

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут

MINISTRY OF DEFENCE OF UKRAINE
Military Institute of Telecommunications and Informatization Technologies
named after Heroes of Kruty



Системи і технології зв'язку, інформатизації та кібербезпеки
№ 9

Communication, informatization and cybersecurity systems and technologies
№ 9

У збірнику викладено статті наукових та науково-педагогічних працівників, докторантів, ад'юнктів (аспірантів), курсантів, здобувачів інституту та інших установ (організацій) за наступними науковими напрямками:

перспективи розвитку телекомунікаційних систем, комплексів та засобів спеціального призначення;
захист інформації в спеціальних інформаційно-комунікаційних системах;
стан і розвиток автоматизованих систем управління військами та зброєю;
інформаційні системи та мережі, системи підтримки прийняття рішень спеціального призначення;
бойове застосування систем зв'язку та автоматизації Збройних сил України;
теорія і практика кібербезпеки та інформаційної боротьби в комп'ютеризованих системах і мережах.
Запрошуємо до співробітництва всі зацікавлені установи та організації, які проводять наукові дослідження та науково-технічні розробки за даними напрямками.

The book contains articles of scientific and teaching staff, post graduate students, adjuncts, institute applicants and other institutions (organizations) applicants in the following fields:

prospects of telecommunications systems, development, facilities and means of special purpose;
in special information protection and communication systems;
automated systems state and development of army weapons;
information systems and networks, decision support systems for special purposes;
combat use of communications systems and automation of Armed Forces of Ukraine;
theory and practice of cyber security and information warfare in computerized systems and networks.

All interested institutions and organizations, who conduct research and development in the directions state, are invited for cooperation.

Київ – 2026 – Kyiv

УДК:621

Редакційна колегія:

Головний редактор: *Радзівілов Г. Д.*, канд. техн. наук, професор

Заступник головного редактора: *Сайко В. Г.*, д-р техн. наук, професор

Відповідальний секретар: *Нестеренко М. М.*, д-р техн. наук, доцент

Члени редколегії:

<i>Беляков Р. О.</i> , д-р техн. наук, доцент;	<i>Романов О. І.</i> , д-р техн. наук, професор;
<i>Жук О. В.</i> , д-р техн. наук, професор;	<i>Хлапонін Ю. І.</i> д-р техн. наук, професор;
<i>Могилевич Д. І.</i> , д-р техн. наук, професор;	<i>Al-Sharify, Mushtaq Talib</i>
<i>Сова О. Я.</i> , д-р техн. наук, професор;	канд. техн. наук, доцент;
<i>Фесьоха В. В.</i> д-р філ., доцент;	<i>Aleksander, Marek</i> , д-р техн. наук, професор

Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. – Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. – 2026. – № 9. – 400 с. – DOI: 10.58254/viti.9.2026.

Наукове фахове видання категорії “Б”
ISSN 2786-6610 (друк)
ID R30-07190

Усі наукові статті, включені до збірника, прорецензовані фахівцями з відповідних галузей та отримали позитивний відгук.

При переддрукуванні матеріалів обов'язкове посилання на збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Статті, розміщені у збірнику, затверджено Вченою радою Військового інституту телекомунікацій та інформатизації імені Героїв Крут (протокол засідання № 8 від 22.05.2026).

Кластер наукового фахового видання та галузі знань і спеціальності, за якими видання публікує наукові праці – **Інформаційні технології та електроніка:**

F3 – Комп'ютерні науки;

F5 – Кібербезпека та захист інформації;

F6 – Інформаційні системи і технології;

G5 – Електроніка, електронні комунікації, приладобудування та радіотехніка.

Засновник – Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
(код за ЄДРПОУ 24978555).

Свідоцтво про державну реєстрацію видання: КВ № 25184-15124 Р від 20.07.2022.

Адреса редакції: 01011, м. Київ, вул. Князів Острозьких, 45/1. Тел. 256-22-73.

Електронна адреса: naukaviti@viti.edu.ua

Електронна адреса сайту: <https://journal.viti.edu.ua/index.php/cicst/issue/archive>

Відповідальний за випуск: Куцаєв В. В.

Зам. № _____. Друк. арк. 50,0. Ум.-друк. арк. 46,5. Обл.-вид. арк. 43,24.

Формат паперу 60×84/8. Тираж ____ прим.

