або інтенсивностей зв'язків).

Адаптивність моделюється через функцію оновлення топології:

$$E_{t+1} = \mathrm{F}\left(E_t, X_t, Y_t\right), \tag{2}$$

де X_t – зовнішні впливи (інформаційні атаки, новини, політичні чи економічні події); Y_t – вектор внутрішніх характеристик акторів (рівень довіри, участі, схильність до кооперації).

В рамках моделі зміна структури мережі відбувається через ітеративні локальні операції:

– Додавання нового зв'язку: для довільної пари (i, j), імовірність додавання ребра e_{ij} на кроці $t+1$ визначається як:

$$P_{ij}^{\text{add}}\left(t+1\right) = \sigma\left(\omega_1 \cdot \mathrm{sim}_{ij}\left(t\right) + \omega_2 \cdot \eta_{ij}\left(t\right) + \omega_3 \cdot \xi_{ij}\left(t\right)\right), \tag{3}$$

де σ – сигмоїдна функція; $\mathrm{sim}_{ij}\left(t\right)$ – поточна структурна або інтересова подібність; $\eta_{ij}\left(t\right)$ – міра взаємної довіри; $\xi_{ij}\left(t\right)$ – зовнішній вплив; $\omega_i, i = \overline{1,3}$ – вагові коефіцієнти.

– Видалення зв'язку: імовірність видалення ребра:

$$P_{ij}^{\text{rem}}\left(t+1\right) = 1 - \sigma\left(\delta \cdot \mathrm{rel}_{ij}\left(t\right) + \zeta_{ij}\left(t\right)\right), \tag{4}$$

де $\mathrm{rel}_{ij}\left(t\right)$ – релевантність/актуальність зв'язку; $\zeta_{ij}\left(t\right)$ – вплив негативних факторів (подій).

Для знаходження топології, що максимізує резильєнтність, застосовується еволюційний алгоритм (ЕА) із функцією пристосованості, що ґрунтується на топологічних інваріантах та інформаційних характеристиках мережі.

Для знаходження топології, що максимізує резильєнтність, застосовується ЕА із функцією пристосованості, що ґрунтується на топологічних інваріантах та інформаційних характеристиках мережі. Формалізація еволюційного алгоритму:

1. Кодування: кожен індивід (вершина) в популяції – це конкретна реалізація графа G_t.

2. Функція пристосованості:

$$\mathrm{F}_{\text{fit}}\left(G\right) = \sum_{i=1}^{2} \lambda_i \cdot R_i\left(G\right) + \lambda_3 \cdot Q\left(G\right), \tag{5}$$

де $R_i\left(G\right)$ – топологічні інваріанти; $Q\left(G\right)$ – міра інформаційної цілісності (наприклад, ентропія потоків); λ_i – вагові коефіцієнти.

3. Оператори: селекція: відбір n кращих структур; кросовер: комбінування частин різних графів (наприклад, підграфів чи зв'язків); мутація: випадкові локальні зміни структури (додавання/видалення/зміна ваги зв'язків).

4. Оновлення**:** на кожній ітерації популяція графів оновлюється відповідно до операторів, функція пристосованості оцінюється для кожної вершини (особини).

5. Критерій зупинки: алгоритм зупиняється, коли протягом кількох ітерацій не відбувається значного покращення резильєнтності.

3. Практичні висновки та рекомендації

Запропонований підхід до формалізації резильєнтності соціальних систем на основі топологічних інваріантів і адаптивних динамічних графів дозволяє кількісно оцінювати стійкість мережевих структур та моделювати їхню здатність до відновлення після зовнішніх впливів. Використання персистентної гомології дає змогу виявляти критичні топологічні особливості, які визначають резильєнтність системи.

Для підвищення резильєнтності рекомендується впроваджувати моніторинг топологічних інваріантів у динаміці, застосовувати еволюційні алгоритми та навчання з підкріпленням для адаптивного управління мережею, а також завчасно реагувати на зниження ключових показників стійкості. Перспективним напрямом подальших досліджень є розробка інтегрованих моделей взаємодії структурних та інформаційних інваріантів, а також апробація запропонованих методів на реальних соціальних даних.

1. McLaughlin, P.M., Kennedy, B., Harris, A., Hamilton, M.S., Richardson, J., & Holman-Jones, S. (2020). Online and social media resilience in young people in vulnerable contexts. Vulnerable Children and Youth Studies, 16, 178 - 188. DOI:10.1080/17450128.2020.1849886.
2. Reuter, C., Ludwig, T., Kaufhold, M., & Hupertz, J. (2016). Social Media Resilience During Infrastructure Breakdowns Using Mobile Ad-Hoc Networks. International Conference on Informatics for Environmental Protection. DOI:10.1007/978-3-319-44711-7_7.
3. Д.І. Симонов. (2024). Метод максимізації ентропії для прогнозування поведінки складних систем в умовах шуму. Журнал обчислювальної та прикладної математики, №2, с. 52-61. DOI: https://doi.org/10.17721/2706-9699.2024.2.03.
4. Symonov, D., Symonov, Y. (2024). Methods for selecting models of functioning of multicomponent information and environmental systems. Scientific Journal «Mathematical Modeling», Vol. 1, No 50, P. 57-63. DOI: 10.31319/2519-8106.1(50)2024.304943.
5. Bracci, F., Contreras, M.D., & Díaz-Madrigal, S. (2020). Topological Invariants. Springer Monographs in Mathematics. DOI:10.1007/978-3-030-36782-4_18.
6. Zhang, L., Tang, L., Huang, Z., Zhang, G., Huang, W., & Zhang, D. (2020). Machine learning topological invariants of non-Hermitian systems. Physical Review A. DOI:10.1103/PHYSREVA.103.012419.

К.В. Булда

РОЛЬ МІСЦЕВОГО САМОВРЯДУВАННЯ У ЗАБЕЗПЕЧЕННІ РЕЗИЛЬЄНЬНОСТІ ГРОМАД В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ

Повномасштабна військова агресія російської федерації проти України стала безпрецедентним викликом для соціальних систем на всіх рівнях. Проаналізуємо ключову роль органів місцевого самоврядування (далі - ОМС) у забезпеченні адаптації, стійкості та функціональної цілісності територіальних громад під час повномасштабної військової агресії. На основі аналізу досліджень хочу висвітлити механізми адаптації ОМС до кризових умов, зокрема в аспектах соціального захисту, інституційної взаємодії та реалізації економічних повноважень.

Громади, що були розташовані в зоні бойових дій у перші тижні повномаштабного вторгнення стали прикладом ефективної локальної резильєнтності – спроможності адаптуватися, відновлюватися та надавати підтримку внутрішньо переміщеним особам (далі – ВПО). В таких громадах створювалися Координаційні центри, розгорталися пункти прийому ВПО, логістики допомоги, засновувалися волонтерські ініціативи, регулярно оновлювалися офіційні канали комунікації. Але в той же час такі громади стикалися з проблемою обмеженості ресурсів, доступу до освіти, медицини, працевлаштування.

На сьогодні, громади, що і досі знаходяться на лінії бойового зіткнення, демонструють здатність до самоорганізації та адаптації. Такі громади та ОМС прогнозують ризики, формують списки потреб на запити громадян, приймають ефективні рішення на місцях для підтримання стійкості громади.

Діяльність органів місцевого самоврядування скоригована у зв'язку з дією правового режиму воєнного стану. Але, крім обмежень у реалізації певних функцій, МС отримало й додаткові можливості для ефективного виконання самоврядних і делегованих повноважень. Президент України підписав Закон України «Про внесення змін до Закону України "Про правовий режим воєнного стану» щодо функціонування місцевого самоврядування у період дії воєнного стану" № 2259-IX (реєстр. № 7269). Цей Закон підсилює спроможність органів місцевого самоврядування, зокрема дозволяє оперативно приймати необхідні для забезпечення життєдіяльності громад рішення [1].

Для прикладу: Нововолинська ТГ прийняла понад 10 тисяч ВПО, що є найвищим показником у Волинській області. Для ефективної роботи з переселенцями було створено окремий сектор при управлінні соціального захисту населення. З метою інтеграції та адаптації ВПО засновано громадську організацію «Незламні разом» та Координаційну раду з питань ВПО. Для інформування переселенців функціонує чат «Нововолинськ SOS».

Громада отримала грант у рамках програми ЄС «Житло для внутрішньо переміщених осіб та відновлення звільнених міст в Україні», що передбачає інвестиції в розмірі 7,1 млн. євро на будівництво житла для ВПО [2]. З бюджету та іноземних донорів регулярно виплачуються матеріальні допомоги, компенсації витрат на тимчасове розміщення ВПО, тощо. Управління соціального захисту населення активно співпрацює з міжнародними організаціями для залучення додаткових інвестицій.

Децентралізація в Україні забезпечила громади повноваженнями та ресурсами, що дало змогу оперативно реагувати на виклики війни. ОМС на місцях стали більш резильєнтними. Вони навчилися збільшувати свої ресурси відповідно до потреб та запитів громадян в умовах військової агресії. Зміни у законодавстві дозволяють залучати додаткові інвестиції в громади, від чого залежить працевлаштованість ВПО та доступ до базових потреб.

Висновки. Резильєнтність громад в умовах військової агресії визначається здатністю ОМС до адаптації, ефективного управління ресурсами та підтримки соціальної згуртованості. Посилення інституційної спроможності, впровадження цифрових технологій та стратегічне планування є ключовими факторами забезпечення стійкості громад.

1. Місцеве самоврядування в умовах війни: підсумки за травень https://uplan.org.ua/analytics/mistseve-samovriaduvannia-v-umovakh-viiny-pidsumky-za-traven/.
2. Нововолинська громада прийняла понад 10 тисяч переселенців. Волинь. 2024. URL: https://www.volyn.com.ua/news/264369-novovolynska-hromada-pryiniala-ponad-10-tysiach-pereselentsiv.

А.В. Ониськова

ПСИХОЛОГІЧНА СТІЙКІСТЬ (РЕЗИЛЬЄНТНІСТЬ) – ЗДАТНІСТЬ ПОДОЛАННЯ СТРЕСУ

Проблема психологічної стійкості (резильєнтності) людини перед обличчям складних життєвих ситуацій завжди була цікава та привертала увагу дослідників і науковців, що вивчали різні аспекти людського життя – психологів, соціальних працівників, педагогів та медиків. Тому поняття «резильєнтність» як особливість людської психіки набуває великого значення через необхідність опору стресам, пов'язаних із актуальними соціально-економічними проблемами – життям в часі повномасштабної війни, соціально-політичних конфліктів, загостренням економічних проблем у державі тощо. Отже, вивчення терміну «резильєнтність» є надзвичайно важливим у наших реаліях життя, тому що розуміння людської спроможності до психологічної позитивної адаптації в несприятливих обставинах може допомогти фахівцям з психічного здоров'я розробляти спеціальні методики для психопрофілактики та розвитку резильєнтності, життєстійкості, стресостійкості; розвитку здатності самостійно долати стресові ситуації [1].

Резильєнтність – це здатність людини впоратися зі складними життєвими подіями та відновитися після труднощів чи стресу. Це поняття прийшло в психологію з фізики, де воно означає здатність пружних тіл відновлювати свою форму після механічного тиску. Резильєнтність у психології – здатність зберігати в несприятливих ситуаціях стабільний рівень психологічного та фізичного функціонування, виходити з таких ситуацій без стійких порушень, успішно адаптуючись до несприятливих змін. Тобто, резильєнтність (стійкість) – це не тільки встояти, це ще і відновитися [3].

Резильєнтність актуалізується в умовах надзвичайних за інтенсивністю впливу ситуацій (втрата роботи, житла чи близької людини, зрада, війна, загрозливе захворювання, автотроща, екологічна або техногенна катастрофа, зустріч з будь-якою формою насилля, репутаційні ризики тощо). Це характеристика, завдяки якій ми можемо прогнутися під дією тиску несприятливих зовнішніх факторів, але не зламатися, а якщо і зупинитися, то лише для того, аби переосмислити ситуацію, зробити висновки і продовжити своє життя, набувши нового досвіду, бачення та сенсів [2].

Із досліджень відомо, що люди народжуються з різним рівнем природньої стійкості. Причому, люди, які народилися з найнижчим рівнем, мають більше можливостей пройти весь шлях і досягти максимальної стійкості. У них більше закладений на це потенціал. Тому, задля збереження власного психічного здоров'я та підтримання ефективності своєї діяльності, варто знати які компетентності важливо в собі розвивати. Однією з них є резильєнтність - стійкість перед стресовими впливами [3].

Психологічна резильєнтність – це здатність людини адаптуватися до будь-яких ситуацій, долати труднощі та рухатись далі, незважаючи на складні життєві обставини. Але це не означає, що люди з високим рівнем резильєнтності не відчувають стресу, болю та інших негативних емоцій і почуттів. Натомість вони володіють набором корисних навичок і внутрішніх ресурсів, які допомагають їм ефективно справлятися з викликами, використовувати негативний досвід для особистого зростання та зберігати психічне благополуччя [4].

Згідно визначенню Американської Психологічної Асоціації, резильєнтність — це процес та результат успішної адаптації до важких життєвих обставин шляхом: розумової, емоційної та поведінкової гнучкості; вміння пристосовуватися до зовнішніх та внутрішніх вимог середовища.

Є кілька чинників, які впливають на здатність людини відновлюватися після складних подій, це: те, як людина сприймає світ та взаємодіє з ним; наявність та якість соціальних ресурсів; конкретні стратегії виживання.

Тобто кожен з нас може підсилити свою резильєнтність, вплинувши на ці показники. І про це говорять абсолютно всі дослідження. Здатність до позитивної адаптації та відновлюваності можна практикувати та розвивати.

Пропонується 10 способів підвищення стійкості:

1. Налагодити зв'язки з тими, хто турбується про тебе. «Прийняття допомоги та підтримки від тих, хто піклується про тебе і слухатиме тебе, зміцнює резильєнтність».

2. Сприймати кризи не як непереборні проблеми, а як виклики. «Спробуй заглянути за межі сьогодення та подивитися, як майбутні обставини можуть бути трохи кращими».

3. Прийняти той факт, що зміни є частиною життя. «Прийняття обставин, які не можна змінити, може допомогти тобі зосередитися на обставинах, які ти можеш змінити».

4. Ставити та рухатися до своїх цілей навіть під час війни. «Регулярно роби що-небудь, навіть якщо це здається невеликим досягненням, яке дозволить тобі рухатися до своїх цілей».

5. У несприятливих ситуаціях не завмирати, а діяти. «Замість того, щоб повністю уникати проблем і стресів, та бажати, щоб вони просто зникли, навпаки — в несприятливих ситуаціях дій ще активніше».

6. Шукати можливості для розвитку та досягнення внутрішньої зрілості. «Люди часто дізнаються щось про себе і можуть виявити, що в результаті своєї боротьби із втратою вони значно виросли».

7. Виховувати позитивне ставлення до себе. «Розвиток впевненості у своїй здатності розв'язувати проблеми та довіра своїм інстинктам допомагає підвищити резильєнтність».

8. Намагатися побачити ширший контекст. «Навіть зіткнувшись із дуже болючими подіями, постарайся розглядати стресову ситуацію в ширшому контексті та дивитися на неї у довгостроковій перспективі».

9. Зберігати надію. «Спробуй візуалізувати те, що ти хочеш, замість того, щоб турбуватися про те, чого ти боїшся».

10. Берегти себе. «Зверни увагу на свої власні потреби та почуття. Займайся тим, що тобі подобається, та знаходь час на відпочинок» [5].

Психологічна стійкість – це не про те, щоб уникати труднощів. Це про те, щоб мати силу йти вперед, незважаючи на них.

1. Дмитришин С. Резильєнтність особистості: сутність феномену та методи розвитку. Вісник Львівського університету. Серія психологічні науки. 2024. Випуск 20. С. 67-74. http://psy-visnyk.lnu.lviv.ua/archive/20_2024/12.pdf.
2. Резильєнтність: як розвинути стійкість особистості в умовах життєвих викликів. https://tr.cdc.gov.ua/news/rezylyentnist-yak-rozvynuty-stijkist-osobystosti-v-umovah-zhyttyevyh-vyklykiv/.
3. Резильєнтність для вчителя – це основна компетентність для управління стресом.
4. https://edudevelop.org.ua/traumapedagogy/101-rezilentnist-dlya-vchitelya-tse-osnovna-kompetentnist-dlya-upravlinnya-stresom.html.
5. Мистецтво подолання життєвих викликів. https://naurok.com.ua/post/psihologichna-rezilentnist-mistectvo-podolannya-zhittevih-viklikiv.
6. Що таке резильєнтність і чому вона важлива? https://rfc.nubip.edu.ua/trening-rezylyentnist-yak-zdatnist-vidnovlyuvatysya-u- skladnyh-zhyttyevyh-obstavynah/.

O.S. Georgadze

DECISION-MAKING SUPPORT SYSTEM IN UKRAINE

A decision support system in energy is a set of information and analytical tools designed to collect, process, analyze, and present information necessary to make the best decisions in energy under conditions of uncertainty, importance, and constraints.

The modern stage of society's development is characterized by a continuous process of informatization and improvement of information technologies. The environment for implementing telecommunication and computing systems is constantly expanding, involving new aspects of society's life. In this regard, a crucial task is to ensure a sufficient level of security for these systems, enabling their effective functioning in the face of emerging information threats, which requires an adequate methodological analysis and management of information risks.

In a modern military conflict, where strategic decisions can determine the outcome, the use of advanced technologies for making thoughtful and strategically sound decisions is important [1].

Decision support systems (DSS) in energy help improve resilience, i.e. the ability of a system to recover from disturbances. They provide convenient access to data and models that allow for decision-making in complex situations, such as power outages or unexpected network failures.

Currently, Ukraine's energy efficiency in the context of war is taking on special importance. In addition to the direct destruction of energy and infrastructure facilities, the war creates additional challenges for Ukraine's energy system.Ensuring a stable energy supply is becoming problematic both for military needs and for supporting the life of the country as a whole, as well as for maintaining economic stability.Therefore, the implementation of measures in the energy sector that allow for the rational use of energy resources is economically feasible and strategically important.

In the context of the war with the Russian Federation, Ukraine constantly faces a number of complex tasks and challenges related to ensuring national security and defense. In such situations, decisions made by the country's leadership and military leaders are crucial for the successful completion of tasks and the achievement of strategic goals. One of the key components of an effective management system, which is discussed below, is the management system in the Armed Forces of Ukraine.

1. *Increasing the speed of response*. In military operations, time is often a critical resource. DSS allows for the prompt collection, analysis and processing of data, which helps commanders to make quick and informed decisions.

2. *Increasing the accuracy of decisions*. DSS uses analytical models and modern technologies to process information, which allows avoiding errors that can have fatal consequences.

3. *Increasing the efficiency of resource use*. The Armed Forces have limited resources, and it is important to use them as efficiently as possible. DSS helps to optimize the use of military personnel, equipment and weapons. Military conflicts often have unpredictable circumstances.

4. *Increasing resilience and adaptability*. DSS helps the army to be prepared for different scenarios and adapt to changing conditions.

5. *Improving communication and cooperation*. DSS facilitates the exchange of information between different levels of command and military units, which increases cooperation and coordination of actions.

6. *Training and education of personnel*. Military leaders and system operators must be equipped with the necessary skills and knowledge to use DSS.

7. *Ensuring cybersecurity*. DSS systems must be protected from cyber threats, as their disruption can lead to serious consequences.

8. *Collecting and processing large amounts of information*. DSS requires powerful computing resources and the ability to process large amounts of data.

9. *Continuous improvement*. Technologies are developing rapidly, and DSS must be updated and adapted to new challenges and opportunities.

Decision support systems are an essential tool for the modernization of military management. They help make decisions more deliberate and rational, which is crucial for the success of national defense strategies [2].

The decision support system is an important tool for the Armed Forces of Ukraine in the face of modern geopolitical challenges. It helps to increase the efficiency and accuracy of decisions, which can decisively affect the success of military operations. However, it is important to understand that DSS is not a panacea, and it should be used together with the experience, intuition and strategic thinking of military leaders. The Armed Forces of Ukraine must continue to improve their DSS in order to remain ready for the challenges of the modern world.

Automation of decision support processes has led to the emergence of several approaches to building DSS. DSS systems are based on the application of modern mathematical decision-making methods, various mathematical models, technical and software tools. Therefore, the definition of the concept of decision-making support systems is often associated with these methods, models, tools.

DSS is a computer information system that is used to support various types of activities during decision-making in situations where it is impossible or undesirable to have an automatic system that fully performs the entire process of creating decisions in complex conditions [3].

Conclusions and prospects for further research. The study has the potential for practical application in strategic communications management in the Armed Forces of Ukraine and similar areas. The direction of further research may be the development of additional information storage blocks for decision-making in the strategic communications system in the form of generalizing experience.

The use of "experience" will allow comparing expert assessment with already made decisions that received a positive or negative assessment. Thus, the

decision support system will probably be able to reduce the time for generating a decision, and the introduction of additional relative criteria for checking the probability of success, in the case of making a decision based on already acquired knowledge, will increase efficiency [3].

1. Decision support systems: the importance of implementation in the structures of the Defense Forces of Ukraine. Access mode: https://softline.org.ua/news/sistemi-pidtrimki-prijnatta-risen-vazlivist-vprovadzenna-u-strukturi-sil-oboroni-ukraini.html.
2. Decision support system: advantages for the Armed Forces of Ukraine. Access mode: https://softline.org.ua/news/sistema-pidtrimki-prijnatta-risen-perevagi-dla-zsu.html.
3. P.I. Bidyuk, O. L. Tymoshchuk, A. Ye. Kovalenko, L. O. Korshevnyuk. Decision Support Systems and Methods: Textbook. Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2022, 610 p.

O.M. Dzhyhun

RESILIENCE OF UKRAINE'S ENERGY SYSTEM

Since the beginning of the full-scale invasion, all Ukrainian-controlled thermal power plants (TPPs), hydroelectric power plants (HPPs), as well as 20 combined heat and power plants (CHPs) have been affected. In particular, the power units of the Burshtyn and Ladyzhyn TPPs (over 4 GW) have been put out of operation.

Total power generation capacity has fallen to almost 50% of its pre-2022 level. More than 19 GW of the nearly 37 GW of installed capacity has been destroyed, damaged or occupied. As is known, capacity reduction affects the stability of electricity supply.

Key energy facilities, including the Kakhovka and Dniprovska hydroelectric power plants, were destroyed. Facilities in the Kharkiv region suffered significant damage: the Zmiivska TPP ("Centrenergo") and Kharkiv TPP-5 were almost completely destroyed. The Trypilska TPP in the Kyiv region was also virtually lost.

A significant blow to the Ukrainian energy sector was the loss of control over the Zaporizhzhia Nuclear Power Plant (ZNPP). Several TPPs are also located in the occupied Russian territories (Vuglehirska, Zaporizhzhia, Kurakhivska and Luhanska). The Slavyanska TPP is close to the front line, so it is regularly shelled by the aggressor.

Total direct losses to the energy sector since the start of the full-scale invasion were estimated at $14.6 billion. Indirect losses to the energy sector due to lost revenues, increased electricity prices, and disruptions due to power outages reached $43.1 billion [1—2].

Ukraine has a significant electricity shortage. Thanks to state and private initiatives, the shortage has been reduced, but it is impossible to fully restore the infrastructure quickly. Therefore, stimulating the restoration of the energy sector is currently one of the most important areas. Support for the energy sector is provided both through the implementation of state programs and through bank initiatives. At the same time, the availability of financial resources for the implementation of state energy development programs is significantly dependent on foreign aid.

Ukraine is working to increase its energy independence and strengthen its energy system to reduce dependence on external sources and be more resilient to various challenges. At present, it is important to talk about the resilience of Ukraine's energy system: its ability to withstand stresses and recover from disruptions, including in wartime.

The upheavals caused by the war in Ukraine have shown how automation of asset management processes helps to respond quickly to accidents and ensure the stability of the energy system. The implementation of asset management systems is becoming an integral part of the successful operation of enterprises in modern

realities, which should be considered as a holistic complex of functional elements that must work harmoniously as a single solution to ensure the reliability of equipment and the continuity of its operation.

Russia's active military actions on the territory of Ukraine have demonstrated the importance of protecting the energy sector. Disrupting the stability of the functioning of Ukraine's energy sector has become one of the main instruments of Russia's military aggression against Ukraine. Russia actively uses various methods to disrupt the stability of Ukraine's vital infrastructure: from indirect influence (economic, informational methods) to direct physical influence. Analysis of the impact of physical threats on the country's energy sector during the active phase of Russia's aggression against Ukraine identifies a number of methods of malicious influence in wartime:

- physical seizure of facilities while maintaining their functionality;
- termination of the operation of facilities;
- damaging or blocking supply routes;
- physically destroying the facility;
- hindering recovery activities;
- conducting cyberattacks on the country's power system [3].

The power supply system can serve as an example of assessing the sustainability of the function of providing consumers with electrical energy and the tasks of the ecosystem elements. The power supply system, which includes individual technological elements (raw material and electricity production facilities, electricity transmission and distribution facilities), as well as service elements (communication, management, sales and billing for consumed electricity) is classified as critical infrastructure. All these elements of the power supply system are interconnected by a continuous production process of electricity production and consumption, and a disruption in the functioning of any of the elements affects the stability of the function of providing consumers with electricity.

Since the beginning of the full-scale invasion and massive shelling of infrastructure facilities, the main emphasis has been on resolving urgent issues in order to avoid the threat of equipment shutdown, which could result in a blackout [4—5].

In this context, the use of asset management systems helps to solve a number of new challenges. Therefore, measures to restore and strengthen the energy system include:

- commissioning new renewable energy sources (RES) capacities;
- working with international partners to obtain financial and technical support;
- development of energy efficiency;
- improvement of network operation and launch of new transmission lines.

To improve the sustainability of Ukraine's energy system, a comprehensive strategy is needed that includes not only the restoration of damaged infrastructure, but also the modernization and development of the energy sector as a whole.

Developing Ukraine's energy infrastructure is one of the key strategic objectives on the path to post-war recovery. Success depends on effective support for the sector through a combination of bank lending, state aid, and international investment. In the face of significant pressure from military spending on the state budget, the availability of funds to finance reconstruction and energy development largely depends on assistance from foreign investors, in particular the European Union.

Given Ukraine's path to European integration, in addition to projects to restore energy capacity, in the coming years, measures will be implemented in the energy sector aimed at approaching EU standards: the development of renewable energy and ensuring energy-efficient consumption. Moreover, in the context of attacks on energy facilities that are still ongoing, it is extremely important to continue decentralizing energy production, developing small-scale generation, and increasing the energy efficiency of buildings.

1. Енергетичний сектор України: шляхи відновлення та стратегічні ініціативи. https://finpuls.com/ua/enerhetychnyi-sektor-ukrayiny-shliakhy-vidnovlennia-ta-stratehichni.html.
2. Н.Гутаревич .Енергетика під час війни в Україні: які зміни в регулівнніhttps://jurliga.ligazakon.net/aktualno/12602_energetika-pd-chas-vyni-v-ukran-yak-zmni-v-regulyuvann.
3. Оцінка стійкості енергетичної інфраструктури України. Аналітичний звіт. https://dixigroup.org/wp-content/uploads/2022/05/dixi-energy-resilience-str.pdf
4. Енергетика під час війни: як системи управління активами надають ефективні рішення для енергетики. https://epravda.com.ua/publications/2024/01/29/709143/.
5. Енергетика під час війни: як системи управління активами надають ефективні рішення для енергетики. https://www.epravda.com.ua/publications/2024/01/29/709143/.

І.М. Ушакова-Кирпач, М.С. Хмельницька

ВПЛИВ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ФАКТОРІВ НА РОЗВИТОК МОЛОДІЖНОГО ПІДПРИЄМНИЦТВА

Сучасне суспільство перебуває в умовах швидких змін, спричинених глобалізацією, технічним прогресом, економічною нестабільністю, збройними конфліктами та іншими зовнішніми викликами. Відтак важливим стає поняття резильєнтності– здатності соціальних систем протистояти кризам, адаптуватися до нових умов і функціонувати далі. Молодіжне підприємництво є елементом соціально-економічної структури, що активно реагує на зовнішні зміни. Тому його розвиток є показником резильєнтності громади, суспільства чи держави загалом.

Молодіжне підприємництво виступає не лише засобом економічної самореалізації, а й чинником соціального згуртування, професійної мобільності та інноваційного розвитку. Однак цей напрям діяльності є чутливим до впливу зовнішніх факторів, адже соціально-економічні умови формують можливості та бар'єри для старту бізнесу серед молоді.

Проведений нами аналіз показує, що серед основних зовнішніх соціально-економічних факторів, які впливають на розвиток молодіжного підприємництва, виділяють наступні:

Таблиця 1 – Вплив основних факторів на розвиток молодіжного підприємництва

Фактор	Позитивний вплив	Негативний вплив
Рівень освіти	Формування підприємницьких компетенцій	Відтік молоді за кордон через відсутність мотивації
Доступ до цифрових технологій	Онлайн-торгівля, платформи для просування ідей	Відсутність цифрової грамотності у частини молоді
Економічна політика держави	Грантові програми, пільги для молоді	Складні регуляторні процедури, нестабільне податкове поле
Стан ринку праці	Мотивація до самозайнятості	Масове безробіття як демотиватор
Соціальне середовище	Підтримка з боку друзів, родини, громади	Нерозуміння з боку старших поколінь

Вищенаведені фактори є системними і взаємопов'язаними. Так, нестача практичної підприємницької освіти призводить до невпевненості у власних

силах, а обмежений доступ до цифрової інфраструктури в сільській місцевості позбавляє молодь рівних стартових можливостей.

Резильєнтність соціальної системи – це не лише здатність «пережити» кризу, а й ефективно трансформуватися. Саме тому важливим є розвиток адаптивного середовища, що сприяє самореалізації молоді. Для цього необхідно:

– удосконалити освітні програми з акцентом на фінансову, цифрову та підприємницьку грамотність;

– сприяти створенню інфраструктури підтримки: молодіжні бізнес-інкубатори, акселератори, хаби;

– розвивати партнерства між державою, бізнесом та громадськими організаціями;

– формувати позитивний імідж підприємництва серед молоді через соціальні мережі, публічні заходи, кейси успішних історій;

– забезпечити доступ до мікрофінансування, зниження стартових бар'єрів для молодих підприємців.

Успішна реалізація цих заходів можлива лише за умови наявності тісного зворотного зв'язку між молоддю та соціальними інституціями. Так, успішною вважаємо стала грантова програма «Власна Справа»– популярний у 2022-2024 рокахпроєкт у рамках урядової програми та використання порталу Дія. Головною її метою є створення нових робочих місць та започаткування чи розширення власного бізнесу. Таким чином уряд підтримує розвиток бізнесу і бореться з безробіттям, а повернення коштів гранту відбувається у вигляді податків та зборів [1].

Згідно аналізу даного проєкту, найпопулярнішими сферами, в яких працюють грантоотримувачі визначено оптову та роздрібну торгівлю, ремонт автотранспортних засобів, тимчасове розміщування й організацію харчування, переробну промисловість, охорону здоров'я та надання соціальної допомоги. Розмір фінансування мікрогрантів варіювався від 50 до 250 тис. грн. з умовою їх витрат на придбання або лізинг обладнання, закупівлю сировини і матеріалів та оренду приміщення. Найбільше грантоотримувачівспостерігалось серед молоді з Києва та Київської, Рівненської, Львівської, Івано-Франківської областей. Серед них 70% жінок та 30% чоловіків [2].

Окрім того, ключову роль у розвитку комунікаційного середовища відіграють громадські організації, де народжуються ініціативи та розвиваються ідеї. Водночас і соціальні мережі стають інструментом мобілізації ресурсів, пошуку партнерів та просування власних проєктів. Роль громади як джерела мікропідтримки та мережевої взаємодії також зростає.

Необхідно враховувати й політичні чинники, що впливають на рівень довіри молоді до державних інституцій. Якщо політична система створює передумови для прозорості, підтримки ініціатив, легкого старту бізнесу – це посилює мотивацію до підприємницької діяльності. В іншому випадку –

молодь шукає можливості за кордоном або відмовляється від бізнесу як шляху самореалізації.

Підприємництво серед молоді вимагає особливої уваги як індикатор соціальної стійкості. Чим більше молодих людей створюють власну справу, тим вища мобільність економіки, адаптивність соціуму до змін і здатність до відновлення після криз.

Отже, зовнішні соціально-економічні фактори безпосередньо впливають на формування та реалізацію молодіжного підприємницького потенціалу. Для підвищення резильєнтності молодіжного підприємництва необхідно створювати сприятливе середовище через розвиток освіти, цифрової інфраструктури, партнерських мереж та ефективної державної політики. Саме системна підтримка молоді сьогодні – це запорука сталого розвитку суспільства завтра.

1. Мікрогрант «Власна справа». Режим доступу: https://cdc.dcz.gov.ua/mikrogranti-2023/.
2. Власна справа-2024. https://www.kmu.gov.ua/news/vlasna-sprava-2024-2-mlrd-hrn-hrantiv-na-rozvytok-biznesu-otrymaiut-8000-peremozhtsiv-prohramy.

Ю.М. Здоренко, С.В. Любарський, В.В.Рой, І.Р.Биндас

АДАПТИВНА МОДЕЛЬ ДЛЯ РЕФАКТОРИНГУ ПРОГРАМНОГО КОДУ НА ОСНОВІ FUZZY-ЛОГІКИ

Стрімкий розвиток інформаційних технологій та їх глобальне використання у різних галузях висуває підвищені вимоги до забезпечення високої якості програмних засобів. Для ефективного рішення завдань проєктування, розробки і супроводження інформаційних систем різного призначення важливо інтегрувати механізми забезпечення якості програмного коду на всіх етапах життєвого циклу програмного забезпечення (ПЗ). Тому невід'ємною складовою всіх етапів життєвого циклу ПЗ є процес рефакторингу програмного коду. Рефакторинг програмного коду використовується для запобігання можливим атакам та дозволяє зменшити ризики інформаційної безпеки. Процес рефакторингу програмного коду має ряд обмежень, які пов'язані з використанням методів штучного інтелекту. Такі методи широко використовуються в різних завданнях програмування, а саме: синтезі (генерації) нового коду, аналізі існуючого програмного коду, виявленні вразливостей, помилок програмування, порушень стилю в програмному коді, недоліків архітектури, автоматизованому удосконалені коду, отриманні безпечного та оптимізованого коду на основі виявлених недоліків тощо. Запропонована в [1] функціональна модель рефакторингу об'єктно-орієнтованого програмного коду на основі методів ШІ дозволяє автоматизувати процес покращення рівня безпеки та якості коду. Аналіз досліджень демонструє можливість використання засобів но основі ШІ для виявлення вразливостей та автоматизованого удосконалення структури коду. Важливим аспектом при використанні таких засобів є коректність та достатність даних для навчання таких систем. Тому для повноцінного функціонуванняя запропанованої в [1] моделі рефакторингу необхідно забезпечити процедуру оцінки поточної якості програмного коду на кожному етапі життєвого циклу ПЗ.

Для рішення цієї задачі пропонується модель оцінки якості програмного коду на основі нечіткої логіки. Оцінювання програмного коду в пропонованій моделі здійснюється на основі ряду ознак (характеристик невідповідності) у програмному коді, які використовуються в якості вхідних даних. Так, в якості таких вхідних даних можуть бути обрані code smells-характеристики, а саме: ступінь повтореності програмного коду, розмірність методів, складність класів, кількість змінних, коментарів, кількість відомих вразливостей тощо. Усунення цих code smells-ознак в програмному коді є задачею подальшого рефакторингу. Однак точне визначення таких нечітких категорій, як: малий, середній, довгий або великий, є доволі суб'єктивною оцінкою. Тому математичний апарат нечіткої логіки [2], [3] може бути застосований для формалізації часткової належності зазначеним підмножинам значень code smells-характеристик, а база продукційних

нечітких правил для опису залежності між code smells-ознаками та вихідною характеристикою - якості програмного коду. Використання моделей на основі нечітких систем для оцінки якості програмного коду запропановано в роботах [4], [5]. Однак вони основані на алгоритмі нечіткого виведення Мамдані та не дозволяють в автоматизованому режимі забезпечити налаштування функцій належності та генерацію продукційних правил. Тому робота з ними зводиться до експертного визначення основних параметрів, що може надавати не коректні результати.

Для автоматизації задач налаштування та адаптації параметрів таких систем можуть бути використані відомі підходи на основі поєднання математичного апарату штучних нейронних мереж та нечіткої логіки. В якості вхідних параметрів пропонується використати значення обраних code smells-характеристик. Вихідний параметр, поточне значення якості програмного коду, буде визначатися в процесі нечіткого логічного виводу. Навчання такої нечіткої системи пропонується здійснювати з використанням гібридного алгоритму на основі оберненого поширення помилки та градієнтного спуску. Дані для навчання можуть бути зібрані в процесі аналізу програмного коду з відкритих репозиторіїв (наприклад, GitHab). Навчання створеної моделі пропонується здійснювати в середовищі Matlab [6]. Використання такої моделі на основі накопичених даних про code smells-характеристики дозволить проводити ефективну оцінку якості програмного коду для його подальшого рефакторингу на всіх етапах життєвого циклу ПЗ.

1. Функціональна модель рефакторингу об’єктно-орієнтованого коду на основі методів штучного інтелекту для забезпечення завдання безпеки програмного коду / Любарський С. В., Кондратюк А. Г., Шарнін С. А., Здоренко Ю. М. // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць – Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. – 2025. – № 7. – 264 с. – С. 81-91., ISSN 2786-6610 DOI: https://doi.org/10.58254/viti.7.2025.
2. URL: https://journal.viti.edu.ua/index.php/cicst/issue/archive.
3. Zadeh, L. A. (1997). Toward a theory of fuzzy information granulation and ITM centrality in human reasoning and fuzzy logic, Fuzzy sets and systems, 90(2), 111–127. DOI: https://doi.org/10.1016/S0165-0114(97)00077-8.
4. Takagi, T, Sugeno, M.: Fuzzy identification of systems and its applications to modeling and control. IEEE Transactions on Systems, Man, and Cybernetics 15(1), 116–132 (1985). https://doi.org/10.1109/TSMC.1985.6313399.
5. Avdagic, Zikrija & Boskovic, Dusanka & Causevic, Aida. (2008). Code evaluation using fuzzy logic.
6. Rajni Sehgala, Deepti Mehrotraa and Manju Balab Prioritizing the refactoring need for critical component using combined approach Decision Science Letters 7 (2018), 257–272.
7. S. N. Sivanandam, S. Sumathi, S. N. Deepa Introduction to Fuzzy Logic using MATLAB / Topics: Mathematical and Computational Engineering, Artificial Intelligence, Computer Imaging, Vision, Pattern Recognition and Graphics, Edition Number 1, pp.430, (2007). https://doi.org/10.1007/978-3-540-35781-0.

М.А. Косовець, Л.М. Товстенко

ГАРАНТОЗДАТНІ ОБЧИСЛЕННЯ ВІДМОВОСТІЙКИХ СИСТЕМ РЕАЛЬНОГО ЧАСУ – ШЛЯХ ДЛЯ ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ДИНАМІЧНИХ СИСТЕМ В ЕНЕРГЕТИЦІ

Анотація. В статті розглянуто гарантоздатні обчислення динамічних систем для підвищення резильєнтності на базі вбудованого відмовостійкого мультипроцесора реального часу для управління процесами в енергетиці з підвищеними вимогами до надійності. Особливу увагу приділено розгляду абстрактного ресурсу – надійності, його виняткову роль при проектуванні та особливості застосування в реальному масштабі часу. Запропонований у цій статті механізм відновлення не тільки забезпечує модульність та простоту системи, але також дає можливість швидкого відновлення та точного прогнозу часу завершення завдання. Система реконфігурується, завдання перерозподіляється між процесорами. За наявності вільних процесорів останні ініціалізуються і включаються в обчислювальний процес. Запропонована та сформульована оцінка ефективності даної відмовостійкої технології. При виникненні помилки системний монітор перезапускає операції, а при її повторенні призупиняє роботу всіх процесорних модулів, визначає збої і відновлює роботу, використовуючи наявні процесори. За відсутності адекватної заміни процеси перерозподіляються. При зменшенні кількості процесорів нижче критичного значення система деградує, процеси перерозподіляються серед «готових до виконання задачі» процесорів, при цьому падає продуктивність системи без погіршення якості. ованість.