Адреса друкарні ВІТІ ім. Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

З М І С Т

1	Антонюк Я. М., Корольов А. П., Лапа В. І., Мацасенко А. М. Оптимізація реалізації цифрових гребінчастих фільтрів на базі сучасних мікроконтролерів для задач обробки сигналів у реальному часі	5
2	Бараннік Д. В., Сінько В. В., Бараннік В. В., Ушань В. М. Методика проєктування розподіленої електронної комунікаційної мережі моніторингу на базі технології LoRa	15
3	Бернацький А. П. Концептуальна модель центру перспективних технологій як адаптивного багатоконтурного циклу формування оборонно-технологічної спроможності на основі оперативного досвіду	34
4	Бовда Е. М., Самохвалов Ю. Я., Клименко В. М. Деякі аспекти концептуального проєктування інфокомунікаційних систем військового призначення	53
5	Грінков В. О., Грінкова Г. В., Слюсар П. П. Математична модель оцінювання кіберстійкості інформаційних систем залежно від топології побудови на основі методу аналізу ієрархій	66
6	Гудима В. П., Яровий В. С., Островський А. О., Андрієнко О. В. Метод комбінованого використання методик ABC- та XYZ-аналізів для оптимізації організації метрологічного забезпечення Збройних Сил України	78
7	Данилюк І. А., Мочалюк В. В. Розробка методики підвищення ефективності обробки неструктурованої текстової інформації в інформаційних, інформаційно-комунікаційних системах оборонного призначення	88
8	Єрохін В. Ф., Радзівілов Г. Д., Коваленко О. О. Методики синтезу і редукції ML-алгоритму розділення-демодуляції нерівнопотужних синхронних сигналів QPSK	100
9	Живилю Є. О., Кучма Ю. В., Поліновський В. В., Плахтій М. О. Fidelity-орієнтована маршрутизація в SDN-керованих квантових мережах	115
10	Коваленко І. Г., Зарубенко А. О., Масесов М. О., Драглюк О. В. Методика оцінки ефективності системи зв'язку за стандартами НАТО з використанням геопросторової інформації	126
11	Ковальчук О. О., Беляков Р. О., Металіди О. Г. Аналіз методів виявлення безпілотних літальних апаратів із використанням бездротових сенсорних мереж	138
12	Куцаєв В. В., Семитківська І. В., Скоропад С. І., Цимбал І. В. Застосування симуляційного середовища Gazebo для наукових досліджень у галузі робототехнічних систем	151
13	Ланко А. В., Рибка Є. М. Оцінка надійності радіоелектронного обладнання за параметрами вібростійкості	164
14	Мазулевський О. Є. Оцінка забезпеченості кібербезпеки оборонного відомства з урахуванням передових міжнародних практик	176
15	Носков О. О. Модель оцінювання ефективності систем передачі даних військового призначення з урахуванням вимог конфіденційності, цілісності та доступності	187
16	Паламарчук С. А., Паламарчук Н. А., Вороной О. В., Побережець Т. В. Модель визначення стійкості користувачів до атак соціальної інженерії на основі теорій навчання та деградації знань	199
17	Панченко І. В., Бондаренко Д. М., Липський О. А., Стефанишин Я. І. Дослідження стійкості мережі 4G/LTE до впливу навмисних завад	210
18	Романенко М. М., Погребняк С. В., Кокошинський В. В. Вплив технологій виготовлення мікроелектроніки на надійність електронних засобів	219
19	Руденко В. І., Зінченко М. О., Яковчук О. В. Аналіз та оцінка ефективності нормативної бази та її функціональної моделі з визначенням шляхів удосконалення електронної комунікаційної мережі спеціального призначення	228
20	Сайко В. Г., Станілога О. О., Пантась С. О., Пантась І. О. Дослідження можливостей підвищення завадостійкості виявлення та пеленгації сигналів стандарту IEEE 802.11bf	246
21	Солодовник В. І. Метод дворежимної просторово-поляризаційної модуляції із модифікованими ансамблями сигналів	263
22	Тлустий А. О., Кузавков В. В. Діагностична модель вихідного транслятора КМОН інтегральної мікросхеми	275
23	Троцько О. О., Кондрусь А. В., Пилипчук І. Ю., Крамарчук В. В. Дослідження методики відновлення інформаційних систем спеціального призначення шляхом застосування підходу Інфраструктура як Код	287
24	Устинов Д. А., Нестеренко М. М. Розробка потокової архітектури класифікації трафіку в мережах SDN в режимі реального часу	299
25	Фесенко О. Д. Математична модель еволюції людино-машинного інтерфейсу на основі ентропії, довіри та цифрових двійників	311
26	Фесьоха В. В., Легкобит В. С. Модель дворівневої організації знань в інтелектуальних системах кіберзахисту на онтологічній основі	332
27	Фесьоха Н. О., Симоненко О. А., Нестеров О. М. Багатокритеріальна методика оцінювання захищеності IoT-пристроїв на основі синтезу методів АНР та TOPSIS	349
28	Хавер А. В. Метод пріоритизації заходів кібербезпеки технологічних систем промислових об'єктів критичної інфраструктури для протидії деструктивним кібератакам в умовах обмежених ресурсів	363
29	Хусаїнов П. В., Штаненко С. С., Чурілова І. С. Проблема реагування на кіберінциденти об'єктів критичної інфраструктури в реальному масштабі часу	382
	Автори номера	394
	Пам'ятка автору	399

CONTENTS

1	Y. Antoniuk, A. Korolov, V. Lapa, A. Matsaienko. Optimization of the digital comb filters implementation based on modern microcontrollers for real-time signal processing tasks	5
2	D. Barannik, V. Sinko, V. Barannik, V. Ushan. Design methodology of a distributed multi-hop LoRa-based sensor network for monitoring extended areas	15
3	A. Bernatskyi. Conceptual model of a centre for advanced technologies as an adaptive, multi-loop cycle for building defence and technological capabilities based on operational experience	34
4	E. Bovda, Y. Samokhvalov, V. Klimenko. Some aspects of conceptual design of military information and communication systems	53
5	V. Hrinkov, H. Hrinkova, P. Sliusar. Mathematical model for assessing cyber resilience of information systems depending on the topology of the structure based on the hierarchy analysis method	66
6	V. Hudyma, V. Yarovyi, A. Ostrovskyi, O. Andriienko. A method for the combined use of ABC and XYZ analysis techniques to optimise the organisation of metrological support for the Armed Forces of Ukraine	78
7	I. Danyliuk, V. Mochaliuk. Development of a methodology for increasing the efficiency of processing unstructured text information in defense information, information and communication systems	88
8	V. Yerokhin, G. Radzivilov, O. Kovalenko. Method of synthesis and reduction of ML-algorithm for division-demodulation of unequal power synchronous QPSK signals	100
9	Y. Zhyvylo, Y. Kuchma, V. Polinovskyi, M. Plakhtii. Fidelity-oriented routing in SDN-managed quantum networks	115
10	I. Kovalenko, A. Zarubenko, M. Masesov, O. Drahliuk. Methodology for assessing the effectiveness of communication system according to NATO standards using geospatial information	126
11	O. Kovalchuk, R. Bieliakov, O. Metalidi. Analysis of methods for detecting unmanned aerial vehicles using wireless sensor networks	138
12	V. Kutsaiev, I. Semytkivska, S. Scoropad, I. Tsymbal. Application of the Gazebo simulation environment for scientific research in the field of robotic systems	151
13	A. Lanko, Ye. Rybka. Reliability assessment of radio-electronic equipment by vibration resistance parameters	164
14	O. Mazulevskyi. Assessment of cybersecurity of the defense department taking into account best international practices	176
15	O. Noskov. Development of a model for determining the efficiency of various types of data transmission systems taking into account the requirements for confidentiality, integrity and availability	187
16	S. Palamarchuk, N. Palamarchuk, O. Voronoi, T. Poberezhets. Model for determining user resistance to social engineering attacks based on the theories of learning and knowledge degradation	199
17	I. Panchenko, D. Bondarenko, O. Lypskyi, Ya. Stefanyshyn. Research on the resilience of 4G/LTE networks to the influence of intentional interference	210
18	M. Romanenko, S. Pohrebniak, V. Kokoshynskyi. Impact of microelectronics manufacturing technologies on the reliability of electronic devices	219
19	V. Rudenko, M. Zinchenko., O. Yakovchuk. Research of the regulatory framework, analysis of the efficiency of the functioning and directions for improvement of the special-purpose electronic communication network	228
20	V. Saiko, O. Staniloha, S. Pantas, I. Pantas. Investigation of methods to improve interference immunity in detection and direction-finding of IEEE 802.11bf signals	246
21	V. Solodovnyk. Dual-mode spatial-polarization modulation method with modified signal constellations	263
22	A. Tlustyi, V. Kuzavkov. Diagnostic model of the CMOS integrated circuit output translator	275
23	O. Trotsko, A. Kondrus, I. Pylypchuk, V. Kramarchuk. Research on the recovery methodology for special-purpose information systems through the application of the infrastructure as code approach	287
24	D. Ustynov, M. Nesterenko. Streaming architecture for real-time traffic classification in software-defined networks	299
25	O. Fesenko. A mathematical model of the evolution of the human-machine interface based on entropy, trust, and digital twins	311
26	V. Fesokha, V. Lehkobyt. A two-level model of knowledge organization in ontology-based cybersecurity systems	332
27	N. Fesokha, O. Symonenko, O. Nesterov. Multi-criteria method for evaluating IoT device security based on the integration of AHP and TOPSIS methods	349
28	A. Khaver. Method for prioritizing cybersecurity measures in technological systems of industrial critical infrastructure facilities to counter destructive cyberattacks under resource constraints	363
29	P. Khusainov, S. Shtanenko, I. Churilova. The Problem Real Time-based Incident Response in Industrial Control System.	382
	About authors	394
	Memo to the author	399

УДК.62-23

Антонюк Я. М ORCID: 0009-0005-7680-5950 (ІТС НАН України)
канд. техн. наук Корольов А. П. ORCID: 0000-0001-6281-063X (ВІТІ ім. Героїв Крут)
Лапа В. І. ORCID: 0009-0006-8017-0334 (ВІТІ ім. Героїв Крут)
канд. техн. наук Мацаєнко А. М. ORCID: 0000-0003-1149-7318 (ВІТІ ім. Героїв Крут)

ОПТИМІЗАЦІЯ РЕАЛІЗАЦІЇ ЦИФРОВИХ ГРЕБІНЧАСТИХ ФІЛЬТРІВ НА БАЗІ СУЧАСНИХ МІКРОКОНТРОЛЕРІВ ДЛЯ ЗАДАЧ ОБРОБКИ СИГНАЛІВ У РЕАЛЬНОМУ ЧАСІ

У статті представлено результати дослідження та практичної реалізації цифрових гребінчастих фільтрів на базі мікроконтролерів серії STM32 (ядро ARM Cortex-M4). Актуальність теми зумовлена необхідністю підвищення обчислювальної ефективності та зниження апаратних витрат у системах цифрової обробки сигналів реального часу. Вдосконалення методики реалізації гребінчастих фільтрів дозволяє оптимізувати процеси децимації в сучасних телекомунікаційних стандартах та покращити якість фільтрації періодичних завад у складних заводських умовах.

Метою статті є дослідження комбінаційного методу програмної та апаратної реалізації рекурсивних та нерекурсивних гребінчастих фільтрів на базі мікроконтролера STM32 для забезпечення їх роботи у режимі реального часу при мінімальному використанні ресурсу пам'яті, а також оцінка їхніх частотних характеристик при обробці сигналів із заданою частотою дискретизації.

Розглянуто математичні моделі рекурсивних і нерекурсивних гребінчастих фільтрів, а також особливості їхньої адаптації до архітектур із обмеженими обчислювальними ресурсами. Запропоновано методику оптимізації алгоритму через використання кільцевих буферів, механізмів прямого доступу до пам'яті та бібліотеки CMSIS-DSP. Проведено порівняльний аналіз завантаженості центрального процесора при використанні арифметики з плаваючою та фіксованою комою. Експериментально підтверджено ефективність запропонованих рішень для фільтрації періодичних завад у реальному часі.

Практичне значення отриманих результатів: зниження обчислювального навантаження на центральний процесор; створення готових програмних шаблонів на базі бібліотеки CMSIS-DSP, що скорочує термін розробки та налагодження вбудованих систем на базі ядер Cortex-M; можливість реалізації фільтрів високого порядку на мікроконтролерах з обмеженими ресурсами без втрати частоти дискретизації.

Ключові слова: гребінчасті фільтри, цифрова обробка сигналів, STM32, ARM Cortex-M4, реальний час, контролери прямого доступу до пам'яті, CMSIS-DSP, оптимізація.

Y. Antoniuk, A. Korolov, V. Lapa, A. Matsaienکو. Optimization of the digital comb filters implementation based on modern microcontrollers for real-time signal processing tasks

The article presents the results of both research and practical implementation of digital comb filters using STM32 series microcontrollers based on the ARM Cortex-M4 core. The topic is important because it addresses the need to improve computational efficiency and reduce hardware costs in real-time digital signal processing systems. Enhancing the methodology for implementing comb filters makes it possible to optimize decimation processes in modern telecommunication standards and improve the suppression of intermittent interference under challenging noise conditions.

The aim of the article is to investigate a combined software–hardware approach to the implementation of recursive and non-recursive comb filters based on the STM32 microcontroller, in order to ensure their real-time operation with minimal memory usage, as well as to evaluate their frequency characteristics during the processing of signals with a specified sampling rate.

Mathematical models of recursive and non-recursive comb filters are considered, as well as the features of their adaptation to architectures with limited computing resources. A method for optimizing the algorithm through the use of ring buffers, direct access to memory and the CMSIS-DSP library is proposed. A comparative analysis of the CPU workload for calculations with floating-point and fixed-point arithmetic is carried out. The effectiveness of the proposed solutions for filtering periodic interference under real time conditions has been experimentally confirmed.

The practical significance of the results includes reduced CPU utilization, the development of software templates based on the CMSIS-DSP library that shorten the development and debugging time of embedded systems based on Cortex-M cores, and the ability to implement high-order filters on resource-constrained microcontrollers without loss of sampling rate.

Keywords: comb filters, digital signal processing, STM32, ARM Cortex-M4, real-time, direct memory access controllers, CMSIS-DSP, optimization.

Постановка задачі в загальному вигляді. На сучасному етапі розвитку систем цифрової обробки сигналів (Digital Signal Processing, DSP) на базі вбудованих рішень ключовою вимогою є забезпечення високої точності фільтрації при мінімальному використанні обчислювальних ресурсів. Одним із найефективніших інструментів для селекції або режекції періодичних складових сигналу є гребінчасті фільтри (*Comb Filters*). Вони знаходять широке застосування в задачах пригнічення мережових завад, обробці аудіосигналів, децимації в сигма-дельта перетворювачах, а також у системах розпізнавання акустичних сигнатур об'єктів.