Ключові слова: готовність, ймовірність безвідмовної роботи, генерація системи, диспетчер, ресурс, інтерфейс, метод доступу, модульність, монітор, мультипроцесор, операційна система, процедура, реконфігурація системи.

ВСТУП

Стійка тенденція зростання наукових публікацій у престижних зарубіжних виданнях щодо проблеми відмовостійкості вбудованих систем реального часу та використання на об’єктах енергетики обумовлена кризою архітектурних моделей, здатних адекватно відобразити прикладне завдання з необхідним значенням надійності. Актуальність побудови систем із заданим значенням надійності особливо важлива при проектуванні автоматизованих систем атомних електростанцій. Сьогодні останні не мають альтернативного рішення.

Інтерес розробників до проблеми проектування вбудованих надійних систем реального часу продиктований появою сучасної елементної бази. Низька вартість, невеликі габарити та мале споживання яких дозволяє проектувати мультипроцесорні системи реального часу, використовуючи повноцінні стійкі до відмов архітектури вбудованих мультипроцесорних мікро-ЕОМ. Проблема з теоретичної перейшла у практичну. А це, у свою

чергу, дозволяє налагодити виробництво нових конкурентоспроможних виробів високої складності та надійності на об’єктах енергетики.

Аналіз проблем, пов'язаних з обробкою діагностичної інформації складних об'єктів, показує, що багато завдань діагностування вирішують за допомогою вбудованих мікро-ЕОМ, архітектура яких не відповідає класу поставлених завдань. Так, завдання діагностування вирішують за допомогою вбудованих мікро-ЕОМ, архітектура яких не відображає проблем організації обчислень, що ранжуються за рівнями гарантоспроможності.

Архітектурні моделі точно представляють функціональні можливості апаратних та програмних компонентів з використанням високорівневої абстракції у вигляді потоків даних та абстрактно представляють технологію реалізації у часі та містять схеми арбітражу, допускають параметризацію та типізацію. Так, параметри конфігурації архітектурної моделі дозволяють визначити співвідношення реалізації функцій апаратними та програмними засобами [1]. Проектування на системному рівні із застосуванням архітектурного моделювання спрощує специфікацію проекту, робить плавним перехід від функціональних вимог до формальних, оскільки поділяє проблеми вироблення функціональних вимог та специфікацій проекту, засобів кількісної оцінки специфікацій.

1. ГАРАНТОЗДАТНІ ОБЧИСЛЕННЯ ВІДМОВОСТІЙКИХ СИСТЕМ РЕАЛЬНОГО ЧАСУ – ШЛЯХ ДЛЯ ПІДВИЩЕННЯ РЕЗОЛЬЄНТНОСТІ ДИНАМІЧНИХ СИСТЕМ В ЕНЕРГЕТИЦІ.

Створення та розвиток складних систем реального часу для динамічних систем в енергетиці, що мають підвищені вимоги по надійності, одна з найважливіших технічних проблем. При цьому надійність включає гарантоздатність обчислень, тобто система виконуватиме задану функцію в заданий період часу за встановлених умов навколишнього середовища. Для фахівців з аналізу систем надійність є основним параметром. Наприклад, відмова динамічної системи в енергетиці може стати причиною невиконання поставленого завдання та призвести до фатального результату, так для атомних електростанцій – до катастрофи. Надійність пов'язана з безпекою, порушенням технологічного циклу на об’єктах в енергетиці може призвести до величезних збитків. Проблема надійності завжди розглядається на стадії проектування. Запобігання відмовам можна досягти різними шляхами, наприклад: застосуванням наднадійних компонентів мультипроцесора; покращенням технічного обслуговування на основі розробки ефективних методів пошуку та усунення несправностей; удосконаленням процедури контролю технологічного процесу виготовлення; випробувань та сертифікації готових виробів; здійсненням резервування апаратних засобів, створенням технології проектування систем, що мають властивості відмовостійкості в умовах, коли дефекти неминуче існують і можуть проявляти себе у формі відмов та випадкових збоїв. Під стійкістю до відмови

розуміємо таку властивість архітектури цифрової системи, яка дозволяє логічній машині продовжувати роботу і тоді, коли в реальній системі, що є її носієм, виникають різноманітні відмови компонентів [2]. Рішенням основного завдання відмовостійкості є відновлення обчислювального процесу з точки виникнення відмови. Для цього необхідно виявити та ізолювати відмовний компонент. Для відновлення працездатності потрібне знання вектора стану на даний момент. Методи відновлення залежать від можливості ізоляції виявленої відмови у системі на найнижчому можливому рівні абстракції системи. Запропонований у цій статті механізм відновлення не тільки забезпечує модульність та простоту системи, але також дає можливість швидкого відновлення та точного прогнозу часу завершення завдання.

Типова система, нечутлива до відмов, повинна проводити розпізнавання всіх можливих помилок та їх ідентифікацію. Для цього використано вбудовані системи контролю та тести. Для виявлення помилки використовується тест змістовності. Після виявлення помилки несправні компоненти локалізуються та виключаються з обчислювального процесу. Система реконфігурується, завдання перерозподіляється між процесорами. За наявності вільних процесорів останні ініціалізуються і включаються в обчислювальний процес з точки відмови. Точка відновлення визначається прикладною програмою, яка зберігає інформацію до точки відновлення. При виявленні помилки в підсистемі, відновлення можливе через рестарт, що недоцільно, оскільки обчислювальний процес починається з вихідного значення, а якщо обчислювальні процеси пов'язані між собою, виникає труднощі ізоляції відмови від впливу на інші паралельні процеси. Тому при розробці програм ретельно структуруємо паралельні процеси, щоб точки відновлення у взаємодіючих процесах були взаємно узгодженими. Повторення одного процесу може поширюватися на інші процеси та події. Іноді з'являється лавина повторів, тоді процес повертається на кілька кроків назад. При цьому неминучі надмірність процесу відновлення та втрата продуктивності.

Складність створення відмовостійких систем полягає в повному перегляді принципів і ідеології проектування. Значення надійності розраховується і закладається на системному рівні і залежить не тільки від апаратних і програмних ресурсів, а більшою мірою від їхньої взаємодії в управлінні ресурсами. В результаті надійність постає як ресурс системи і варіюється в залежності від завдання, що виконується.

Відмовостійкість забезпечується апаратною, програмною або апаратно-програмною надмірністю. Відмова окремого процесорного модуля виявляється в обмеженому контурі. Відмовостійкість під час роботи визначається виявленням помилки, реконфігурацією компонентів системи та відновленням безпомилкової роботи мультипроцесора.

Домінуючим напрямком проектування вбудованих мікро-ЕОМ є вибір архітектури зі збільшеними значеннями продуктивності, пам'яті та інших

ресурсних показників. Принцип організації високопродуктивних обчислювачів, в основі яких лежить організація макроконвеєрних обчислень, заснований на паралелізмі алгоритмів, що зводяться до системи слабозв'язаних та незалежних операцій гілок алгоритму, не зазнав кардинальних змін. Процес створення вбудованої системи з вбудованим стійким для відмови процесором реального часу дуже трудомісткий.

Формальний опис бази організації обчислень, що ранжуються за рівнями гарантоспроможності, має вигляд таблиці, що задає відповідність між об'єктами та операціями, що застосовуються до них. Визначення об'єктів полягає в типі об'єкта, атрибутах об'єкта та інтерпретації об'єкта набором операцій, що застосовуються до нього. Зазначимо, що гарантоспроможне завдання, що відновлюється – семантичні різновиди завдання, а завдання – видозмінений аналог звичайного завдання. Інші об'єкти вищеназваної бази в концептуальному та формальному відношенні ідентичні відповідним об'єктам канонічної бази організації макроконвеєрних обчислень.

Під ресурсом обчислювальної системи прийнято вважати пам'ять, процесорний час, канали введення-виведення, інтерфейси. Ресурс перетворився на абстрактну структуру, до якої потрібний доступ. До системних ресурсів відносимо програми, які управляють обчислювальним процесом і визначаються у системі як об'єкти. Доцільно інтерпретувати абстрактний ресурс: достовірність, продуктивність, надійність як системні ресурси. Це дозволяє використовувати операційі системи як механізми управління абстрактними ресурсами: достовірності, продуктивності, надійності.

Для формалізації обчислювального процесу створюємо логічні ресурси та механізм доступу до них. Управління логічними ресурсами зручніше, ніж фізичними. Організацію взаємодії у такій гіпотетичній машині покладено на операційну систему. Метою її є визначення середовища для створення та виконання програм, створення методів доступу та управління обчислювальними ресурсами, побудова інтерфейсів між різними рівнями абстракції обчислювальної системи. Фактичним стандартом засобів інтерпретації макроконвеєрних обчислень є багатозадачна операційна система. Об'єктно-орієнтована архітектура операційних систем дає можливість застосування математичних методів дослідження ефективності варіантів апаратно-програмної реалізації паралельних алгоритмів. Побудова оптимального варіанта засобів реалізації заданого алгоритму забезпечує багатоваріантний арбітраж системної магістралі та резидентних ресурсів. Таким чином, однокристальні мікро-ЕОМ є основою великого класу мультипроцесорних мікро-ЕОМ з розподіленою магістраллю, підвищення продуктивності яких досягається за рахунок одночасної реалізації паралельних компонентів алгоритму. Використання обмінної пам'яті вбудованого мультипроцесора з метою взаємного контролю функціонування мікро-ЕОМ дозволяє виявити факт порушення правильності роботи мікро-ЕОМ. Проте не вирішено питання захисту від збоїв. Отже, однокристальні

мікро-ЕОМ недостатньо придатні для обробки діагностичної інформації при дефіциті ресурсів надійності, особливо найбільш відповідальних режимів функціонування об'єкта. Істотна взаємозалежність надійності та продуктивності визначає необхідність створення вбудованих мікро-ЕОМ зі змінним співвідношенням продуктивності та достовірності. Проектування мікро-ЕОМ такого класу висуває ряд актуальних завдань, до найбільш складних з яких відноситься формальна інтерпретація проблем обробки інформації при дефіциті ресурсів надійності.

Якщо процес визначити як такий що виконується, а процедуру як послідовність машинних команд, його можна виділити як один із системних об'єктів. Кожному керованому об'єкту приписується певний тип. Об'єкти цього типу управляються за допомогою спеціально призначеного для цього механізму. Програми, залежно від способу передачі управління, розширюють функції апаратури та виконуються як процес, інші - є обслуговуючими та не мають відповідного запису у черзі диспетчера. Програми, що обслуговують нижній рівень це примітиви, програми синхронізації, диспетчеризації, обробки переривань. Вводимо поняття глобального процесу – програм, які вимагають тимчасового ресурсу з метою оцінки використання різних ресурсів мультипроцесора, наприклад, завдання варіації надійності і продуктивності, збору статистики та інші, що вимагає переформування черги диспетчера.

Системи управління, збору та обробки діагностичної інформації складних об'єктів мають ієрархічну організацію та відповідають поняттю горизонтальної структури. Перевага горизонтальної структури полягає у простоті включення нових обчислювальних ресурсів. Зміні підлягає лише нижній рівень за допомогою додавання нових драйверів. Для виконання міжрівневих переходів є формальні апаратно підтримувані механізми. Потрібно зважити на час, який додатково витрачається на переходи. Вертикальна структура операційної системи дозволяє мінімізувати тимчасові витрати та досягти високої функціональної інтеграції.

Діагностична модель на системному рівні є спрямований граф G(U,V), званий діагностичним графом, в якому кожна вершина V відповідає деякому модулю системи, а кожна дуга U , що з'єднує пару вершин і - наявності тесту t , що генерується модулем для перевірки модуля. Діагностичне ядро легко реалізується операційною системою, тому його зручно використовувати у мультипроцесорі. Використовуючи плаваюче діагностичне ядро, кожен модуль можна перевірити сукупністю тестів, що видаються з інших модулів.

Створюючи концептуальну модель стійкого до відмови мультипроцесора реального часу, де процесорні елементи слабо пов'язані між собою, особливе місце відводиться міжмодульним інтерфейсам. Це спростить підтримку, модифікацію та налагодження програмного забезпечення мультипроцесора реального часу для систем із розподіленою обробкою.

Введемо поняття системного монітора, що є сукупністю процедур, призначеного керувати ресурсами певного типу. Кожен тип системних ресурсів управляється своїм монітором. Наприклад, монітор центрального процесора, ресурс надійності. Кожному монітору надано виключне право доступу до системних таблиць та інших структур, пов'язаних з даним типом ресурсів. Монітор відповідає за розподіл ресурсів, взаємопов'язаних та взаємозалежних із ресурсом надійності, а також за звернення з боку інших програм, наприклад, що потребують зміни ресурсу надійності.

Процеси розподіляються через мережу слабопов'язаних процесорних модулів, призначених для розподіленої обробки. Утворюється черга процесів та паралельне виконання взаємодіючих процесів. Кожен процесорний модуль зберігає свій стан – локальні змінні процесу та стан процесора на різних етапах роботи.

При реалізації обміну між взаємодіючими процесами у стійкій до відмови структурі потрібно враховувати наступне: обмін між процесами здійснюється через мережу зв'язку необхідної надійності, яка при необхідності може нарощуватися і задовольняти вимогам процесів; є можливість запобігання відмовам; структура мережі має бути прозорою для керованих процесів; процеси та процесори виконують лише покладені на них функції.

Повна декомпозиція системи на основні елементи дає можливість реалізувати принцип структурного програмування програмах управління окремими процесами. При "динамічній" декомпозиції системи вибір незалежних змінних може привести до складності а, отже, і вартості реалізації. Сутність декомпозиції в тому, щоб виявити та використати основні особливості природної структури системи. Зазначимо основні принципи декомпозиції вбудованої мультипроцесорної мікро-ЕОМ реального часу: використання природної декомпозиції, результатом якої є низка квазінезалежних процесів із відносно слабкою взаємодією; обмін між процесами здійснюється шляхом передачі повідомлень через мережу зв'язку, інтерфейс якого має бути уніфікованим; процеси повинні бути реалізованими за відведений час, для запобігання критичним перехідним характеристикам бажано кожному процесу привласнити свій процесор – це забезпечить максимум використання обчислювальних ресурсів шляхом підтримки високого ступеня паралелізму функціонування її окремих елементів та простоту реалізації у зв'язку з наявністю дешевих процесорних елементів. Поруч із робочими характеристиками необхідна надійність здійснення окремих процесів – одної з основних критеріїв декомпозиції системи.

Операційна система з боку користувача завжди асоціюється із механізмом управління ресурсами. Ресурс - абстрактна структура з цілим рядом атрибутів, що характеризують способи доступу до цієї структури та її фізичне уявлення в системі. Для управління ресурсами у системі приймається стратегія управління ними, яка приймається виходячи з розв'язуваних завдань, вимог до системи. Виникає необхідність спільного

використання обчислювальних ресурсів. Ресурсами можна керувати за необхідності, і динамічно, використовуючи механізм пріоритетів інтенсивності їх використання. Обидва механізми мають свої переваги та свої недоліки. Так, при динамічному управлінні можливі затримки через тимчасову недоступність тих чи інших ресурсів. Виконуюча програма перетворюється на стан очікування до того часу, поки потрібні ресурси не звільняться, утримуючи раніше захоплені ресурси, що може призвести до глухої ситуації. Розв'язання задачі має забезпечуватись у заданий проміжок часу, і реальний процес не завжди дозволяє зробити перезапуск завдання із самого початку. Проблема полягає в інтегральному характері ресурсу надійності і для його визначення потрібний процесорний час. Надійність мультипроцесора розраховується, іноді нетривіально, наприклад, вводячи обчислювальну, алгоритмічну надмірність ми підвищуємо стійкість до відмови системи, що в свою чергу призводить до збільшення надійності системи. Причому характер збільшення надмірності процесорного ресурсу не прямо пропорційний збільшенню надійності, оскільки залежить від програмного забезпечення та надійності елементної бази. Ресурс надійності - це межа якої завжди прагне надійність системи. Варіюючи ресурсом продуктивності та достовірності, ми можемо максимально використовувати ресурс надійності в бортових системах, оскільки їм завжди притаманний дефіцит ресурсів надійності, що накладає особливі вимоги під час проектування вбудованої апаратури. Важливо, щоб параметр надійності був передбачуваним і, що найважливіше, при зменшенні ресурсу надійності нижче допустимого, система повинна деградувати поступово, виконуючи при цьому свою штатну задачу з подальшим відсіканням прикладних завдань у міру їх важливості, і так до повної зупинки, попередивши взаємопов'язані системи та запам'ятавши свої результати. Організація обчислень при дефіциті ресурсів надійності вимагає розподілу завдань між процесорами, що базується на апріорних та прогнозних характеристиках ресурсів продуктивності та надійності процесорів. Розподіл завдань між процесорами включає вихідний розподіл завдань між процесорами та наступні розподіли, пов'язані з відмовами процесорів. З метою такого розподілу завдань кореневе завдання містить задачу координації, що визначає вихідну та наступну прив'язку процесорів до завдань. В результаті розв'язання задачі координації кожен процесор виділяє завдання відновлюваних завдань, що відповідають позиції процесора. При цьому фактична продуктивність мультипроцесорної мікро-ЕОМ залежить від співвідношення часу, що витрачається на вирішення відновлюваних завдань і часу, що витрачається на вирішення завдань гарантоспроможних завдань. Очевидно, що нижня межа продуктивності досягається у тому випадку, якщо всі завдання належать гарантоспроможним завданням, а верхня межа – якщо задачі гарантоспроможних завдань відсутні.

Розглянемо спочатку питання вирішення завдання при вимогах, які не накладають суттєвих обмежень на структурну надмірність засобів реалізації

алгоритмів. Практика відображення проблем, пов'язаних з обробкою інформації при дефіциті ресурсів надійності, на архітектуру мультипроцесора показала, що мінімальним базисом засобів інтерпретації макроконвеєрних обчислень, що ранжуються за рівнями гарантоспроможності, може служити мультипроцесорна мікро-ЕОМ, що містить тріаду процесорів з вбудованими засобами. Цей ресурс дає можливість взаємного контролю функціонуванням процесорів, заснованих на тому, що кожну задачу відновлюваних завдань вирішує один процесор, а кожну задачу гарантоспроможних завдань – тріада процесорів [3]. Взаємний функціональний контроль процесорів здійснюється шляхом розподіленого мажоритарного порівняння рішень, що передаються системною магістралі до архівів розв'язків задач гарантоспроможних завдань. При правильному функціонуванні всіх процесорів реалізується взаємне копіювання архівів завдань, що відновлюються. При виявленні фактів неправильного функціонування будь-якого процесора тріади справні процесори забороняють (за допомогою засобів конфігурації) доступ неправильно функціонуючого процесора до системної магістралі і встановлюють очікуваний час його відновлення. Справні процесори вирішують завдання координації, перерозподіляють завдання, що відновлюються. Вони також вирішують завдання відновлюваних завдань, виключеного процесора через повернення до ретроспективних рішень.

Після того, як очікуваний час відновлення функціонування процесорів спливає, справні процесори долучаються до системної магістралі виключеного процесора і оцінюють правильність вирішення гарантоспроможних завдань, отриманих поверненим процесором. Якщо ці завдання вирішені правильно, попередній стан процесора трактується як порушення правильного функціонування, обумовлене збоєм, і відновлюється вихідний розподіл завдань. В іншому випадку стан процесора трактується як несправне, і повторно забороняється надання доступу до системної магістралі несправному процесору.

Таким чином, модифікація структури мультипроцесорної мікро-ЕОМ полягає в перетвореннях конфігурації, пов'язаних з типом завдання, що виконується, і перетвореннях конфігурації, викликаних неправильним функціонуванням процесорів.

ВИСНОВОК

В статті розглянуто гарантоздатні обчислення динамічних систем для підвищення резильєнтності на базі вбудованого відмовостійкого мультипроцесора реального часу для управління процесами в енергетиці з підвищеними вимогами до надійності. Задача підвищення резольєнтності зводиться до системного проектування вбудованого відмовостійкого мультипроцесора реального часу з варіацією співвідношення продуктивності і достовірності при дефіциті ресурсів надійності. Особливої актуальності розглянуті питання набувають при проектуванні динамічних систем в

енергетиці для управління та діагностування у реальному масштабі часу. Розглянуто відмовостійкий вбудований мультипроцесор реального часу для управлінням ресурсами. Особливу увагу приділено абстрактному ресурсу – надійність і можливого управління ним при вирішенні прикладного завдання. Побудована гіпотетична модель мультипроцесора реального часу зі співвідношенням ресурсів продуктивності і достовірності, що варіюються та їх взаємозв'язку. При кількісному визначенні ресурсу надійності, визначальні параметри якого мають «розмитий» характер, використано наближені «евристичні» методи розрахунків, створені задля збільшення граничного значення параметра надійності мультипроцесорної мікро-ЕОМ за рахунок реконфігурації системи у процесі вирішення задачі. Відмовостійкість системи з мінімальною тимчасовою надмірністю та завершенням процесу до виникнення тупикової ситуації, особливо важлива в динамічних системах реального часу на об'єктах енергетики.

1. F. Reghenzani, Z. Guo, W. Fornaciari. Software Fault Tolerance in Real-Time Systems: Identifying the Future Research Questions. 2023. ACM Comput. Surv. 30 pages. https://doi.org/10.1145/3589950.
2. Avizienis A. Fault-Tolerant Computing: Progress, problem, and prospects / A. Avizienis // Proc. IFIP Congress '77. – Toronto, Canada, 1977. – P. 405 – 420.
3. *Косовец Н.А.* Об аппаратных средствах повышения надежности отказоустойчивых микропроцессорных систем. / Кибернетика и вычислительная. - 1993. - Выпуск №99. Сложные системы управления. с.102-104.

С.Д. Винничук

СТРУКТУРА ГРАФА РОЗПОДІЛУ ПОТОКІВ ПОВІТРЯ ПРИ МОДЕЛЮВАННІ ПРОЦЕСІВ РОЗГЕРМЕТИЗАЦІЇ ВІДСІКІВ ЛІТАКА

Авіаційні правила FAR 25 / CS 25 п. 365 передбачають виконання ряду безпекових умов, серед яких вимоги щодо надійності конструкції герметичних відсіків літака за умов розгерметизації [1]. Вона має бути сконструйована таким чином, щоб витримувати вплив раптового скидання тиску через отвір визначеного розміру у будь-якому відсіку на будь-якій робочій висоті, що забезпечить безпечний подальший політ та приземлення.

На практиці надійність конструкції характеризується граничними значеннями різниці тисків між суміжними відсіками. При виникненні раптової (аварійної) розгерметизації тиск у відсіках динамічно змінюється, де різниці значень тиску між суміжними відсіками не повинні перевищити деякі встановлені граничні значення. Експериментальні дослідження з питань розгерметизації недоцільно проводити. Тому оцінку надійності конструкції перегородок між відсіками здійснюють на основі моделювання гідравлічних процесів у відсіках літака для режимів виникнення можливої раптової розгерметизації в кожному з відсіків.

Згідно авіаційних правил CS 25 п. 365 e), f), g) [1] за результатами оцінки небезпеки має бути встановлено, які конструкції повинні витримувати результуючі навантаження через перепад тиску. При цьому розмір отвору в перегородках між відсіками слід розглядати лише як елемент математичного апарату щодо розрахункових навантажень при граничному тиску з метою запобігання руйнуванням вторинних елементів конструкції.

Визначені в CS 25 п. 365 правила дозволяють розглядати кожен з відсіків як вузол з відомим об’ємом, де встановлюється єдине значення тиску. Гідравлічні процеси для кожного з моментів часу можна вважати квазістаціонарними, де динамічний процес зміни тиску характеризує зміну маси повітря у відсіках при його витіканні через отвір визначеного розміру. Тому систему відсіків можна представити розрахунковою схемою гідравлічної мережі. Проте така мережа формує граф, у якого можлива значна кількість паралельних гілок (довільні дві паралельні гілки описуються одними і тими ж вузлами). Така структура графа спричинена особливостями конструкції перегородок між відсіками.

Між відсіками можливе перетікання повітря через нещільності конструкції перегородок, через вентиляційні отвори (існуючі отвори в конструкції), або спеціальні панелі (люки), які відкриваються під тиском. Для всіх таких варіантів перетікання принципово різними є моделі гідравлічних процесів. У випадку нещільностей (модель 1-го типу) при малій величині гідравлічного діаметру процес можна вважати ламінарним. При

перетіканнях через вентиляційні отвори слід враховувати втрати тиску входу та виходу потоку (модель 2-го типу). А у випадку наявності спеціальних панелей (лючків), які відкриваються під тиском, - враховувати значення тиску, при якому починається відкривання та степінь відкриття при збільшенні тиску (модель 3-го типу). А кожен з лючків може характеризуватися окремим значенням тиску. За таких умов узагальнена структура потоків, що визначають вид розрахункового графа гідравлічної мережі, який містить всього два відсіки, матиме вигляд, представлений на рис. 1.

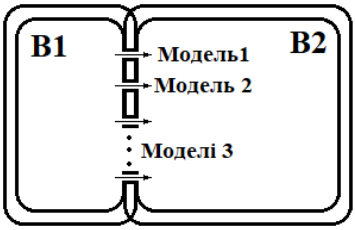

Рисунок 1 – Узагальнена структура потоків для двох відсіків

На рис. 1 символами B1 та B2 позначено відсіки 1 та 2. Потоки в напрямку від відсіку 1 до 2 (напрям вказано стрілкою) відповідають умовам моделей 1-3. Як видно, кількість таких потоків не регламентується. Якщо B1 та B2 сприймати як вузли графа 1 та 2 відповідно, то кожен з потоків буде гілкою (ребром) графа, що починається у вузлі 1 та закінчується у вузлі 2.

Для таких задач гідравлічного розрахунку граф розрахункової схеми гідравлічної мережі пропонується формувати у вигляді розширеного списку інциденцій, де вузлами будуть номери відсіків, які визначають узагальнену гілку, дані про яку задаються за правилом:

1. задати вузол початку узагальненої гілки;
2. задати вузол кінця узагальненої гілки;
3. задати вид моделі та дані, необхідні для гідравлічного розрахунку;
4. задавати дані згідно п.3 до тих пір, поки не появиться ознака ознаку закінчення даних про потоки між відсіками.

Пропонований варіант структури даних забезпечує можливість формування даних про гідравлічну мережу системи відсіків для довільних існуючих способів реалізації конструкції перегородок між відсіками та її врахування при гідравлічних розрахунках.

1. EASA. Decompression – Small Compartments. Взято 07.06. 2025 р. https://Generic CRI on Decompression Small Compartments.pdf.

Ф.О. Коробейніков

БЕЗПЕКА СОЦІОТЕХНІЧНИХ СИСТЕМ В КОНТЕКСТІ ТЕОРІЇ СКЛАДНОСТІ

Якщо розглядати соціотехнічні системи не в інженерно-операційному, а в системно-онтологічному ракурсі, виявляється фундаментальна дихотомія, що структурує множину таких систем на дві принципово різні категорії: функціонально-стабільні та еволюційно-динамічні системи.

Перша категорія — **функціонально-стабільні системи**. Це світ фабрик і заводів, електростанцій і центрів обробки даних — технологічних ансамблів, в яких вся структура і діяльність підпорядковані чіткій і незмінній функції: виробництву продукту, перетворенню ресурсів у матеріальні або інформаційні цінності. Їхня архітектура несе відбиток детермінованості, і людська роль тут зведена до механістичної функції, обмеженої, чітко регламентованої і, відтак, потенційно відтворюваної машиною, роботом або штучним інтелектом.

Друга категорія — **еволюціонуючі соціотехнічні системи**. Це держави та організації, комерційні компанії та соціальні інститути, релігійні спільноти та національні утворення — те, що складає живу тканину суспільства і формує його внутрішню структуру.

В основі таких систем лежать не функції, а *інваріанти* — глибинні принципи, норми, закони і цінності, що визначають їхню онтологічну сутність. Інваріанти виконують роль інтегративної матриці, що скріплює різнорідні елементи в когерентне ціле, визначаючи як внутрішню логіку самоорганізації, так і характер зовнішньої комунікації. Це смислова інфраструктура системи, її символічний код, що виражає місію і формує основу її взаємодії з іншими системами в просторі кооперації або конфлікту.

Еволюціонуючі системи поводяться не як машини, а скоріше як живі організми, демонструючи здатність до самоорганізації, адаптації та еволюції [1]. Їх динаміка підпорядковується нелінійним законам складних систем, а трансформації відбуваються через каскади біфуркацій, фазові переходи та емерджентні процеси.

Різниця між цими двома типами систем не є тривіальною класифікацією за функціональною ознакою — вона виражає більш глибоку відмінність між двома модусами системного буття. Один — світ закритих, функціонально орієнтованих, лінійно описуваних "машин", інший — світ відкритих, здатних до трансформації, та самоорганізації "організмів" [2]. Отже, управління та забезпечення безпеки цих систем вимагає не просто різного інструментарію, а різного режиму мислення, здатного враховувати їхню нелінійність, множинність станів, емерджентність і залежність від шляху.

Наука про складність, що виникла як відповідь на кризу редукціонізму в природничих і соціальних науках, надає тут необхідний понятійний апарат. Її центральна евристика — розуміння системи як ансамблю взаємодій, в яких

властивості цілого не виводяться з властивостей частин, але проявляються як емерджентні ефекти, що виникають у процесі нелінійної координації між компонентами [3]. У цій логіці поведінка системи визначається не стільки її складом, скільки конфігурацією зв'язків, їх синхронізацією, щільністю, ізоморфізмами і режимами зворотних зв'язків. Більш того, в складних системах ці зв'язки не статичні: вони можуть еволюціонувати, переналаштовуватися, зникати і з'являтися, формуючи нову системну онтологію в реальному часі.

Таке розуміння веде нас до п'яти ключових аксіом складних систем, від яких слід відштовхуватися при розробці стратегій управління та безпеки [4]:

1. **Нелокальність і множинність системних компонентів**. Складні системи складаються з множини компонентів, що взаємодіють між собою і з навколишнім середовищем різними способами. Кожен компонент може виконувати безліч функцій, вступати в різнорідні взаємодії і породжувати нелінійні ефекти на різних рівнях організації. Часто ці компоненти об'єднуються в вузли мереж і самі по собі можуть представляти цілі підсистеми — так звані системи-систем (systems-of-systems). Це означає, що онтологічний статус компонента відносний: в одному контексті він може бути елементом, в іншому — цілою структурою з власною внутрішньою динамікою. Поведінка таких систем нелокальна: локальна зміна може викликати глобальні ефекти. Сама інформація тут не стільки передається, скільки народжується всередині взаємодій. Це означає, що редукція поведінки системи до її частин логічно необґрунтована: не існує лінійної кореляції між знанням про частини і розумінням цілого.

2. **Емерджентність**. Однією з ключових характеристик складних систем, що радикально відрізняє їх від простих або лінійно агрегованих систем, є емерджентність — явище, при якому поведінка цілого не може бути виведена з властивостей його складових елементів [5]. У простих системах, навіть тих, що мають велику кількість компонентів, макроскопічні властивості можуть бути передбачувано реконструйовані з мікроскопічних: сила результуючого вектора, сумарна маса, рівновага або стійкість — всі ці параметри допускають лінійну редукцію. Інакше кажучи, знання частин дає знання цілого. Однак у випадку складних систем це правило перестає працювати. Тут поведінку цілого неможливо вивести з властивостей компонентів. Це не недолік знання, а принципова властивість складних систем.

Саме тому складні системи вимагають не просто інших підходів до забезпечення безпеки, а нової філософії, в якій взаємодія елементів системи стає первинною по відношенню до їх складу і властивостей. Емерджентність в цьому контексті - не аномалія, а необхідна умова існування складного.

3. **Нелінійна динаміка і залежність від шляху**. Складні системи розвиваються нерівномірно і, як правило, незворотньо. Їх поведінка може бути хаотичною, при цьому не випадковою, а чутливою до початкових умов. Вони не повертаються - вони еволюціонують. На відміну від механістичних

систем, поведінку яких можна описати як лінійну функцію часу і вхідних впливів, складні системи існують у часі інакше — не як повторення, а як становлення, в якому малі флуктуації можуть приводити до радикальних реорганізацій.

Складні системи, здебільшого, нелінійні за своєю природою: їхні змінні змінюються асинхронно, іноді з затримками, іноді — з експоненціальним прискоренням. Більш того, багато таких систем демонструють множинні режими стійкості - вони можуть залишатися структурно стабільними в штатних умовах, але ставати надзвичайно чутливими при наближенні до критичних порогів. Саме в цих точках можливі біфуркації - моменти, коли система переходить в інший стан, незворотньо змінюючи траєкторію свого розвитку.

Деякі системи демонструють хаотичну поведінку: вони залишаються детермінованими на рівні рівнянь, але непередбачуваними на рівні траєкторій, демонструючи так званий "ефект метелика".

Також, особливе значення має феномен залежності від шляху (path dependence): у складних системах майбутнє визначається не тільки поточним станом, але і всією попередньою історією.

Це означає, що стратегії безпеки щодо складних систем не можуть бути зведені до простих реакцій на зовнішні впливи, до лінійної схеми «загроза — відповідь». В умовах нелінійної динаміки, структурної чутливості та залежності від шляху, будь-яка адаптивна трансформація не ізольована, а вписана в ланцюг попередніх рішень, кожне з яких не просто коригує траєкторію, а перевизначає конфігурацію майбутнього. Саме тому безпека таких систем не може бути досягнута через локальну оптимізацію — вона вимагає глибокого стратегічного мислення.

4. **Самоорганізація**. Однією з найбільш загадкових і водночас фундаментальних властивостей складних систем є самоорганізація — здатність до формування стійких, цілісних структур за відсутності зовнішнього плану або центрального керуючого початку [6]. На відміну від технічних конструкцій, в яких порядок задається ззовні, в самоорганізованих системах порядок виникає зсередини, як результат множинних, локальних, часто простих взаємодій між елементами, які в своїй сукупності виробляють нетривіальні глобальні патерни поведінки. У цій динаміці *управління* не зникає, але розподіляється — воно не зосереджене в одній точці, а інтегровано в тканину взаємодій, реалізуючись у вигляді зворотних зв'язків, кореляцій, синхронізацій і локальних узгоджень.

Така система не управляється - вона управляє собою, не тому, що їй притаманна цілепокладаюча раціональність, а тому що структура взаємодій містить внутрішню логіку координації, здатну стабілізувати поведінку, породжувати нові форми і, в певних умовах, — еволюціонувати.

У контексті забезпечення безпеки складних еволюціонуючих систем особливий інтерес представляє феномен самоорганізованої критичності — станів, в яких система природним чином налаштовується на межу між

хаосом і порядком, перебуваючи в зоні, де навіть незначна подія може викликати лавиноподібну перебудову, а вся структура стає чутливою до мікроскопічних флуктуацій. Патерни, що виникають при цьому, часто мають властивості самоподібності, відображаючи фрактальну організацію системи, в якій локальне повторює глобальне, а дрібне — структурно подібне до великого.

Самоорганізація підтверджує можливість порядку без директиви, і в цьому полягає її фундаментальне значення для розуміння принципів забезпечення безпеки соціотехнічних систем, оскільки саме в здатності системи спонтанно організовувати себе — в безперервній координації, перерозподілі та реорганізації — криється ключ до життєздатності в світі, де стабільні структури неминуче руйнуються.

5. **Адаптація**. Складні системи, на відміну від простих, не прагнуть до статичної стійкості — вони еволюціонують, безперервно перебудовуючись у відповідь на збурення, ризики та флуктуації середовища [7]. Основа їхнього розвитку та безпеки — не повернення до попереднього стану, а здатність зберігати функціональну ідентичність через трансформацію форми.

У цьому — фундаментальна відмінність між поведінкою простого об'єкта, що рухається до рівноваги (скажімо, маятника, що затухає в точці мінімуму), і поведінкою складної системи, здатної перезібрати себе в процесі адаптації [8].

Стратегії виживання, засновані на здатності складних систем до самоорганізації та адаптаційної перебудови своєї структури, виходять далеко за межі не тільки робастності, але й навіть і резильєнтності (яка досі ще трактується більшістю лише як здатність системи повернутися до початкового стану). У контексті забезпечення безпеки соціотехнічних систем концепти робастності та резильєнтності безумовно важливі, але вони орієнтовані на підтримку *status quo*, а не на перебудову.

У той час як робастність передбачає стійкість до змін, а резильєнтність — "відновлення після інцидентів", характерною реакцією складних систем на деструктивний вплив є адаптація — не повернення до вихідного стану, а структурна, функціональна і поведінкова перебудова, що забезпечує виживання в нових умовах.

Для позначення цієї форми граничної адаптивності пропонується ввести поняття ***трансморфність*** (*transmorphance*). Трансморфність визначається як властивість, що визначає здатність складних еволюціонуючих систем адаптуватися шляхом радикальної структурної трансформації — змінюючи внутрішню архітектуру, траєкторію розвитку, функціональні та ресурсні контури, але при цьому зберігаючи онтологічні інваріанти, які визначають її системну ідентичність.

Реалізація трансморфності може відбуватися як через поступові, безперервні зміни і накопичення малих адаптацій, так і через дискретні, стрибкоподібні трансформації, аналогічні фазовим переходам або

біфуркаціям. В обох випадках вона спрямована на досягнення нової, більш стійкої форми системного буття в мінливих умовах.

Трансморфна система не чинить опору змінам і не намагається відтворити колишній порядок — вона використовує дестабілізацію як умову становлення нової форми, більш пристосованої до умов середовища, в якому функціональна узгодженість досягається вже на іншому рівні організації. У цьому сенсі трансморфність — це не просто результат, але режим динамічної адаптації, що активується в умовах, коли традиційні стратегії забезпечення безпеки виявляються неспроможними. На відміну від робастності та резильєнтності, які можна описувати в рамках кількісних відхилень і повернення до норми, трансморфність вимагає переосмислення самої норми — система виживає не завдяки збереженню форми, а завдяки здатності форму змінювати.

В епоху, коли звичні парадигми розвитку та безпеки втрачають прогностичну та захисну силу, концептуальний горизонт домену безпеки повинен бути розширений за межі стійкості в її класичному розумінні. Саме в цьому контексті трансморфність може стати необхідним критерієм, здатним забезпечити виживання соціотехнічних систем в умовах, де волатильність середовища стає не тимчасовою аномалією, а стійким фоном, а стохастичність набуває властивості системної характеристики.

1. Carmichael, T., Hadžikadić, M. (2019). The Fundamentals of Complex Adaptive Systems. In: Carmichael, T., Collins, A., Hadžikadić, M. (eds) Complex Adaptive Systems. Understanding Complex Systems. Springer, Cham. https://doi.org/10.1007/978-3-030-20309-2_1.
2. Keller, Evelyn Fox. “Organisms, Machines, and Thunderstorms: A History of SelfOrganization, Part Two. Complexity, Emergence, and Stable Attractors.” Historical Studies in the Natural Sciences 39.1 (2009): 1-31. http://dx.doi.org/10.1525/hsns.2009.39.1.1.
3. Holden LM. Complex adaptive systems: concept analysis. J Adv Nurs. 2005 Dec;52(6):651-7. doi: 10.1111/j.1365-2648.2005.03638.x. PMID: 16313378.
4. M. De Domenico, D. Brockmann, C. Camargo, C. Gershenson, D. Goldsmith, S. Jeschonnek, L. Kay, S. Nichele, J.R. Nicolás, T. Schmickl, M. Stella, J. Brandoff, A.J. Martínez Salinas, H. Sayama. Complexity Explained (2019). DOI 10.17605/OSF.IO/TQGNW.
5. Heylighen, F. (1989). Self-Organization, Emergence and the Architecture of Complexity. In in: Proceedings of the 1st European Conference on System Science, (AFCET, Paris), p. 23-32. http://pespmc1.vub.ac.be/Papers/SelfArchCom.pdf.
6. Anzola, D., Barbrook-Johnson, P. & Cano, J.I. Self-organization and social science. Comput Math Organ Theory 23, 221–257 (2017). https://doi.org/10.1007/s10588-016-9224-2.
7. Tzafestas, S.G. (2018). Adaptation, Complexity, and Complex Adaptive Systems. In: Energy, Information, Feedback, Adaptation, and Self-organization. Intelligent Systems, Control and Automation: Science and Engineering, vol 90. Springer, Cham. https://doi.org/10.1007/978-3-319-66999-1_8.
8. Holland, J. H. (1992). Complex Adaptive Systems. Daedalus, 121(1), 17–30. http://www.jstor.org/stable/20025416.