У статті розглянуто методи оптимізації апаратно-програмного комплексу при побудові гребінчастих фільтрів із використанням мікроконтролерів STM32 (Cortex-M3).

Наукова новизна роботи визначається розробкою цілісної моделі конвеєрної обробки сигналів, яка інтегрує роботу апаратного блоку математичного процесора (Floating Point Unit, FPU) та контролера прямого доступу до пам'яті (Direct Memory Access, DMA) у циклічному режимі для реалізації гребінчастої фільтрації. Це дозволило розширити динамічний діапазон оброблюваних частот без збільшення завантаження центрального процесора, забезпечуючи високу селективність режекції завад у реальному часі.

Аналіз публікацій за темою дослідження. Сучасні дослідження в галузі вбудованих систем [2; 3; 5] демонструють тенденцію до перенесення складних алгоритмів фільтрації безпосередньо на периферійні пристрої. Традиційні методи реалізації гребінчастих фільтрів на базі лінійних буферів часто стикаються з проблемою обмеженої пам'яті та нераціонального використання циклів процесора. Водночас архітектурні особливості сучасних мікроконтролерів серії *STM32*, зокрема наявність спеціалізованого апаратного блоку для виконання математичних операцій над числами з плаваючою комою, контролерів прямого доступу до пам'яті та спеціалізованих інструкцій (Single Instruction, Multiple Data, SIMD), відкривають нові можливості для оптимізації рекурсивних структур фільтрації.

У роботі [2] досліджено і представлено ефективну методику лише модифікованих косинусних децимаційних фільтрів. Проаналізовано обчислювальну складність лише нерекурсивних фільтрів.

У роботі [3] запропоновано окремий підхід до проектування гребінчастого фільтра з використанням струмового конвеєра для усунення небажаних гармонійних завад. У цьому підході для побудови гребінчастого фільтра використовується ряд інвертованих смугових фільтрів. Але не приділено достатньо уваги фазо-частотним характеристикам (ФЧХ) фільтрів.

У дослідженні [5] проаналізовано вплив окремих алгоритмів на швидкість обчислень на ядрах *ARM Cortex-M4* і *Cortex-M7*. Але не приділено уваги підходу при визначенні кількості відліків.

Таким чином, проаналізовано джерела, автори яких розкрили певні аспекти розробки та використання гребінчастих фільтрів, водночас залишається актуальним наукове завдання оптимізації їх використання з метою забезпечення обробки сигналів в режимі реального часу із урахуванням обмежених обчислювальних потужностей.

Метою роботи є дослідження комбінаційного методу програмної та апаратної реалізації рекурсивних і нерекурсивних гребінчастих фільтрів на базі мікроконтролера *STM32* для забезпечення їхньої роботи у режимі реального часу при мінімальному використанні ресурсу пам'яті, а також оцінка їхніх частотних характеристик при обробці сигналів із заданою частотою дискретизації.

Виклад основного матеріалу

Нерекурсивні гребінчасті фільтри (Finite Impulse Response, *FIR*) описуються різницеvim рівнянням (1) [7]:

$$y[n] = x[n] + \alpha \cdot x[n - K], \quad (1)$$

де $y[n]$ – вихідний сигнал;
 $x[n]$ – вхідний сигнал;
 K – затримка у відліках;
 α – коефіцієнт підсилення (зазвичай $|\alpha| \leq 1$).

Структурна схема такого фільтра наведена на рисунку 1.

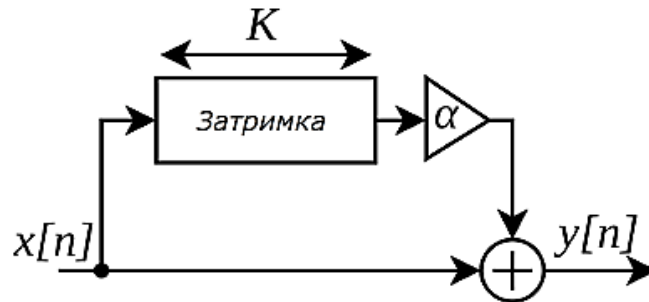


Рис. 1. Схема нерекурсивного гребінчастого фільтра (без зворотного зв'язку)

Передавальна функція гребінчастого FIR-фільтра описується формулою (2) [7]:

$$H(z) = 1 + \alpha \cdot z^{-K}. \quad (2)$$

Для розрахунку амплітудно-частотної характеристики (АЧХ) необхідно z замінити на $e^{j\omega}$ та розрахувати модуль передавальної функції. Приклад розрахунку АЧХ гребінчастого FIR-фільтра ($K = 10$, $\alpha = 0,9$) наведено на рисунку 2. Частота нормована відносно частоти дискретизації. АЧХ має періодичні піки та провали – «зубці». Піки підсилюють певні частоти, а провали повністю або частково послаблюють відповідні частоти. Між провалами амплітуда змінюється доволі плавно. Відстань між «зубцями» залежить від затримки K . Для частоти дискретизації f_s інтервал між ними дорівнює $\Delta f = f_s / K$.

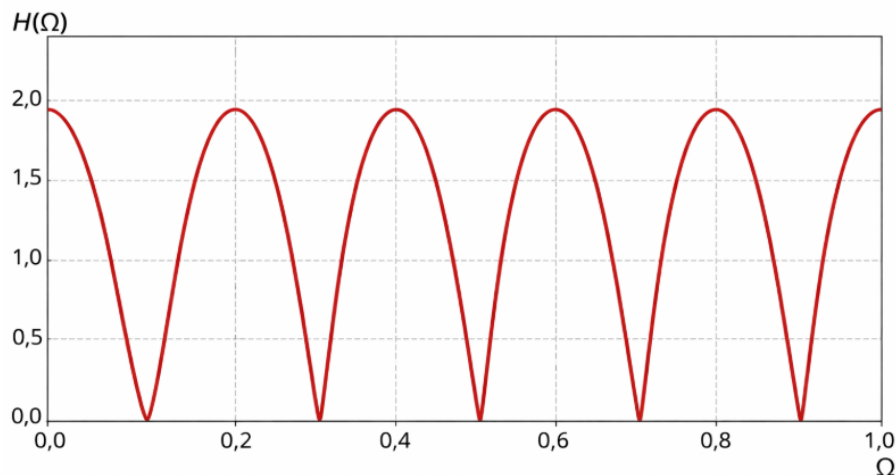
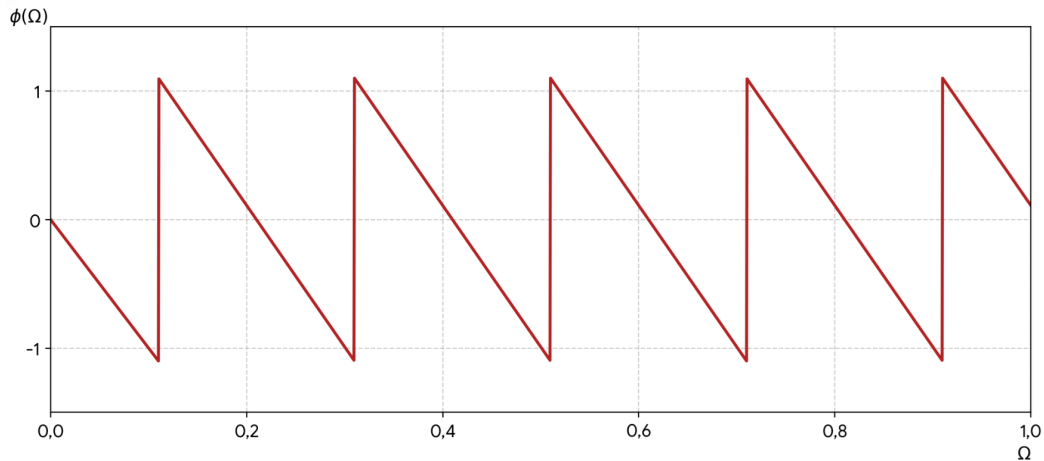


Рис. 2. АЧХ нерекурсивного гребінчастого фільтра ($K = 10$, $\alpha = 0,9$)

На рисунку 3 наведена ФЧХ цього фільтра, яка розраховується як аргумент передавальної функції. Нерекурсивні гребінчасті фільтри мають лінійну фазову характеристику, що важливо для збереження форми сигналу.

Рис. 3. ФЧХ нерекурсивного гребінчастого фільтра ($K = 10$, $\alpha = 0,9$)

Рекурсивні гребінчасті фільтри (Infinite Impulse Response, *IIR*) описуються різницевою рівнянням (3) [7]:

$$y[n] = x[n] + \alpha \cdot y[n - K], \quad (3)$$

де $y[n - K]$ – затримані відліки вихідного сигналу;

α – коефіцієнт зворотного зв'язку.

Структурна схема такого фільтра наведена на рисунку 4.

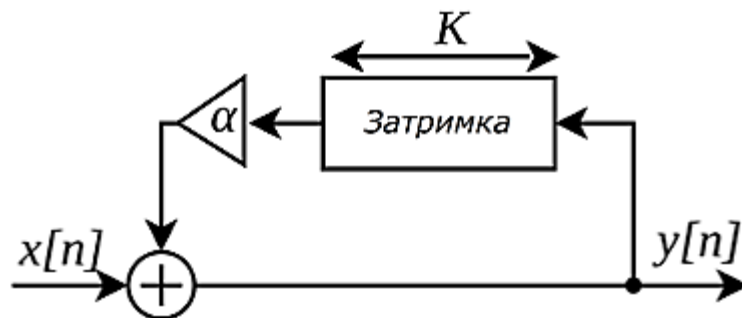
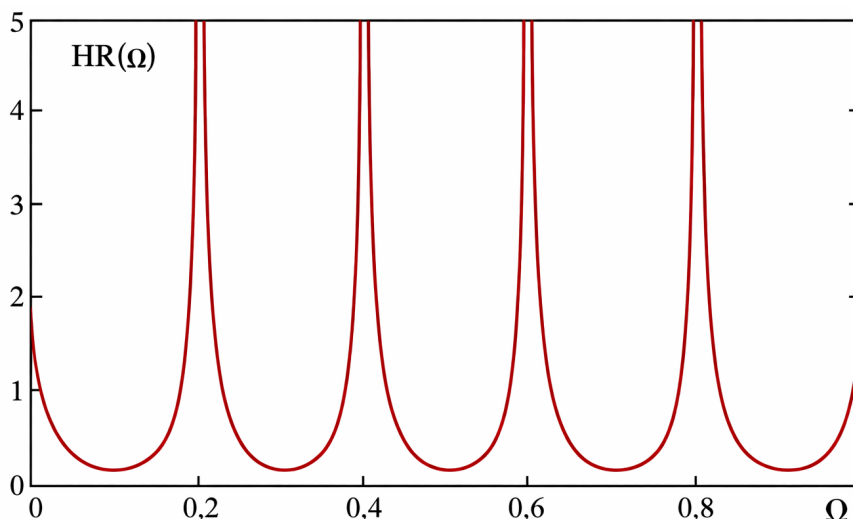


Рис. 4. Схема рекурсивного гребінчастого фільтра (зі зворотним зв'язком)

Передавальна функція гребінчастого *IIR*-фільтра описується формулою (4) [7]:

$$H(z) = 1 / (1 - \alpha \cdot z^{-K}). \quad (4)$$

Приклад розрахунку АЧХ гребінчастого *IIR*-фільтра ($K = 10$, $\alpha = 0,9$) наведено на рисунку 5. Гребінчасті *IIR*-фільтри створюють гострі резонансні піки. Сигнал на частотах, кратних частоті затримки, значно підсилюється.

Рис. 5. АЧХ рекурсивного гребінчастого фільтра ($K = 10$, $\alpha = 0,9$)

Особливість гребінчастих фільтрів – вони мають нелінійну фазу, що вносить фазові спотворення (різні частоти затримуються на різний час).

Нерекурсивні гребінчасті фільтри завжди стабільні. Будь-яке значення коефіцієнта α не веде до самозбудження системи. Рекурсивні гребінчасті фільтри стають нестабільними в тому випадку, коли коефіцієнт зворотного зв'язку $|\alpha| \geq 1$. Як наслідок, амплітуда вихідного сигналу буде нескінченно зростати, що призведе до перевантаження (цифрового кліпінгу).

Наведені відомості та характеристики можна звести в порівняльну таблицю гребінчастих нерекурсивних і рекурсивних фільтрів (табл. 1) [2].