В.М. Горбачук, Т.О. Бардадим, В.В. Годлюк, Т.Г. Голоцукова, Д.О. Рибачок

ЗАХОДИ ДО РЕЗИЛЬЄНТНОСТІ СУЧАСНИХ ЕНЕРГОРИНКІВ

Ландшафт короткострокового й алгоритмічного трейдингу електроенергією зараз зазнає істотних змін, зумовлених кількома основними трендами [1]. По-перше, енергетичний перехід стимулює швидке нарощування виробництва відновлюваної енергії та розгортання гнучких активів (наприклад, BESS (Battery Energy Storage System)), які необхідно оптимізувати та диспетчеризувати через короткострокові ринки електроенергії. По-друге, зростання волатильності створило трейдингові можливості, залучаючи нові типи учасників ринку (наприклад, торговельні майданчики (trading shops) та хедж-фонди), які збагачують трейдингове середовище різноманітними стратегіями та підходами. По-третє, регулятори та розробники стратегій нещодавно посилили свою увагу до короткострокових ринків електроенергії, розширюючи сферу та глибину наглядової діяльності та розширюючи складні регуляторні вимоги.

Регулювання торговельних операцій та ІТ-інфраструктури може сприяти ринковій резильєнтності [2]. Учасники ринку, які використовують алгоритмічні рішення для трейдингу (які передбачають обмежене втручання людини чи взагалі його не передбачають), покладаються на витончені засоби аналітики даних, алгоритми машинного навчання та складні ІТ-інфраструктури при обробці великих обсягів даних (наприклад, перехресних цін на ринках, даних книг замовлень, погодних і сіткових даних тощо) майже в режимі реального часу [3]. Такий трейдинг передбачає підвищені рівні операційних ризиків на рівні окремих учасників ринку, що може вести до негативних наслідків на рівні даного ринку [4].

Для зниження цих системних ризиків, було прийнято кілька регулювань, щоб гарантувати, що учасники ринку, залучені до алгоритмічного трейдингу, встановлюють свої процеси і системи резильєнтним чином [5].

MiFID (Markets in Financial Instruments Directive) I, Директива Європейської комісії 2004/39/ЕС, мала на меті замінити Директиву 93/22/ЕЕС, прийняту в 1993 р. [6], що створює єдиний ринок інвестиційних послуг і діяльностей, який поліпшує конкурентоспроможність на ринках ЄС. Хоча Директива 93/22/ЕЕС мала успіх у зниженні цін і розширенні варіантів для інвесторів, слабкі сторони в структурі ISD (Investment Services Directive) стали очевидними під час фінансової кризи 2008 р. MiFID I також мала на меті внесення змін до трейдингу акцій та встановлення рекомендацій щодо використання пов’язаних фінансових інструментів. MiFID I була введена з метою зменшення системного ризику та посилення існуючого захисту інвесторів. MiFID II про ринки фінансових інструментів є директивою ЄС (2014/65/EU), прийнятою у 2014 р. замість MiFID I. MiFID II разом зі своїм супровідним Регламентом (Regulation (EU) № 600/2014) забезпечує правову базу для ринків цінних паперів, інвестиційних посередників, а також торгових

майданчиків. MiFID II забезпечує гармонізоване регулювання інвестиційних послуг держав-членів Європейського економічного простору, куди входять 24 держави-члени ЄС та 3 держави Європейської асоціації вільної торгівлі (Ісландія, Норвегія, Ліхтенштейн). Основними цілями MiFID II є підвищення конкуренції та захисту інвесторів, а також вирівнювання умов для учасників ринку інвестиційних послуг. Директива 2014/65/EU та супровідний Регламент (набули чинності з 3 січня 2018 р.) містять менше винятків і розширюють сферу застосування MiFID I, щоб охоплювати ширше коло компаній та фінансових продуктів.

Зниження операційного ризику, властивого процесам алгоритмічного трейдингу висуває вимоги до його учасників: коли учасники ринку здійснюють діяльність з таким алгоритмічним трейдингом, що підпадає під дію REMIT II (Risk inherent Algorithmic Trading Processes), стаття 5a, то учасники ринку, які використовують алгоритми на фізичних ринках електроенергії, мають відповідати регуляторним вимогам, подібним вимогам до фінансових гравців згідно з MiFID II, стаття 17 [7]. Цей обов'язок учасників ринків згадує частина 2.4. (iv) (54) Керівних принципів REMIT щодо застосування Регламенту (ЄС) № 1227/2011 Європейського Парламенту та Ради від 25.10.2011 р. про цілісність та прозорість оптового ринку енергії [8]. MiFID II через RTS (Regulatory Technical Standard; регуляторний технічний стандарт) 6 окреслює детальні вимоги до систем алгоритмічного трейдингу. RTS 6 спирається на 5 опор: 1) організаційні вимоги (статті 1–5); 2) розробка, тестування та валідація (статті 6–11); 3) фреймворк контролю та резильєнтності (статті 12–18); 4) прямий електронний доступ (Direct Electronic Access (DEA)) (статті 19–23); 5) кліринг (статті 24–27).

Опора 1) запроваджує формалізований фреймворк врядування, який встановлює чіткі правила відповідальності та розподілу обов'язків, а також вимагає набуття та підтримки набору мінімальних навичок для своїх співробітників, з акцентом на функціях управління ризиками та дотримання вимог: визначення ролей; визначення завдань; роль функції дотримання вимог; кадрове забезпечення; аутсорсинг і закупівля.

Опора 2) зобов'язує до ретельного тестування та валідації систем алгоритмічного трейдингу, оцінюючи продуктивність та поведінку алгоритмів цих систем за різних сценаріїв, включаючи сценарії стрес-тестування. Результати цих тестів повинні бути задокументовані, а будь-які ідентифіковані питання мають з'ясовуватися перед розгортанням алгоритмів у реальних середовищах трейдингу. Також вимагається щорічний процес самооцінки та валідації для перегляду своїх стратегій алгоритмічного трейдингу, фреймворку врядування, домовленостей щодо забезпечення безперервності справи та відповідності чинному регулюванню: перевірка відповідності; середовища тестування; кероване розгортання; щорічний перегляд; стрес-тестування; менеджмент матеріальних змін.

Опора 3) передбачає кілька рівнів, що впливають на щоденні операції та технічне налаштування алгоритмів: функція припинення процесу (kill-

functionality); автоматизоване спостереження; безперервність справи; дотрейдингові та пост-трейдингові заходи контролю; моніторинг в реальному часі; IT-безпека. Функція припинення процесу в контексті інвестиційних фірм стосується здатності негайно скасувати будь-які або всі невиконані заявки, надіслані на торговельні майданчики. Ця функція є важливим інструментом ризик-менеджменту, який дозволяє фірмам звужувати потенційні збитки, швидко завершуючи помилкові або небажані угоди.

3а) Однією з первинних вимог фреймворку контролю є встановлення дотрейдингових заходів контролю. Ці заходи контролю включають ліміти на внесення заявок (order entry), призначені для запобігання поданню помилкових заявок, що можуть підривати ринкову діяльність. Кожна фірма має дотримуватися своїх цінових діапазонів (price collars), максимальної вартості заявок, порогових обсягів для гарантування того, що заявки знаходяться в межах прийнятних параметрів, щоб автоматично відхиляти заявки, які перевищують попередньо визначені ліміти ризику чи виявляють незвичайні моделі трейдингу.

3б) Крім дотрейдингових заходів контролю, RTS 6 наголошує на важливості моніторингу в режимі реального часу, що забезпечується за допомогою набору запобіжних заходів (safeguards) для уникнення збоїв (плани Kill-Switch (аварійного завершення роботи) та забезпечення безперервності справи). План Kill-Switch – це стратегія в розробці та розгортанні ПЗ, яка дозволяє негайно деактивувати або відкликати (rollback) функцію (feature), послугу чи застосунок при виявленні критичних проблем. Цей план діє як екстрений захід для запобігання катастрофічним збоям і для швидкого звуження негативних наслідків.

3в) Фірми зобов'язані впроваджувати системи пост-трейдингового моніторингу для виявлення підозрілої трейдингової діяльності, наприклад, ринкових маніпуляцій або передумов порушень регуляторних вимог. Така система включає спостереження за моделями трейдингу, потоками заявок і ринковими умовами, щоб вчасно ідентифіковувати та звужувати (mitigate) потенційні ризики.

Опора 4) переводить вимоги опор 1), 2), 3) у контекст клієнтів DEA: заходи контролю від провайдера DEA; специфікації та вимоги системи; оцінка належної перевірки (due diligence) клієнтів; перегляд клієнтів DEA. Такі вимоги особливо актуальні для трейдингових компаній, що пропонують послуги трейдингу (агентом) від імені клієнта чи трейдинг у кооперації з третіми сторонами. Учасник ринку завжди несе відповідальність за виконання вимог.

Опора 5) визначає вимоги до належної перевірки, контролінгу та моніторингу для систем фірм, що діють як клірингові фірми: система і заходи контролю; оцінка належної перевірки фірм; ліміти позиції; вимоги розкриття інформації (disclosure). Важливо також зазначити, що інвестиційна фірма залишається повністю відповідальною за свої зобов'язання, якщо вона передає

на аутсорсинг або закуповує програмне чи апаратне забезпечення, яке використовується в діяльності алгоритмічного трейдингу.

Еволюція ландшафту енергоринків і зростаюча залежність від відновлюваних джерел енергії потребують витончених механізмів внутрішнього контролю. Регуляторні вимоги наголошують на важливості робастного ризик-менеджменту, передових систем моніторингу, комплексних фреймворків відповідності для забезпечення цілісності та прозорості ринку. Впроваджуючи подібні заходи контролю, учасники ринку можуть ефективно орієнтуватися в складнощах алгоритмічного трейдингу, звужувати потенційні ризики, сприяти справедливому та стабільному ринковому середовищу, зберігаючи прибутковість і самопідтримуваність алгоритмічної ділової ситуації.

Вимоги, які раніше були актуальними лише для фінансових інструментів згідно з MiFID II, тепер застосовуються також до трейдингової діяльності на оптових ринках енергії. З часів лібералізації енергоринків у Європі на початку 2000-х рр. ландшафт торгівлі енергією зазнав значних змін через Brexit, пандемію COVID-19, нові технології, збройну агресію в Європі, водночас створюючи ризики й можливості для всіх учасників ринків [9].

1. Spinella, D., Passenberg, I., Holler, J. (2025). *Future-proofing energy trading: the new algorithmic trading framework*. PwC Germany, 30 p.
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. 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.
4. 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.
5. Горбачук, В. М., Єрмольєв, Ю. М., Єрмольєва, Т. Ю. (2016). Двоетапна модель еколого-економічних рішень. *Вісник Одеського національного університету. Економіка*, 21 (9), 142–147.
6. Council Directive 93/22/EEC of 10 May 1993 on investment services in the securities field. (1993). *Official Journal of the European Union*, 11.6.93, 27–46.
7. Regulation (EU) 2024/1106 of the European Parliament and of the Council of 11 April 2024 amending Regulations (EU) No 1227/2011 and (EU) 2019/942 as regards improving the Union's protection against market manipulation on the wholesale energy market (Text with EEA relevance). (2024). *Official Journal of the European Union*, 17.4.2024, 1–32.
9. ACER Guidance on the application of Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency. 6.1st Edition. 18 December 2024. (2024). Ljubljana, Slovenia: European Union Agency for the Cooperation of Energy Regulators (ACER), 137 p.
10. Горбачук, В., Гавриленко, С. (2020). Вплив ціноутворення хмарних сервісів на прибуток провайдера, споживчий надлишок і суспільний добробут. *Проблеми програмування*, 2−3, 237−245.

С.Я. Гільгурт

ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ РЕКОНФІГУРОВНИХ СИГНАТУРНИХ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ШЛЯХОМ ВИКОРИСТАННЯ РЕГУЛЯРНИХ ВИРАЗІВ

Реконфігуровні системи, побудовані на базі ПЛІС типу FPGA, наближаючись за швидкодією до спеціалізованих апаратних розробок, одночасно забезпечують безпрецедентну гнучкість завдяки можливості майже миттєво створювати (фактично – виготовляти) всередині сучасних мікросхем програмованої логіки будь-який цифровий пристрій довільної складності (при наявності підготовленого заздалегідь відповідного файлу конфігурації) [1]. В галузі технічного захисту інформації (ТЗІ) це дозволяє після виникнення зовнішнього руйнівного впливу шляхом завантаження в ПЛІС потрібної конфігурації суттєво змінювати технічні характеристики системи та навіть її функціонал, дозволяючи тим самим відтворювати реакцію, потрібну для здійснення резильєнтної поведінки. Наприклад, мережеві системи виявлення вторгнень (Network Intrusion Detection System – NIDS), побудовані за сигнатурним принципом, здатні змінювати склад та номенклатуру зловмисних дій, які вони здатні ідентифікувати, що дозволяє протистояти гібридним багатоплановим атакам.

Реалізувати адаптивні здібності реконфігуровних систем ТЗІ (і не тільки) можливо шляхом використанні так званої процедури оперативного оновлення (ПОО) [2]. Сутність підходу полягає в організації обчислювального процесу під час функціонування реконфігуровної системи таким чином, щоб забезпечити можливість здійснити ПОО в будь-який момент часу. Для цього в цифровій структурі системи ТЗІ від постійних компонентів виокремлюються змінні блоки, для яких формуються відповідні алгоритми їх оптимізації та генерації (синтезу). В момент ініціалізації ПОО в залежності від зовнішніх умов в автоматичному режимі запускаються процедури створення потрібних конфігурацій та їх завантаження в ПЛІС.

Чіткість та визначеність алгоритмів здійснення ПОО забезпечують властивості сигнатурного підходу, якому притаманні висока надійність та низький (порівняно з іншими підходами) рівень хибних спрацювань. Відносно велика ресурсоємність сигнатурного принципу компенсується швидкодією сучасної програмованої логіки. Інший недолік сигнатурних систем – нездатність розпізнавати принципово нові атаки, для яких поки ще не знайдено сигнатур, в даному випадку може погіршувати ситуацію, якщо зловмисник здійснює відому атаку, але модифікує її з метою спотворити наявні сигнатури. Або окремі етапи атаки можуть здійснюватися в різних послідовностях та способах їх комбінування.

Суттєво підвищити гнучкість та адаптивність сигнатурних систем здатне використання апарату так званих регулярних виразів (RegEx), які на відміну від фіксованих патернів (рядків символів) дозволяють розпізнавати широко коло варіацій та комбінацій символів. Даний підхід відомий вже багато років [3, 4]. Одним з основних факторів стримування його розповсюджування була неможливість стандартних реконфігуровних засобів динамічно оновлювати шаблони регулярних виразів під час функціонування. В даному дослідженні ця проблема вирішується шляхом використання описаної вище процедури ПОО.

Сутність механізму RegEx полягає в тому, що за допомогою так званих символів-джокерів (таких як "*", "?", "+", "$", "^","|" та ін.) формуються шаблони, які припускають певний перелік варіацій, що можуть складатися з фрагментів рядків та окремих символів, наприклад: наявність будь-якого символу (або довільної кількості символів) у певній позиції; різні варіанти підрядків символів; відстань між фіксованими патернами у довільну кількість знаків, та багато інших.

В таблиці наведено перелік деяких символів-джокерів у відповідності зі стандартом, сумісним з мовою Perl (Perl Compatible Regular Expressions – PCRE), який є на сьогодні одним з найпоширеніших форматів для завдання регулярних виразів.

Таблиця – Приклади символів-джокерів за стандартом PCRE

Джокер	**Значення**	**Джокер**	**Значення**
. (точка)	будь-який символ, крім нового рядка	|	або символ перед оператором, або символ після нього
*****	нуль або більше повторень символу / групи символів	**[ ]**	будь-який із перелічених в квадратних дужках через кому символів / виразів
+	одне або більше повторень символу / групи символів	**^**	символ початку рядка
?	нуль або одне повторення символу / групи символів	**$**	символ кінця рядка

Бази даних сигнатур сучасних NIDS містять велику кількість регулярних виразів. За деякими спостереженнями частка таких сигнатур складає до 40% від їх загальної кількості. Гнучке розпізнавання надає багато можливостей для виявлення найбільш складних та витончених атак на комп'ютерні системи та мережі. Відносно висока ресурсоємність механізму регулярних виразів усувається за рахунок максимального розпаралелювання процедури розпізнавання в ПЛІС на апаратному рівні шляхом одночасної обробки багатьох RegEx-шаблонів.

На практиці реалізація апарату регулярних виразів реконфігуровними засобами зазвичай здійснюється шляхом побудови недетермінованого скінченного автомата (Nondeterministic Finite Automaton – NFA). На рис. 1 наведено діаграму роботи цифрового автомата, що реалізує вираз (A|B)CD+, а на рис. 2 – структурну схему побудови відповідного NFA.

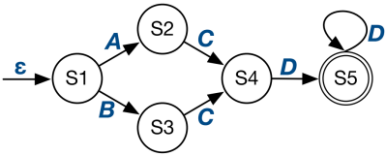

Рисунок 1 – Діаграма роботи цифрового автомата NFA

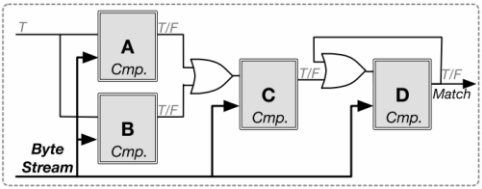

Рисунок 2 – Структурна схема побудови цифрового автомата NFA

В роботі також досліджується підхід, спрямований на подальший розвиток апаратних засобів реалізації на ПЛІС механізмів RegEx, якій здійснює багатосимвольну обробку регулярних виразів на базі недетермінованого скінченного автомата (Multi-Character NFA – MC-NFA). Розглянуто програмно-апаратне рішення та відповідну структуру MC-NFA.

Висновки. В дослідженні показано, як використання регулярних виразів дозволяє підвищити резильєнтність реконфігуровних сигнатурних систем технічного захисту інформації. Розвинуто інструментарій реалізації механізмів RegEx, на ПЛІС за рахунок багатосимвольної обробки.

1. Hilgurt S. A Concise Review of FPGA-Based Hardware Solutions for Network Intrusion Detection. Proceedings of the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T′2021), Kharkiv, Ukraine, 5 – 7 Oct. 2021, IEEE. – P. 164-168.
2. Гільгурт С.Я., Жуков І.А. Підхід до реалізації адаптивних можливостей реконфігуровних систем захисту інформації сигнатурного типу. XV Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології». Тези доп., 25 – 26 квітня 2024. – К.: НАУ, 2024. – С. 31-34.
3. Sidhu R., Prasanna V.K. Fast Regular Expression Matching Using FPGAs. 9th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2001). – 2001, Institute of Electrical and Electronics Engineers Inc. – P. 227-238.
4. Kim J., Park J. FPGA-based memory efficient shift-and algorithm for regular expression matching. Lecture Notes in Computer Science. 14th International Symposium on Applied Reconfigurable Computing, Vol. 10824. – 2018, P. 132-141.

С.О. Гавриленко, Г.В. Голоцуков, Т.Г. Голоцукова, О.С. Кушнір

СТРУКТУРОВАНІ ЕЛЕКТРОННІ ДОКУМЕНТИ - ОСНОВА ЦИФРОВІЗОВАНОЇ СТІЙКОСТІ ФУНКЦІОНУВАННЯ ДИНАМІЧНИХ СИСТЕМ

Сучасні технології забезпечення стійкості, керованості, резільєнтності у застосуванні до цифровізованих технічних систем з метою підвищення їх ступеню адаптації до критичних зовнішніх та внутрішніх змін і впливів, в тому числі у «форс-мажорних», повинні бути застосовані в задачах моніторингу, оцінки стабільності, аналізу відхилень стану, прогнозу аварійних ситуацій і підвищення надійності функціонування багато-рівневої розгалуженої інфраструктури, розподіленої в просторі і часі. Такі технології, за всяк час, спираються на системи інформаційного і організаційного управління інфраструктурою виробничого і економічного функціонування територіально-розгалуженої мережі динамічних систем і підсистем з власними математичними моделями і методами забезпечення резільєнтності, керованості, ідентифікації критичних загроз, резервування ресурсів. Але значною складовою таких систем і технологій є інформаційна і документарна база, що забезпечує їх працездатність і, що більш важливо, подання даних в доступному для персоналу (будь якої кваліфікації та горизонтального або вертикального місця в виробничій ієрархії) вигляді.

Інформаційне розподілене середовище сучасної цифровізованої інфраструктури спирається на технології хмарних обчислень, розподілених, паралельних, децентралізованих баз даних, розподілених та децентралізованих файлових ресурсів, розподілених структурованих документів з використанням всіх механізмів інформаційних систем (ІС) та інформаційних технологій (ІТ), в тому числі і розподілених (РІТ). В якості прикладів можна привести торент, блокчейн технології, які мають варіації від розподілених централізованих (наприклад, централізована ідентифікація або система адресації) до повністю автономних (незалежних) децентралізованих (з централізованим стартом та Р2Р мережевою взаємодією).

Електронний документообіг структурованими електронними документами в багаторівневій цифровізованій інфраструктурі (для процедурного, регламентного, інформаційного, функціонального забезпечення організаційного управління мережею динамічних систем) може бути реалізованим на існуючих програмно-інформаційних механізмах і технологіях, зокрема, розподілених баз даних, блокчейн технологіях та інших.

В якості реалізації вказаних задач пропонується РІТ Корпоративна система електронного документообігу (КСЕД) структурованими електронними документами (СЕД) (КСЕД СЕД), яка була впровадження за

останні 25 років в кількох великих проєктах державної і корпоративної інфраструктур.

Основна мета КСЕД СЕД, як резільєнтної системи - забезпечити надійність структурованих електронних документів в середовищі розподілених інформаційних технологій корпоративного електронного документообігу в цифровізованих державних і корпоративних багаторівневих інфраструктурах

Загальний архітектурний підхід, характерний для більшості корпоративних розподілених інформаційних систем і технологій (КРІСТ), розроблених фахівцями Інституту кібернетики імені В.М. Глушкова НАН України, і, створених на загальних принципах відкритої архітектури АСУ (в сучасному втіленні) корпоративного та інфраструктурного організаційного документ-орієнтованого типу.

Такого роду ІС та ІТ узагальнено базуються на такому наріжному камінні:

- Об'єктні майданчики документообігу комунікаційної інфраструктури;
- Суб'єктна модель кінцевих користувачів наявних і віртуальних суб'єктів діловодства – осіб, що приймають рішення;
- Корпоративне документарне середовище, забезпечене авторизованим (в тому числі і персональним) сховищем, базою даних;
- Комунікаційне середовище (віртуальна експедиція), яке забезпечує гарантовану реєстрацію, маршрутизацію та доставку проектів документів, підписаних, завірених або довірчо переданих на стадіях виконання;
- Застосована номенклатура справ (готується, ведеться і застосовується канцелярією), що описує суб'єктів діловодства, їх документарну базу, схеми виконання ними дій над проектами документів, інструкції і регламенти їх виконання;
- Всеохоплююча версійність – особно суб'єктна, об'єктна і перманентна, яка за моделлю будь-яких документів та елементів інформаційної моделі предметної області перенесе автоматизований процес виконання в минуле або сьогодення (в майбутнє не можливе, оскільки віднесено не до виконання, а до інструкції або регламенту виконання);
- Складові частини документа, документарної і документ-орієнтованої інформації, структурованого електронного документа (СЕД);
- Верстові камені схем виконання дій над проектами документів відповідно до інструкцій і регламентів їх виконання.

Виділені деякі архітектурні елементи є найбільш важливими для трансформації будь-яких документ-орієнтованих систем в хмарне середовище. Тезами можна зазначити:

- Об'єкти - майданчики документообігу інфраструктури в хмарному середовищі повинні враховувати модель розгортання хмари;

- Суб'єктна модель кінцевих користувачів наявних і віртуальних суб'єктів діловодства істотно розширюється виключенням одних та включених інших осіб, яким делеговано повноваження;

- Корпоративне документарне середовище розшароване за моделлю розгортання;

- Комунікаційне середовище (віртуальна глобальна експедиція отримує замість одного джерела авторизації та перевірки легітимності підпису кілька таких джерел;

- Застосована номенклатура справ готується, ведеться і застосовується не однією канцелярією, а кількома, що потребує окремий механізм суміщення і сумісності багатьох канцелярій;

- Всеохоплююча версійність внутрішньо-корпоративного середовища включає таку ієрархію версій: номенклатура об'єктів, електронний документ, елемент інформаційної моделі предметної області, проект СЕД, подання СЕД, а хмарне середовище накладає ще версії моделі розгортання;

- Складові частини документа, документарної і документ-орієнтованої інформації, СЕД повинні містити ідентифікаційну частину щодо моделі розгортання.

- Верстові камені схем виконання дій над проектами документів повинні бути прив'язані до включених суб'єктів, об'єктів джерел авторизації та перевірки легітимності підпису, віртуальної глобальної канцелярії і експедиції.

Основні елементи архітектури, що схильні до трансформації під час переходу у хмарне середовище зазвичай випробуються на стадіях технічного проектування підсистем і розподілених інформаційних технологій, напрклад. у складі Єдиної інформаційної системи підтримки задач управління науково-організаційною діяльністю (ЄІС НОД або РІТ НОД) НАН України.

Концептуальні моделі закладені в ІС і РІТ на основі технологій КСЕД СЕД включають:

- Концепція КСЕД СЕД.
- Електронний Документ.
- Особливості електронного документа:

1. СЕД, структура подання, документ КСЕД СЕД
2. Декларативне визначення СЕД КСЕД.
3. Електронний Документообіг СЕД.
4. Особливості електронного документообігу.
5. Основні операції над проектами СЕД, версіями проектів СЕД в КСЕД СЕД

- Архітектура управління корпоративного контенту (ECM).
- Трансформація ECM в архітектуру управління інтелектуальною інформацією ІІМ.
- Особливості документ-орієнтованих систем в хмарному середовищі.

Резільєнтність, безпека та захист інформаційних систем і розподілених інформаційних технологій – це не тільки аспекти фізичного та нематеріального доступу, а це цілісність і адекватно-спрямована доступність інформаційних ресурсів – структурованих електронних документів з будь-якими паралельно-існуючими видами реального матеріального і нематеріального подання документів: ідентифікаційних, реєстраційних, звітних та інших офіційних державних, відомчих, корпоративних форм (формалізованих за структурою і змістом). РІТ КСЕД СЕД - це аналітична інформаційна система (АІС):

- організаційного управління Line of Business (LOB),
- управління бізнес проєктами електронних документів (ЕД),
- логістичними технологіями інфраструктури,
- вертикального та горизонтального документообігу,
- розподілених інформаційних технологій забезпечення мережевого планування та управління електронним документообігом інфраструктури,
- повнофункціональних реєстрів і класифікаторів державного та інфраструктурного рівня у формі СЕД,
- управління суб'єктами ЕДО, типами і видами СЕД, версіями типів і видів СЕД, екземплярів ЕД, операції над пакетами ЕД.

У цифровому середовищі РІТ КСЕД СЕД бізнес-операцій кожного СЕД робочий процес виконання документів (автоматичних і автоматизованих регламентних дій над СЕД) виглядає як рудимент, але в коротко-строковому та оперативному управлінні документарної діяльності є незамінним.

Велике значення в плані резільєнтності ІС, основаній на КСЕД СЕД є інструментальна категорія версійність, як даних, класифікаторів, довідників, форм СЕД, видів подання СЕД, екземплярів електронних документів, пакетів екземплярів електронних документів та комплектів або пачок екземплярів електронних документів, що разом є забезпеченням конкретної документарної кампанії.

Склад версійності щодо конкретної форми структурованого електронного документа спирається на легітимізацію конкретного вигляду форми СЕД, та фіксується датами (діапазоном дат) легітимізації, тобто дати юридичної актуалізації та дати припинення чинності, форми СЕД на заміну, пов'язані на рівні даних інші форми СЕД, інфраструктурні ланки актуальності даної форми СЕД (групи суб'єктів виконання). З версійністю конкретної форми СЕД пов'язані версії подання екземпляру СЕД (виконаного СЕД або робочого екземпляру СЕД). Подання СЕД є відмінні за складом або зовнішні виглядом матеріальні представлення екземпляру СЕД, зокрема, в процесі виконання або заповнення проєкту СЕД (незавершеного екземпляру СЕД), призначені для зберігання та відображення екземпляру СЕД на виконанні або після затвердження проєкту СЕД.

Версії екземплярів СЕД є збережені дані форми СЕД певної версії (та сформовані декі подання) на будь якій стадії виконання (частково або повністю виконаним або заповненим конкретним виконавцем регламентної дії).

Для фіксації версійності в КСЕД СЕД використовується система часових інтервалів, тобто кожна версія форми СЕД може бути актуальною з заокругленої (рік, місяць, тиждень, декада, день, час, тощо) дати по заокруглену дату легітимізації наступної версії форми СЕД, наприклад, «форма паспорту ХХХХ вводиться з дд.мм.рррр», «звіт ХХХХХХ за рік вводиться з 31.12.рррр». Для часових інтервалів, що повторюються, може бути застосовано їх перелічені значення, наприклад, «друге півріччя», «жовтень», «літо» та інші.

Велике значення мають версії видів екземплярів документів, наприклад, «звіт», «зведений звіт контрагентів», «зведений план учасників», «звіт інфраструктурного суб'єкта районного рівня», які можуть відображати технологічні процеси суб'єктів від початку проведення, наприклад, бюджетної кампанії інфраструктури до фіксації стадії виконання цієї кампанії.

В якості аргументів підтвердження стійкості ІС організаційного управління інфраструктурою можна привести реальний випадок, коли Уряд прийняв законодавчий акт 30.03.рр про зміну структури і тарифів оподаткування з 01.01.рр та алгоритми їх нарахування, а приблизно 1 млн. підприємств і ФОП повинні були подати пов'язані з попередніми формами податкової звітності автоматизовані перераховані звіти за новими алгоритмами і формами звітування з 01.04.рррр по 10.04.рррр в дворівневу інфраструктуру прийому звітності, а КСЕД СЕД дозволив провести звітну кампанії інфраструктури майже без затримки.

С.В. Сушко

АСПЕКТИ ВІДДАЛЕНОГО МОНІТОРИНГУ ПАРАМЕТРІВ ЕЛЕКТРОЕНЕРГЕТИЧНИХ МЕРЕЖ

В контексті розгляду резильєнтності електроенергетичних мереж варто розглянути такі мережі, як систему, що побудована для виконання енергозабезпечення споживачів з урахуванням можливих технічних, технологічних та військових пошкоджень елементів електроенергетичних мереж. Таким чином набуває важливості контроль усіх елементів електроенергетичної мережі.

Інформаційну структуру як традиційних електроенергетичних мереж, так і більшою мірою електроенергетичних мереж Smart Grid загалом можна представити у вигляді трьох компонентної схеми:

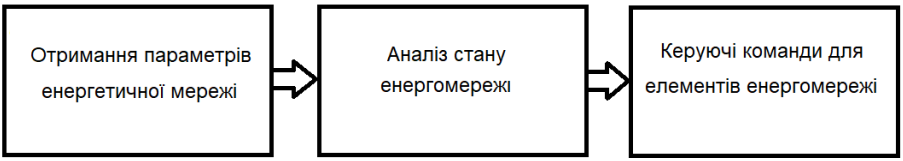

Рисунок 1 – Загальна інформаційна структура енергетичних мереж

Енергетичні мережі Smart Grid, що стали набувати поширеність останнім часом, потребують більшого обсягу інформації про енергомережу і в той же час мають засоби для аналізу і до змін в енергомережі. Контроль параметрів електроенергетичних мереж важливий як для мереж змінного струму [1] так і для мереж постійного струму [2].

Розглянемо мікрогрід – відносно невелику енергомережу, яка може бути використана для військових, виробничих або комунальних застосунків. Очевидно, що частини такої енергомережі можуть бути віддалені одна від одної. У військовому застосуванні можуть бути десятки і навіть сотні територіально віддалених як елементів генерації так і споживачів. Відповідно, потрібно мати можливість віддалено контролювати стан усіх компонентів енергомережі.

Загалом, чим більше оператор мережі отримує параметрів мережі в реальному часі, тим більше поінформованість про власне стан мережі і тим швидше може бути прийняте рішення про дії у разі виникнення загрозливої або аварійної ситуації. Дані мережі отримуються від спеціалізованих сенсорів, що розміщені в найбільш критичних вузлах мережі. Застосовані типи сенсорів наведено в Таблиці 1.

Дані, отримані сенсорами в різних вузлах енергетичної мережі можуть використовуватися як з метою безпосередньо керуванням генерацією і споживанням енергетичної мережі, так і для накопичення інформації щодо

характеру навантаження по часу і об’єктам енергетичної мережі. Отримані та оброблені дані можуть бути використані для моделювання [3], проектування та розгортання подальших енергетичних систем.

Таблиця 1 – Можливі типи сенсорів для віддаленого вимірювання параметрів електроенергетичних мереж

Тип сенсору	Параметри сенсорів		
	Струм	Параметри, що вимірюється	Приклади застосування
Сенсор напруги постійного струму	Постійний	Напруга	Вимірювання напруги акумулятора; Вимірювання напруги сонячних батарей; Вимірювання напруги електричних мереж постійного струму.
Сенсор напруги та постійного струму	Постійний	Напруга, сила струму	Контроль напруги та заряду акумулятора; Вимірювання напруги та потужності мереж постійного струму.
Сенсор напруги та змінного струму	Змінний	Напруга, сила струму	Контроль напруги і споживаного струму для ліній 220 В.
Сенсор наявності напруги	Змінний	Напруга	Дозволяє моніторити мережу змінного струму на наявність напруги: контроль ліній 220 В, виходу генераторів та інверторів
Сенсор рівня палива		Рівень палива	Вимірювання рівня палива в баках генератора

1. X. Hou *et al*., "Distributed Hierarchical Control of AC Microgrid Operating in Grid-Connected, Islanded and Their Transition Modes," in *IEEE Access*, vol. 6, pp. 77388-77401, 2018, doi: 10.1109/ACCESS.2018.2882678.
2. Muchande, S. & Thale, Sushil. (2022). Hierarchical Control of a Low Voltage DC Microgrid with Coordinated Power Management Strategies. Engineering, Technology & Applied Science Research. 12. 8045-8052. 10.48084/etasr.4625.
3. Саух, С. і Борисенко, А. 2025. МОДЕЛЮВАННЯ ЕЛЕКТРОЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ ТА ОЦІНЮВАННЯ ЇЇ РЕЗИЛЬЄНТНОСТІ В УМОВАХ СИСТЕМАТИЧНИХ ТЕРОРИСТИЧНИХ АТАК. *ТЕХНІЧНА ЕЛЕКТРОДИНАМІКА*. 2 (Бер 2025), 057. DOI: https://doi.org/10.15407/techned2025.02.057.

О.А. Даниленко, В.О. Демченко

РЕЗИЛЬЄНТНІСТЬ ЯК ДРАЙВЕР СУЧАСНОЇ ПРАКТИКИ ЗАЛУЧЕННЯ ПЕРСОНАЛУ ЧЕРЕЗ СОЦІАЛЬНІ МЕРЕЖІ

У сучасному турбулентному світі, де економічні кризи, технологічні революції та глобальні виклики стають нормою, резильєнтність (здатність динамічної системи успішно адаптуватися до викликів, що загрожують її функціонуванню, виживанню або розвитку [1]) набуває статусу ключової якості як для організацій, так і для їхніх працівників. Здатність організації швидко адаптуватися до змін, відновлюватися після потрясінь та ефективно функціонувати в умовах невизначеності безпосередньо залежить від її трудового потенціалу.

Саме тому в умовах дефіциту робочої сили пошук та залучення різнобічно талановитих працівників, готових змінити роботу, стає пріоритетним завданням для HR-фахівців. Це, своєю чергою, висуває вимогу до резильєнтності самого процесу добору персоналу в організаціях. Здатність швидко перебудовувати, оптимізувати етапи добору і відбору, адаптуватися до нових джерел кандидатів, методів та інструментів їх оцінювання є життєво важливою для своєчасного закриття потреб у персоналі.

У XXI столітті соціальні мережі стали невід'ємною частиною нашого повсякденного життя. Вони трансформували способи спілкування, отримання інформації та взаємодії між людьми. Ці зміни суттєво вплинули і на сферу управління персоналом, зокрема на процес рекрутингу. Соціальні мережі перетворилися на вагомий канал комунікації та потужний інструмент для так званого «соціального рекрутингу», пропонуючи безпрецедентні можливості для прямого та таргетованого контакту з потенційними кандидатами.

Нині соціальний рекрутинг – це практика використання соціальних мереж для пошуку, залучення та наймання потенційних працівників. Він включає використання платформ, таких як: LinkedIn, Facebook, Twitter, Instagram, TikTok як інструменти для пошуку кандидатів, реклами вакансій і взаємодії з ними. Соціальний рекрутинг дозволяє організаціям розширити охоплення кандидатів та знаходити таланти чи просто потрібних працівників у тих місцях, де вони проводять час онлайн. Він може включати використання профілів, груп і рекламних інструментів соціальних мереж для пошуку підходящих кандидатів [2].

Сучасні тренди соціального рекрутингу узагальнено за літературними джерелами [2-7].

1. Еволюція рекрутингу: від оголошень до цифрових платформ.

Традиційний рекрутинг переважно спирався на газетні оголошення, зовнішні агенції чи внутрішні рекомендації. Згідно з нещодавнім опитуванням Harvard Business Review, понад 75% іноземних фахівців з рекрутингу зараз вважають соціальні мережі критично важливим каналом

для пошуку талантів. Сьогодні ж близько 84% іноземних компаній використовують соціальні мережі для пошуку кандидатів [3; 4]. Платформи як LinkedIn, Facebook, Instagram та навіть TikTok перетворилися на нові «майданчики працевлаштування», які дозволяють досягати ширшої аудиторії та цільових професіоналів.

2. LinkedIn – професійний стандарт.

У 2023 році LinkedIn мав 930 мільйонів учасників. На початок 2025 року його кількість перевищила 1,1 мільярда користувачів. LinkedIn – це більше, ніж просто соціальна мережа, це глобальний центр наймання. Маючи понад 67 млн. компаній та мільйони шукачів роботи, він відіграє вирішальну роль у тенденціях рекрутингу та галузі. Серед усіх соціальних мереж найбільш популярною в контексті професійного рекрутингу є LinkedIn. За даними LinkedIn Statistics: 2025, понад 72% рекрутерів використовують LinkedIn для пошуку талантів [5]. Функції таргетованого пошуку, професійні рекомендації, автоматизовані системи відбору значно прискорюють процес наймання потрібних кандидатів.

3. Facebook та Instagram – не лише для брендингу.

Facebook дозволяє створювати вакансії напряму на сторінках організацій, а Instagram – завдяки візуальності – ідеально підходить для промоції корпоративної культури. Наприклад, згідно з дослідженням SHRM (2022), 40% кандидатів вважають Instagram важливим каналом для розуміння атмосфери компанії ще до співбесіди [6]. Нині Facebook та Instagram використовуються в процесі добору персоналу, зокрема, для залучення кандидатів, які активно не шукають роботу. Ці соціальні мережі дозволяють організаціям розширювати охоплення пошуку та потенційно знаходити більш широкий пул кандидатів. Крім того, їх можна використовувати для попереднього відбору кандидатів.