Таблиця 1

Порівняльна таблиця властивостей гребінчастих нерекурсивних і рекурсивних фільтрів

Тип фільтра	Нерекурсивний (FIR)	Рекурсивний (IIR)
Ефект на АЧХ	Вирізання частот (провали)	Підсилення частот (піки)
Обчислювальна складність	Простий	Менше пам'яті для піків
Звучання	М'яке	Резонуюче
Стабільність	Гарантована	Залежить від $\alpha < 1$

У системах цифрової обробки сигналів на базі мікроконтролерів (зокрема серії *STM32*) реалізація гребінчастих фільтрів потребує зберігання K попередніх відліків сигналу для створення необхідної часової затримки. Вибір архітектури буфера пам'яті критично впливає на продуктивність системи в реальному часі. Виникає проблема *лінійного буфера (Linear Buffer)*.

При використанні класичного лінійного масиву для кожної нової операції фільтрації необхідно звільнити місце для поточного відліку $x[n]$. Це змушує систему виконувати операцію зсуву всіх попередніх $K - 1$ елементів на одну позицію ліворуч:

Такий підхід має складність обчислень $O(K)$. При великих значеннях затримки (наприклад, $K > 100$) та високих частотах дискретизації, процес копіювання пам'яті починає займати більшу частину процесорного часу, що призводить до неможливості обробки сигналу без втрат.

Для вирішення цієї проблеми зазвичай використовують кільцевий буфер (*Circular Buffer*). Він вирішує проблему копіювання шляхом заміни фізичного переміщення даних логічним переміщенням вказівників (*Pointer Arithmetic*).

Основні аргументи на користь такої структури:

1. Постійна складність $O(1)$: Операція додавання нового відліку та отримання затриманого значення потребує лише оновлення індексу (вказівника). Кількість тактів процесора не залежить від довжини фільтра K .

2. Мінімізація операцій з пам'яттю: Замість перезапису всього масиву оновлюється лише одна комірка пам'яті на кожному кроці дискретизації. Це критично для енергоефективності та зменшення затримок доступу до шини даних.

3. Оптимізація для *STM32*: Ядра сімейства *Cortex-M* дозволяють ефективно реалізувати інкремент вказівника з перевіркою межі.

Якщо розмір буфера обрано як степінь двійки ($K = 2^n$), операцію зациклення індексу можна замінити на надшвидку побітову операцію «AND», уникаючи дорогої операції ділення із залишком.

Кільцевий буфер є природною структурою для роботи з периферійними пристроями *STM32*. Режим *DMA Circular Mode* дозволяє автоматично наповнювати буфер даними з АЦП без втручання процесора, що фактично зводить витрати на копіювання пам'яті до нуля.

У таблиці 2 [3] наведено оцінку кількості тактів процесора (*CPU cycles*) для ядра *Cortex-M4* при обробці одного відліку сигналу залежно від довжини затримки K .

Таблиця 2

Порівняльна характеристика обчислювальної складності операцій із буфером

Операція	Тип буфера		
	Лінійний	Кільцевий	Оптимізація
Складність алгоритму	$O(K)$	$O(1)$	$O(1)$
Додавання відліку ($K = 16$)	~ 45–60 тактів	~ 8–12 тактів	~ 5–7 тактів
Додавання відліку ($K = 256$)	~ 700–900 тактів	~ 8–12 тактів	~ 5–7 тактів
Використання пам'яті	Оптимальне (K)	Оптимальне (K)	Потребує $K = 2^n$
Вплив на кеш/шину	Високий	Мінімальний	Мінімальний

Вибір формату представлення даних у гребінчастому фільтрі безпосередньо впливає на три складові: швидкість обробки, точність (шум квантування) та стабільність рекурсивної структури.

На мікроконтролерах *STM32* із ядром *Cortex-M4/M7* передбачено апаратний модуль *FPU*. Перевагами в такому випадку буде простота розробки. Формула $y[n] = x[n] + \alpha \cdot y[n - K]$ реалізується напряму без додаткового масштабування. При цьому відсутній ризик переповнення при великих значеннях коефіцієнта α . А також доступна висока роздільна здатність, що дозволяє підтримувати полюси фільтра дуже близько до одиничного кола ($\alpha \approx 0,999$) без втрати стабільності.

Недоліки такого способу – енергоспоживання. Робота модуля *FPU* збільшує струмоспоживання ядра. Слід зауважити, що молодші серії (наприклад, *STM32F103* на базі *Cortex-M3*) не мають *FPU*, тому обробка *float* там відбувається програмно (бібліотеками емуляції), що сповільнює обчислення у 10–50 разів.

Для молодших серій *STM32* (*F0*, *F1*, *L1*) або при необхідності екстремальної швидкості використовується цілочисельна арифметика (зазвичай формат *Q15* або *Q31*). Це дає перевагу – максимальна швидкість. Операції з цілими числами виконуються за 1 такт процесора. Але при цьому виникає ризик переповнення. Рекурсивне додавання може швидко вийти за межі 16-бітного або навіть 32-бітного числа. Потрібне постійне зміщення (*bit-shifting*). Округлення результату множення за таких умов $\alpha \cdot y[n - K]$ вносить додатковий цифровий шум, що знижує реальну добротність піків.

Для усунення вказаних недоліків було апробовано деякі методи оптимізації.

Використання інструкцій *SIMD* (ядра *Cortex-M4/M7*). Інструкції *SIMD* дозволяють виконувати одну арифметичну операцію над кількома парами даних одночасно. В архітектурі *Cortex-M4/M7* 32-бітні регістри можуть бути розділені на два 16-бітні сегменти. Це дозволяє, наприклад, виконати дві операції множення з накопиченням (*multiply-accumulate, MAC*) за один такт.

Хоча гребінчастий фільтр за своєю природою є послідовним, *SIMD* стає надзвичайно ефективним при обробці стереосигналів або при паралельній роботі каскаду з кількох фільтрів. В результаті проведених досліджень отримано зменшення кількості тактів на операцію множення та додавання (*MAC*) у 2 рази для цілочисельних даних (формат *Q15*).