4. TikTok-рекрутинг – тренд нового покоління.

TikTok став несподіваним, але ефективним каналом для залучення молоді. Кампанії на зразок TikTok доводять, що короткі відео-резюме можуть бути не менш інформативними за традиційні CV. Згідно з даними Forbes (2022), більше 30% покоління Z схильні подавати заявки саме через відеоформати [7]. Нині платформа TikTok активно використовується для створення резюме (#TikTokResumes), дозволяючи претендентам креативно демонструвати свої навички. TikTok планує розвивати майданчик для пошуку роботи, особливо для покоління Z.

Отже, соціальні мережі стають не лише доповненням, а подекуди й головним каналом залучення необхідного персоналу. Успішне використання цих соціальних платформ вимагає не лише технічної грамотності, але й стратегічного бачення HR-фахівців. Враховуючи динамічний розвиток цифрового середовища, організаціям варто постійно адаптуватися, експериментувати з новими форматами й залишатися відкритими до змін.

До основних переваг залучення персоналу через соціальні мережі можна віднести: швидкість охоплення, таргетинг на певні професійні групи,

зниження витрат на пошук персоналу, одночасне просування HR-бренду. Однак є й виклики – це ризики упередженості, поверхневе оцінювання кандидатів, питання конфіденційності. Тому важливо поєднувати цифрові інструменти з професійною аналітикою та етичними стандартами соціального рекрутингу.

Небхідно розробляти нові підходи, які дозволять ідентифікувати та залучати через соціальні мережі саме тих кандидатів, які здатні проявляти необхідні компетентості, як от: стійкість, адаптивність та гнучкість в умовах постійних змін. Це дозволить організаціям не лише оперативно заповнювати вакансії, але й формувати високоефективні та стресостійкі команди, здатні долати будь-які виклики. Такий підхід забезпечить організаціям стратегічну перевагу, дозволяючи їм будувати міцний кадровий фундамент для сталого розвитку та успіху в епоху постійних змін.

1. Masten A. S., Lucke, C. M. Nelson, K. M., & Stallworthy I. C. Resilience in development and psychopathology: Multisystem perspectives. Annual Review of Clinical Psychology. 2021. № 17, 521–549. URL : https://doi.org/10.1146/annurev-clinpsy-081219-120307.
2. Gündüzyeli B. The Role of Social Media and Artificial Intelligence (AI) in Enhancing Digital Marketing Resilience During Crises. *Sustainability*. 2025. № 17(7), 3134. URL : https://doi.org/10.3390/su17073134.
3. Leveraging Social Media and Digital Platforms for Talent Acquisition. *EUROENGINEERJOBS.* URL : https://www.euroengineerjobs.com/article/940/leveraging-social-media-and-digital-platforms-for-talent-acquisition.
4. 2024 Employ Job Seeker Nation Report: Keeping Pace with the Perceptions of Modern Workers. *JOBVITE*. URL : https://www.jobvite.com/lp/employ-job-seeker-nation-report-2024/.
5. LinkedIn Statistics: 2025 Shocking Facts You Need to Know. March 11, 2025. URL : https://columncontent.com/linkedin-statistics/.
6. Using Social Media for Talent Acquisition. 2022. *SHRM*. URL : https://www.shrm.org
7. TikTok Resumes and the Future of Job Hunting. 2022. *FORBES.* URL : https://www.forbes.com.

Г.П. Дубинський

ОЦІНЮВАННЯ ХАРАКТЕРИСТИК РЕЗИЛЬЄНТНОСТІ ЛАНЦЮЖКІВ ПОСТАЧАННЯ ЯК ДИНАМІЧНИХ СИСТЕМ

Актуальність теми. У глобалізованому середовищі ланцюжки постачання стали вразливими до широкого спектра вразливостей– від природних катастроф і геополітичних конфліктів до пандемій та кібератак. Поняття резильєнтності ланцюжків постачання охоплює здатність системи не лише протистояти збоям, але й адаптуватися до змін і швидко відновлюватися після потрясінь (IBM, 2023; Tukamuhabwa et al., 2015). Необхідність інтеграції підходів з оцінювання резильєнтності у формальні математичні моделі дозволяє не тільки пояснити динаміку реагування, а й оптимізувати рішення у стратегічному управлінні.

Мета та завдання дослідження. Метою є дослідження впливу збурень на поведінку ланцюжків постачання на основі відповідної динамічної моделі. Основні завдання:

– формалізувати поняття резильєнтності у вигляді параметрів TTR (Time-to-Recovery), TTS (Time-to-Survive);

–дослідити можливість застосування системи диференціальних рівнянь, яка описує зміну в часі запасів, попиту та обсягів постачання, для аналізу резильєнтних властивостей ланцюжків постачання;

– розглянути можливість оцінювання стійкості ланцюжків постачання на основі аналізу власних чисел матриці відповідної системи диференційних рівнянь;

– оцінити вплив різних стратегій (мультисорсинг, буфери, цифрова видимість) на швидкість відновлення.

Методологія. Для моделювання застосовано підхід системної динаміки. Кожен етап ланцюжка постачання (виробник, дистриб'ютор, споживач) представлений через змінні: запаси, рівень попиту, замовлення, постачання. Модель формалізується у вигляді системи диференціальних рівнянь першого порядку. Ключовим індикатором резильєнтності вважається співвідношення між TTS і TTR. У стійкій системі TTS ≥ TTR (Simchi-Levi, MIT).

Формування моделі динаміки ресурсного потенціалу системи. Розглянемо наступний графік динаміки ресурсного потенціалу системи у відповідь на зовнішнє збурення (рис.1). На графіку збурення починається в момент часу t = 5, і спад триває до t = 7. В процесі такого спаду ресурсний потенціал системи знижується до рівня в 5%.

Зважаючи на природню інерційність реальних систем, будемо вважати, що на відміну від миттєвого падіння, зменшення ресурсного потенціалу системи відбувається поступово і описується експоненціальною залежністю.

Далі, будемо вважати, що в момент часу t = 7 на систему подіяв стрибок позитивного впливу, який зупинив спад і спричинив відновлення ресурсного потенціалу до рівня 30%, тож в період часу з t = 7 до t = 8 ресурсний

потенціал системи перебував на цьому рівні. Починаючи з t = 8, система переходить до стадії відновлення, яке триває до t ≈ 23.

У даному прикладі:

– час до відновлення (TTR) ≈ 15 одиниць часу;

– час виживання (TTS) ≥ 15 – за умови буферизації система зберігає функціональність.

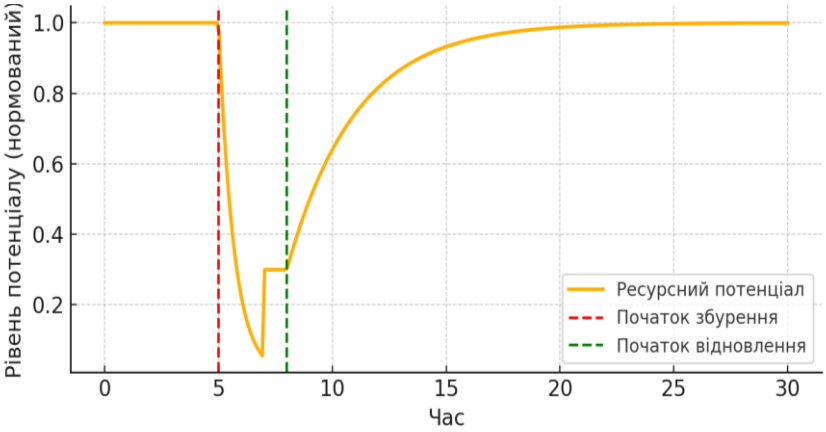

Рисунок 1 – Графік динаміки зміни ресурсного потенціалу

На цьому графіку динаміки ресурсного потенціалу можна побачити точку зламу, де крива відновлення змінює свій характер: зі стадії стрибкоподібного відновлення переходить у стадію сповільнюваного відновлення з постійним зменшенням темпу відновлення ресурсного потенціалу. На стадії до зламу система активно мобілізує ресурси, тоді як після зламу — відновлення продовжується, але зі зменшенням швидкості.

Зрозуміло, що експоненціальний характер процесу відновлення, який в розглянутому прикладі починається з моменту t = 8, є припущенням. Але таке припущення дає можливість оцінювати певні характеристики цієї експоненти (або досліджувати відповідне диференційне рівняння чи вивчати відповідну лінійну динамічну систему). Проте (і для прикладу), можна навести два інші варіанти динаміки відновлення:

1. Двофазна експоненціальна модель динаміки відновлення: включає два періоди експоненціального зростання – початковий період (до відповідної точки зламу) з подальшим переходом до більш повільного експоненціального насичення. Така модель буде складатися вже з певної комбінації двох експонент і являти собою систему двох лінійних диференційних рівнянь з розривними часовими характеристиками.

2. Логістична модель динаміки відновлення, яка являє собою симетричну S-подібну криву з явною точкою інфлексії.

На рис.2 наведено графіки цих двох варіантів динаміки відновлення ресурсного потенціалу в порівнянні з однофазним експоненціальним варіантом. Одразу слід зазначити, що для однієї й тієї ж системи точка зламу двофазної експоненціальної моделі має співпадати з точкою перегину логістичної моделі, проте на рисунку ці точки рознесені лише з ілюстративною метою.

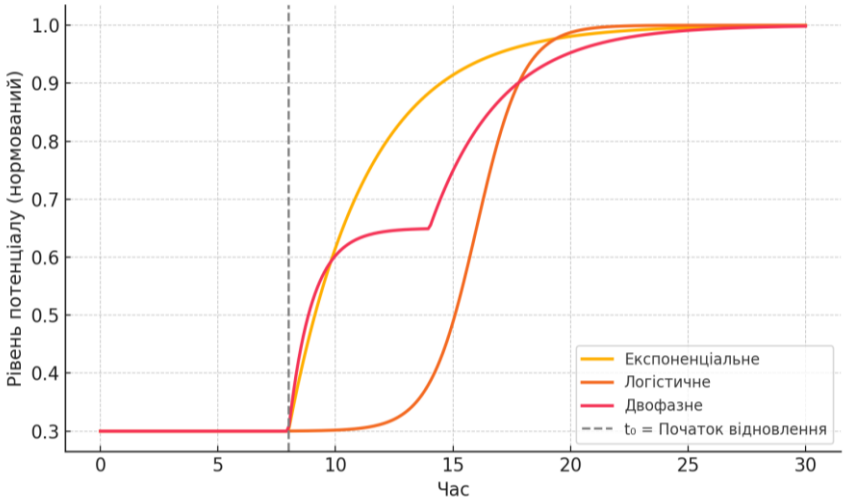

Рисунок 2 –Графіки варіантів динаміки відновлення ресурсного потенціалу

Форма кривої відновлення має ключове значення для оцінювання характеристик резильєнтності, і саме наявність точок зламу або перегину дозволяє краще передбачати ефекти виснаження адаптаційних можливостей системи та обґрунтувати необхідність контролю темпу відновлення. Тож залежно від типу системи, доцільно застосовувати відповідну модель: експоненційну однофазну, експоненційну двофазну, або логістичну. Це відкриває шлях до точнішої оцінки параметрів TTR та оптимізації управлінських рішень у ланцюгах постачання.

Основні результати. Результати свідчать, що:

– запровадження стратегічних буферних запасів значно скорочує TTR;

– мультисорсинг (альтернативні джерела постачання) зменшує ризик від збоїв окремих вузлів;

– цифрові інструменти (digital twins, control towers) забезпечують кращу реакцію на збурення за рахунок видимості і прогнозування;

– критичним параметром є коефіцієнт адаптації – надто агресивне реагування може дестабілізувати систему.

Ці висновки узгоджуються з аналізом кейсів Toyota, Cisco та Pfizer, де саме цифровізація, буферизація і сценарне планування стали ключовими компонентами резильєнтності (SupplyChainDive, 2021).

Висновки. Динамічні моделі дозволяють формалізовано оцінювати кількісні характеристики резильєнтності ланцюжків постачання та є ефективним інструментом при ухваленні рішень щодо стратегій буферизації, диверсифікації джерел та параметризації політик замовлення. Перспективи подальших досліджень пов'язані з інтеграцією елементів стохастики, оцінкою ripple effect та використанням штучного інтелекту для адаптивного управління у реальному часі.

1. IBM. (2023). What Is Supply Chain Resilience? https://www.ibm.com/think/topics/supply-chain-resiliency.
2. Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: definition, review and theoretical foundations. CLoK UCLAN.
3. Simchi-Levi, D. (2020). Time-to-Recover and Time-to-Survive metrics. MIT Center for Transportation & Logistics.
4. McKinsey & Co. (2021). Digital twins in supply chains. https://www.mckinsey.com
5. SupplyChainDive (2021). Resilient supply chains in COVID and beyond. https://www.supplychaindive.com.

А.В. Ковилін

ВИКОРИСТАННЯ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ (GNN) ДЛЯ ПРОГНОЗУВАННЯ КАСКАДНИХ ВІДМОВ В ЕНЕРГЕТИЧНИХ СИСТЕМАХ: ДОСЛІДЖЕННЯ ТА ПРОТОТИП

Резильєнтність енергетичних систем – критичний чинник національної безпеки, особливо в умовах зростаючих кіберзагроз і можливості каскадних відмов. Такі відмови можуть призвести до масштабних збоїв з економічними і соціальними наслідками. Традиційні методи прогнозування часто не враховують структуру мережі. Сучасний підхід на основі графових нейронних мереж (GNN) [1] дозволяє моделювати взаємозв'язки між елементами системи та передбачати поширення збоїв у топології.

Саме тому метою даного дослідження стала оцінка ефективності графових нейронних мереж (GNN) для прогнозування каскадних відмов у критичній інфраструктурі (на прикладі енергетичних мереж). Для цього розроблено та валідаційно протестовано двошарову модель типу Graph Convolutional Network (GCN) [2], здатну оцінювати ризик ураження вузлів з урахуванням топології мережі. Додатково реалізовано інтерактивний прототип для сценарного тестування та аналізу моделі в реальному часі, що дозволяє перевіряти адаптивність підходу та підтримувати прийняття рішень у контексті забезпечення кібер резильєнтністності.

Для побудови топології енергетичної мережі використовувався граф типу scale-free, що імітує характерну особливість реальних мереж – наявність центральних хабів із великою кількістю з'єднань. Така структура спостерігається в електроенергетичних системах різних країн, зокрема Великої Британії, Німеччини, США.

Кожен вузол описується вектором:
type_idx – тип вузла (категоріальна ознака),
in_degree, out_degree – кількість вхідних/вихідних з'єднань,
depth – відстань до джерела ураження,
is_source – бінарна ознака джерела ураження.

Дані ознаки були нормалізовані. У наборі даних реалізовано балансування класів, щоб уникнути зміщення у бік здорових вузлів (типова проблема для мережевого аналізу) і подано у форматі, сумісному з GCN.

У дослідженні застосовано двошарову архітектуру Graph Convolutional Network (GCN), яка дозволяє моделі враховувати як властивості самих вузлів, так і їхнє оточення у мережі. Перший шар моделі збирає та узагальнює інформацію від сусідніх вузлів, створюючи для кожного з них вектор контексту, що враховує їхнє місце у структурі графа. Такий процес називається обміном повідомленнями (message passing)[3] і є ключовим для розуміння взаємозв'язків у мережі. Другий шар на основі цих векторів

виконує класифікацію – визначає, наскільки ймовірно, що кожен вузол буде ураженим. Для цього модель формує оцінку (логіти), яка перетворюється на ймовірність за допомогою функції softmax. Таким чином, модель дозволяє оцінити ризик ураження кожного вузла, враховуючи як його індивідуальні характеристики, так і топологічні зв'язки. Це є критично важливим для точного прогнозування каскадних відмов у складних мережах.

З метою пояснення внутрішньої логіки прийняття рішень графовою нейронною мережею було проведено аналіз ваг прихованого шару двошарової GCN-моделі. Для кожного з 16 нейронів другого шару отримано вектор ваг, що відповідає впливу окремих ознак вузлів на вихід моделі.

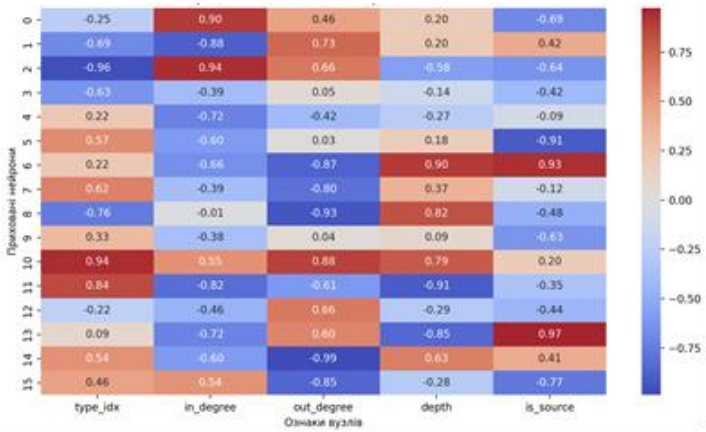

Рисунок 1 – Вагові коефіцієнти між ознаками вузлів і нейронами GCN-моделі

Дані спостереження підтверджують, що модель формує внутрішні механізми розпізнавання структурних закономірностей, які є характерними для каскадного поширення відмов. Висока інтерпретованість ваг забезпечує можливість довіри до результатів використання нашої моделі.

Для демонстрації можливостей моделі та її практичного застосування було розроблено інтерактивний прототип, що дозволяє здійснювати взаємодію з моделлю у режимі реального часу. Запропонований інтерфейс орієнтовано на фахівців, що працюють із інфраструктурними системами, зокрема операторів диспетчерських центрів (SCADA), аналітиків кібербезпеки (SOC), дослідників мережевої резильєнтності тощо. Прототип сприяє швидкій перевірці гіпотез, інтерпретації моделей та підтримці прийняття рішень у критичних умовах. Основними функціональними можливостями прототипу стали: редагування параметрів вузлів, оновлення прогнозу, візуалізація ризиків, сценарне моделювання.

Для оцінки ефективності побудованої моделі графової нейронної мережі було проведено серію експериментів із різними значеннями порогу класифікації, в діапазоні від 30 до 70 відсотків. Це дозволило перевірити, наскільки стабільно модель працює при зміні умов прийняття рішення – зокрема, як вона реагує на різні рівні чутливості при визначенні уражених вузлів. Результати показали, що модель демонструє стабільну якість прогнозування ризиків, незалежно від вибраного порогу, з чіткою адаптацією до змін у топології графа. Найвищі ймовірності ураження *P(class=1)* спостерігалися для таких категорій вузлів:

- Вузли з високим ступенем зв'язаності – як за вхідними (in_degree), так і за вихідними (out_degree) з'єднаннями. Це вказує на їхню роль у потенційному поширенні збоїв.
- Вузли, близькі до джерел ураження (depth = 1 або 2), що фізично або логічно розміщені у зоні первинного впливу.
- Вузли критичних типів (type_idx) – зокрема, генератори, маршрутизатори, трансформатори, які є ключовими для функціонування мережі та не мають альтернативних шляхів живлення.

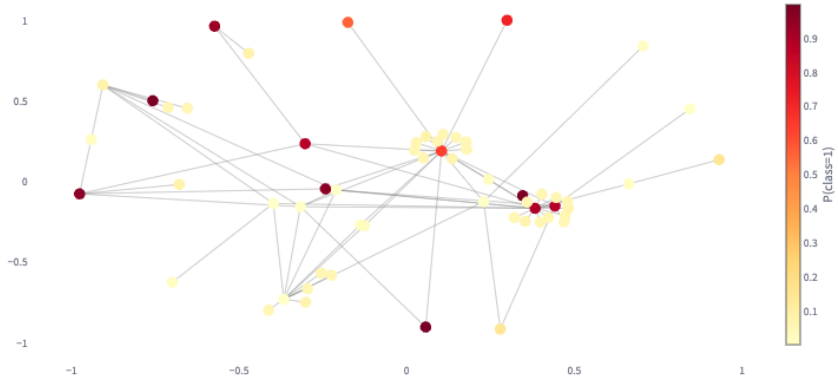

Рисунок 2 – Мережева карта ризиків за результатами GCN-прогнозування

Загалом модель підтвердила свою здатність виявляти вразливі компоненти мережі, які є критичними з точки зору ризику каскадних відмов, навіть без явного задання топологічних правил чи експертних знань.

Висновок**.** Проведене дослідження засвідчило ефективність застосування двошарової графової нейронної мережі (GCN) для прогнозування ризику ураження вузлів в енергетичних мережах. Запропонована модель здатна враховувати не лише локальні характеристики вузлів, а й їхнє топологічне оточення, що є критично важливим для виявлення потенційних каскадних відмов.

Аналіз поведінки прихованих нейронів свідчить, що модель не обмежується запам’ятовуванням вихідних міток, а формує узагальнені структурні патерни, характерні для типових сценаріїв поширення збоїв у складних системах. Розроблений інтерактивний прототип підтвердив практичну придатність підходу: він дозволяє в реальному часі моделювати різні варіанти розвитку подій, змінювати параметри мережі та миттєво отримувати прогноз ризику для кожного вузла. Це створює передумови для інтеграції GNN-моделей у процес підтримки прийняття рішень в умовах роботи критичної інфраструктури.

У якості подальших напрямів дослідження розглядається:

- застосування attention-архітектур (зокрема Graph Attention Networks, GAT) для покращення селективності моделі;
- використання більш гнучких підходів агрегації, таких як Graph Isomorphism Network (GIN), для підвищення здатності моделі до узагальнення у складних топологіях;
- підключення до тестових середовищ що імітують реальні SCADA системи для навчання моделі на фактичних сценаріях.

Таким чином, дослідження закладає підґрунтя для створення інтелектуальних систем оцінки ризиків у реальному часі, орієнтованих на підвищення кіберрезильєнтності критичних енергетичних мереж.

1. Jie Zhou, Ganqu Cui, Shengding Hu, Zhengyan Zhang, Cheng Yang, Zhiyuan Liu, Lifeng Wang, Changcheng Li, Maosong Sun. AI Open Volume 1, 2020, Pages 57-81. Graph neural networks: A review of methods and applications. https://doi.org/10.1016/j.aiopen.2021.01.001.
2. Vibha Bharilya , Neetesh Kumar. Vehicular Communications Volume 46, April 2024, 100733. Machine learning for autonomous vehicle's trajectory prediction: A comprehensive survey, challenges, and future research directions. https://doi.org/10.1016/j.vehcom.2024.100733.
3. Junshu Sun, Chenxue Yang, Xiangyang Ji, Qingming Huang, Shuhui Wang. Towards Dynamic Message Passing on Graphs. https://doi.org/10.48550/arXiv.2410.23686.

О.Ф. Буткевич, Н.Т. Юнєєва, Т.М. Гурєєва, А.Р. Слободян, Д.В. Самойленко

РЕЗИЛЬЄНТНІСТЬ І ЖИВУЧІСТЬ ЕНЕРГОСИСТЕМ ТА РОЛЬ ПРОТИАВАРІЙНОЇ АВТОМАТИКИ У ЇХ ЗАБЕЗПЕЧЕННІ

Термін *резильєнтність*, яким позначають відповідне поняття, давно використовують в різних сферах людської діяльності, проте трактують його в кожній із таких сфер дещо по-різному, і відмінності таких трактувань бувають досить значними. В публікаціях, пов'язаних з електроенергетичними системами (ЕЕС), цей термін почав з'являтися порівняно не так давно, до того ж спочатку з досить довільними трактуваннями, що зводилися до поняття *стійкості* (наразі його не використовують у відповідних нормативних документах). Причини цього, очевидно, полягають у тому, що одне із поширених визначень *резильєнтності*, яке іноді використовували і для ЕЕС, має витоки з механіки, де трактується, з одного боку, як *фізична здатність матеріалу повертатися до початкового (вихідного) стану*, а з іншого (якщо переходити до систем) – семантично ототожнюється з *асимптотичною стійкістю* (відповідні терміни «стійкість в малому» та «статична стійкість» якраз привнесені в ЕЕС з механіки разом із математичною теорією стійкості О.М. Ляпунова). Проте таке визначення *резильєнтності* для ЕЕС було б досить «вузьким», крім того, воно повністю «перекривалося» б *статичною стійкістю*. Тому *резильєнтність* ЕЕС здебільшого трактують як спроможність ЕЕС виконувати свої функції (навіть з частковою деградацією), зазнаючи впливів, що перешкоджають функціонуванню. Очевидно, що для оцінювання резильєнтності *post factum* можна використовувати або дані, пов'язані з функціональною деградацією ЕЕС (обсяг невідпуску електроенергії за певний період часу чи/та сумарна тривалість обтяжених режимів з ненормативними значеннями окремих показників якості електричної енергії), або, якщо зазначена деградація не мала місця, – кількістю «відбитих» спроб-атак (впливів) перешкодити функціонуванню ЕЕС (у таких випадках лише підтверджується резильєнтність ЕЕС, а кількість таких «відбитих» спроб може слугувати певним показником резильєнтності). Якщо брати до уваги, що ЕЕС на сучасному етапі свого розвитку – це не лише складні нелінійні динамічні системи, а і складні багатовимірні людино-машинні системи, засоби моніторингу та управління якими стають об'єктами хакерських атак та активованих латентних загроз (різновидів «троянських коней» у широкому їх розумінні), то для оцінювання резильєнтності ЕЕС у другому випадку (за кількістю «відбитих» спроб перешкодити функціонуванню ЕЕС) потрібно попередньо систематизувати множину різновидів таких спроб та «нормувати» їх. Очевидно, що на шляху виконання такого завдання існує багато перешкод, але навіть у разі його виконання практично користуватися результатами буде складно (громіздко), тому можливість і практична

доцільність оцінювання резильєнтності ЕЕС за кількістю «відбитих» спроб наразі виглядають сумнівними.

Резильєнтність ЕЕС, на відміну від *стійкості ЕЕС,* наразі можна оцінювати лише *post factum*, а не за «запасами» a priori. Трактування *резильєнтності ЕЕС* не є усталеним, цей термін не використовують в нормативних документах. Але нормативні документи періодично переглядають і вносять за потреби зміни, зокрема і в частині термінів. Наприклад, свого часу поняття *живучості енергосистеми* трактували як *здатність енергосистеми протистояти ланцюжковому розвиткові аварійних режимів* [1], а з урахуванням останніх змін до чинного «Кодексу системи передачі» [2] *живучість енергосистеми* трактують як *здатність енергосистеми зберігати обмежену працездатність в аварійних ситуаціях, протистояти аварійним ситуаціям винятkового типу та забезпечувати їх ліквідацію і відновлення енергопостачання споживачів*. Наведені в [1] та [2] визначення *живучості ЕЕС* відрізняються. Справа у тому, що в [1] *аварійний режим* – це *режим роботи енергосистеми за умови виникнення аварій*, що не тотожно виникненню аварійної ситуації в [2], де *аварійна ситуація* – це *виявлене та можливе або таке, що вже відбулося, пошкодження елемента, що включає елементи системи передачі, елементи значних користувачів, а також елементи системи розподілу, якщо вони впливають на операційну безпеку системи передачі*. Визначення живучості ЕЕС, наведене в [2], стосується і *можливого пошкодження елемента,* тоді як в [1] однозначно йдеться про аварію. Однак у визначенні *живучості ЕЕС* в [2] використано поняття *аварійної ситуації винятkового типу – одночасного виникнення декількох аварійних ситуацій, викликаних загальною причиною. Це означає, що не одна аварія, а кілька одночасно виникають через одну й ту ж причину, що може мати значний негативний вплив на роботу енергосистеми*. Зауважимо, що *одночасне виникнення* – це не *ланцюжковий розвиток,* як в [1], оскільки *ланцюжковий* – це послідовний, а не одночасний. Але в [2] наведено пояснення до визначення *аварійної ситуації винятkового типу*, в якому *аварійні ситуації* замінено не тотожним за семантикою словом *аварії.*

Викладене вище свідчить, що нормативні документи теж можуть містити неточності та «огріхи». Однак вони не впливають на практичне застосування різнобічних заходів та засобів, підпорядкованих завданню забезпечення живучості ЕЕС (поняття резильєнтності ЕЕС має «ширші» рамки ніж поняття живучості ЕЕС, оскільки має більше «вимірів», але забезпечуючи живучість ЕЕС, підвищуємо і її резильєнтність).

Одним із напрямів забезпечення живучості та підвищення резильєнтності ЕЕС є розвиток засобів релейного захисту (РЗ) та протиаварійної автоматики (ПА). Адекватність моделювання ланцюжкового розвитку аварійних процесів може досягатися лише з використанням моделей засобів РЗ та ПА в комплексній моделі ЕЕС. Це стосується як нормальних, так і ремонтних режимів, оскільки в ремонтних режимах забезпечення

виконання критерію «N-1» для ремонтних схем можливо за рахунок оперативного обмеження потужності електростанцій та електричних підстанцій ПС або із застосуванням пристроїв ПА, що діють на обмеження їхньої потужності.

Побудова ПА в ЕЕС відбувається за принципом «ешелонованої оборони», дія якої, зазвичай, «рознесена» у часі: якщо дії першого (чи чергового) «ешелону» виявляються недостатніми (недостатньо ефективними), щоб зупинити розвиток аварійних процесів, то діяти починає ПА наступного «ешелону». З огляду на зазначену послідовність дій ПА, до першого «ешелону» відносимо автоматику припинення порушення стійкості (АППС), яку на практиці можуть утворювати декілька різних технічних комплексів. До другого «ешелону» відносимо автоматику припинення асинхронного режиму (АЛАР). У свою чергу АППС подається кількома підсистемами, найпростіші з яких поєднують, наприклад, РЗ та автоматику повторного увімкнення (АПВ) чи РЗ та автоматику (пристрої) резервування відмови вимикача (ПРВВ). Функціонування таких підсистем поширюється на енерговузли та енергорайони, у той час, коли АЛАР зазвичай охоплює енергорайони та ЕЕС. Передбачено можливість (одна із вимог, що стосується побудови моделей ПА) подання АППС та АЛАР кількома ступенями, враховуючи можливість реалізації дозованих керуючих дій (впливів).

Частотну ПА утворюють автоматики обмеження підвищення частоти (АОПЧ) та автоматики обмеження зниження частоти (АОЗЧ). Ці автоматики функціонують у разі порушення балансу активної потужності і використовують (і поєднують) як централізовані, так і децентралізовані засоби (до останніх належить автоматика частотного розвантаження – АЧР, що подається у вигляді «черг», послідовне спрацьовування кожної з яких залежить від досягнутого значення частоти в ЕЕС (ОЕС).

Враховуючи, що моделювати потрібно різні пристрої ПА, для побудови моделей ПА використано принцип формування *елементарних* (атомарних) умов, згідно з яким слід дати відповіді на запитання «де?», «що?», «скільки?», тобто вказати «об'єкт», «величину чи дію, що контролюється», «уставку чи величину впливу» [3]. Об’єктами є вузли, лінії електропередачі, перетини ЕЕС. За логічно-обчислювальними умовами перевіряються, наприклад, значення певних режимних параметрів, сальдо потужності перетину та інше, контролюється стан (увімкнений чи вимкнений) певних елементів ЕЕС, час затримки (витримки часу) на виконання (якщо задовольняються відповідні умови) наступної дії. Крім того, використання моделей різних пристроїв ПА під час моделювання аварійних режимів ЕЕС обов’язково мають забезпечуватися потреби введення в роботу чи виведення із роботи окремих пристроїв чи підсистем РЗ і ПА, моделювання їхнього функціонування за заданою часовою програмою та моделювання відмов окремих пристроїв [4].

На рис. 1 та 2 показано фрагмент протоколу реєстрації подій та модельовані режимні параметри повітряної лінії (ПЛ) 330 кВ для режиму максимальних навантажень 2016 р. ОЕС України. Послідовність моделювання аварійних впливів була такою: 3-фазне коротке замикання тривалістю 0.12 с у вузлі 803; відмова вимикача на відключення ПЛ 330 кВ, що поєднує ПС Шепетівка–Житомир; спрацьовування пристрою резервування відмови вимикача (ПРВВ) на ПС 330 кВ Шепетівка; внаслідок ворожого ракетного удару втрата генерації на Трипільській ТЕС.

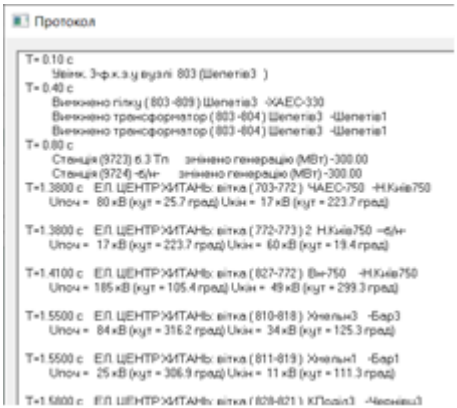

Рисунок 1 – Фрагмент протоколу подій під час моделювання аварійного режиму з АЛАР

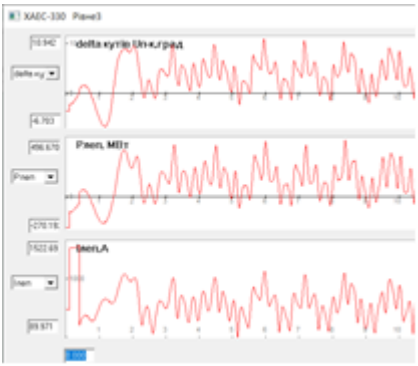

Рисунок 2 – Результати моделювання перехідного процесу ПЛ-330кВ ПС Хмельницька АЕС – ПС Рівне

Висновки.

1. Поняття *живучості* та *резильєнтності ЕЕС* близькі, але мають відмінності. Забезпечення живучості ЕЕС сприяє підвищенню резильєнтності ЕЕС. Показано, що в чинному «Кодексі системи передачі» визначення *живучості енергосистеми* містить «неточності».

2. Використання ПА є необхідною умовою забезпечення живучості та підвищення резильєнтності ЕЕС.

3. Побудова та використання моделей пристроїв ПА під час моделювання аварійних режимів ЕЕС є необхідною умовою адекватності результатів моделювання.

1. ДСТУ 3440-96 Системи енергетичні. Терміни та визначення. – 45 с.
2. Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг. 06.05.2025 № 677: Зміни до Кодексу системи передачі.
4. Буткевич О.Ф., Гурєєва Т.М., Юнєєва Н.Т. Особливості розроблення та використання моделей протиаварійної автоматики енергосистем. *Electrical and*

Power Engineering and Electromechanics (EPEE 2024). Odesa, Ukraine, May 15, 2024. Odesa Military Academy. С. 17–18. DOI: https://doi.org/10.6084/m9.figshare.25858477.

5. Буткевич О., Гурєєва Т., Юнєєва Н. Питання розроблення моделей системної автоматики для дослідження аварійних режимів електроенергетичних систем. *Праці Інституту електродинаміки НАН України*. 2024. Вип. 69. С. 29-35. DOI: https://doi.org/10.15407/publishing2024.69.029.

І.П. Каменева

АНАЛІЗ РЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНИХ СИСТЕМ НА ОСНОВІ ТЕОРІЇ КАТАСТРОФ

Вступ. Серед сучасних методів дослідження і оцінювання стану безпеки енергетичної галузі особлива увага надається інтегрованим інформаційним системам і засобам, де досвід людини поєднується з обчислювальними можливостями сучасних комп'ютерних систем як інтегруючого середовища для аналізу великих обсягів різноманітних даних. В рамках системного аналізу енергетичної безпеки [1] розроблено ряд інформаційних моделей та засобів подання знань [2, 3 тощо], які запропоновано адаптувати для проблеми дослідження та оцінювання стійкості енергетичних підприємств і прилеглих територіальних систем, які перебувають в зоні військового конфлікту, терористичних загроз і природних катаклізмів.

Нагадаємо, що в окремих галузях науково-технічної діяльності під впливом подій останнього часу виникла необхідність переходу від концепції захисту складних систем від руйнування до ***концепції резильєнтності***, яка наразі активно обговорюється серед науковців різних країн.

Під час військової агресії та її руйнівних наслідків для нашої країни суттєво зросла актуальність проблеми аналізу і оцінювання *резильєнтності критичної інфраструктури*. В першу чергу це забезпечення стійкості та резильєнтності енергетичної системи України, яка наразі потребує особливої уваги. Для енергетичної системи в цілому або окремих її підприємств резильєнтність – це здатність енергетичного сектору або його складових адаптуватися до шокових загроз і стресових навантажень, тобто протистояти, реагувати та швидко відновлюватись після руйнівних подій [4].

Розвиток й удосконалення наукових методів оцінювання поточного стану енергосистем та їх адаптивності до руйнівних впливів за допомогою комп'ютерного моделювання може забезпечити збереження фінансових та матеріальних ресурсів, оскільки своєчасне виявлення високих ризиків та передбачення руйнівних наслідків може суттєво зменшити витрати, необхідні для відбудови або відновлення дієздатності пошкоджених підприємств енергокомплексу, зокрема, теплових та атомних станцій.

Постановка задачі. Проблема стійкості енергетичних систем може досліджуватись у двох напрямках: статичному та динамічному. Можна вважати, що система залишається *статично стійкою*, якщо структура і стан цієї системи не змінюються під впливом незначних коливань її параметрів. Така система буде стабільною в певному околі змін, але значні коливання можуть її зруйнувати. На практиці періоди стабільності та періоди стрімких змін параметрів досліджуваних систем чергуються між собою. Складні системи оперують механізмами зворотного зв'язку: негативними для збереження існуючого стану, або позитивними, які можуть забезпечити можливості стійкого функціонування на іншому рівні.

Для динамічної системи стійкість запропоновано досліджувати за допомогою спеціальних математичних методів теорії катастроф та засобів когнітивного моделювання, де розроблено математичний апарат для аналізу поведінки складних динамічних систем [5, 6].

Отже, основна мета даного напрямку робіт полягає в дослідженні та подальшій розробці методів та комп'ютерних технологій, що можуть забезпечити систематизацію, інтерпретацію та інтеграцію даних для оцінювання поточного стану складних енергетичних систем. Більш конкретно розглянемо методи та засоби, спрямовані на моніторинг і оцінювання рівня стійкості енергосистем в умовах високого ризику.

На перших етапах дослідження потрібно виділити основні показники (фактори ризику), які мають вплив на динаміку досліджуваної системи. Для прикладу можна уявити, що стан динамічної системи характеризує певне число k, яке має бути «системним коефіцієнтом підсилення». Якщо $k > 1$, система здатна до відтворення і розширення. Якщо $k < 1$, то система рухається до загибелі. При наявності такої характеристики ризики може створювати довільний неконтрольований фактор, який може зменшити величину k. В даному випадку ступінь ризику можна оцінювати в залежності від значення цієї величини. Допустимий ризик призводить до незначних змін: k залишається більше 1. При критичних значеннях ризику величина k буде наближатися до 1, що сприяє вразливості для багатьох інших ризиків. При фатальних значеннях ризику процес набуває незворотного характеру, тобто система виходить із нормального режиму або руйнується

Відомо, що складні процеси описуються набором рівнянь з великою кількістю змінних, які вирішуються чисельними методами. Проте, в певних випадках для дослідження стійкості системи на якісному рівні можна обрати невелику кількість найбільш впливових характеристик [2].

Щоб розібратися в подіях, які мають небезпечний вплив, важливо побудовані моделі, точніше, результати моделювання, порівняти з наявними спостереженнями. Таке зіставлення спостережень з уже відомими образами призводить до попередніх висновків. Процес порівняння може включати використання аналогій та прототипів. Зокрема, на основі аналізу фізико-хімічних систем, де вивчаються перехідні процеси з порушенням стійкості, можна провести аналогії для інших досить схожих систем, де закони зміни окремих складових наразі ще не досліджені.

Тобто на основі спостережень вибирається модель, що виглядає найбільш адекватною для опису об'єкта дослідження. Потім відбувається вихід за межі аналогії, щоб уточнити в рамках даної моделі специфічні особливості кожного процесу, які слід врахувати при моделюванні. До таких особливостей в кожній задачі має належати вибір параметрів порядку, які визначають динаміку системи в цілому [6].

Складна поведінка відрізняється від простої (лінійної) насамперед наявністю певного спектра можливостей для адаптації при різкій зміні

зовнішніх умов. Здатність до переключення між різними типами поведінки дає можливість вибору однієї з кількох альтернатив.