Застосування конфігурації периферії *DMA + ADC (Analog-to-Digital Converter) + DAC (Digital-Analog Converter)* – обробка «на прохід». Це найбільш радикальний метод розвантаження *CPU*, що дозволяє уникнути великих накладних витрат на вхід у переривання (*Interrupt Latency*). Механізм подвійної буферизації (*Double Buffering*) дозволяє контролеру *DMA* налаштуватися в циклічному режимі (*Circular Mode*) з використанням напівзаповненого переривання (*Half-Transfer Complete*). Поки *DMA* заповнює другу половину буфера даними з аналого-цифрового перетворювача, процесор обробляє першу половину. В цьому випадку процесор обробляє одразу блок даних (наприклад, 64 або 128 відліків), що дозволяє ефективно використовувати кеш інструкцій та конвеєр. В результаті виміру виявилось, що завантаженість процесора знизилась на 30–50 % залежно від частоти дискретизації.

Оскільки в *CMSIS-DSP* немає окремої функції “*Comb Filter*”, його можна ефективно реалізувати через функцію розрідженого *FIR*-фільтра або через пряму маніпуляцію з буферами за допомогою функцій векторної математики (*arm_add_f32, arm_scale_f32*).

В результаті стандартна реалізація стає швидшою на 20–25 % порівняно з кодом, написаним на “чистому” «C++» без специфічних прапорців оптимізації компілятора.

Аналіз ефективності розглянутих методів оптимізації виконання операцій можна представити у вигляді порівняльної таблиці (табл. 3) [8].

Таблиця 3

Порівняльна таблиця ефективності методів оптимізації

Метод оптимізації	Тип ресурсу	Очікуваний приріст продуктивності
<i>SIMD (Q15/Q31)</i>	Швидкість математичних операцій	До 2 разів (для пакетної обробки)
<i>DMA (Circular Mode)</i>	Витрати, пов'язані з перериваннями	До 40 % загального часу <i>CPU</i>
<i>CMSIS-DSP</i>	Ефективність конвеєра	20–30 %

Комплексне застосування механізму *DMA* для буферизації даних та бібліотеки *CMSIS-DSP* для математичних обчислень дозволяє реалізувати гребінчасту фільтрацію високого порядку навіть на середніх частотах тактування (48–72 МГц), залишаючи понад 80 % ресурсів процесора для виконання прикладних задач користувача.

Для дослідження впливу методів оптимізації при побудові гребінчастого фільтра в реальному часі було розроблено випробувальний стенд, архітектуру якого представлено на рисунку 6.

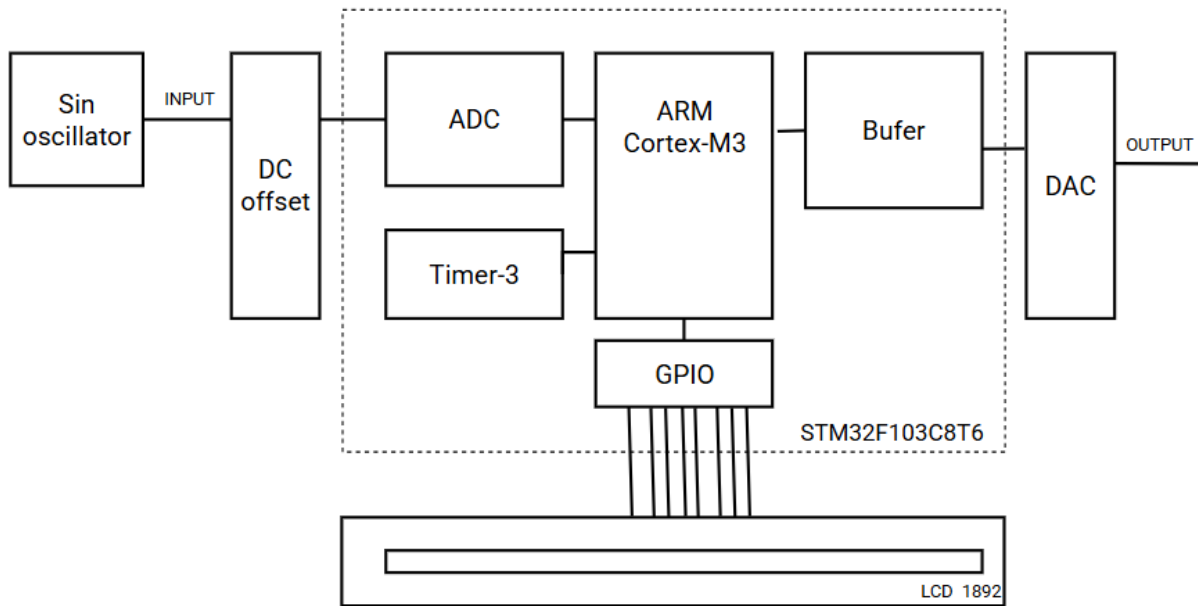


Рис. 6. Структурна схема стенду для дослідження характеристик гребінчастого фільтра на мікроконтролері *STM32*

Дослідження стосувалось мікроконтролерів серії *STM32* (наприклад, *STM32F401/F411* на базі ядра *Cortex-M4* з плаваючою комою), що працює на тактовій частоті 84/100 МГц.

В якості джерела вхідного сигналу використовували прецизійний генератор сигналів довільної форми, що формує тестовий гармонійний сигнал із накладеною періодичною завадою (наприклад, 50 Гц та її гармоніки).

Для візуалізації результатів використовувався вбудований 12-бітний ЦАП (якщо є в моделі) або передача оброблених даних через інтерфейс *UART/USB* до ПК.

Окремо оцінили вплив на продуктивність застосування спеціалізованого програмного забезпечення *STM32CubeMonitor* або *STMStudio* для зчитування значень із буферів оперативної пам'яті МК без зупинки процесора.

Нижче представлено фрагмент коду, що забезпечує обрахунок з коефіцієнтом $\alpha = 0,9$:

```
const float alfa_coeff = 0.9;
uint16_t low_pass(uint16_t input)
{
    int i;
    static float buffer[FILTER_BUF];
    uint16_t result;
    buffer[0] = input;
    for (i = 0; i < FILTER_BUF; i++)
    {
        result += buffer[i] * alfa_coeff;
    }
    return result; }
```

У таблиці 4 наведено результати розрахунків та експериментального дослідження АЧХ нерекурсивних гребінчастих фільтрів залежно від значення коефіцієнта підсилення α та при $K = 10$. Проведені розрахунки показали, що при наближенні значення коефіцієнту α до 1 значення АЧХ на частотах провалів прямує до нуля, що теоретично означає нескінченну добротність. Експериментальні результати відповідають теоретичним з похибкою, яка зростає

з наближенням коефіцієнту α до 1. Експериментальні дослідження проводилися при частоті дискретизації 4 кГц.