Методи дослідження стійкості. Динаміку станів складної системи можна відобразити як векторне поле в фазовому просторі. Точка фазового простору визначає поточний стан системи. Відповідний вектор вказує на швидкість зміни стану. Точки, в яких вектор дорівнює нулю, визначаються як точки рівноваги, де стан не змінюється з часом.

В загальному випадку досліджується система диференційних рівнянь певного типу, визначена для обмеженої області H, яка представляє фазовий простір для спостереження за системою. Зокрема, для n = 2 це буде фазова площина. Як правило, функції, що утворюють праву частину, нелінійні.

Нагадаємо найбільш відомі визначення стійкості щодо поведінки такої системи в фазовому просторі, які добре узгоджуються між собою.

Визначення стійкості за Пуанкаре. Якщо система в момент t перебуває в стані рівноваги, то в певний момент t_1 вона може вийти із цього стану, зберігаючи свою структуру. Стан системи можна вважати стійким за умови, що система в певному околі може повертатись у стан рівноваги.

Стійкість за Ляпуновим. Стан системи вважається стійким, якщо за деяких початкових збурень параметрів система продовжує перебувати у певному околі стану рівноваги.

Стійкість за Лагранжем розуміється як певна обмеженість щодо можливих траєкторій цієї системи, тобто система не повинна виходити за межі певної обмеженої області.

В такому контексті резильєнтність системи може розглядатися як відтворення стану гомеостазу для різних рівнів порядку досліджуваної системи за умови, щоб основні фактори, що визначають функціонування елементів системи, не виходили за межі допустимих значень, критичних для збереження цілісності системи та підтримки її основних функцій.

Згідно з наведеними визначеннями, траєкторію в фазовому просторі H динамічної системи можна вважати ***стійкою***, якщо динаміка траєкторій з близькими початковими умовами мало відрізняється від даної траєкторії.

Нагадаємо, що під *фазовими портретами* розуміють певні варіанти поведінки траєкторій в фазовому просторі, що відображують динаміку системи в околі стану рівноваги. Найбільш типові фазові портрети визначені ще в 1897 р. Анрі Пуанкаре, роботи якого стали важливим етапом розвитку досліджень в цій галузі. Пізніше теорія катастроф поєднала в собі теорію біфуркацій Пуанкаре та теорію особливостей Уїтні, яка в свою чергу узагальнила дослідження на екстремуми для функцій декількох змінних [5]. Таким чином, теорія катастроф спрямована на якісний аналіз поведінки динамічних систем в умовах нестабільності та невизначеності.

В загальному випадку стан досліджуваної системи визначає певна сукупність параметрів. Якщо хоча б один із параметрів приймає критичне значення, система втрачає поточний стан рівноваги і переходить в інший режим функціонування. Для визначення та аналізу стану досліджуваних

систем необхідно обрати невелику кількість інформативних показників, які досить точно відображують поточний стан системи [2].

Отже, ефективне практичне використання теорії катастроф для задач дослідження резильєнтності енергетичних систем на початкових етапах потребує необхідної інформаційної підтримки, зокрема, розробки баз знань та визначення імовірнісних оцінок, які характеризують як ризики ураження та руйнування підприємств критичної інфраструктури, так і адаптивні можливості щодо підтримки окремих виробництв або їх взаємодії (з урахуванням розташування та імовірних наслідків руйнівного впливу).

Слід підкреслити необхідність поглибленого дослідження енергетичної структури країни, спрямованого на систематизацію та аналіз відповідної інформації, що допоможе надалі перейти до стислого відображення й моніторингу окремих структур в фазовому просторі.

Висновки. Для ефективного використання методів та можливостей теорії катастроф в задачах аналізу резильєнтності енергетичних систем необхідно вирішити питання, спрямовані на підготовку та інтеграцію наявних інформаційних ресурсів і створення баз знань.

На першому етапі запропоновано визначити найбільш важливі індикатори стійкості, за якими можна буде оцінювати поточний стан досліджуваних систем. Зокрема, це можна зробити на основі методів та засобів, представлених в роботі [2]. Другий етап включає засоби організації та проведення моніторингу і контролю, а також виявлення можливостей щодо корекції стану досліджуваних систем на основі базових індикаторів, визначених на першому етапі.

1. Суходоля О. М., Харазішвілі Ю. М., Бобро Д. Г та ін. Енергетична безпека України: методологія системного аналізу та стратегічного планування: аналітична доп. / за заг. ред. О. М. Суходолі. – Київ: НІСД, 2020. – 178 с. [Електронний ресурс] Режим доступу: sukhodolia_energy_security_sayt-1.pdf (niss.gov.ua).
2. 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.
3. Каменева І.П., Артемчук В.О., Яцишин А.В, Владимирський О.А. Імовірнісні моделі подання знань для підтримки прийняття рішень в умовах ризику та невизначеності на прикладі галузі охорони атмосферного повітря // Електронне моделювання, 2024, 46, № 1, с. 3 –20.
4. Stout S., Lee N., Cox S., Elsworth J., Leisch J. Power sector resilience planning guidebook. – U.S. Department of Energy’s NREL and USAID. – 2019. – 82 p. – URL https://www.nrel.gov/docs/fy19osti/73489.pdf.
5. Gilmore R. Catastrophe Theory for Scientists and Engineers. John Wiley & Sons Inc., 1981. – 686 c.
6. Nikolis, G., Prigogine, I. Exploring complexity: An introduction. W.H. Freeman and Company, New York, 1989. – 328 c.

Д.С. Матушкін

ІНТЕГРАЦІЯ ФОТОЕЛЕКТРИЧНИХ СТАНЦІЙ ДЛЯ ЗМІЦНЕННЯ РЕЗИЛЬЄНТНОСТІ ТЕПЛОВИХ ЕЛЕКТРОСТАНЦІЙ

Теплові електростанції (ТЕС) залишаються фундаментальною складовою світового енергетичного міксу, забезпечуючи близько 60–70 % виробництва електроенергії в багатьох країнах. Завдяки здатності стабільно генерувати базове навантаження та оперативно реагувати на зміну попиту, вони залишаються ключовим інструментом диспетчерського регулювання енергосистеми. Водночас експлуатація ТЕС супроводжується значними викидами CO_2, оксидів сірки (SO_2), оксидів азоту (NO_x) та дрібнодисперсного пилу, що зумовлює необхідність жорсткіших екологічних стандартів і виконання зобов'язань за Паризькою угодою [1, 2].

Протягом 2022–2023 рр. ціни на природний газ і вугілля зросли на 50–70 %, що призвело до різкого збільшення експлуатаційних витрат ТЕС і сприяло пошуку альтернативних рішень. Одночасно інфраструктура багатьох ТЕС застаріла та працює за межами оптимального ресурсу, що призводить до зростання експлуатаційних витрат та підвищення ризику аварій. Пандемія COVID-19 і геополітичні кризи додатково виявили вразливість централізованих енергосистем і підкреслили важливість гібридних рішень для зміцнення резильєнтності енергетики.

У контексті глобальних цілей декарбонізації та зміцнення резильєнтності енергосистем, інтеграція фотоелектричних станцій (ФЕС) у роботу ТЕС стає актуальною. Таке гібридне рішення може дозволити зменшити споживання викопного палива в пікові години, зберігаючи надійність мережі та значно скорочуючи викиди CO_2 без потреби у масштабних реконструкціях існуючої інфраструктури.

У світлі необхідності скорочення викидів парникових газів і зменшення залежності від викопного палива, оперативний перехід до відновлюваних джерел енергії (ВДЕ) є критично важливим. За оцінками Міжнародного агентства з відновлюваної енергії (IRENA), темпи впровадження ВДЕ мають бути збільшені в шість разів, щоб утримати глобальне підвищення температури на рівні не вище за 2 °C. При цьому важливу роль відіграє балансування навантажень на рівні промислових споживачів для поєднання нерегулярної генерації ВДЕ з її попитом.

Фотоелектрика сьогодні є найбільш економічним методом виробництва електроенергії в багатьох регіонах світу: собівартість продукції впала до 0,015–0,02 $/кВт·год, а встановлена потужність подвоюється приблизно кожні три роки. Таке зниження вартості зумовлене конкурентними цінами на фотомодулі (–80 % з початку 2010-х) та розвитком систем трекінгу, концентрованої сонячної енергії з накопиченням тепла, що забезпечує безперервну генерацію навіть у нічний час або при хмарності.

Водночас нестабільність сонячної генерації можна компенсувати за рахунок розширення електричних мереж на великі території, вдосконалення систем зберігання енергії та впровадження цифрових рішень (AI-диспетчеризація, IoT-моніторинг). Інсталяція ФЕС створює нові робочі місця і знижує довгострокові енерговитрати регіонів.

За даними досліджень, заміщення 1 МВт·год енергії, виробленої на вугіллі, фотоелектрикою дозволяє скоротити викиди CO_2 на 800–1200 кг [3]. У країнах ЄС масштабне впровадження ФЕС призвело до зменшення викидів понад 200 млн т CO_2 за останнє десятиліття. Порівняльний аналіз життєвого циклу енергогенерації показує, що середні викиди ФЕС-генерації складають 11–37 г CO_2-екв./кВт·год, тоді як традиційні ТЕС – від 434 (газовий цикл-комбінований) до 1023 г CO_2-екв./кВт·год (вугілля) (рис. 1).

Рисунок 1 – Викиди парникових газів протягом життєвого циклу різних джерел енергії

Таким чином, інтеграція ФЕС у роботу ТЕС є одним із найефективніших заходів одночасного зниження вуглецевого сліду й підвищення стійкості енергосистем.

На підставі зазначених викликів і переваг ФЕС далі розглядаються шість сценаріїв інтеграції ФЕС у роботу ТЕС.

Оцінка економічної та екологічної ефективності ФЕС, що застосовуються для часткової декарбонізації роботи ТЕС, є ключовим етапом визначення доцільності інтеграції ВДЕ в традиційні енергосистеми. Для всебічного аналізу були використані наступні показники:

- Total Cost of Ownership (TCO) — загальна вартість володіння ФЕС протягом її життєвого циклу;
- Net Present Value (NPV) — чистий приведений дохід від впровадження ФЕС на ТЕС;
- Internal Rate of Return (IRR) — внутрішня норма прибутковості інвестицій;
- Payback Period (PP) — строк окупності капіталовкладень;

– Levelized Cost of Energy (LCOE) — усереднена вартість електроенергії;

– Carbon Abatement Cost (CAC) — вартість скорочення однієї тонни CO_2;

– Energy Return on Investment (EROI) — коефіцієнт енергетичної віддачі при будівництві ФЕС.

На основі цих параметрів, було запропоновано шість сценаріїв інтеграції ФЕС:

– Сценарій 1 (S1, базовий) – часткова заміна генерації у світловий період доби: ФЕС потужністю 224 МВт виробляє приблизно 333 млн кВт·год на рік, заміщуючи денне виробництво ТЕС, тоді як ТЕС забезпечує решту енергопостачання в нічний період.

– Сценарій 2 (S2) – гібридна система з акумулюванням: ФЕС потужністю 224 МВт інтегрується із системою накопичення енергії, що дозволяє зберігати надлишкову електроенергію та використовувати її у перехідні періоди (ранок/вечір) або під час пікових навантажень.

– Сценарій 3 (S3) – інтеграція з модернізацією ТЕС і розгортання інтелектуальної енергомережі (SmartGrid): повна модернізація ТЕС, включаючи інтеграцію ФЕС та SmartGrid, що дозволяє автоматизоване перемикання між джерелами енергії відповідно до споживчого попиту.

– Сценарій 4 (S4) – інтеграція через довгострокові договори на купівлю електроенергії (PPA): укладається договір купівлі-продажу електроенергії між постачальником ФЕС і ТЕС, що гарантує стабільне денне постачання електроенергії з ФЕС та дозволяє зменшити навантаження ТЕС у денний період.

– Сценарій 5 (S5) – децентралізована інтеграція через мікромережі: на території ТЕС або в її околицях розгортаються малі локальні ФЕС, що формують локальні мікромережі для оптимізації споживання електроенергії та зниження втрат під час енергопередачі.

– Сценарій 6 (S6) – інтеграція ФЕС із системами керування на основі елементів ШІ та машинного навчання (AI/ML): упроваджуються інтелектуальні системи керування енергетичними потоками на основі елементів AI та машинного навчання (ML), що дозволяє автоматично оптимізувати роботу ФЕС і ТЕС з урахуванням попиту на енергію, прогнозу погоди та ринкових умов.

Таблиця 1 містить опис сценаріїв інтеграції ФЕС у роботу ТЕС з метою досягнення оптимального балансу між економічною ефективністю та екологічними показниками. Запропоновані сценарії можуть сприяти вибору найбільш доцільного рішення залежно від інвестиційних можливостей, рівня готовності інфраструктури, стратегічних пріоритетів щодо скорочення викидів та економічної доцільності.

Таблиця 1 – Сценарії інтеграції фотоелектричних електростанцій у роботу теплових електростанцій

Сценарій	Замінена електроенергія (млн кВт·год/рік)	Екологічні показники
S1	333	- Скорочення викидів ≈ 300 тис. т CO_2/рік; - CAC ≈ $36,24/т; - EROI ≈ 37,17.
S2	400	- Скорочення викидів ≈ 360 тис. т CO_2/рік; - CAC ≈ $36,13/т; - EROI ≈ 37,31.
S3	360	- Скорочення викидів ≈ 324 тис. т CO_2/рік; - CAC ≈ $36,24/т; - EROI ≈ 37,19.
S4	333	- Скорочення викидів ≈ 300 тис. т CO_2/рік; - CAC ≈ $36,27/т; - EROI ≈ 37,17.
S5	240	- Скорочення викидів ≈ 216 тис. т CO_2/рік; - CAC ≈ $36,18/т; - EROI ≈ 37,27.
S6	440	- Скорочення викидів ≈ 396 тис. т CO_2/рік; - CAC ≈ $36,16/т; - EROI ≈ 37,29.

Табл. 2 містить порівняльний аналіз інвестиційних витрат, операційних витрат, фінансової доцільності та строків окупності для різних сценаріїв інтеграції ФЕС.

Таблиця 2 – Узагальнення економічних показників для сценаріїв інтеграції фотоелектричних електростанцій у роботу теплових електростанцій.

Сценарій	Потужність ФЕС (МВт)	CAPEX (млн $)	OPEX (млн $/рік)	Витрати на заміну (млн $)	Дисконтовані OPEX (млн $)	TCO (млн $)	LCOE ($/кВт·год)	Щорічний дохід (млн $)	NPV (млн $)	IRR (%)	Строк окупності (років, без дисконтування)
S1	224	224	3,36	11,2	39,16	272	≈ 0,07	26,68	+39,30	8,9	10-11
S2	268	268	4,02	13,4	46,88	325,14		27,98	+48	10	9,6
S3	242	242	3,63	12,1	42,3	293,57		28,8	+42	9-9,5	9,6
S4	224	224	3,36	11,2	39,16	272		26,68	+39,30	8,9	10-11
S5	161	161	2,42	8,05	28,2	195,38		19,2	+28	8-8,5	8-8,5
S6	295	295	4,43	14,75	51,67	358,0		35,2	+52	10-11	9,6

Результати показують, що Сценарій S6 забезпечує найвищий рівень заміщення електроенергії та найвищу економічну ефективність (найбільший NPV), тоді як сценарій S1 є найпростішим для реалізації, проте має нижчий рівень фінансової ефективності. Сценарії S2 та S3, які передбачають використання систем накопичення енергії та технологій SmartGrid,

демонструють компромісний баланс між інвестиціями та економічною доцільністю.

Усі сценарії демонструють подібні базові показники:

– LCOE залишається на рівні ≈$0,07/кВт·год, що свідчить про стабільну економічну ефективність у всіх сценаріях;

– CAC становить ≈$36/т CO_2, що вказує на однаковий вплив сценаріїв на скорочення викидів;

– EROI ≈37, що свідчить про високу енергоефективність у всіх варіантах;

– Строк окупності ≈9,5–10 років, що підтверджує подібні терміни повернення інвестицій у всіх сценаріях (без урахування дисконтування);

– NPV варіюється від +28 млн $ (S5) до +52 млн $ (S6), причому сценарій S6 має найбільший NPV, а сценарій S5 – найменший;

– IRR збільшується від ≈8–8,5% (S5) до ≈10–11% (S6), що корелює з ростом NPV.

Незалежно від обраного сценарію, ФЕС сприяють оптимізації операційних витрат і підвищенню енергоефективності системи, зберігаючи конкурентоспроможність з низьким LCOE та забезпечуючи позитивні фінансові результати (NPV, IRR).

Усі сценарії передбачають часткову заміну генерації ТЕС сонячною енергією, що дозволяє скоротити викиди CO_2 у діапазоні 216 тис. – 396 тис. т/рік та знизити операційні витрати на $14,4–26,4 млн на рік.

Базовий сценарій (S1) – часткова денна заміна – є найпростішим і найшвидшим у реалізації, оскільки передбачає роботу ТЕС лише у нічний час. Це дозволяє зменшити використання палива, знизити операційні витрати та викиди CO_2 на 300 тис. т/рік. Однак цей сценарій обмежений, оскільки не вирішує проблему пікового навантаження у вечірні та ранкові години.

Гібридна система з накопичувачами енергії (S2) дозволяє накопичувати надлишкову сонячну енергію протягом дня та використовувати її ввечері та вночі. Це сприяє заміні до 50% генерації ТЕС та зменшенню викидів CO_2 на 360 тис. т/рік, що робить цей сценарій одним із найбільш ефективних в екологічному аспекті.

Інтелектуальне керування на базі SmartGrid (S3) забезпечує динамічне перемикання між ФЕС і ТЕС залежно від погодних умов і попиту споживачів. Цей підхід дозволяє знизити викиди CO_2 на 324 тис. т/рік та операційні витрати на $21,6 млн/рік завдяки оптимізації режимів роботи ТЕС.

Довгострокові PPA-договори на купівлю електроенергії (S4) забезпечують фінансову стабільність, гарантуючи прогнозоване скорочення викидів CO_2 на 300 тис. т/рік та стабільні економічні переваги.

При розгляді локальних рішень децентралізована інтеграція через мікромережі (S5) сприяє оптимізації виробництва та споживання енергії на місцевому рівні, забезпечуючи до 30% заміщення генерації ТЕС, скорочення викидів CO_2 на 216 тис. т/рік та підвищення регіональної енергетичної

автономії. Однак цей підхід має обмежену масштабованість, що може ускладнювати його широке впровадження.

Перспективним варіантом є використання елементів штучного інтелекту (S6), оскільки він забезпечує максимальне скорочення викидів (396 тис. т CO_2/рік) та економію витрат у розмірі $26,4 млн/рік. Завдяки точному прогнозуванню генерації ФЕС та адаптивному керуванню роботою ТЕС цей сценарій досягає найвищого рівня фінансової ефективності, забезпечуючи найбільші значення NPV та IRR.

Результати аналізу свідчать, що сценарії з вищим рівнем інтеграції ФЕС (S2, S3, S6) забезпечують найвищу фінансову та екологічну ефективність, проте вимагають вищих капітальних витрат. Простіші варіанти (S1, S5) є менш витратними, але забезпечують нижчі економічні показники.

1. Маляренко, О., Горський, В., Іваненко, Н., Євтухова, Т., & Матушкін, Д. (2025). Комплексна оцінка заходів зі зниження викидів забруднюючих речовин в атмосферу. Системні дослідження в енергетиці, (1 (81), 100-110. https://doi.org/10.15407/srenergy2025.01.100.
2. Маляренко, О., Євтухова, Т., Іваненко, Н., Горський, В., & Коберник, В. (2024). Співставлення структури споживання палива та викидів забруднюючих речовин для визначення напрямів їхнього скорочення. Системні дослідження в енергетиці, (2а (78), 19-20. вилучено із https://systemre.org/index.php/journal/article/view/843.
3. World Nuclear Association. Energy and the environment: 'Clean coal' technologies, carbon capture & sequestration. URL: https://world-nuclear.org/information-library/energy-and-the-environment/clean-coal-technologies#related-information.

В.С. Волошин

ПРО ОДИН ПОРІВНЯЛЬНИЙ КРИТЕРІЙ ПО ВІДНОШЕННЮ ДО ДЕЯКИХ БІОЛОГІЧНИХ ПОПУЛЯЦІЙ, ЛЮДИНИ ТА СТВОРЕНИХ НИМ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Предметом нашого дослідження є системи, параметричний аналіз яких може дати відповіді на деякі питання релевантних відносин і які мають деякі ключові порівняльні функції. Це, для порівняння: мурашині колонії, людське суспільство і створені ним неорганічні системи штучного інтелекту.

Відомо, що час є одним з основних факторів еволюційного розвитку в природі. На рисунку 1 показані основні часові інтервали, протягом яких розвивалися досліджувані системи. Людський мозок оволодів дещо іншим механізмом прискореної еволюції, ніж інші біологічні системи як самоорганізована система пізнавальної діяльності. Це дозволило людині досягти дивовижних результатів за набагато коротший еволюційний період, яких ніколи не досягали інші біологічні популяції на планеті.

Формування «колективного розуму» у мурах було пов'язане з розвитком феромонної інформації в ранньому крейдяному періоді, а спеціалізація в професіях - з початком так званої еусоціальності. Професійні спеціалізації в мурашиній колонії є способом децентралізованого життєзабезпечення. До такого результату (*децентралізованого управління*) людина прийшла лише через 2 мільйони років свого існування в XXI столітті, створивши так звані технології «blockchain» з розподіленими реєстрами і, об'єктивно, без централізованого управління.

У людини подібні етапи зародження розуму пов'язані зі збільшенням обсягу мозкової речовини і розвитком когнітивізму, а досягнення в спеціалізації прийшли мало не з появою перших міських цивілізацій, надлишком продовольства з землеробства і тваринництва. Розвиток тваринництва було пов'язано з взаємовигідними відносинами з іншими тваринами і комахами. Розвиток рослинництва пов'язаний з мінімізацією збиральництва і пошуком інших шляхів отримання їжі. Однак факт залишається фактом: ще за 100 мільйонів років до появи людини на поверхні нашої планети з'явилися зачатки землеробства і тваринництва. Це були мурашині колонії, які знаходили способи існування не тільки в збиранні, але і в штучних біологічних технологіях.

Дуже короткий, але інтенсивний період розвитку штучного інтелекту дозволяє виділити в їх часових інтервалах порівняння лише двох його складових: ємність генеративної пам'яті машини і людини, і виникнення замісних (для людини) спеціалізацій. Якщо потужність активних нейронів мозку дорівнює байтам $2{,}5 \cdot 10^{15}$, то порівнянна потужність суперкомп'ютера **Frontier** (США) - $1{,}1 \cdot 10^{15}$ байт. Ази виробничої спеціалізації людина отримала близько 4,5 тисяч років тому (всього 10-15 тисяч професій), а ШІ лише пару десятиліть тому (дані класифікації O*NEET, США), але вже в кількості 470 видів професій.

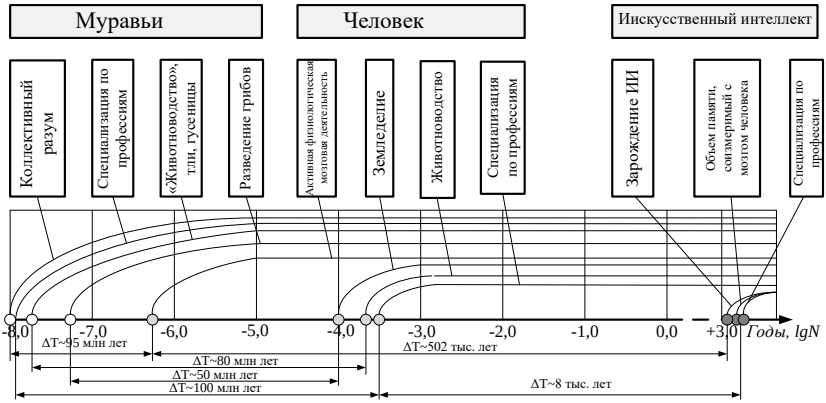

Рисунок 1 – Позначення на часовій шкалі основних порівнянних еволюційних етапів у розвитку популяцій мурах, людини та штучного інтелекту

В якості ще одного показника, який може характеризувати дві розглянуті популяції, а також штучний інтелект, ми будемо використовувати такий узагальнюючий параметр, як зміна (збільшення) ентропії в досліджуваних системах. Це показник ступеня деградації або розвитку, це порівнянний рівень організації досліджуваних систем. Порівняння двох чисто біологічних систем, а особливо з неорганічною системою (штучним інтелектом), яка бурхливо розвивається, може бути дуже повчальним для людини.

Термодинамічна складова такої ентропії дає уявлення про можливий розподіл енергії в системі, а її інформаційна компонента оцінює невизначеність або обсяг інформації, пов'язаної зі станами мурашиних суперколоній. За точку відліку візьмемо термодинамічний стан колективної області – суперколонію мурах, яка розташована на європейському узбережжі Середземного моря (Італія, Франція, Іспанія).

Термодинамічні характеристики мурашиної колонії можна розрахувати двома способами. Якщо розглядати мурашину колонію як систему теплообміну, де джерелами тепла є нескінченна кількість самих мурах, а також сонячне світло, вентиляційні та утеплювальні системи, то зміна ентропії розраховується відповідно до другого закону термодинаміки $\Delta S = \Delta E/T$, где $\Delta E = 5 \cdot 10^{-28}$ Дж/особь [1]; $T = 291$К – температура в колонії. Тоді зміна термодинамічної ентропії в суперколонії з 10^9особин за часовий інтервал в одну секунду складе $\Delta S = \frac{5 \cdot 10^{-28} \cdot 10^9}{291} = 1{,}695 \cdot 10^{-21}$ Дж/(К· с).

Існує і другий, альтернативний, метод розрахунку, який передбачає взяття за основу хаотичні механізми руху кожного індивіда в повному обсязі. У класичному випадку для термодинамічної ентропії використовується наступний вираз: $\Delta S = k_b \ln(\Omega)$, де Ω — кількість можливих мікростанів в залежності від чисельності мурах, їх розподілу по території і їх взаємодій

(наприклад, форми контактів, генерація феромонів), типу взаємодії (по «професіям»); k_b=1.38×10^{-23} Дж/К – константа Больцмана.

Параметрами для розрахунку зміни термодинамічної ентропії в даному випадку є:

- опосередкована температура в мурашнику; $T = 295K$
- температура навколишнього середовища; $T = 291K$
- кількість мурах N =10^9;
- площа колонії;$F = 6000$ км^2
- енергія взаємодії мурах за допомогою феромонів, при русі, а також витрата енергії на підтримку активності, температури тіла, температури гнізда $E = 5 \cdot 10^{-28}$ Дж/особь [1];

-прийняті професії та види взаємодії: фуражири (0,45), солдати (0,15), годувальники (0,115), няні (0,11), будівельники (0,072), санітари (0,04), розвідники (0,035), пастухи (0,03), переробники відходів (0,015)

Скористаємося розрахунковою моделлю [2], яка описує число можливих мікростанів в залежності від енергії взаємодії E_i, площі i –того ареалу F_i і числа мурах в $i-$ому ареалі N_i

$$\Omega \approx \sum \frac{F_i N_i}{E_i} = k_{\text{ср}} \sum \frac{N_i^2}{E_i},$$

де $k_{\text{ср}}$ – опосередкований коефіцієнт щільності особин, які обслуговують *i*-ю зонуF_i

Розрахунок зміни ентропії зводиться до визначення параметра Ω і отриманні значення ΔS, зведеного до одиниці часу (1 с). Для популяції мурах в заданому розмірі розрахункове значення для порівняння $\Delta S = 1{,}202 \cdot 10^{-21}$Дж/(К· с).

Цікаво порівняти термодинамічну ентропію людського мозку (6,4· 10^{-2}Дж/(К· с), розрахованої на основі [3] і популяції з $3{,}44 \cdot 10^5$ мурах, сумарний нейронний мозок яких за кількістю нейронів приблизно відповідає мозку однієї людини. головного мозку людини. Припустимо, що в даній популяції зберігається така ж ступінь спеціалізації. Тоді для мурах цифра розрахункового приросту ентропії становила $\Delta S == 0{,}92 \cdot 10^{-21} \cdot$ с), що на порядки нижче, ніж для аналогізованого таким чином людського мозку.

Мурашині поселення характеризуються дуже дбайливим ставленням до наявного тепла. Його зберігають для підтримки оптимальної температури (18°C) заради личинкам, попелиці, одомашненим гусеницям, грибкам. Зокрема, тепловтрати в суперколонії мурах чисельністю $1 \cdot 10^9$ особин за рахунок вентиляційних каналів в кількості 120 од / га і з середнім діаметром ~0,06 м складають $1{,}27 \cdot 10^{-14}$ Дж/сут [1], що відповідає зміні ентропії $\Delta S \approx 4{,}35 \cdot 10^{-22}$Дж/(К · с). Для порівняння, втрати тепла від розподілу енергії для потреб міста з населенням 1 млн осіб і площею 700 км^2 (без урахування промислової складової) перевищують 5,18· 10^5 Дж/сут, що відповідає зростанню ентропії $\Delta S \approx 0{,}0198$ Дж/(К · с). Різниця в термодинамічній ефективності вимірюється десятками порядків.

Мозок людини – це компактна нейронна система з відносно низьким енергоспоживанням (20 Вт), на відміну від розподіленого колективного мозку мурахів, кожна умовна клітина якого потребує на порядки менше енергії внаслідок синергетичних ефектів і поступається людському мозку за функціональністю.

У свою чергу, штучна нейронна мережа, заданої розмірності і в залежності від обсягу параметрів, а також структури даних і використовуваних алгоритмів, як носій штучного інтелекту, у вигляді неорганічної системи, вимагає величезних, в порівнянні з мозком людини або мурашки, енергетичних витрат (умовно більш 1,0 кВт). І, як будь-яка штучна неорганічна система, створена людиною, вона запрограмована на значні великі втрати енергії і зростання ентропії в опосередкованих розмірах $\Delta S \approx 9{,}2$ Дж/(К · с). Зведені дані цього та аналогічних розрахунків наведені в таблиці 1, де можна буде оцінити ефективність такого показника, як ентропія системи як критерій організації та можливості розвитку розглянутих біологічних і неорганічних систем.

Таким чином, індекс термодинамічної ентропії в ретроспективі розвитку показує значні відмінності між тим, що людина створила за останні 40 тисяч років свого існування на основі неорганічних систем (міста, машини, підприємства, комунікації, мережі) і організованим біологічним світом, який був створений і вдосконалений нашими двійниками – мурашиними колоніями – протягом 100 мільйонів років. Тією мірою, якою їх некогнітивний «колективний розум» дозволяє їм це робити.

Інформаційна ентропія - це друга частина системи оцінки взаємодій всередині мурашиної суперколонії, яка відповідає за впорядкованість і ступінь її організації**.** Для розрахунку інформаційної ентропії ми будемо враховувати такі параметри:

- *потік* інформації, що передається між мурахами в суперколоніях, наприклад, за допомогою феромонів, сигналів про пошук їжі, захисту і т.д.;

-*невизначеність стану*: невизначеність або випадковість, з якою кожна мураха виконує своє завдання, що збільшує ступінь ентропії;

- *обсяг переданої інформації*: це кількість інформації, необхідної для опису стану системи (наприклад, місцезнаходження мурах, їх поведінки і т.д.).

Інформаційна ентропія обчислюється за формулою Шеннона $H = -\sum p_i \log(p_i)$, де p_i — ймовірність того, що система знаходиться в стані i. Для суперколонії мурах ці ймовірності можуть означати, що мураха знаходиться в певному місці або виконує конкретне професійне завдання.

Розрахунок зводиться до обчислення зміни ентропії на мурашку за одиницю часу: $H \approx 1{,}999$ біт/с. або $\approx 0{,}019 \cdot 10^{-21}$Дж/(К· с). Для заявленої популяції в 1 мільярд мурах інтегральна інформаційна ентропія може становити $H_{total} = 1{,}9 \cdot 10^{-14}$ Дж/(К· с).

Таблиця 1 – Порівняльні дані про зміну ентропії для деяких органічних і неорганічних систем

№№ п/п	Назва системи		Зміна ентропії, Дж/(К· с)	
			термодинамічної	інформаційної
1	Мурашина популяція	$N = 10^9$	$1{,}202 \cdot 10^{-21}$	$1{,}9 \cdot 10^{-14}$
		$N = 3{,}44 \cdot 10^5$	$0{,}92 \cdot 10^{-21}$	$1{,}9 \cdot 10^{-14}$
2	Людський мозок		$6{,}4 \cdot 10^{-3}$	$6{,}91 \cdot 10^{-20}$
3	Урбосистема с $N = 1 \cdot 10^6$ мешканців		$1{,}98 \cdot 10^{-2}$	$1{,}44 \cdot 10^{-17}$
4	Система штучного інтелекту		9,2	$3{,}5 \cdot 10^{-18}$

Таким чином, в термодинамічному плані, і в ретроспективі 100 мільйонів років існування, колонії мурах термодинамічно набагато більш організовані, ніж більшість з того, що створила людина, включаючи його самого за 2 мільйони років існування. Зростання термодинамічної ентропії у відомих суперколоніях мурах на кілька порядків нижче, ніж зростання цієї ж ентропії в системах, створених людиною, включаючи її мозок (див. таблицю 1).

Інші результати є в області інформаційної ентропії. Тут переваги людини і всього доступного, що вони створили, на кілька порядків вище, ніж у мурашиних популяцій з їх стомільйонною історією, що очевидно. Це пов'язано з тим, що людський мозок в силу своєї когнітивності створює величезну палітру потреб і одягає їх у все зростаючі інформаційні потоки (потреби в якості життя, способи досягнення, результати, втрати, відповідність запрограмованим і т. д.), які до недавнього минулого оброблялися сумірними можливостями самого мозку і паперових носіїв, а пізніше і за допомогою комп'ютерної техніки, величезних за швидкістю обробки можливостей. А остання є штучно створеними людиною неорганічними системами. В результаті більш ефективним стає умовний «мозок» людини, який сам по собі є унікальним інформаційним інструментарієм, ефективність якого на багато порядків перевищує все, що існує в біологічному світі. Це підтверджується мінімізацією зміни інформаційної ентропії для таких систем (див. таблицю 1).

Мурашині колонії зі своїм «колективним мозком», на відміну від людей і систем штучного інтелекту, мають набагато менший набір інформаційних інструментів. Це:

- тактильні органи чуття, їх у них не більше $6{,}5 \cdot 10^{-15}$ Дж/((К· с) інформаційних ентропійних витрат;

- феромонні залози, з їх $3{,}1 \cdot 10^{-14}$ Дж/((К· с) інформаційних ентропійних витрат;

- мінімальний набір потреб - харчування і біологічна підтримка, розмноження, безпека, що корелює з $1{,}8 \cdot 10^{-14}$ Дж/((К· с) інформаційного ентропійного навантаження. нагрузки.

Подібний мінімум споживаної інформації для мурашиних колоній робить їх уразливими за багатьма показниками життєздатності, на відміну від людини.

Можна зробити висновок, що інформаційна складова на рівнях організації людського суспільства, в тому числі і тих штучних інформаційних систем, які вже створена людиною, є можливим напрямком, в якому людина спроможна послідовно перевершити найбільш організовані біологічні системи, навіть незважаючи на те, що багатомільйонний досвід еволюції деяких з цих систем дозволяє розглядати їх ближче до оптимальних, у порівнянні з твореннями рук людських. У розвитку інформаційної складової людського буття вбачається перспектива її розвитку як симбіозу органічної та неорганічної речовини.

Повертаючись тепер до рис. 1, можна сформулювати логічне припущення, що якщо штучний інтелект завдяки своєму необмеженому кількісному інформаційному ресурсу досягне здатності оволодівати однією і тією ж унікальною властивістю – когнітивними взаємодіями, то швидкість його розвитку буде непорівнянною навіть у порівнянні з темпами розвитку людства. І наслідки такого еволюційного руху в значно коротші проміжки часу матимуть уже не характер еволюційного, а революційного розвитку, відкриваючи нові можливості для неорганічного світу, якщо продовжувати порівнювати його зі світом біологічного життя.

Відкритим залишається питання: чи зможуть системи штучного інтелекту, що володіють необмеженим інформаційним ресурсом і здатністю здійснювати найпростішу логічну екстраполяцію, оволодіти когнітивними механізмами пізнання і оцінки природної сутності, як це робить людина.

Висновки.

1. Запропонований показник ефективності, а саме зміна (зростання) ентропії, який може бути використаний для порівняння багатьох біологічних популяцій та окремих неорганічних систем на планеті, дозволяє розглядати такі системи дещо по-іншому, наприклад, з точки зору їх існування, співіснування та конкуренції.

2. Термодинамічна складова цього показника дозволяє судити про ті природні ресурси, які не використовуються людиною, і прикладом для яких є біологічні системи мурах або інші органічні системи.

3. Інформаційна складова ентропії на рівнях організації людського суспільства, в тому числі і тих інформаційних систем, які вже створила людина, є можливим напрямком, в якому він зможе послідовно перевершити найбільш організовані біологічні системи, незважаючи на те, що багатомільйонний досвід еволюції цих систем дозволяє розглядати їх ближче до оптимальних в порівнянні з твореннями рук людини.

4. Людина не може не погодитися з тим, що тільки відсутність когнітивного компонента в системах штучного інтелекту обмежує його розвиток, темпи якого і зараз перевищують темпи розвитку будь-яких інших біологічних систем на планеті.

1. Hölldobler B., Wilson E. O. The Superorganism: The Beauty, Elegance, and Strangeness of Insect Societies. W.W. Norton & Company New-York, 2009. P. 103–120.

2. Gordon, D. M. Ant Encounters: Interaction Networks and Colony Behavior. Front Cover. Princeton University Press, 2010. 152 p.
3. Волошин В. С., Азархов О. Ю. Чому людина починає програвати конкуренцію за термодинамічну нерівноважність, як фактор розвитку в навколишньому техногенному середовищі. Вісник Приазовського державного технічного університетуСерія: Технічні науки Вип. 49. Т. 2, 2024. С. 86-93.

В.С. Волошин

ЩОДО ПИТАННЯ ПРО ОЦІНКУ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ В ІНТЕРНЕТІ

Для того, щоб оцінити ступінь неправдивості або недостовірності інформації, в роботі пропонується звернути увагу на такий об'єктивний показник цієї інформації, як її ентропія. Це міра невизначеності або випадковості в повідомленні. Однак сама по собі ентропія не визначає, правдива чи хибна інформація. Однак це впливає на якість інформації, пов'язаної зі структурною надійністю і передбачуваністю, що може бути використано як ознака правдоподібності [1].

1. Правдива інформація часто має помірну ентропію, оскільки містить ієрархічно взаємопов'язане і структуроване, логічне і зв'язне подання даних, передбачувані зв'язки між частинами на основі знань про реальний світ;

2. Неправдива інформація може мати аномально високу або аномально низьку ентропію, що характеризується великою кількістю неструктурованих, незрозумілих і суперечливих фрагментів. Якщо ентропія близька до максимуму, то елементи однаково ймовірні, а повідомлення близьке до «шуму», до хаосу. Якщо ентропія близька до нуля, повідомлення є передбачуваним до точки примітивності.

Ентропія впливає на структурну когерентність інформації [2, 3]. Це не абсолютний критерій істини, але зміни структурної когерентності можуть бути показником потенційного обману, особливо якщо порівнювати з іншими структурами повідомлення.

Під структурною когерентністю інформації ми розуміємо ступінь зв'язності, узгодженості і логічності елементів повідомлення, яка виражається через впорядкованість розподілу інформації і зменшення несподіванок між частинами тексту. З точки зору інформаційної ентропії Шеннона, структурна когерентність - це нерівномірний, незначимий розподіл ймовірностей появи елементів, де кожне наступне повідомлення передбачувано в контексті попереднього, але не тривіально. Це підтверджується об'єктивністю сучасних систем штучного інтелекту, де лінгвістичні екстраполяції вербальних структур є головною об'єктивністю генерування нових зв'язних текстів.

Розглянемо приклад когерентного, помірно ентропійного, логічного повідомлення на кшталт: «*Економічне зростання країни збільшилося в другому кварталі, чому сприяло зростання внутрішнього споживання і стабільність на світових ринках*». Тут важливі такі параметри:

- передбачуваність, коли кожна наступна фраза логічно випливає з попередньої;

- помірна ентропія, заснована на виборі строго обмежених контекстом слів;

- висока когерентність пов'язана з причинно-наслідковими зв'язками між словосполученнями.

Допустимо, що $H_k(p)$ – ентропія Шеннона для когерентного висловлювання. Тоді *N(H)* – функція змістовної новизни (когерентності) що виявляється як

$$N(H) = -\left|H - H_{opt}\right| + const, \quad (1)$$

де $H_{opt} = log_2(p)$ - оптимальна (когерентна) ентропія явно нетривіального тексту.

У когерентному тексті, про який йде мова, всього 17 слів. Всі слова унікальні, ймовірність кожного p = 1/17 = 0,0588. Ентропія кожного слова $H_k(p) = -p \cdot log_2(p) = 0{,}2404$. Сумарна ентропія повідомлення $H = 17 \cdot 0{,}2404 = 4{,}0868$.

І наведемо приклад навмисно некогерентного, високоентропійного або хаотичного повідомлення: «*Розвиток переривається, автомобіль рухається, розвинена автомагістраль, розрив, початок, дорога, кінь, автомобіль*». Він має *хаотичну структуру* з низькою передбачуваністю, відсутністю зв'язності тексту, низькою когерентністю та логічними зв'язками. Для нього показник хаотичної функції можна визначити як

$$C(H) = -H \cdot D, \quad (2)$$

де $D -$ міра дисперсії розподілу хаосу.

У цьому хаотичному тексті всього 11 слів. Два слова повторюються, а 9 слів є унікальними. Для них $p_1 = \frac{2}{11} = 0{,}1818$ і $p_i = \frac{1}{11} = 0{,}0909$, а $\bar{p} = \left(\frac{1}{10}\right) \cdot \left(\frac{2}{11} + 9 \cdot \frac{1}{11}\right) = 0{,}1$. Дисперсія $D = \frac{1}{n}\sum(p_i - \bar{p})^2 = 0{,}0069$ є достатньо високою для такої вибірки. Сумарна ентропія заданого хаотичного виразу $H_h^{11} = -[0{,}1818 \cdot (-2{,}459) + 9 \cdot 0{,}0909 \cdot (-3{,}468)] = 3{,}2815$. Функція хаосу в повідомленні, про яке йде мова *C(H)*=−3.2815·0.0069≈−0.0226. Досить низьке і негативне значення вказує на високу випадковість в моделі повідомлення. Тобто розподіл слабо нерівномірний з невисокою інформаційною ентропією. Якби вираз мав більш нерівномірні частоти (наприклад, одне слово повторювалося 5 разів, інші по черзі) і ентропія залишалася високою, то хаотичність *C(H)* була б більш вразливою (∼-0,0854).

І проміжний приклад некогерентного, але низькоентропійного, шаблонного повідомлення: «*Китай зростає. Китай сильний. Китай завжди перемагає. Китай – найкращий*". Воно, перш за все, *банальне*, про що свідчить надмірна передбачуваність, низька ентропія, і, зокрема, формалізована, але не значуща зв'язність, що виражається в повторенні банальних гасел. Тут функція банальності зменшується зі збільшенням *H* за експоненціальною залежністю

$$B(H) = \exp(-\lambda H). \quad (3)$$

Банальний текст містить лише 9 слів: «Китай» – 4 рази: p=4/9=0,4444; $H_6^4 = -p \cdot log_2(p) = 0{,}52$. Інші п'ять слів, для кожного p=1/9=0,1111

$H_6^1 = -p \cdot log_2(p) = 0{,}3522$. Ентропія кожного слова $H_6^1 = -p \cdot log_2(p) = -0{,}0909 \cdot log_2(0{,}0909) = 0{,}3145$. Сумарна ентропія $H_6^9 = H_6^4 + 5H_6^1 = 0{,}52 + 5 \cdot 0{,}3522 = 2{,}281$.

Отже, обчислена ентропія для порівнянних текстів: когерентного - H=4,0868; хаотичного - H=3,2815; банального - H=2,281. Це свідчить про те, що семантична новизна (когерентність) - це максимум інформативності при її структурованому викладі. Інформаційна ентропія висока, але не максимальна. Хаотичний посил – це дезорганізованість, випадковість. Ентропія може бути високою, але сенс при цьому не читається. А банальний меседж – це надмірне повторення, гасла. Інформаційна ентропія низька, тому що елементи передбачувані і однотипні.

Таким чином, можна припустити, що неправдивість текстового повідомлення часто знаходиться в зонах надмірної випадковості (високий H і високий D) або банальності (низький H і високий рівень повторень). Істина може існувати в зоні структурованої новизни ($H \approx 3{,}8$ і $D \approx 1 \cdot 10^{-4}$). Відповідно, будемо розрізняти три типи режиму інформаційної структури (табл. 1).

Таблиця 1 – Режими інформаційних структур для повідомлень в межах прийнятих параметрів

Категорія інформації	Ентропія	Структура	Зв'язковість (когерентність)	Змістовна новизна	Типова неправда
Банальна	Низька	Повторюваність, шаблонність	Висока формально, але низька за змістом	Низька	Пропаганда, кліше
Хаотична	Висока	Випадкова, фрагментарна	Низька	Низька	Фальсифікація, дезінформація
Когерентна	Середня	Логічно впорядкована	Висока	Висока	Малоймовірна, частіше правда

Помітимо особливі моменти на досліджуваних залежностях (рис. 1), а саме, при H<3,5 випадковість інформації майже дорівнює нулю, а при H>3,5 випадковість інформації починає різко зростати. Це означає, що навіть висока інформаційна ентропія в поєднанні з відсутністю структури і високою дисперсією робить текст хаотичним, важким для читання і підозрілим до об'єктивності.

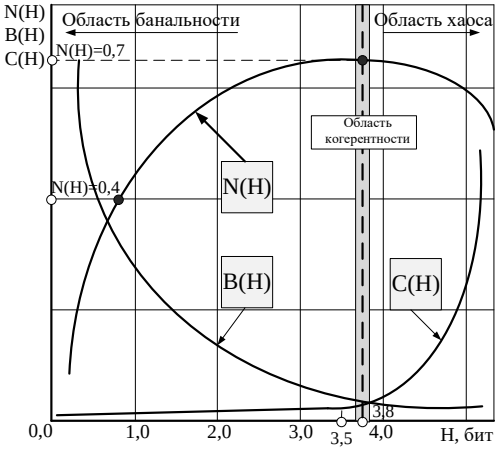

Рисунок 1 – Співвідношення зв'язного, банального і хаотичного в інформаційному просторі правди. Тут: $N(H)$– функція когерентності; $B(H)$- функція банальності; $C(H)$- функція випадковості

Вертикальна лінія, що проходить через H = 3,8 - це область максимальної новизни інформації, коли її банальність майже зникає, а хаос ще не настав. Такий діапазон значень ентропії може бути характерний для об'єктивно інформативних, логічних, зв'язних тверджень.

Безумовна відносність при цьому присутня.

Запропонований алгоритм пошуку та відрізнення неправдивих текстових повідомлень в мережі Інтернет за параметрами, що розглядаються, включає наступне (рис. 2).

Збір статистичних даних по текстовому повідомленню, з розбивкою тексту на окремі слова, словосполучення за змістовним значенням з визначенням частоти слів в угрупованнях. На основі цієї інформації про повідомлення розраховується ентропія структури тексту, оцінюються параметри когерентності *N*(*H*), банальності *B*(*H*), хаотичності *C*(*H*)) тексту в порівнянні з їх ентропією у відносних одиницях від 0,0 до 1,0. Такий алгоритм дозволяє аналізувати текстові повідомлення в мережі Інтернет на предмет їх достовірності в залежності від структурної ентропії тексту, використовуючи поняття зв'язності, банальності і випадковості інформації в повідомленні. Модель може бути представлена у вигляді скрипта на Python для конкретних рішень, що дозволяє розрахувати ентропію, зв'язність, банальність і випадковість Шеннона на основі статистики повторення слів у тексті, і зробити формалізовані висновки про його достовірність.

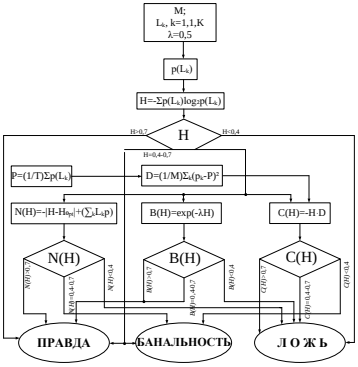

Рисунок 2 – Алгоритм пошуку неправдивої інформації в текстових повідомленнях. Тут: M – загальна кількість слів у повідомленні; L_k –кількість слів в k –ій групі однотипових слів; λ –коефіцієнт банальності висловлювання; $p(L_k)$ – частота слова в k –ій групі однотипових слів

Зі структури самого алгоритму видно, що найбільше число варіантів розподілу ентропії відноситься до хаотичних станів інформації з відносно низькою ентропією, що знаходяться в області інформаційної рівноваги.

Розглянемо кілька прикладів гіпотетичних повідомлень, вихідні дані і результати розрахунків для яких представлені в таблиці 2. Для умовного повідомлення з 128 слів, згрупованих у три приклади, ми обчислимо ентропійний стан кожного повідомлення та спробуємо формалізовано оцінити їх валідність

Таблиця 2 – Порівняльні дані інформаційно-ентропійного аналізу умовного повідомлення, що складається з 128 слів (під четвертим варіантом мається на увазі реальне текстове повідомлення)

Показник	Варіант 1	Варіант 2	Варіант 3	Oboz.ua
Структура груп Слів	12 × 2; 5 × 3; 5 × 4; 2 × 5.	**25 × 2; 1 × 3; 1 × 4; 2 × 5**	**25 × 2; 25 × 3**	128× 1; 34 × 2; 8 × 3; 7 × 4; 4 × 5; 3 × 6; 1 × 13
Число унікальних слів	59	61	3	185
Ентропія Шеннона *(H)*	6,14	6,33	5,66	7,228
Когерентність, *N(H)*	6,64 ($H_{opt} = 6.5; C = 7$)	6,83	6,16	0,6789
Банальність, *B(H)*	0,00216	0,00178	0,00345	7,5314
Дисперсія ймовірності *D*	0,60	0,55	0,30	0,0272
Хаотичність повідомлення, *C(H)*	-3,684	-3,480	-1,698	-0,000149
Інтерпретація достовірності	Помірно правдоподібна, частково шаблонна	Найбільш природня, збалансована	Малоймовірна, шаблонно-синтетична	С імовірністю 90% об'єктивне, не фейкове

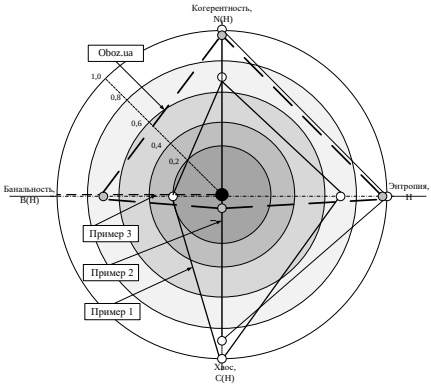

Рисунок 3 – Радар-графік для оцінки стану формалізованих повідомлень, що складаються з 128 слів в різних групах початкових сигналів (слів)

Очевидними є результатами аналізу рівнів довірчості змодельованих повідомлень за допомогою радар-графіків (рис. 3), на яких зображені всі три версії наших прикладів. Чим більша «площа» фігури на графіку, тим різноманітніша та збалансованіша інформація у повідомленні. Інформативність графіків полягає в наступному.

1. Друга версія повідомлення має найбільш рівномірний і найширший показник радіолокації, що свідчить про високу достовірність інформації. Вона має найвищу когерентність і ентропію, а також збалансовану випадковість, що в сукупності дає сигнал правдоподібності.

2. Варіант 3 повідомлення має компактну, лаконічну форму – ознака як мінімум інформаційної одноманітності. Він вирізняється дуже низькою хаотичністю та відносно високою банальністю – це ознака шаблонного, банального тексту.

3. Текст за варіантом 1 показав помірні значення за всіма показниками, що підтверджує його проміжну позицію.

На завершення розглянемо текст реального повідомлення, взятого зі стрічки новин українського контент-Oboz.ua за 01.06.2025. У повідомленні йдеться про питання енергозабезпечення України влітку 2025 року та про те, до чого українцям варто готуватися. Обсяг тексту становив 299 слів, включаючи 7 видів груп з однаковими словами по два, три і т.д. слів (див. табл. 3, остання колонка).

Результатом такого аналізу є судження про те, що це повідомлення від Oboz.ua 01.06.2025 є об'єктивним і далеким від хибності, принаймні в обсязі даних, які викладені в повідомленні.

Висновок. Запропонована методика оцінки рівнів неправдивості текстових повідомлень за прямими і непрямими показниками, незважаючи на її формалізацію, дозволяє в першому наближенні оцінити достовірність конкретних повідомлень та більш об'єктивно підходити до інформації в

мережі Інтернет, яка довгий час обходилася без критики і цензури, і має стійку тенденцію до розвитку фальшивості цілих інформаційних потоків. Такі підходи можуть бути корисними, зокрема, в наукових дослідженнях, при рецензуванні наукових статей і книг.

1. Peter Grunwald P., Vitányi P. Shannon Information and Kolmogorov Complexity. arXiv.org, 2004. 45 p.
2. Gray R.M. Entropy and Information Theory. 1990, США, Springer, 412 p.
3. Tishby N., Pereira F.C., Bialek W. The Information Bottleneck Method. 2000, США, arXiv.org. 10 p.

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

ЩОДО ЗАБЕЗПЕЧЕННЯ РЕЗИЛІЄНТНОСТІ НА ОСНОВІ ФОРМАЛЬНИХ МЕТОДІВ І ЗАСОБІВ ПРИ ПРОЄКТУВАННІ

Наявні свідчення дають підстави вважати, що здійснення контролю впливу людського фактору на артефакти процесу розроблення критичного програмно-алгоритмічного забезпечення (ПАЗ) із залученням формальних методів і засобів є обґрунтованим кроком [1], оскільки супроводжується дуальним корисним ефектом – і у частині виявлення можливих дефектів розроблюваного ПАЗ, і у контексті забезпечення самоконтролю розробників у розрізі підвищення ступеню довіри до відповідних результатів [2]. Показовими предметними областями, де функціонують комп'ютерні системи критичного призначення, на основі яких реалізуються предметно орієнтовані інформаційно-керуючі процеси, є, у тому числі, енергетика [3], транспортна галузь (системи керування рухом залізничного транспорту) [4, 5], аерокосмічна галузь [6] тощо.

У контексті означеного вище пропонується опрацьовувати засади забезпечення резилієнтності енергетичної інфраструктури на рівні розроблюваного ПАЗ комп'ютерних систем критичного призначення, на основі яких реалізується належне функціонування вказаної інфраструктури і відповідних компонентів, вже на ранніх етапах процесу розроблення. Увага зосереджується саме на етапі проєктування. Це рішення прийнято на тій підставі, що архітектурна складова (структура і міжкомпонентні зв'язки) розроблюваного ПАЗ формується безпосередньо на даному етапі.

Засади забезпечення резилієнтності пропонується реалізовувати і розвивати, виходячи із наступних основоположних позицій: залучення концепції структурно мінливої електроенергетичної системи [7], що дозволить належним чином реагувати на виклики і загрози, які постають перед енергетичною інфраструктурою України по причині неспровокованого повномасштабного вторгнення; використання дієвого формального методу перевірки на моделі TLC (TLA Checker), а також відповідних засобів – формалізму TLA+ темпоральної логіки дій TLA (Temporal Logic of Actions) Л. Лемпорта, алгоритмічної мови PlusCal, а також супутніх засобів автоматизації – у якості засобів забезпечення контролю артефактів проєктування ПАЗ за показником несуперечливості [8–11]. Такий крок дозволить розробнику/розробникам своєчасно виявляти і усувати прояви небажаного впливу людського фактору.

Дослідження проведено у рамках вирішення задач НДР 0125U000326 «Розвинення теоретичних засад формалізації подань процесів опрацювання оперативної інформації в енергетиці», виконуваної Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

1. Clarke, E. M., Grumberg, O., Kroening, D., Peled, D., & Veith, H. (2018). *Model checking* (2nd ed.). The MIT Press.
2. Shkarupylo, V., Blinov, I., Dusheba, V., & Alsayaydeh, J. A. J. (2023). Case driven TLC model checker analysis in energy scenario. *CEUR Workshop Proceedings*, 3392, 65–75. https://doi.org/10.32782/cmis/3392-6.
3. Pakonen, A. (2021). Model-checking I&C logics – insights from over a decade of projects in Finland. *Proc. 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, NPIC&HMIT 2021*. *American Nuclear Society (ANS)*, (P. 792–801). https://doi.org/10.13182/T124-34322.
4. Cheng, R., Chen, D., Song, H., Liu, H., & Cheng, H. (2025). Formal modeling and verification methods for the system requirement specifications of train control systems: a survey. *IEEE Transactions on Intelligent Transportation Systems*, 26(2), 1419–1440, https://doi.org/10.1109/TITS.2024.3513717.
5. Limbrée, C., Haxthausen, A.E., Gori, G., & Fantechi, A. (2025). Formal verification of railway interlockings: a compositional approach based on a library of pre-verified components / T. Margaria & B. Steffen (Eds.), *Leveraging Applications of Formal Methods, Verification and Validation. Application Areas. ISoLA 2024. Lecture Notes in Computer Science*, 15223. Springer, Cham., https://doi.org/10.1007/978-3-031-75390-9_9.
6. Chrszon, P., Maurer, P., Saleip, G. et al. (2025). Model checking of spacecraft operational designs: a scalability analysis. *Software and Systems Modeling*, https://doi.org/10.1007/s10270-025-01281-6.
7. Saukh, S.Ye. (2023). Concept of building a structurally variable power system of Ukraine. *Technical Electrodynamics*, 2023(5), 48–54, https://doi.org/10.15407/techned2023.05.048.
8. Lamport, L. (2002). *Specifying systems: The TLA+ language and tools for hardware and software engineers*. Addison-Wesley Longman Publishing Co., Inc.
9. Lamport, L. (2009). The PlusCal algorithm language / M. Leucker, & C. Morgan (Eds.), *Theoretical Aspects of Computing – ICTAC 2009. ICTAC 2009. Lecture Notes in Computer Science* (P. 36–60), 5684. Springer. https://doi.org/10.1007/978-3-642-03466-4_2.
10. Шкарупило, В. В., Душеба, В. В., Зайко, Т. А., Шкарупило, В. В., & Скрупський, С. Ю. (2024). Індуктивний підхід до побудови формалізованих подань програмно-алгоритмічного забезпечення при проєктуванні. *Вчені записки Таврійського національного університету імені В.І.Вернадського, серія «Технічні науки»*, 35(74), 4, 224–229. https://doi.org/10.32782/2663-5941/2024.4/33.
11. Шкарупило, В. В., Душеба, В. В., Зайко, Т. А., & Шкарупило, В. В. (2025). Ієрархічний підхід до варіювання рівня деталізації формальних специфікацій. *Збірник матеріалів XLIII Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, м. Київ, ІПМЕ ім. Г.Є. Пухова НАН України. (С. 130–131). https://ipme.kiev.ua/wp-content/uploads/2025/05/Materialy-KMV-2025.pdf

О.О. Ципляк, В.О. Артемчук

ВИКОРИСТАННЯ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ: ОГЛЯД РЕКОМЕНДАЦІЙ МІНІСТЕРСТВА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

Від моменту релізу моделі GPT-3.5 (листопад 2022 р.), стрімка популяризація генеративного штучного інтелекту призвела до його всебічного використання у більшості існуючих галузей. Вже станом на травень 2024 у 80 країнах світу існували державні та приватні ініціативи з глобального дослідження і використання генеративного штучного інтелекту. [2]. Досліджено і описано вплив генеративного штучного інтелекту на процеси у:

- медицині та психології [3];
- освіті на усіх рівнях [3];
- науковій діяльності [3];
- медіа та журналістиці [4];
- розробці програмного забезпечення [2].

Усі технології мають обмежене поле ефективного застосування та умови за яких їх використання не експертами може задіяти шкоду. І генеративний штучний інтелект не є винятком, особливо через психологічний ефект, відомий як «ілюзії глибини розуміння» [5].

Описаний у 2002 році Леонідом Розенблітом та Френком Кейлом феномен підмічає, що суб'єктивне відчуття розуміння окремою особою певного явища часто розходиться з її фактичною здатністю дати окреме роз'яснення. В контексті генеративного штучного інтелекту це спрацьовує у двох аспектах:

1) Ілюзія експертності у окремому, часто неправильно сформульованому, питанні - згенерований стислий текст на основі часто неідентифікованих та неавторитетних джерел, не є альтернативою експерту у конкретній області.
2) Ілюзія необмеженого авторитетного джерела істини – мовні моделі не оперують знаннями, а лише генерують текст з контексту питання. Помилка, яку містить згенерована відповідь і яку користувач не може перевірити, може переконати недосвідченого користувача в істинності хибного твердження.

Обидва ефекти посилюються комерційною зацікавленістю дистриб'юторів систем генеративного штучного інтелекту у тому, щоб кінцеві користувачі задавали якомога більше питань і якомога більше довіряли окремо взятій мовній моделі.

Через згаданий вище ефект з точки зору резильєнтності суспільних інститутів до популярності некоректного використання генеративного

штучного інтелекту - доцільним є інформування широкого загалу про принципи безпечної роботи з даною технологією.

Розглянемо і підсумуємо останню ініціативу із створення таких рекомендацій від Міністерства цифрової трансформації України, які поки ще не набули широкого розголосу.

У червні 2025 року було випущено «Рекомендації з відповідальної розробки систем із використанням технологій штучного інтелекту» [6]. Поданий в [6] матеріал схематично можна узагальнити у вигляді наступного рисунку (див. рис. 1).

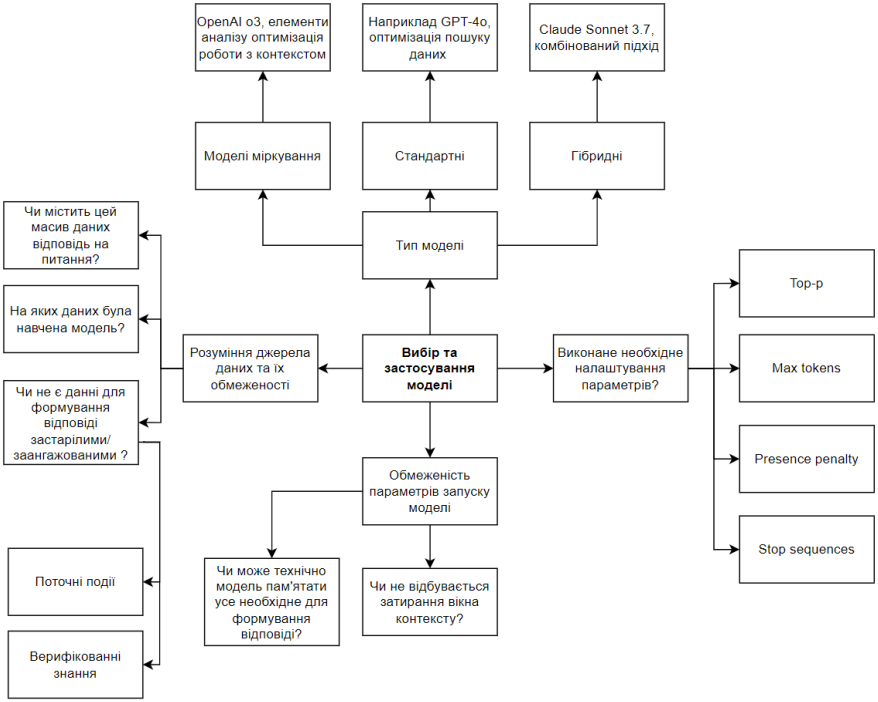

Рисунок 1 – Вибір та застосування моделі

Також, автори [6] рекомендують звертати увагу на умови використання кожної конкретної моделі та авторські права на згенерований контент: у деяких моделях усі права належать провайдеру моделі, у деяких випадках користувач несе юридичну відповідальність у разі застосування моделі до контенту, що захищається авторськими правами.

Окремо експерти в [6] посилаються на інтерактивну порівняльну таблицю від Microsoft, що має на меті допомогти користувачам обрати оптимальну модель під конкретну ситуацію [7].

Таким чином, використання великих мовних моделей трансформувало численні процеси у сучасному суспільстві. Простота використання даної технології призвела до відчуття феномену «ілюзії глибини розуміння» багатьма верствами населення, що не мають достатнього розуміння обмежень використання даної технології. Ініціатива Міністерства цифрової трансформації України надає ряд практичних рекомендацій, частину з яких було розглянуто у даній роботі.

Подальше дослідження буде сфокусовано на інших рекомендаціях Міністерства цифрової трансформації України для різних галузей та професій, а також вивченні міжнародного досвіду.

1. ChatGPT — Release notes. (n.d.). OpenAI Help Center. Retrieved June 6, 2025, from https://help.openai.com/en/articles/6825453-chatgpt-release-notes#h_bd3d8ef1eb.
2. Khan, N., Khan, Z., Koubaa, A., Khan, M. K., & Salleh, R. bin. (2024). Global insights and the impact of generative AI-ChatGPT on multidisciplinary: A systematic review and bibliometric analysis. Connection Science, 36(1). https://doi.org/10.1080/09540091.2024.2353630.
3. Shahzad, M. F., Xu, S., Liu, H., & Zahid, H. (2024). Generative Artificial Intelligence (ChatGPT-4) and social media impact on academic performance and psychological well-being in China's higher education. European Journal of Education, 60(1). https://doi.org/10.1111/ejed.12835.
4. Watson, S., Brezovec, E., & Romic, J. (2025). The role of generative AI in academic and scientific authorship: An autopoietic perspective. AI & Society. https://doi.org/10.1007/s00146-024-02174-w.
5. Rosenblit, L., & Keil, F. (2002). The misunderstood limits of folk science: An illusion of explanatory depth. Cognitive Science, 26(5), 521–562. https://doi.org/10.1207/s15516709cog2605_1.
6. Міністерство цифрової трансформації України. ШІ для розробників. – Київ, 2025. – 54 с.
7. Azure AI Foundry. (n.d.). https://ai.azure.com/explore/models/leaderboard.

С.В. Кулик, А.В. Давидюк

РЕЗИЛЬЄНТНІСТЬ В ПРОЦЕСАХ УПРАВЛІННЯ ДАНИМИ НАТО

Організація Північноатлантичного договору (НАТО) була заснована в 1949 році і являє собою групу з 32 країн Європи та Північної Америки, яка існує для захисту людей і території своїх членів. Альянс заснований на колективній обороні, тобто якщо атакують одного члена НАТО, нападу піддаються всі члени НАТО [1]. Для побудови ефективної колективної оборони критичну роль мають процеси управління даними. З огляду на зазначене 30 квітня 2025 року, НАТО опублікувала публічну версію своєї першої стратегії даних. Стратегія, узгоджена членами Альянсу в лютому 2025 року, спрямована на прискорення використання даних Альянсом для досягнення сумісності та інтеграції в усіх сферах діяльності [2].

Стратегія визначає, як краще збирати, зберігати та поширювати інформацію в Альянсі за єдиними стандартами. Вимоги створять захищену та ефективну екосистему обміну даними, де Альянс, промисловість і наукові кола зможуть безпечно отримувати доступ і співпрацювати, включно з моделями штучного інтелекту (AI) і машинного навчання (ML), забезпечуючи при цьому членам Альянсу контроль над своїми даними.

На фоні мінливого геополітичного ландшафту синхронізація між державами-членами НАТО ніколи не була такою важливою. Цифрові системи та всі стандарти та політики навколо них мають бути сумісними та безпечними в будь-який час, у будь-якому середовищі та за будь-якої класифікації. Вони повинні підтримуватися інфраструктурою, яка може еластично масштабуватися, щоб задовольнити непередбачуваний попит.

Роль головного комітету Ради НАТО з управління інформацією, управління даними та використання даних виконує Комітет цифрової політики (DPC) [3]. Стратегія даних для Альянсу (DaSA) встановлює амбітні цілі на 2030 рік, зосереджуючись на обробці даних, управлінні та навичках робочої сили. Стратегія даних для Альянсу має на меті прискорити перехід НАТО в орієнтовану на дані організацію, використовуючи якісні дані для бездоганної взаємодії та інтеграції в усіх сферах, надаючи вказівки щодо управління даними НАТО та оперативного їх використання для спільних і багатодоменних операцій. Інтеграція з ширшою Стратегією цифрової трансформації НАТО забезпечує узгодження з ключовими ініціативами, включаючи створення Екосистеми обміну даними Альянсу (ADSE) та цифрової магістралі НАТО [4].

ADSE в галузі оборони і безпеки підтримуватиме цифрову трансформацію НАТО і зусилля з швидкого запровадження технологій

подвійного застосування. Вона посилить існуючу спроможність підприємства НАТО, урядових агентств країн Альянсу, промисловості і науки, а також інших провідних зацікавлених сторін. Пілотний етап триватиме до кінця 2025 року, і спочатку буде зосереджений на відкритих і несекретних даних на підтримку наших пріоритетних сфер: безпеки критичної підводної інфраструктури; геопросторової інформації; оцінки інформаційного простору; і обізнаності про ситуацію на морі. Підключення ADSE до інших ініціатив з обміну даними, таких як постійне спостереження Альянсу з космосу, буде примножувати здатність НАТО використовувати дані і вести операції в різних сферах водночас [5].

Щоб підтримати ці зусилля, користувачі та програми перейдуть від ізольованих приватних сховищ даних до спільних просторів даних і об'єднаних мереж даних, які пропонують засоби для контрольованого обміну продуктами даних. Ці середовища спільного використання підтримуватимуться, захищатимуться та оптимізовані відповідно до вимог місії. Ця Стратегія підкреслює вимогу до узгодженого впровадження технологій і управління даними як стратегічних засобів для з'єднання окремих компонентів піраміди прийняття рішень на основі даних (рис. 1).

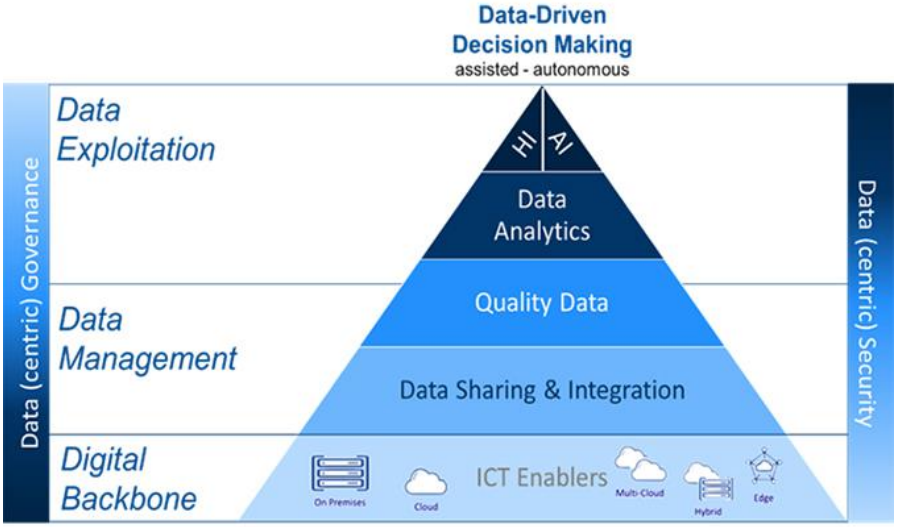

Рисунок 1 – Піраміда прийняття рішень на основі даних [4]

Метадані відіграють вирішальну роль у забезпеченні обміну даними. Щоб полегшити виявлення активів даних, користувачі та програми нададуть метадані для всіх даних, опублікованих у спільних просторах даних, відповідно до Специфікації основних метаданих НАТО (NCMS), яка стандартизована через STANAG 5636. NCMS надає загальний набір

структурованих атрибутів, які підтримують виявлення та ефективне використання ресурсів даних за допомогою інструментів пошуку. Виробники інформації визначатимуть бажаний рівень виявлення для активу даних. NCMS включає найкращі практики розробки метаданих від DCMI, Міжнародної організації стандартів, інших військових і цивільних стандартів метаданих. Метадані, пов'язані з безпекою, надаватимуться для кожного активу даних відповідно до STANAG 4774, щоб забезпечити контрольований доступ до активів, де прив'язка метаданих до даних визначена в STANAG 4778 [6]. Каталоги даних додатково підтримуватимуть сумісність шляхом рекламування та організації активів даних у спільнотах і в Альянсі за допомогою інтегрованого «каталогу каталогів». Ці об'єднані каталоги будуть доступні через веб-інтерфейси та API як для користувачів, так і для автоматизованих систем.

Крім того, DaSA створює цілісну структуру управління даними, яка узгоджує ініціативи через уніфіковану модель, сприяє розвитку ADSE та встановлює вимоги до підготовки військового та цивільного персоналу.

У цьому контексті DaSA зосереджується на двох основних сферах. По-перше, він консолідує поточну діяльність НАТО, пов'язану з даними, і визначає прогалини в переході Альянсу до підходу, орієнтованого на дані. По-друге, він реконтекстуалізує ці зусилля в рамках орієнтованого на дані управління та скоординованого управління даними для підтримки розвитку надійної екосистеми обміну даними.

Щоб досягти значущих результатів від ініціатив Альянсу щодо даних, у Стратегії визначено наступні стратегічні цілі:

1. управління даними;
2. цінність даних;
3. безпека, орієнтована на дані;
4. аналітична зрілість;
5. екосистема, керована даними [4].

Рівень кількох федерацій зацікавлених сторін у цифровій магістралі НАТО (NDBB) — це місце, де хмари різних зацікавлених сторін інтегрують, перетворюють і використовують дані. Для цього цим зацікавленим сторонам потрібні спільні служби безпеки, такі як Федеративна ідентичність та управління доступом (рис. 2).

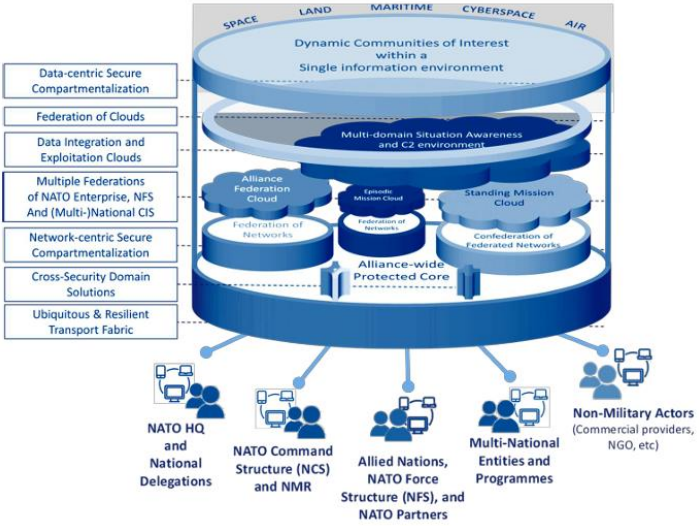

Рисунок 2 – Багаторівневе подання контекстної діаграми NDBB [7]

Контекст NDBB охоплює цифровий континуум, який з'єднує межу з тими, хто приймає рішення, і виконавцями. Політичні консультації, а також гібридний характер багатодоменних операцій вимагатимуть, щоб цифрова магістраль забезпечувала точку входу для загальнодоступних просторів даних та для інших невійськових суб'єктів, які діятимуть як джерела даних, надаючи дані цифровій магістралі (рис. 3).

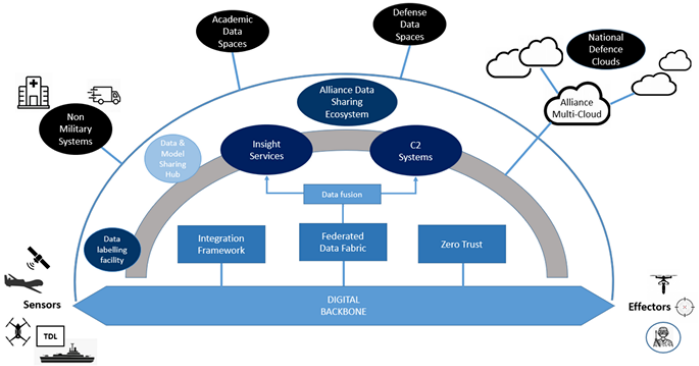

Рисунок 3 – Контекст NDBB [7]

Як приклад, щоб візуалізувати три основні виміри NDBB, слід розглянути уявний куб, який об'єднує різні осі, такі як «Операційний домен», «Рівні класифікації безпеки, а також несекретна інформація» та «Рівень ведення війни», і забезпечує потоки даних і співпрацю в цих вимірах (рис. 4).

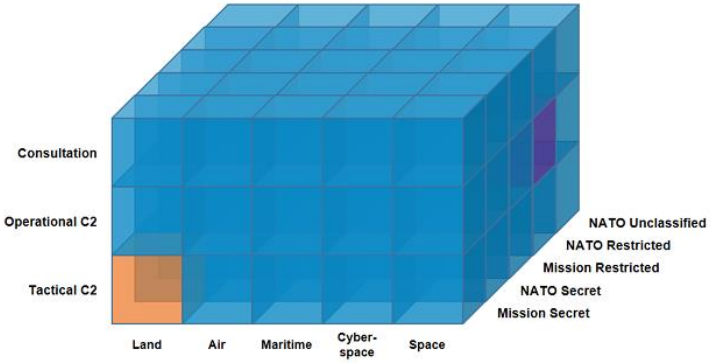

Рисунок 4 – Виміри NDBB [7]

З огляду на зазначене такий підхід має як сильні сторони, так певні виклики. До сильних можна віднести системність та стандартизацію, технологічність та гнучкість. Зокрема використання федеративної ідентичності та моделей управління доступом дозволяє підтримувати баланс між суверенітетом даних і спільним користуванням. Координація ініціатив на рівні Комітету цифрової політики (DPC) сприяє синхронізації стратегічних зусиль у межах Альянсу. Резильєнтності цієї системи сприяє децентралізація контролю, зокрема відсутність єдиного «центру довіри», який би став критичною точкою відмови. При збереженні загального середовища, кожен учасник має незалежну інфраструктуру аутентифікації. Метадані можуть бути оновлені без зміни основного контенту — адаптація до нових умов (наприклад, підвищення рівня загрози).

До викликів можна віднести те, що країни-члени Альянсу мають різні рівні цифрової зрілості, що ускладнює повну інтеграцію в єдину екосистему даних. Значна частина ADSE спирається на комерційні хмарні рішення, які є вразливими до кібератак, особливо в умовах гібридних загроз. Незважаючи на формальне впровадження інструментів автоматизації, ризики через слабку підготовку персоналу залишаються актуальними. Архітектура NDBB є складною й потенційно вразливою до дезінтеграції під час багатовекторних атак. Важливим є контрольоване делегування доступу навіть при змінах умов безпеки.

З досвіду війни в Україні розглянуті процеси управління даних можливо зробити більш резильєнтними, зокрема за рахунок використання децентралізованих рішень (Starlink, edge-комп'ютинг), що дозволило б зберегти доступ до критичних даних в умовах фізичних атак на центри обробки даних. В Україні громадянські ініціативи стали джерелами даних для прийняття оперативних рішень, що може бути масштабовано в рамках ADSE через окремі контури (досвід авторів, узагальнений з практики).

Враховуючи значні ризики кібератак доцільним є запровадження підходу нульової довіри (Zero Trust) у всіх сервісах обробки й обміну даними, включно з ADSE та NDBB. Також корисним є створення цифрових двійників критичних компонентів NDBB для моделювання відмов, атак і рішень у стресових ситуаціях. Додатково необхідним є масове впровадження програм з кібергігієни, управління даними та кризового реагування на базі бойового досвіду союзників.

Водночас для інтеграції в такі процеси НАТО Україні необхідним є прийняти та імплементувати стандарти STANAG 4774/4778, NCMS, STANAG 5636 для метаданих і контролю доступу до даних. Гармонізація законодавства про захист персональних даних, кібербезпеку та інформаційні потоки з директивами ЄС та політиками НАТО. Впровадити національний аналог ADSE — безпечної платформи спільного обміну даними між силовими, цивільними та партнерськими структурами. Адаптувати цифрові платформи до NDBB: підтримка API-сумісності, безперервного обміну та політик федеративного доступу. Постійно здійснювати відповідне навчання персоналу. Додатково корисною буде участь України в робочих групах DPC як спостерігача або асоційованого члена та створення платформи для технічного, правового та організаційного узгодження. Для повноцінної інтеграції з підходом НАТО Україна має перейти від окремих технологічних кроків до стратегічної цифрової доктрини. Це не лише відкриє шлях до членства в Альянсі, а й зміцнить кіберрезильєнтність держави.

Резильєнтність в управлінні доступом у НАТО — це не захищеність даних, а й здатність систем швидко адаптуватися, масштабуватися, самоорганізовуватися і працювати в умовах дестабілізації. Вона досягається через поєднання технологічної децентралізації, стандартизованих політик, гнучкого федеративного управління і політичної координації. Резильєнтність процесів управління даними в НАТО має міцне теоретико-технологічне підґрунтя, однак вимагає подальшого розвитку за рахунок адаптації до реальних загроз і практичного досвіду партнерів, зокрема України. Впровадження децентралізованих архітектур відкритих даних, Zero Trust моделей та навчання персоналу є критичними чинниками підвищення резильєнтності Альянсу в умовах нових загроз.

1. 10 things you need to know about NATO. (n.d.). NATO. https://www.nato.int/cps/en/natohq/126169.htm.
2. NATO releases strategy to use data for enhancing collective defence. (n. d.). NATO. https://www.nato.int/cps/en/natohq/news_234941.htm.
3. Comité des orientations pour le numérique (DPC). (n. d.). NATO. https://www.nato.int/cps/fr/natohq/topics_69279.htm.
4. Data strategy for the alliance. (n. d.). NATO. https://www.nato.int/cps/en/natohq/official_texts_234937.htm.
5. NATO steps up Alliance-wide secure data sharing. (n. d.). NATO. https://www.nato.int/cps/en/natohq/news_229523.htm.
6. Associate metadata with data assets. (n. d.). Access Denied. https://nhqc3s.hq.nato.int/apps/DCRA_Report/id-29d4122b072148f5aaf4882ecc5d963c/elements/id-1c7b9901-611e-11ef-4529-005056901351.html.
7. NATO digital backbone & nato digital backbone reference architecture executive summary. (n. d.). nato.int. https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf.

О.Ю. Будякова

СТАЛА БІОЕКОНОМІКА ДЛЯ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ДИНАМІЧНИХ ЕКОСИСТЕМ

Ризик невиконання Україною поставлених кліматичних цілей та зниження сільськогосподарського виробництва й як наслідок ризики для продовольчої безпеки обумовлюють пошук концепцій, здатних забезпечити резильєнтність в контексті адаптації екосистем [1].

Біоекономіка пропонує сталі рішення для підвищення резильєнтності та адаптації екосистем до військового екоциду під час воєнного стану та повоєнного відновлення України [1].

Поняття «резильєнтність» використовується в різних сферах для опису характеристик, які дають можливість системам або організаціям бути стійкими до впливу різних видів криз. Незважаючи на те, що існує безліч концепцій резильєнтності в різних сферах, погляди на те, що означає стійкість, також відрізняються в різних галузях.

Розрізняють консервативно-реактивне, адаптивне та трансформаційне розуміння резильєнтності. Така диференціація може призвести до суперечливих інтерпретацій при спробі проаналізувати та розвинути чинники стійкості для конкретного суб'єкта або системи, оскільки результати будь-якого з цих підходів будуть суттєво відрізнятися [2].

Для міждисциплінарних концепцій, таких як біоекономіка, це особливо актуально. Біоекономіка представлена як концепція стійкості, яка заснована на концепції сталого розвитку.

На основі оцінки біоекономіки як концепції, що базується на концепції резильєнтності та стійкості, система або суб'єкт господарювання повинні відповідати трьом критеріям, щоб продовжувати функціонувати в кризових ситуаціях: по-перше, вона повинна просувати концепцію резильєнтності другого порядку, тобто таку, що враховує інші контексти; по-друге, інтерпретація використовуваної концепції резильєнтності повинна бути прояснена – тобто, чи є вона консервативно-реактивною, адаптивною або трансформаційною; і, по-третє, вона повинна містити чітко визначену нормативну базу, яка буде сприяти її розвитку [2].

Концепція сталої біоекономіки виникла як перспективна основа для вирішення проблем, пов'язаних з виснаженням ресурсів, утворенням відходів та погіршенням стану навколишнього середовища. Біоекономіка зосереджена на сталому використанні біологічних ресурсів для виробництва товарів та послуг з одночасною мінімізацією негативних наслідків природним екосистемам та довкіллю. Замикаючи ресурсні цикли, зменшуючи залежність від невідновлюваних ресурсів та застосовуючи цілісний та відновлювальний підхід, стала циркулярна біоекономіка пропонує потенціал для переходу до більш резильєнтної та життєздатної економіки.

Стала біоекономіка визнає фундаментальну важливість збереження та відновлення природних екосистем у досягненні її цілей. Як складна та динамічна екосистема, природні ресурси є основою для сільськогосподарського виробництва, збереження біорізноманіття та переробки поживних речовин. Розуміння значення послуг природних екосистем в контексті сталої біоекономіки є ключовим для розробки ефективних стратегій та політик сталого управління ресурсами.

Стала біоекономіка пропонує теоретичний контекст для реорганізації та контролю природних ресурсів, продуктів харчування, переробної промисловості для досягнення сталого добробуту у гармонії з природою. Вимоги споживачів, екологічні виклики та відповідні інноваційні рішення, зміни в доступі до ресурсів є рушійними силами зростання економіки. Міжнародні практики впровадження на розвитку біоекономіки, інновації та науково-технічний прогрес, а також поєднання нанотехнологій, біотехнологій, технологічних інновацій, знання та зелений та цифровий перехід є драйверами даних процесів.

Основою біоекономіки є біомаса, й відповідно, біорізноманіття. Оскільки біорізноманіття впливає на здатність біологічних систем адаптуватися та змінюватися в мінливому середовищі, його збереження є критично важливим для забезпечення резильєнтності та стійкості біологічних ресурсів. Отже, для резильєнтності концепції біоекономіки потрібні діючі політики та стратегії щодо збереженні біорізноманіття.

Стала біоекономіка надає перспективне вирішення взаємопов'язаних суспільних проблем, таких як продовольча безпека та безпека харчування, залежність від викопного палива, дефіцит природних ресурсів, зміна клімату, захист екосистем, збереження біорізноманіття тощо, й водночас сприяє досягненню сталого економічного розвитку.

В усьому світі визнана нагальна потреба трансформувати світову економіку у все більш екологічно систему, яка спирається на природні активи, що потребують менше ресурсів або не використовують викопне паливо, відому як біоекономіка. Біоекономіка передбачає використання природних активів, методів і цінностей для виробництва товарів і пропонує рішення у всіх сферах економіки [3].

Стала біоекономіка спрямована на досягнення Цілей сталого розвитку, забезпечує продуктами харчування [4], вирішує проблеми зміни клімату та адаптації до них [5], водночас покращує якість життя, доступ до санітарії та чистої води, виробництво біоенергії, можливості працевлаштування та економічний розвиток [6] у сталий та інклюзивний спосіб.

Стала біоекономіка сприяє зеленій трансформації та зеленому переходу [7] різних сфер. До таких сфер належать промисловість, інновації, інфраструктура, екологічно чисті міста [8], виробництво біоенергії, біотоплива, свідоме споживання, захист довкілля тощо.

Більше п'ятдесяти країн вже зробили просування біоекономіки своїм головним пріоритетом. [9].

Ідея екосистемних послуг привертає все більше уваги останніми роками, проте її зв'язок з функціями природних екосистем та методами управління все ще недостатньо визначений. Функції екосистем та екосистемних послуг є важливими для виробництва продуктів харчування, скорочення викидів парникових газів та забезпечення додаткових екологічних перспектив. Сільське господарство надає пріоритет продуктивності над іншими функціями екосистем, такими як очищення води, зберігання вуглецю, збереженню біорізноманіття, поживних речовин тощо. Багато чинників впливають на дисбаланс у функціях екосистем.

Окрім продуктів харчування, плани біоекономіки спрямовані на збільшення сільськогосподарського виробництва непродовольчих товарів, таких як біоенергія та матеріали для заміни викопних ресурсів. Довгострокові перспективи розвитку біоекономіки та інші соціальні цілі потребують забезпечення балансу екосистемних послуг при одночасному зменшенні деградації екосистем. Щоб не поставити під загрозу ресурсозберігаючі цілі, виробництво біомаси має відповідати принципам ефективності використання ресурсів та резильєнтності динамічних екосистем.

1. Будякова, О.Ю. (2024). Біоекономічна резильєнтність в контексті адаптації екосистем. Резильєнтність динамічних систем, наук.-практ. конф. Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали (Київ, 27 грудня 2024 р.). Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 143-146.
2. Lenze, S. (2022). Bioeconomy as a Normative Concept of Resilience: Challenges and Opportunities. In: Lanzerath, D., Schurr, U., Pinsdorf, C., Stake, M. (eds) Bioeconomy and Sustainability. Springer, Cham. https://doi.org/10.1007/978-3-030-87402-5_18.
3. Anikwe, M. A. N., & Ife, K. (2023). The role of soil ecosystem services in the circular bioeconomy. Frontiers in Soil Science, 3, 1209100.
4. Будякова, О.Ю., & Дьяконов, І.О. (2023). Біоекономіка: перспективи розвитку агропромислового комплексу України для подолання продовольчої кризи. *Цифрова економіка та економічна безпека, 6*(06), 68-74. DOI: https://doi.org/10.32782/dees.6-13.
5. Будякова, О. Ю. (2024). Біоекономіка як перспективне вирішення проблеми зміни клімату . *Здобутки економіки: перспективи та інновації,* (10). https://doi.org/10.5281/zenodo.13924099.
6. Будякова, О.Ю. (2023). Біоекономіка як вектор інклюзивного економічного розвитку в формуванні людського капіталу. *Цифрова економіка та економічна безпека, 9*(09), 68-77. DOI: 10.32782/dees.9-12.
7. *Зелена трансформація та стала біоекономіка : монографія* / за наук. ред. А. А. Олешко, О. Ю. Будякової. Київ : КНУТД, 2024. 497 с. DOI 10.30857/978.617.7763.34.4 https://er.knutd.edu.ua/handle/123456789/27008.
8. Будякова, О. Ю. (2025). Смарт міста в контексті зеленого та цифрового переходу. *Наукові перспективи (Naukovì perspektivi)*, 1(55), 643–660.
9. Олешко, А. А., Будякова, О. Ю. (2024). Європейські знання для сталої біоекономіки в Україні: навч. посіб. Київ: КНУТД, 156 с. URL: https://er.knutd.edu.ua/bitstream/123456789/26220/1/EZSBU_NP_2024.pdf.

MILITARY OPERATIONS AS MISSION-RESILIENT SYSTEMS

The Concept **of Mission Resilience.** Multidisciplinary research on resilience suggests that this property stems from the dynamism of systems. Resilience works on many levels that are connected with each other. For individuals and households, it means being prepared and able to manage on their own during a crisis. Communities and local governments take care of resources, organize volunteers, and help keep people connected. At the national level, resilience is part of how infrastructure is managed, how security strategies are made, and how the country gets ready for emergencies. On the international level, alliances like NATO focus on working together and supporting each other to build stronger shared resilience [1].

According to [2], resilience is defined as: "The ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper." Shifting the vantage point from an organization to a mission reframes how we understand resilience. Instead of focusing on an organization's survival and adaptability, we now focus on the continuity and adaptability of achieving mission objectives, even in the face of disruptions.

Accepting this shift, we can accept following definition of mission's resilience as: "The ability of a mission *to continue achieving its essential objectives and functions under changing conditions, including disruptions, adversities, or high-impact events.*"

Fundamental Differences Between Military and Business Missions. The concept of "mission" in business and military operations shares similarities but diverges significantly in purpose, execution, and risk management approaches.

The first difference is a purpose of mission. In business, a mission typically defines the organization's long-term goals, values, and purpose. It serves as a guiding principle for decision-making and strategy, aiming to achieve market success, customer satisfaction, and sustainable growth. In military operations, a mission is a specific, time-bound objective that must be accomplished to achieve strategic or tactical goals. It often involves high-stakes scenarios where success or failure can have immediate and significant consequences.

The major difference is in risk management. In business, risk management focuses on identifying, assessing, and mitigating risks that could impact profitability, reputation, or operational efficiency. The approach is often proactive, with contingency plans and risk diversification strategies. In military operations, risk management is more dynamic and immediate. It involves assessing threats to personnel, equipment, and mission success in real-time. Decisions often require balancing acceptable risks against the potential for mission failure or loss of life.

Also there is a significant difference in *stakeholders* domain. Business missions prioritize stakeholders such as customers, employees, shareholders, and the community. The risks are managed to protect these interests while ensuring

long-term viability. Military missions prioritize national security, allied forces, and civilian safety. Risk management is geared toward minimizing casualties and achieving strategic objectives under challenging conditions.

Adaptability in a military context has significant limitations. Businesses often have the flexibility to adjust their mission or strategy based on market trends and external factors. Military missions are less flexible once initiated, as they are bound by strict operational plans and real-time decision-making. These constraints are crucial because adaptability is the cornerstone of resilience.

Mission-resilient approach to system's dynamics. The task of building the resilience can be attributed to the step 'plan', also tentatively called "Get Ready". This task can be divided into the following successive steps (Fig.1):

1) definition of critical system-wide mission objectives and key results
2) definition of critical operations for each critical objective or result
3) identification of critical risks for each critical operation
4) identification and prioritization measures to mitigate critical risks
5) implementation of mitigation measures.

This approach is the same for business and military missions. Prioritization of mitigation measures is a multifactorial task. Relaxation of the problem consists of choosing the strategy "maximum possible recovery in limited time" or "maximum possible recovery with limited resources", and the chosen strategy affects the identification where to focus efforts to build mission resilience. A well-known top-to-bottom approach to solve that problem using objectives and key results (OKRs) is depicted on the Fig. 3.

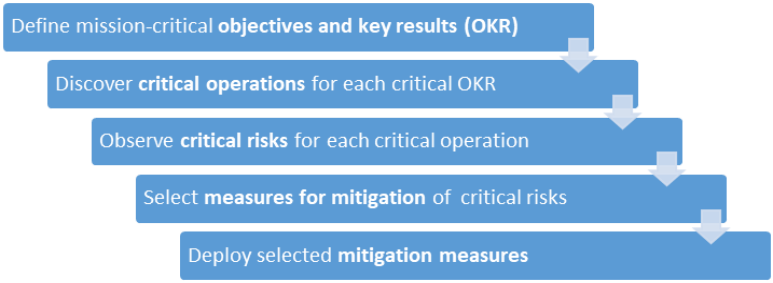

Figure 1: Mission-focused resilience built with OKR approach

'Risk to mission' and 'resilience by design' goals and processes are tightly intersecting and inseparable. But this makes it difficult to distinguish one from the other. In terms of risk management, here are higher-level Mission Essential Functions (MEF) and Mission Essential Tasks (MET). Both MEF and MET are among deliverables of threat analysis process and can be easily traversed to critical functions and critical operations.

Approaches to measurments of the resilience. Resilience analysis complements traditional risk analysis by shifting the focus from pre-event prevention to post-event adaptability. While risk analysis strengthens systems to withstand known threats, resilience analysis ensures that when failures occur, essential functions can continue operating by shedding or reallocating non-critical processes.

Without measurable indicators, it's difficult to assess resilience levels, justify investments, or guide decision-making during disruptions. Thus, in resilience analysis, implementing measurements, metrics, and KPIs is crucial to quantify system performance under stress, define acceptable degradation thresholds, and track improvements over time.

The definition of indicators requires the operationalizing resilience the objectives of each step. Then, for each objective, it is necessary to formulate key results that can be achieved through specific operations. The results will be the subject of assessment. Since operational resilience differs for different systems, sets of resilience metrics will also differ for different beneficiaries which use the resilience framework. The metric can be determined after passing the decomposition chain (Fig.2)

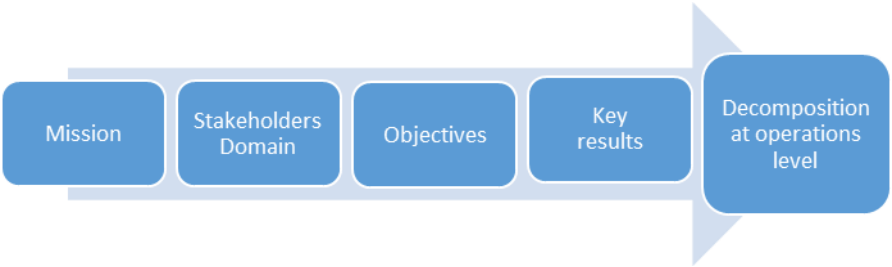

Figure 2: Stages of introducing the resilience into operations

Conclusion and future work. Concept of resilience has gained prominence, offering a more comprehensive view of risk management, focused on a system's ability to absorb and recover from harmful events. In military operations, resilience means being able to keep missions going even if cyber systems come under attack. It’s not just about strong systems—it also means being able to adapt, take a hit, and bounce back quickly. To do this, strategies should be used that make attacks harder and more expensive for the enemy, while also limiting the damage if something does go wrong. These ideas need to be part of every stage of planning and operations, from how systems are built to how they are used in the field.

This leads to challenges of big-picture defence. Given cyber as fifth domain of military operations since 2016, NATO allies haven’t yet cyber deterrence strategy. Modeling cyber operations as dynamic systems can help understanding if a new concept of ‘visible resilience’ [3] be a deterring trigger in cyber domain.

1. Christie, E. H., & Berzina, K. (2022). NATO and societal resilience: All hands on deck in an age of war [Policy Brief]. The German Marshall Fund of the United States. https://www.nato.int/.
2. ISO. (2024). ISO/DIS 22372:2024 - Security and resilience — Community resilience — Guidelines for resilient infrastructure. International Organization for Standardization.
3. Jonny Hall & Hugh Sandeman. NATO's Resilience: The first and last line of defence. LSE IDEAS Strategic Update. May 2022. URL: https://www.lse.ac.uk/ideas/Assets/Documents/updates/2022-SU-NATO-HallSandeman.pdf/.

А.В. Бойченко, В.Р. Сенченко

ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ БОЙОВИХ СИСТЕМ ЕНЕРГОПОСТАЧАННЯ

Бойові системи енергопостачання (БСЕ) вирізняються підвищеними вимогами до живучості, мобільності та автономності, оскільки функціонують у високоризикових, динамічних умовах бойових дій. БСЕ мають забезпечувати стабільне енергоживлення критично важливих об’єктів, таких як пункти управління, системи зв’язку, вогневі засоби, радіо-електроггої боротьби (РЕБ) та безпілотні літальні апарати (БПЛА). Енергетична інфраструктура має бути захищеною від впливу перешкод, навмисного ураження, кібератак, а також мати можливість швидкого переміщення або розгортання в польових умовах.

За останні роки кількість наукових публікацій, присвячених БСЕ, суттєво зросла. Це зумовлено як глобальними змінами в характері сучасних воєнних конфліктів, зокрема досвідом України, яка стикається з масованими атаками на енергетичну інфраструктуру. Дослідження охоплюють як теоретичні аспекти, так і практичні методи підвищення живучості систем енергозабезпечення у воєнних умовах, зокрема шляхом впровадження нових технологій захисту, резервування та швидкого відновлення енергопостачання [1, 2].

У міжнародній науковій спільноті опубліковано чимало статей, присвячених аналізу життєвого циклу, оптимізації резервних джерел живлення, впровадженню мікромереж та інтеграції відновлюваних джерел енергії для підвищення стійкості військових об’єктів. Наприклад, у дослідженнях [3, 4] розглядаються методики оцінки та порівняння понад сорока різних архітектур енергетичної резильєнтності для військових баз, а також використання сучасних інструментів моделювання, системного аналізу та машинного навчання для виявлення вразливостей і оптимізації процесів відновлення

Особлива увага приділяється системи живлення БПЛА та РЕБ, які є високоенерговитратними та критичними для ведення розвідки, наведення та вогневого ураження. БПЛА вимагають легких, швидкозарядних джерел енергії або мобільних пунктів заряджання, зокрема на основі акумуляторних батарей, сонячних панелей або генераторів. РЕБ потребують стабільного, безперебійного джерела енергії з високими показниками потужності та захисту від імпульсних електромагнітних впливів, що вимагає використання дизель-генераторів з фільтрацією, акумуляторних буферних систем та стабілізаторів напруги.

Крім технічних об'єктів, системи енергопостачання бойових госпіталів, польових штабів і пунктів життєзабезпечення повинні гарантувати постійну подачу електроенергії навіть у випадках повного знеструмлення регіону. Важливо забезпечити резервування (двох- або триконтурне), автоматичне

перемикання джерел живлення, а також енергетичну безпеку для медичного обладнання і засобів зв’язку. Для цього необхідні дизель-генераторні установки, джерела безперебійного живлення, акумуляторні блоки та можливість під’єднання до зовнішніх джерел.

Оскільки БСЕ мають інтегруватися у загальну структуру управління бойовими операціями, пропонується виділити системи стратегічного, оперативного та тактичного рівнів, відповідно до масштабу операцій та потреб підрозділів.

На тактичному рівні головна увага приділяється мобільності, компактності та швидкому розгортанню. Це включає живлення окремих солдатів (портативні акумулятори для радіостанцій, приладів нічного бачення), невеликих груп (портативні генератори для зарядки БПЛА або роботи тимчасових пунктів зв'язку), а також легких бойових машин. Ключовими характеристиками тут є низька вага, мінімальний шум, ефективність при малих навантаженнях, використання взаємозамінних та уніфікованих д жерел енергії для спрощення логістики та ремонту.

На оперативному рівні БСЕ забезпечують діяльність військових частин, штабів, польових госпіталів, мобільних РЛС та артилерійських комплексів. Тут використовуються потужніші та стійкіші джерела енергії, такі як дизельні та газотурбінні генератори середньої та великої потужності, здатні забезпечувати безперебійне живлення протягом тривалого часу. На оперативному рівні зростає важливість резервування та дублювання, а також впровадження інтелектуальних систем управління для оптимізації споживання та моніторингу стану обладнання. Енергетична автономність є критично важливою, оскільки об'єкти часто розташовуються далеко від централізованих енергомереж.

Стратегічний рівень охоплює БСЕ, які забезпечують потреби великих угрупувань збройних сил та стратегічно-важливої критичної інфраструктури. До них належать великі польові енергетичні центри, мобільні електростанції, резервні потужності об’єктів стратегічного значення, а також системи інтеграції з цивільною енергетичною інфраструктурою. Вони забезпечують стабільність енергопостачання для оперативно-тактичних угруповань, центрів прийняття рішень, систем ППО, а також інфраструктури тилу й логістики.

На нашу думку основою для проектування стійких і гнучких БСЕ, здатних ефективно функціонувати в умовах бойових дій, атак противника та інформаційного тиску є наступні умови:

- автономність енергетичних модулів;
- багаторівневе резервування;
- інтеграція з бойовим управлінням;
- мобільність;
- масштабованість архітектури;
- захищеність від кіберзагроз;

– здатність до швидкого відновлення.

Розглядаємо БСЕ як мережу з трьома підграфами: стратегічним GS, оперативним GO та тактичним GT. Кожен рівень описується:

1) Вузлами: V={v1,...,vn} (дизель-генератори, підстанції, акумулятори).

2) Ребрами: E (фізичні/інформаційні зв'язки).

3) Вагами ребер: w(e) (пропускна здатність, час реагування).

Визначимо критерії резильєнтності для кожного рівня.

Стратегічний: RS=1−d/v,

де v – загальна кількість вузлів d – кількість зруйнованих.

Оперативний: RO=min(A1,A2,...,An),

Ai = fi/(fi+ri) − доступність і-ї підсистеми оперативного рівня (наприклад, генераторної групи, підстанції, системи зв'язку),

де fi − середній час між відмовами, ri − середній час відновлення.

Тактичний: RT = q/p,

де q – час автономної роботи, p – планова вимога

Інтегральний показник:

R=αRS+βRO+γRT ,

ваги – (α+*β*+*γ=1)*.

Однією з найнебезпечніших загроз для БСЕ може бути системне перевантаження. У випадку виходу з ладу одного джерела живлення, решта компонентів зазнають надмірного навантаження, що може призвести до пришвидшення зносу обладнання або аварійного вимкнення. Це особливо критично в бойових умовах, де висока динамічність подій потребує стабільної енергетичної підтримки. Відсутність ефективних механізмів балансування та автоматичного регулювання енергопостачання збільшує ризики неконтрольованих збоїв.

В Інституті проблем реєстрації інформації НАН України створено моделюючий комплекс для дослідження сценаріїв управління складних територіально-розподілених систем управління. Одним з напрямків досліджень є виникнення та розвиток каскадних ефектів. Каскадні ефекти в БСЕ можуть виникнути, коли збій в одному компоненті спричиняє серію пов'язаних відмов в інших частинах системи. Моделювання дозволить прогнозувати поведінку БСЕ в умовах бойового навантаження, атак чи відмов. За допомогою агентно-орієнтованих та мережевих моделей передбачається відтворити сценарії втрат вузлів, перевантаження, порушення зв'язків та перевірити ефективність резервування й перерозподілу потужностей. Це дозволить приймати обґрунтовані рішення щодо конфігурації системи, визначення критичних точок і оптимізації структури БСЕ для різних бойових завдань. [5, 6].

Використання засобів штучного інтелекту (ШІ) дозволить підвищити ефективність моделювання БСЕ. Зокрема, методи глибокого навчання та аналізу часових рядів, дозволяють прогнозувати споживання енергії, виявляти аномалії у роботі генераторів чи акумуляторів, передбачати можливі відмови або атаки. ШІ-системи можуть автоматично

перерозподіляти енергетичні потоки, ізолювати пошкоджені ділянки, запускати резервні модулі або координувати роботу між тактичними, оперативними та стратегічними рівнями енергетичної мережі. ШІ-рішення забезпечують цифрових двійників БСЕ – віртуальні копії енергетичних систем, що функціонують паралельно з реальними та постійно оновлюються. Це уможливить тестувати наслідки можливих загроз чи втручань, оцінювати ефективність контрзаходів і підтримувати готовність системи до дій у змінному бойовому середовищі. Таким чином, комбінація моделювання та ШІ забезпечить передумови для побудови резильєнтної інфраструктури, здатної зберігати функціональність навіть у критичних ситуаціях. [7,8].

1. Lyons, J. W., Chait, R., & Valdes, J. J. (2011). Assessing the army power and energy efforts for the warfighter. Center for Technology and National Security Policy, National Defense University.
2. Barry, N., & Santoso, S. (2022). Modernizing Tactical Military Microgrids to Keep Pace with the Electrification of Warfare. Military Review.
3. Kwak, K., Kwak, D., & Yoon, J. (2015). Design of instantaneous high power supply system with power distribution management for portable military devices. Journal of Power Sources, 288, 328-336.
4. Mallery, J., Van Bossuyt, D. L., & Pollman, A. (2022). Defense installation energy resilience for changing operational requirements. Designs, 6(2), 28.
5. Бойченко А.В., Сенченко В.Р. Дослідження взаємозв'язків об'єктів критичної інфраструктури. Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023». Збірник матеріалів конференції. Київ. 2023. – с. 102-103.
6. Бойченко, А. В., & Сенченко, В. Р. (2023). Підхід до моделювання геопросторових каскадних ефектів критичних інфраструктур. Інформаційні технології та безпека. 56(7). – с. 35-40.
7. Сенченко, В. Р., Бойченко, А. В., Коваль, О. В., Бисько, Р. М., & Хоменко, О. М. (2024). Огляд методів і технологій сценарного аналізу каскадних ефектів. Реєстрація, зберігання і обробка даних, 26(1), 24-54. DOI: 10.35681/1560-9189.2024.26.1.308506.
8. 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.

С.Б. Бурченко, І.І.Сватовський

ЗАСТОСУВАННЯ СУЧАСНИХ ІННОВАЦІЙНИХ ІТ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ РЕЗИЛЬЄНТНОСТІ ДИНАМІЧНИХ СИСТЕМ

У сучасному світі, де зростає кількість і масштабність природних катастроф, кіберзагроз та системних криз, концепція резильєнтності набуває особливої актуальності. Поняття резильєнтності означає здатність систем не лише витримувати дію негативних зовнішніх факторів, а й швидко адаптуватися та відновлюватися після них. Резильєнтність системи є комплексною характеристикою, яка охоплює: стійкість до збоїв (fault tolerance); швидке відновлення після аварій (disaster recovery); автоматичну самокорекцію; масштабованість; адаптивність до змін навколишнього середовища; кібербезпеку. Особливо важливо це для **динамічних систем**, які постійно змінюються, мають розподілену архітектуру, взаємодіють із великою кількістю користувачів, даних і зовнішніх сервісів.

У цьому контексті застосування **сучасних інноваційних ІТ-технологій** стає не просто доцільним, а необхідним. Це стосується як фізичної інфраструктури, так і соціотехнічних систем. Результати сучасних досліджень підкреслюють зростаючу важливість адаптивної здатності до трансформації подібних систем для підвищення їхньої власної стійкості до впливу критичних умов функціонування. Забезпечення резильєнтності стає стратегічною метою як для урядів, так і для бізнесу, критичної інфраструктури та оборонних систем. Резильєнтна система може продовжувати працювати навіть у разі часткових відмов, атак або масштабних змін у навантаженні.

Застосування штучного інтелекту (ШІ) для моніторингу, прогнозування та управління динамічних систем стає ключовим інструментом для забезпечення їх резильєнтності. Завдяки можливостям ШІ можна:

- Аналізувати великі обсяги даних у реальному часі для виявлення аномалій та потенційних загроз;
- Прогнозувати розвиток кризових ситуацій, таких як екстремальні погодні явища, з високою точністю;
- Автоматизувати процеси реагування та управління в умовах надзвичайних ситуацій;
- Адаптувати системи до нових умов;
- Виявляти кібератаки на інформаційну інфраструктуру (наприклад, шляхом аналізу мережевого трафіку та аномалій поведінки системи);
- **Автоматизувати відновлення** систем на основі використання ШІ.

Технології великих даних (Big Data) повинні бути основою для прийняття рішень. Аналіз Big Data дозволяє:

- Інтегрувати інформацію з різних джерел (сенсори, соціальні мережі, супутникові знімки і т.п.) для створення повної картини ситуації;
- Виявляти приховані закономірності та взаємозв'язки, що сприяє більш точному прогнозуванню ризиків;
- Підтримувати прийняття рішень у реальному масштабі часу, особливо в умовах апріорної невизначеності.

Аналіз результатів сучасних досліджень показує, що використання великих даних у поєднанні з ШІ значно підвищує ефективність управління ризиками та реагування на надзвичайні ситуації .

Застосування інших сучасних технологій, таких як: цифрові двійники, IoT, хмарні та edge-обчислення, квантови обчислення, дозволяє додатково підсилити можливості резильєнтності динамічних систем.

Цифрові двійники (Digital Twins). Це віртуальні копії фізичних об’єктів або систем, які дозволяють відслідковувати стан, моделювати зміну поведінки у кризових умовах та оцінювати ефективність сценаріїв реагування. Цифровий двійник енергетичної мережі може виявити, як аварія на підстанції вплине на стабільність системи в інших регіонах.

IoT (Інтернет речей). Це масивна сукупність датчиків, що з'єднані в єдину мережу, дозволяють постійно фіксувати параметри стану об'єктів, що є основою для раннього виявлення відхилень (наприклад, тиск у трубопроводах або навантаження на мости).

Хмарні обчислення та технології дозволяють масштабувати обчислювальні потужності за потреби. Edge-обчислення передбачає обробку даних не в хмарі, а на місцевих вузлах - це зменшує час реакції, особливо в умовах перебоїв зв’язку чи дій ворожих атак.

Використання квантових комп’ютерів з відповідними алгоритмами дозволяють швидко знаходити оптимальні рішення для динамічних систем. У поєднанні з іншими ці технології створюють багаторівневу архітектуру, здатну до автономної адаптації.

Системи раннього попередження: запобігання та реагування на негативні зовнішні фактори. Системи раннього попередження (СРП) є критично важливими для мінімізації наслідків надзвичайних ситуацій. СРП забезпечують своєчасне інформування про наближення загроз (повені, землетруси, урагани). Також вони дозволяють вжити превентивних заходів для захисту населення та інфраструктури і підвищити загальну готовність суспільства до реагування на надзвичайні ситуації.

За даними Всесвітньої метеорологічної організації, ефективні СРП можуть зменшити шкоду від катастроф на 30% .

Таким чином, можна зробити висновок, що інтеграція інноваційних технологій - ШІ, аналізу великих даних, цифрових двійників, IoT, хмарних та edge-обчислень, квантових обчислень та системи раннього попередження - є ключовою для підвищення резильєнтності сучасних динамічних систем. Реалізація такого комплексного підходу дозволяє не лише ефективно реагувати на загрози, а й адаптуватися до них, забезпечуючи стійкий

розвиток суспільства в умовах постійних змін. У п**ерспективі** подальший розвиток технологій, зокрема квантових обчислень і автономних систем, відкриває нові можливості для підвищення резильєнтності.

1. Pasupuleti, M. K. (2024). AI and Big Data for Climate Resilience: Predictive Analytics in Environmental Management. International Journal of Academic and Industrial Research Innovations.
2. Texas A&M University. (2023). Leveraging Big Data and AI for Disaster Resilience and Recovery.
3. NIST Special Publication 800-190 – Application Container Security Guide
4. Google Site Reliability Engineering (SRE) Books
5. Chaos Engineering Principles by Gremlin Inc.
6. IEEE Transactions on Resilient Computing and Systems.

О.А. Снєосіков, О.П. Нарєжній

МОДЕЛЬ ЗАГРОЗ ТА МОДЕЛЬ ПОРУШНИКА АВТОНОМНОЇ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ

Глобальні навігаційні супутникові системи (GNSS) є фундаментальною складовою сучасної критичної інфраструктури, забезпечуючи функціонування широкого спектра галузей, зокрема цивільної авіації, морської навігації, транспорту, геодезії, енергетики, фінансових систем, телекомунікацій, оборонної сфери та інших секторів, де ключового значення набувають як точне позиціонування, так і високоточна синхронізація часу [1,2]. Незважаючи на широку інтеграцію GNSS-технологій, базова точність відкритих сигналів не завжди задовольняє зростаючі вимоги сучасних високотехнологічних застосувань та операційних середовищ. З метою підвищення точності координатних і часових параметрів у реальному часі застосовуються функціональні надбудови GNSS - системи диференціальної корекції (DGNSS) [3]. Такі системи реалізуються у вигляді програмно-апаратних комплексів, що обробляють дані з мережі наземних контрольно-коригуючих станцій (ККС), обчислюють поправки та передають їх користувачам через веб сервер високої доступності, забезпечуючи високоточне позиціонування незалежно від сторонніх сервісів.

Відповідно до чинного законодавства України, зокрема Закону України «Про критичну інфраструктуру» № 1882-IX від 15 листопада 2021 року, системи диференціальної корекції, як складова частина GNSS, відносяться до об’єктів критичної інфраструктури, де у переліку критично важливих сфер визначено «космічну діяльність, космічні технології та послуги» як одну з таких галузей [4].

Сучасні глобальні навігаційні супутникові системи (GNSS) залишаються вразливими до широкого спектру кіберзагроз, що потенційно загрожують їх стабільному функціонуванню. До найбільш критичних загроз як для базових GNSS, так і для систем диференціальної корекції (зокрема автономних систем диференціальної корекції - АСДК), належать:

- Глушіння сигналу (GPS jamming): навмисне створення перешкод у діапазонах частот GNSS з метою повного або часткового блокування прийому супутникових сигналів, включно із сигналами, які надходять до контрольно-коригуючих станцій (ККС);
- Спуфінг сигналу (GPS spoofing): генерація фальсифікованих навігаційних сигналів з метою введення в оману приймачів GNSS, зокрема ККС.
- Кібератаки на наземну та хмарну інфраструктуру GNSS: впливи на мережеві та обчислювальні ресурси систем обробки, зберігання, передавання й управління даними, а саме:
    - DDoS-атаки: масовані розподілені атаки, спрямовані на виведення з ладу серверів обробки диференціальних поправок.

- Атаки на програмне забезпечення: експлуатація вразливостей у програмному забезпеченні ККС і центрів обробки даних, включно з переповненням буферу та виконанням шкідливого коду.
- Фізичний вплив: несанкціонований доступ або знищення компонентів наземної інфраструктури.

У 2021–2025 роках активно досліджуються методи виявлення атак GPS jamming та GPS spoofing на GNSS, зокрема із застосуванням машинного та глибокого навчання [5-6]. Однак більшість робіт фокусуються на сигнальних аспектах безпеки GNSS, приділяючи недостатньо уваги специфічним кіберзагрозам для наземної інфраструктури DGNSS. Навіть у звітах ENISA [7] та CrowdStrike [8] загрози для систем диференціальної корекції розглядаються лише поверхово. Існуючі моделі загроз (STRIDE, DREAD, VAST, PASTA, OCTAVE, LINDDUN) [9] та стандарт IEC 62443 лише частково охоплюють специфіку DGNSS-інфраструктури.

Отже, у сучасних дослідженнях спостерігається суттєва недостатність уваги до питань моделювання загроз та порушників стосовно систем диференціальної корекції GNSS. Це зумовлює актуальність розробки формалізованих моделей загроз і порушників, які враховують специфіку архітектури автономних DGNSS, особливості протоколів передачі поправок, вразливості програмного забезпечення та можливі сценарії атак.

Метою цієї роботи є побудова формалізованих моделей кіберзагроз та порушника для автономних систем диференціальної корекції (АСДК). Проведено аналіз існуючих методів моделювання загроз та їх застосовності до архітектури автономних DGNSS (STRIDE, DREAD, VAST, PASTA, OCTAVE, LINDDUN). Запропоновано модель загроз, що враховує особливості протоколів передачі поправок, вразливості контрольно-коригуючих станцій, мережевих вузлів, веб-сервера та клієнтського програмного забезпечення. Розроблено модель порушника з урахуванням рівня доступу, технічних можливостей і мотивації атакуючих суб'єктів. На основі моделей визначено типові сценарії атак з оцінкою наслідків та обґрунтованими контрзаходами. Для формалізації використано міжнародні стандарти ISO/IEC 27001, NIST SP 800-30/53, IEC 62443 та національні НД ТЗІ 2.5-004-99 і 2.5-005-99.

З урахуванням архітектурних особливостей АСДК запропоновано комбінований підхід до формалізації моделі загроз, що інтегрує переваги кількох існуючих методик і забезпечує одночасно високий рівень деталізації атак і комплексне охоплення вразливостей усіх компонентів системи на архітектурному рівні:

- PASTA - забезпечує побудову сценаріїв атак з урахуванням бізнес-цілей, моделі порушника, технічної архітектури та ризик-орієнтованого підходу, що є актуальним для складних об'єктів критичної інфраструктури.

- MITRE ATT&CK - надає деталізовану базу тактик, технік та процедур (TTPs), характерних для реальних атакуючих, з фокусом на OT-системи, мережеву, хмарну інфраструктуру та програмні компоненти ІКС АСДК.
- STRIDE - застосовується для початкової класифікації загроз та ідентифікації базових категорій уразливостей кожного компоненту архітектури.

Висновки

У роботі проведено формалізацію моделі загроз та порушника для автономних систем диференціальної корекції GNSS з урахуванням сучасних кіберзагроз зокрема до наземної інфраструктури. Запропонований комбінований підхід, що інтегрує PASTA, MITRE ATT&CK та STRIDE, дозволяє забезпечити комплексний аналіз вразливостей на архітектурному, технічному та процедурному рівнях. Використання міжнародних та національних стандартів забезпечує відповідність моделі сучасним вимогам з інформаційної безпеки. Отримані результати можуть бути застосовані для розробки систем захисту, виявлення атак та підвищення кіберстійкості автономних DGNSS як елементів критичної інфраструктури.

1. European Union Agency for the Space Programme // EUSPA EO and GNSS Market Report. 2024. Iss. 2. LU: Publications Office, 2024. URL: https://data.europa.eu/doi/10.2878/73092/.
2. Precision Matters: Exploring the Importance of GPS Precision Accuracy. Taoglas. 20.07.2024. URL: https://www.taoglas.com/blogs/precision-matters-exploring-the-importance-of-gps-precision-accuracy.
3. DGNSS Fundamentals - Navipedia. URL: https://gssc.esa.int/navipedia/index.php?title=DGNSS_Fundamentals.
4. Про критичну інфраструктуру // Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/go/1882-20/.
5. Ghanbarzade A., Soleimani H. GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning. arXiv, 2025. DOI:10.48550/arXiv.2501.02352.
6. Radoš K., Brkić M., Begušić D. Recent Advances on Jamming and Spoofing Detection in GNSS. Sensors. Vol. 24, № 13. С. 4210. DOI:10.3390/s24134210.
7. European Union Agency for Cybersecurity., Space threat landscape. LU: Publications Office, 2025. URL: https://data.europa.eu/doi/10.2824/8841206.
8. 2025 Global Threat Report | Latest Cybersecurity Trends & Insights | CrowdStrike. CrowdStrike.com. URL: https://www.crowdstrike.com/en-us/global-threat-report/.
9. Naik, Nitin & Jenkins, Paul & Grace, Paul & Naik, Dishita & Phd, Shaligram & Song, Jingping. (2024). A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. 10.1007/978-3-031-74443-3_16.

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

ПІДВИЩЕННЯ РЕЗИЛЬЄНТНОСТІ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ ВПРОВАДЖЕННЯМ У КІБЕРБЕЗПЕКОВІ ПРОЦЕСИ ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Відповідно до [1], галузь енергетики відіграє ключову роль у забезпеченні кібербезпеки усієї економіки держави. Як видно з рис. 1, енергетика є фундаментом побудови будь-якої системи і, водночас, за відсутності електроенергії жодна система, що залежить від неї, може втратити свій функціонал.

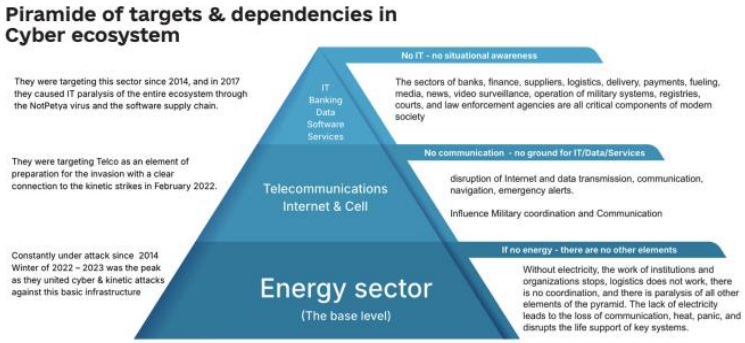

Рисунок 1 – Піраміда цілей та залежностей в існуючій екосистемі забезпечення кібербезпеки [1]

Важливість забезпечення кібербезпеки в енергетиці для резильєнтності нашої держави, як великої динамічної системи, обумовлюється і підвищеною кількістю кібератак на енергетику в останні роки. Підтвердженням цьому є приклад динаміки кібератак упродовж 2021–2024 рр. (рис. 2 [1]).

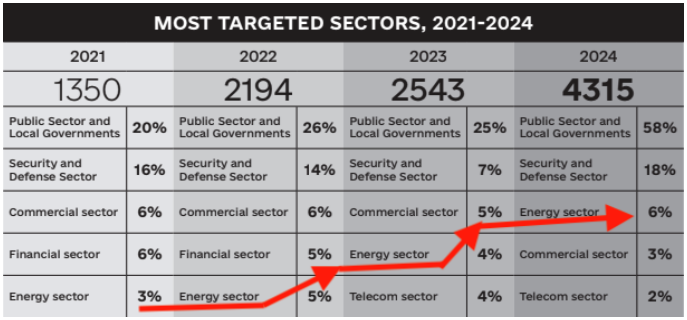

Рисунок 2 – Тенденція до підвищення кібератак на галузь енергетики [1]

Відповідно до міжнародних стандартів розроблення кіберрезильєнтних систем [2] важливу роль у даному процесі відіграють центри безпекових операцій (англ. Security Operations Center, SOC). Ними виконуються дві важливі функції – виявляння і реагування на кібератаки в реальному часі, а також ведення проактивного захисту – виявлення вразливостей [3].

Для виконання цих функцій у SOC використовують різноманітне програмне забезпечення [3]:

- Security information and event management (SIEM) – забезпечується моніторинг кіберактивності у системі;
- Endpoint protection systems – захищається мережа, до якої мають доступ кінцеві пристрої;
- Security orchestration, automation, and response (SOAR)solutions – зменшують участь людини у реагуванні на кібератаки завдяки автоматизуванню даного процесу;
- Firewalls – здійснюється моніторинг мережевого трафіку;
- Automated application security – тестується програмне забезпечення на вразливості в реальному часі;
- Asset discovery systems and asset inventories – відстежується активність об’єктів в системі;
- Data monitoring tools – оцінюється безпека та цілісність даних в системі;
- Governance, risk and compliance (GRC) systems – відстежуються дотриманням загальних правил та політик;
- Vulnerability scanners and penetration testing tools – сканується мережа на вразливості;
- Log management systems – записується історія функціонування системи.

З огляду на на велику кількість різноманітного програмного та апаратного забезпечення, основу будь-якого SOC – внутрішнього, віртуального, глобального, гібридного, хмарного – становить персонал. Відповідно до його функцій і завдань, усіх співробітників можна поділити в межах таких рівні [3]:

Перший рівень (рівень першої відповіді) – працівники визначають небезпечність загрози та, за потреби, передають її на другий рівень.

Другий рівень (рівень реагування на інциденти) – працівники цього рівня здатні вирішувати проблеми та позбуватися негативних наслідків інцидентів і, за потреби, передавати інциденти для подальшого – більш глибокого дослідження.

Третій рівень (рівень проактивних безпекових операцій) – спеціалісти цього рівня виконують пошук вразливостей та загроз, а також розслідують інциденти. При цьому вони зазвичай використовують багато різноманітних інструментів та аналізують великий обсяг інформації.

Четвертий рівень (рівень продуктивності та інтеграції) – співробітники на цьому рівні здійснюють управління командами та забезпечують зв'язок між підрозділом кібербезпеки та іншими підрозділами всередині організації.

При цьому на кожному з наведених рівнів обсяг інформації, яку треба проаналізувати значно зростає. А оскільки для аналізу треба сприйняти інформацію і в основному сприйняття інформації відбувається через зір, то виникає проблема ефективного візуалізування інформації. Цю проблему для персоналу на 3 та 4 рівнях – де обсяг інформації надзвичайно великий можна вирішити за допомогою використання технології доповненої реальності [4]. Це дозволить уникати пропусків і оперативно виявляти події з ознаками інциденту та реагувати на них. Тому таке використання дозволить підвищити резильєнтність енергетичної інфраструктури.

1. Державна служба спеціального зв'язку та захисту інформації України. Analytical report: War and cyber: three years of struggle and lessons for global security. https://cip.gov.ua/services/cm/api/attachment/download?id=69131.
2. NIST Special Publication 800-160, Volume 2 Revision 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, December 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1.
3. Chrissy Kidd What Is a SOC? Security Operations Centers: A Complete Overview 31.03.2025. https://www.splunk.com/en_us/blog/learn/soc-security-operation-center.html.
4. Ракович, В.С., Цуркан, В.В. (2023). Аналіз прикладних застосувань технології доповненої реальності. У В.Д. Самойлов, & І.В. Плетяний (Ред.) *Науково-практичній конференції Технології створення і використання засобів підготовки персоналу на об'єктах критичної інфраструктури* (с. 12–14). Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. https://doi.org/10.5281/zenodo.15130175.

ENHANCING RESILIENCE STRESS TESTING FOR HIGH-IMPACT LOW-PROBABILITY EVENTS: THE AGILE PROJECT APPROACH

Introduction to the AGILE Project. In response to the rising frequency of disruptive natural, technological, and hybrid disasters, there is a growing need for innovative approaches to systemic risk management. High-Impact Low-Probability (HILP) events, in particular, present formidable challenges to the resilience of critical infrastructure, often rendering traditional risk management methods inadequate. The AGILE project ("AGnostic risk management for high Impact Low probability Events"), funded under Horizon Europe by the European Commission and UK Research and Innovation (UKRI), aims to develop a flexible, agnostic framework for stress testing and risk management [1]. The AGILE Consortium (Agile, n.d.) is developing practical methodologies and adaptable tools for stress-testing complex systems, with the capacity to be tailored to multiple sectors. The conceptual structure of the AGILE framework is shown in Figure 1.

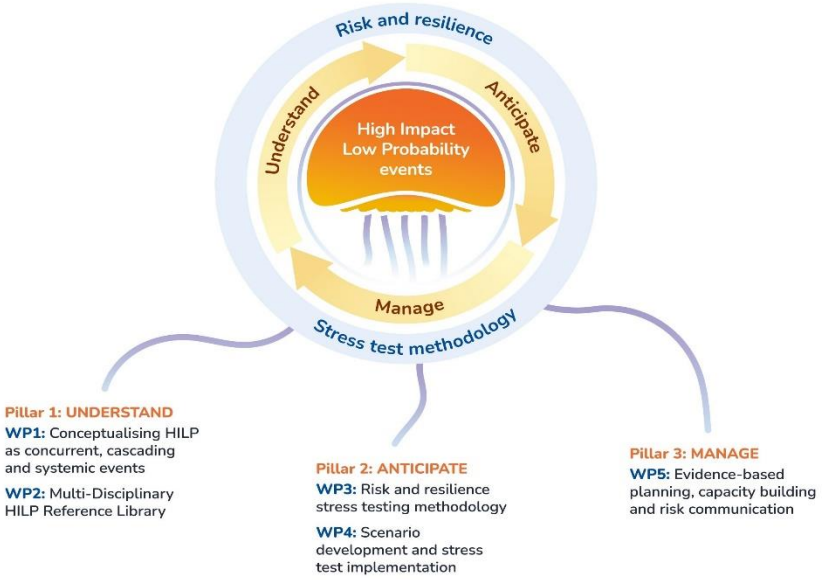

Figure 1 – The AGILE Project Concept

Within the AGILE Consortium, Ukraine is represented by the G.E. Pukhov Institute for Modelling in Energy Engineering (PIMEE) of the National Academy of Sciences of Ukraine. Against the backdrop of ongoing warfare and persistent hybrid threats, Ukraine provides a unique and challenging context for validating and refining stress-testing frameworks under genuine high-risk conditions.

Tiered Approach to Resilience Stress Testing. In disaster risk reduction, assessing the resilience of critical infrastructure through structured stress testing is crucial. The AGILE project adopts a tiered, multi-level approach (see Figure 2) for stress testing, as described by Linkov et al [2].

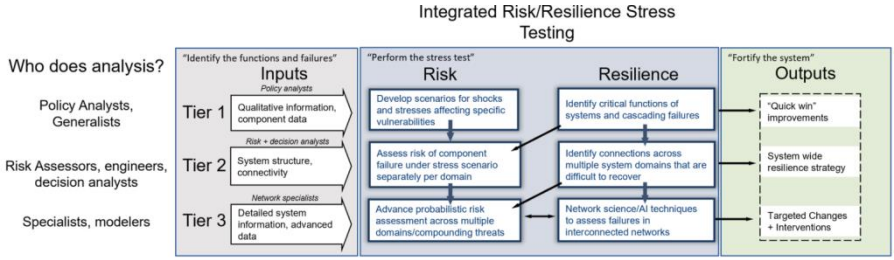

Figure 2 – Tiered approach to integrated risk and resilience stress testing for critical infrastructure

This methodology consists of three tiers: Tier 1 offers a screening-level assessment, pinpointing critical system functions and evaluating connectivity changes under stress. Tier 2 applies simplified system models to analyze and quantify cross-domain interactions affecting critical functions. Tier 3 employs advanced modeling techniques—including network science and artificial intelligence—to deeply investigate the dynamic responses of interconnected networks to both random and targeted threats [3].

Case Study: Digital Resilience in Ukraine. The PIMEE case study addresses the digital resilience of Ukraine's critical infrastructure, providing a comprehensive analysis of current practices for maintaining, restoring, and advancing digital infrastructure and services amid ongoing kinetic and cyber threats—chiefly those arising from Russian military aggression. The study emphasizes the interconnected technological, organizational, and human challenges present. Stress testing is particularly focused on the cascading impacts of disruptions in the power sector on communication and information systems (CIS), which are vital for business continuity, electronic communication, media, and public services. By serving as a national testbed, PIMEE examines the adaptation and transfer of European methodologies to Eastern European infrastructure under continuous crisis. The core methodology leverages structured risk assessment with multi-level stress testing (ST-1 to ST-3), customized to the realities of Ukraine's resource-limited, uncertainty-prone, and threat-exposed environment. Rather than assuming full infrastructure functionality, PIMEE's

approach investigates adaptive system behaviors and partial service continuity during disruptions, with an emphasis on service recovery speed and resilience. This approach allows for the fine-tuning of stress-testing parameters under HILP scenarios that have become tangible, not merely theoretical.

Preparations to the Tiers 1 and 2 Testing. The essential part of tiered stress testing is a system description. Stress test partners describe the system to be tested by answering three questions as follows.

Q1. To whom or what do we aim to enhance resilience and preparedness for HILPs?

A1. We aim to enhance the resilience of electronic communications, digital services, and supply chains of digital services to subscribers in response to cascading failures originating from disruptions in the energy system caused by HILP events

Q2. What is the heuristic definition of the system?

A2. The system can be heuristically defined as an interconnected network of energy-dependent digital infrastructure, including telecommunications networks, cloud computing services, data centers, and digital service providers, which collectively ensure the continuity of digital services to end-users. This system operates within a broader socio-technical and regulatory environment that influences its resilience to cascading failures from energy disruptions.

Q3. The primary objectives of this system's functioning.

A3: the primary objectives are:

- Ensuring continuity of critical digital services (e.g., emergency communications, financial transactions, public services) despite energy disruptions.
- Implementing redundancy and failover mechanisms to mitigate cascading effects.
- Enhancing coordination between energy providers, digital service operators, and regulatory bodies to improve crisis response.
- Developing adaptive recovery strategies that enable rapid restoration of services following disruptions.
- Strengthening cyber-physical resilience by integrating energy management solutions and backup power infrastructures.

Further Work and Activities. A key element of PIMEE's participation is fostering dialogue among local stakeholders (see Figure 3) via workshops and scenario-based exercises. These sessions are designed to integrate AGILE's methodological advances into the operational realities faced by Ukrainian infrastructure operators [4]. PIMEE prioritizes the proactive involvement of practitioners and decision-makers to jointly define relevant HILP scenarios and to

validate stress-testing outcomes. The insights and results from the Ukrainian case study will be incorporated into the AGILE project's overarching dataset and methodological toolkit, forming the basis for actionable strategic recommendations in HILP risk management. These outputs will enhance stakeholder capacities at local, national, and European levels, ensuring the adaptation of European approaches to the risk landscapes of countries experiencing ongoing or potential threats.

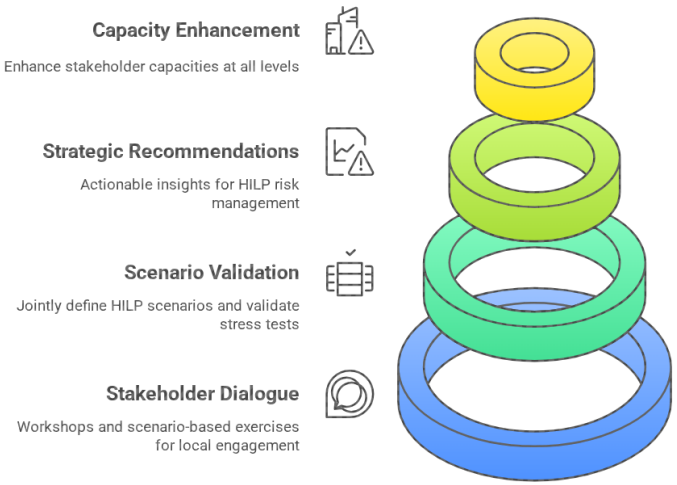

Figure 3 – Strategic risk management framework

As highlighted in the Grant Agreement (№101121356, Section 1, pp. 8–9), *"The* project *will ultimately improve the strategic and operational risk management capacities and capabilities of DRM (Disaster Risk Management) stakeholders on local, regional and national level and thus strengthen the societal resilience to new and emerging risks in Europe and beyond."*

1. Agile – Consortium (n. d.) Available: https://www.project-agile.eu/consortium/ (Accessed on 12.05.2025).
2. Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., & Panda, A. (2022). Resilience stress testing for critical infrastructure. *International Journal of Disaster Risk Reduction, 82,* 103323. https://doi.org/10.1016/j.ijdrr.2022.103323.
3. Linkov, I., Fox-Lent, C., Read, L., Allen, C. R., Arnott, J. C., Bellini, E., & Woods, D. (2018). Tiered approach to resilience assessment. Risk Analysis, 38(9), 1772-1780. https://doi.org/10.1111/risa.12991.
4. Palma-Oliveira, J. M., Trump, B. D., Wood, M. D., & Linkov, I. (2017). Community-driven hypothesis testing: A solution for the tragedy of the anticommons. Risk Analysis, 38(3), 620-634.

М.С. Дунаєвський

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗБАЛАНСОВАНОСТІ РИНКУ ЕЛЕКТРОЕНЕРГІЇ

Вступ. Модернізація та підвищення резильєнтності вітчизняної енергетичної системи в організаційно-технологічному аспекті передбачає повсюдні процеси інтенсивної цифровізації та децентралізації її основних складових; більш активне та безпосереднє залучення суб'єктів ринку, включаючи кінцевих споживачів; зростаючу роль локальних електроенергетичних систем (ЛЕС) на основі розподілених джерел генерації електроенергії та систем накопичення енергії [1, 2].

Виникає запит на розроблення та впровадження сучасних інформаційних систем (ІС) динамічного управління виробництвом, пропозицією, попитом, передачею та споживанням електроенергії в таких ЛЕС. Одною з найважливіших складових таких ІС є ефективний механізм ціноутворення, адже саме він, з однієї сторони, визначає рівень економічної мотивації учасників ринку, а з іншої сприяє збалансованості ЛЕС. Модернізація об'єднаної енергосистеми (ОЕС) потребує значних фінансових інвестицій. В той же час чим більше перспектив в оновленій ОЕС бачитимуть для себе локальні виробники електроенергії, тим активніше вони інвестуватимуть в модернізацію свого енергогенеруючого та енергозберігаючого обладнання, тим самим сприяючи розвитку локального децентралізованого сегменту енергоринку. Споживачі, що зацікавлені мати вибір із кількох альтернативних постачальників з обґрунтованими ринковими цінами та гарантованим обсягом постачання теж доєднаються до такого ринку. Оновлена ОЕС, що гармонійно поєднає як централізований так і децентралізовані сегменти матиме підвищену резильєнтність та гнучкішу систему динамічного управління.

Мета та завдання. Мета та завдання цієї роботи – розглянути сучасні технології прогнозування даних часових рядів на основі моделей генеративного штучного інтелекту та запропонувати їх використання для прогнозування стану ринку щодо обсягу та ціни електроенергії.

Виклад основного матеріалу. Локальний енергетичний ринок (ЛЕР) є досить новітньою концепцією для реалій України. Зазвичай активні споживачі електроенергії (prosumers), тобто домогосподарства які і споживають, і генерують електроенергію (наприклад за рахунок встановлених фотоелектричних сонячних панелей або вітрових станцій), звично продають надлишок наявної електроенергії на централізований ринок. ЛЕР є наступним етапом розвитку розподіленої енергомережі на якому відбувається об'єднання у кластер місцевих виробників та споживачів електроенергії. До кола учасників ЛЕР входять також учасники-агрегатори, – юридичні особи, що викуповують (агрегують) енергоресурси від менших виробників та продають їх місцевим споживачам, що потребують значних обсягів. Також учасники-агрегатори

продають сукупний надлишок на центральний ринок. Варто зауважити, що з математичної точки зору, агреговані показники легше піддаються прогнозуванню, оскільки процес агрегації згладжує індивідуальну варіативність обсягів проданої електроенергії від кожного окремого продавця. З логістичної точки зору ця математична властивість сприяє вищому рівню збалансованості ЛЕР.

Традиційно механізм балансування ринку забезпечується механізмом ціноутворення за якого непроданий обсяг електроенергії (скоріш за все виставлений виробниками на продаж за суттєво вищою ціною порівняно з рівноважною ціною ринку) викуповується оператором ринку (ОР) за певною умовною мінімальною ціною ОР; і в той же час оператор ринку компенсує незабезпечений попит на електроенергію (скоріш за все заявка на покупку була з суттєво нижчою ціною порівняно з рівноважною ціною ринку) за умовною максимальною ціною ОР. Фізично, дефіцитний обсяг електроенергії забезпечується оператором системи розподілу (ОСР). По суті, продаж та викуп електроенергії для балансування ринку оператором ринку відбувається за «штрафними» тарифами для учасників, які не знайшли свого контрагента. Різниця в тарифах стає винагородою оператора ринку, та є мотивацією для учасників встановлювати ціни максимально наближені до рівноважних цін локального енергоринку.

Таким чином, для всіх учасників ринку пріоритетної важливості набирає прогнозування обсягів та цін на ЛЕР, зокрема короткострокові прогнози на внутрішньодобовому ринку та ринку на добу наперед [3]. Оскільки ЛЕР є новим організаційним компонентом системи (а отже відсутні історичні дані щодо циклічності та тренду торгів які могли б бути використані традиційними методами прогнозування часових рядів), а також через те, що кожна ЛЕР має своїх унікальних учасників, шаблони торгів тяжко прогнозувати. Потенційно перспективним є використання новітніх технологій на основі генеративного штучного інтелекту, наприклад прогнозних моделей Chronos [4]. За основу вони використовують трансформер архітектуру великої мовної моделі (Large Language Model (LLM)) T5. Розробники Chronos моделей використали суттєву кількість публічно доступних наборів даних часових рядів та навчили (pretrained) різні за розміром моделі (від 8 млн до 710 млн параметрів). Відкритий доступ до натренованих моделей надається відповідно до умов ліцензії Apache-2.0, через платформу GitHub [5]. Зауважимо, що до наборів даних, використаних для навчання моделей, в тому числі ввійшли дані щодо генерації сонячної та вітрової електроенергії (частота вимірів від 5 хв до 1 тижня).

Інноваційність підходу полягає в тому, що часовий ряд, шляхом квантизації та масштабування, перетворюється на послідовність токенів. Надалі мовну модель навчають на цих токенах, використовуючи функцію втрат перехресної ентропії (cross-entropy loss). Навчена модель генерує ймовірнісні прогнози на основі множинних вибірок можливих майбутніх траєкторій розвитку процесів (цінової динаміки та/або обсягів постачання електроенергії) зважаючи на уже

наявні дані щодо їх розвитку. Наскільки успішно великі мовні моделі (LLM) генерують кожне наступне слово відповіді, настільки ж успішно за цього підходу генерується кожне наступне значення часового ряду. Зважаючи на той факт, що Chronos навчена на великій кількості наборів даних (а також на синтетичних даних згенерованих за допомогою Гаусівських процесів), модель досить успішно «відчуває» шаблони та тренди розвитку процесів у часі навіть в ситуаціях з мінімальним контекстом (Zero Shot). В таблиці 1 наводимо порівняльну ефективність Chronos моделей на 27 тестових наборах даних (які не використовувались під час навчання Chronos моделей) [4]. В ролі порівняльного показника використано агреговане відносне значення зваженої квантильної функції втрат (Weighted Quantile Loss) (чим нижче значення тим краща модель).

Таблиця 1 – Порівняльна ефективність Chronos моделей

Модель	**Тип моделі**	**Агрегований відносний WQL**
Chronos-Bolt (Base)	Попередньо навчена (pretrained Zero Shot)	0.624
Chronos-Bolt (Small)	Попередньо навчена (pretrained Zero Shot)	0.636
TFT	Спеціалізована для певного завдання	0.639
Chronos-Bolt (Mini)	Попередньо навчена (pretrained Zero Shot)	0.644
Chronos (Large)	Попередньо навчена (pretrained Zero Shot)	0.645
Chronos (Base)	Попередньо навчена (pretrained Zero Shot)	0.662
Chronos (Small)	Попередньо навчена (pretrained Zero Shot)	0.667
Chronos-Bolt (Tiny)	Попередньо навчена (pretrained Zero Shot)	0.668
N-HiTS	Спеціалізована для певного завдання	0.672
Chronos (Mini)	Попередньо навчена (pretrained Zero Shot)	0.678
N-BEATS	Спеціалізована для певного завдання	0.681
PatchTST	Спеціалізована для певного завдання	0.684
Chronos-GPT2	Попередньо навчена (pretrained Zero Shot)	0.687
TimesFM	Попередньо навчена	0.692
Moirai-1.0-R (Base)	Попередньо навчена	0.696
Moirai-1.0-R (Large)	Попередньо навчена	0.720
SCUM	Локальна статистична модель	0.728
DeepAR	Спеціалізована для певного завдання	0.733
DLinear	Спеціалізована для певного завдання	0.757
AutoARIMA	Локальна статистична модель	0.761
AutoTheta	Локальна статистична модель	0.793
LLMTime	Попередньо навчена (pretrained Zero Shot)	0.804
AutoETS	Локальна статистична модель	0.838
WaveNet	Спеціалізована для певного завдання	0.842
Seasonal Naïve	Локальна статистична модель	1.000
Lag-Llama	Попередньо навчена	1.097
Naïve	Локальна статистична модель	1.152

Методологія розгортання Chronos моделей в хмарному середовищі AWS (Amazon Web Services), на основі SageMaker Jump Start, з використанням SageMaker Python SDK, представлена в Jupyter ноутбуку (notebooks/deploy-chronos-bolt-to-amazon-sagemaker.ipynb) репозиторію проекту [5]. Звичайно Chronos моделі можна використовувати для досліджень та експериментів на локальній ЕОМ, проте умови промислової експлуатації містять набагато суворіші вимоги щодо кібербезпеки, масштабованості, надійності та резильєнтності (high availability). Модель прогнозування стає лише одним із компонентів набагато більшої системи. Скоріш за все це буде система побудована на основі сучасної мікросервісної архітектури, та, відповідно, розгорнута Chronos модель стане одним із сервісів (технічно SageMaker endpoint). Цей сервіс буде налаштований отримувати веб запити POST типу (що міститимуть дані часових рядів в JSON форматі) та надсилати у відповідь згенеровані прогнозні значення тренду розвитку процесу торгівлі електроенергією на локальному енергоринку.

Висновки. Технології генеративного ШІ мають значний потенціал щодо використання для прогнозування часових рядів даних торгів електроенергією на локальному енергоринку. Розгорнута LLM по типу Chronos в хмарному середовищі AWS може бути гармонійно інтегрованою в операційні процеси аналітичного супроводження динамічного управління ЛЕС, допомагатиме учасникам ринку в режимі реального часу розуміти короткостроковий прогнозний рівноважний стан ринку, та, відповідно, обрати стратегію, що максимізуватиме їх фінансовий результат.

1. Борукаєв З.Х., Євдокімов В.А., Остапченко К.Б. (2025). Концептуальна модель організації децентралізованої торгівлі електричною енергією в Україні. Збірник тез науково-практичної конференції «*Використання блокчейн технологій в енергетиці – 2025*». (с. 19 – 22). Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України. URL: https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bte-2025/.
2. Горбачук В.М. та ін. (2025). Основи децентралізованих ринків електроенергії. Збірник тез науково-практичної конференції «*Використання блокчейн технологій в енергетиці – 2025*». (с. 15 – 18). Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України. URL: https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bte-2025/.
3. Дунаєвський М.С. (2025). Інформаційні моделі торгівлі на внутрішньодобових ринках електроенергії. Збірник тез науково-практичної конференції «*Використання блокчейн технологій в енергетиці – 2025*». (с. 63 – 66). Інститут проблем моделювання в енергетиці імені Г.Є. Пухова НАН України. URL: https://ipme.kiev.ua/konferencii/naukovo-praktichna-konferenciya-bte-2025/.
4. Fatir A. et al. (2024) Chronos: Learning the Language of Time Series. Url: https://arxiv.org/abs/2403.07815 (accessed at: 6th of June 2025).
5. Fatir A. et al. (2024) GitHub репозиторій проєкту Chronos. Url: https://github.com/amazon-science/chronos-forecasting (accessed at: 6th of June 2025).

Н.В. Трушкіна

ТРЕНДОВИЙ АНАЛІЗ ВЗАЄМОЗВ'ЯЗКУ МІЖ КРИТИЧНОЮ ІНФРАСТРУКТУРОЮ ТА КІБЕРРИЗИКАМИ

У глобальному світі відбувається постійний динамічний процес, який призводить до структурних змін (економічних, соціальних, організаційних, екологічних тощо) об'єктів і мереж інфраструктури в багатокомпонентній просторовій системі. На даному етапі особливої актуальності набувають питання трансформації енергетичних систем [1-2] шляхом переходу ключових елементів критичних інфраструктур до якісно нового рівня розвитку за рахунок адаптації до ризиків і загроз зовнішнього середовища. Одним із таких ризиків є кібератаки на важливі об'єкти енергетичної інфраструктури. Тому незаперечним є той факт, що надійний захист від кібератак активно впливає на економічну, політичну, оборонну та інші складові національної безпеки держав. Очевидним є той факт, що кібербезпека критичної інфраструктури має стати одним із пріоритетів національної безпеки у країнах світу [3] в умовах мінливого інформаційного простору.

За даними Європейського агентства з мережевої та інформаційної безпеки ENISA, кількість кібератак на критичну інфраструктуру в ЄС зросла за 2019-2020 рр. у 2 рази або зі 150 до 300. За 2022-2023 рр. кількість кібератак у світі збільшилася на 62%. За експертними оцінками, глобальні втрати від кібератак у 2020 році становили приблизно 945 млрд дол. Прогнозується, що збитки від кіберзлочинності на глобальному ринку перевищать до 2026 р. 20 трлн дол.

У зв'язку з цим дане дослідження присвячено аналізу впливу кіберризиків і загроз на розвиток критичної інфраструктури з використанням трендового підходу [4], суть якого полягає у визначенні контекстуальних і часових закономірностей розвитку поглядів науковців, що досліджують вплив кіберризиків і загроз на розвиток критичної інфраструктури у країнах світу. Для цього застосовується інструментарій трендового аналізу – Google Trends. На підставі трендового аналізу за 2004-2024 роки виявлено високий рівень інтересу у всьому світі до тематики «критична інфраструктура» ("Critical Infrastructure") (у середньому 17 балів) і «кіберризик» ("Cyber risk") (у середньому 13 балів).

Якщо розглядати у часі, то можна побачити, що у 2004 р. рівень популярності теми, пов'язаної з кіберризиками, становив о балів, а з розвитком критичної інфраструктури 35 балів. З 2008 р. почалася популяризуватися тематика з проблем кібербезпеки, а розвитку критичної інфраструктури знижуватися. У 2012 р. рівень зацікавленості за обидвома темами становив 12 балів. Починаючи з 2017 р. рівень зацікавленості з управління кіберризиками щорічно зростає, а

критичної інфраструктури скорочується. Так, у 2019 р. значення даного показника становило 25 і 12 балів, відповідно; у 2023 р. – 47 і 24 бали.

Запитам надаються бали від 0 до 100, де 100 балів означають місце розташування з найбільшою часткою популярності запиту, 50 балів – місце розташування, рівень популярності запиту в якому вдвічі нижчий, ніж у першому. 0 балів означає місце розташування, за яким недостатньо даних про запит, що розглядається. Варто відзначити, що чим більше балів, тим вища частка відповідних запитів від усіх запитів, а не їхня абсолютна кількість. Тому маленькій країні, де запити зі словами «кіберризик» (“Cyber risk”) або «критична інфраструктура» (“Critical infrastructure”) становлять 80% від усіх запитів, буде привласнено вдвічі більше балів, ніж великий, де лише 40% усіх запитів містять це слово.

Тематика, яку присвячено вирішенню актуальних питань розвитку критичної інфраструктури з урахуванням кіберзагроз і ризиків знову актуалізувалася з 2022 р. Це обумовлено повномасштабним вторгненням росії на територію України та постійними кібератаками на критично важливі об’єкти інфраструктури у всьому світі.

На даний час у більшості країн світу в останні 20 років популярними є теми кіберризики, загрози, кібератаки, кібервійни, кібербезпека тощо. У ряді країн частка запиту з проблематики, яку присвячено кіберризикам, перевищує 50% від загальної кількості запитів у відповідній країні. Наприклад, в Італії значення цього показника становить 81%, Швейцарії – 77, В’єтнамі – 72, Кореї та Великобританії – 71, Франції – 68, Нідерландах – 64, Португалії – 61, Німеччині – 59, Ізраїлі – 58, Іспанії – 56, Туреччині – 55, Норвегії – 54, Канаді та Польщі – 50%. А у деяких країнах набирає популярності та поширеності серед пошуку джерел – різноманітні аспекти розроблення та впровадження стратегій розвитку критичних інфраструктур. Так, рівень популярності теми «розвиток критичної інфраструктури» (“Critical infrastructure development”) у Фінляндії та Японії становить 51%, Австралії – 53, США – 57, Україні – 59, Чехії – 62, Румунії – 64% від загальної кількості запитів у відповідній країні.

Серед лідерів за популярністю можна назвати такі теми: кібербезпека (100 балів); управління кіберризиками (50); управління ризиками (49); ризик у кібербезпеці (35); оцінка ризиків (28); оцінка кіберризиків (27); управління ризиками в кібербезпеці (26); страхування кіберризиків (17); кіберстрахування (15); інформаційна безпека (14); кібератака (14); кіберзагроза (13); кібербезпека та управління ризиками (10 балів).

До найрозповсюджених запитів пошуку користувачів у країнах світу можна віднести такі: безпека критичної інфраструктури (100 балів); захист критичної інфраструктури (85); критична національна інфраструктура (64); кібербезпека (36); кібербезпека критичної інфраструктури (35); закон про критичну інфраструктуру (31); сектори критичної інфраструктури (26); системи критичної інфраструктури (25); визначення критичної

інфраструктури (20); захист критичної інформаційної інфраструктури (10 балів).

Аналіз показує, що тематика «кіберзагроза» (“Cyber threat”) почала активізуватися з 2016 року. Якщо у 2004 р. рівень популярності за даною проблематикою становив 0 балів, то у 2016 р. – 12, у 2017 р. – 15, у 2019 р. – 26, у 2022 р. – 39, у 2023 р. – 46 балів. Цією темою особливо цікавляться при пошуку в Інтернет-ресурсах користувачі з Індонезії (84% від загальної кількості запитів у країні), Малайзії (75%), Бразилії (75%), Туреччини (73%), Пакистану (72%), Кореї (69%), В’єтнаму (69%), Франції (69%), Ізраїлю (69%), Великобританії (67%), Португалії (60%), Італії (60%), Японії (57%), Польщі (56%), Угорщини (54%), Німеччини (54%), Канади (47%), США (46%), України (45%), Китаю (34%) тощо.

З 2014 р. популярною тематикою пошуку користувачів в усьому світі стала кібератака (Cyber attack). Динаміка популярності щороку змінювалася: у 2014 р. рівень зацікавленості становив 14 балів, у 2017 р. – 100, у 2020 р. – 40, у 2021 р. – 59, у 2023 р. – 61 бал. До країн-лідерів, у яких користувачі активно шукають інформацію за даною проблематикою, можна віднести такі: Великобританія (94% від загальної кількості запитів у країні), Пакистан і Франція (92%), Туреччина (91%), Ізраїль (90%), Канада, Швейцарія, Швеція (87%), Німеччина (84%), США та Японія (83%), Іран і Польща (80%), Республіка Корея (74%).

Серед лідерів при пошуку користувачів за ключовим словом «кіберзагроза» (“Cyber threat”) можна назвати кіберзагроза (100 балів), загроза безпеці (97), розвідка про загрози (66), кіберрозвідка (63), розвідка про кіберзагрози (63 бали). Популярними запитами з тематики «кібератака» (“Cyber attack”) є кібератаки (54 бали) і типи кібератак (17 балів).

Таким чином, дослідження трендових закономірностей публікаційної активності з аналізу взаємозв’язку між поняттями «кіберризик» (“Cyber risk”) та «критична інфраструктура» (“Critical infrastructure”) засвідчили значну популярність цієї проблематики у наукових колах, а також її перманентне зростання.

Виходячи з вищевикладеного можна дійти таких висновків. На даний час вкрай важливе значення має забезпечення належного рівня безпеки, у тому числі кібербезпеки критичних об’єктів інфраструктури. При цьому надзвичайно важливим є діагностика стану кібербезпеки як ефективного інструменту, процедура якої має включати такі етапи: оцінювання стану кібербезпеки за NIST Cybersecurity Framework; визначення цільового стану кібербезпеки; розроблення рекомендацій (high-level design, специфікації технічної архітектури, операційні моделі кібербезпеки); розроблення дорожньої карти впровадження рекомендацій; повторна оцінка кібербезпеки.

За результатами кібердіагностики об’єкти критичної інфраструктури мають отримати комплексну оцінку цифрової захищеності; рекомендації щодо підвищення рівня кіберзрілості та готовності до кіберінцидентів; покрокову інструкцію з розроблення стратегії цифрової трансформації [5].

Крім цього, урядам більшості країн світу доцільно приділяти увагу розробленню або вдосконаленню національних стратегій кібербезпеки, під якими слід розуміти визначення концепції, спільних цілей, принципів і пріоритетів, якими має керуватися країна у вирішенні проблем кібербезпеки; опис кроків, програм та ініціатив (тобто «Дорожня карта»), які держава має зробити для захисту своєї критичної інфраструктури (у тому числі інформаційної) та для підвищення рівня безпеки, захисту та стійкості.

Тому у подальших дослідженнях планується приділити особливу увагу обґрунтуванню теоретико-методологічних положень Національної стратегії кібербезпеки критичної інфраструктури в Україні з урахуванням кращих світових практик.

1. Trushkina, N., Pahlevanzade, A., Pahlevanzade, A., & Maslennikov, Ye. (2021). Conceptual provisions of the transformation of the national energy system of Ukraine in the context of the European Green Deal. *Polityka Energetyczna – Energy Policy Journal*, 24(4), 121-138. https://doi.org/10.33223/epj/144861.
2. Kwilinski, A., Khaustova, V., & Trushkina, N. (2024). Transformation of the Energy Infrastructure in the Context of the Implementation of the European Green Deal. In: V. Babak, A. Zaporozhets (Eds.), *Systems, Decision and Control in Energy VI. Studies in Systems, Decision and Control* (vol. 561, pp. 59-79). Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-68372-5_3.
3. Хаустова, В. Є., & Трушкіна, Н. В. (2024). Ризики та загрози національній безпеці: сутність і класифікація. *Бізнес Інформ*, 10, 6-22. https://doi.org/10.32983/2222-4459-2024-10-6-22.
4. Kwilinski, A., & Trushkina, N. (2024). Impact of Cyber Risks and Threats on the Critical Infrastructure Development: Visualization of Scientific Research. *Proceedings of the 12th International Conference on Applied Innovation in IT (ICAIIT)*, 12(2), 107-119. http://dx.doi.org/10.25673/118123.
5. Khaustova, V., Kyzym, M., Trushkina, N., & Khaustov, M. (2024). Digital transformation of energy infrastructure in the conditions of global changes: bibliometric analysis. *Proceedings of the 12th International Conference on Applied Innovations in IT*, 12(1), 135-142. http://dx.doi.org/10.25673/115664.

ЗМІСТ

МАТЕРІАЛИ
ІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«РЕЗИЛЬЄНТНІСТЬ ДИНАМІЧНИХ СИСТЕМ»

12 червня 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