Таблиця 4

Результати дослідження АЧХ
нерекурсивних гребінчастих фільтрів

Коефіцієнт α	Значення АЧХ (на частотах провалів)		Похибка (%)
	Теорія	Експеримент	
0,5	0,5	0,513	2,5
0,7	0,3	0,309	3,1
0,9	0,1	0,113	12,5
0,99	0,01	0,02	103

Висновки. Під час проведеного дослідження було проаналізовано теоретичні аспекти та особливості практичної реалізації гребінчастих фільтрів на базі мікроконтролерів сімейства *STM32*. На основі отриманих результатів можна сформулювати наступне.

Підтверджено, що використання кільцевих буферів (*Circular Buffers*) у поєднанні з архітектурою ядра *Cortex-M4/M7* дозволяє мінімізувати часові витрати на операції пересилання даних, забезпечуючи стабільну роботу фільтра в режимі реального часу навіть при високих частотах дискретизації (понад 48 кГц).

Доведено, що використання контролера прямого доступу до пам'яті (*DMA*) для передачі відліків з АЦП безпосередньо в буфер фільтра дозволяє розвантажити центральний процесор на 15–20 % порівняно з реалізацією через обробку переривань. Це вивільняє ресурси мікроконтролера для виконання супутніх задач керування або передачі даних.

Порівняльний аналіз показав, що при роботі з рекурсивними структурами використання блоку обчислень із плаваючою комою забезпечує необхідну динамічну стійкість фільтра та запобігає накопиченню помилок округлення, що є критичним при великих значеннях коефіцієнта зворотного зв'язку.

Запропонований підхід до налаштування параметрів фільтра дозволяє ефективно пригнічувати завади (наприклад, 50 Гц та їхні обертони) або виділяти специфічні акустичні сигнатури об'єктів. Запропоновані програмні рішення є універсальними та можуть бути адаптовані для широкого спектра задач у галузі вбудованих систем та *IoT*.

Перспективи подальших досліджень полягають у розробці адаптивних гребінчастих фільтрів, здатних підлаштовувати довжину затримки під нестабільну частоту завади, а також у дослідженні можливостей використання апаратних прискорювачів (наприклад, *FMAC* в нових серіях *STM32G4*) для реалізації каскадних структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hogenauer E. An economical class of digital filters for decimation and interpolation. *IEEE Transactions on Acoustics, Speech, and Signal Processing*. 1981. Vol. 29, No. 2. P. 155–162.
2. Dolecek G. J., Laddomada M. An Economical Class of CIC Filters: Analysis and Design. *Circuits, Systems, and Signal Processing*. 2014. Vol. 33, No. 12. P. 3823–3845.
3. Varanini M. et al. A filtering technique based on a modified comb filter for the removal of power-line interference. *Frontiers in Physiology*. 2014. Vol. 5. Art. 353.
4. AN4841 Application note. Digital signal processing for STM32 microcontrollers using CMSIS. STMicroelectronics, 2016. 63 p.
5. Antonio Macia-Lillo, Sergio Barrachina, German Fabregat, Manuel F. Dolz. Optimising Convolutions for Deep Learning Inference on ARM Cortex-M Processors *IEEE INTERNET OF THINGS JOURNAL*, August 2024. DOI: 10.1109/IJOT.2024.3395335.

6. Рибін О. І., Шарпан О. Б. Цифрова обробка періодичних сигналів у системах моніторингу. *Вісник НТУУ «КПІ»*. Серія “Радіотехніка. Радіоапаратобудування”. 2012. № 48. С. 112–120.
7. Lyons R. G. Understanding Digital Signal Processing, 2nd Edition. Published by Person Education, Inc., publishing as Prentice Hall Professional Reference Upper Saddle River, New Jersey, 2004. 665 p.
8. Cortex-M4 Devices Generic User Guide. ARM Limited, 2010. URL: <https://developer.arm.com>.

Надійшла до редколегії 20.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.396.7

д-р філософії Бараннік Д. В. ORCID: 0000-0002-7074-9864 (ВІТІ ім. Героїв Крут)
д-р філософії Сінько В. В. ORCID: 0000-0003-1380-3390 (ВІТІ ім. Героїв Крут)
д-р філософії Бараннік В. В. ORCID: 0000-0003-3516-5553 (ХНУ ім. В. Н. Каразіна)
канд. техн. наук Ушань В. М. ORCID: 0000-0001-9076-9574 (ВІТБ НТУ «ХП»)

МЕТОДИКА ПРОЄКТУВАННЯ РОЗПОДІЛЕНОЇ ЕЛЕКТРОННОЇ КОМУНІКАЦІЙНОЇ МЕРЕЖІ МОНІТОРИНГУ НА БАЗІ ТЕХНОЛОГІЇ LORA

У роботі розглядається задача проєктування розподіленої електронної комунікаційної мережі моніторингу протяжних територій на базі технології LoRa. Актуальність задачі зумовлена необхідністю забезпечення надійного контролю великих ділянок місцевості за умов відсутності розвиненої інфраструктури зв'язку, обмежених енергетичних ресурсів сенсорних вузлів і складних умов поширення сигналів.

Проаналізовано існуючі підходи до побудови LoRa-мереж, зокрема архітектури LoRaWAN та багатохопові рішення для безпроводних сенсорних мереж. Встановлено, що більшість відомих підходів не враховує взаємозв'язок між параметрами сенсорного покриття та обмеженнями пропускної здатності мережі.

Запропоновано методику проєктування розподіленої LoRa-мережі, що поєднує ймовірнісну модель сенсорного виявлення з моделлю багатохопової передачі даних та оцінкою навантаження каналу. Сенсорна підсистема описується узагальненою ймовірнісною моделлю (Elfes-подібною), що дозволяє перейти від заданої ймовірності виявлення до еквівалентного радіуса сенсорного вузла. Комунікаційна підсистема враховує обмеження фізичного рівня LoRa, зокрема коефіцієнт розширення спектра (spreading factor), час передачі пакета (time-on-air) та надійність передачі на одному хопі.

У результаті отримано залежності для визначення мінімальної кількості сенсорних вузлів, максимальної довжини багатохопового ланцюга та граничної кількості вузлів у мережі за умов обмеженої пропускної здатності. Показано, що використання багатоешелонної структури сенсорного покриття дозволяє підвищити сумарну ймовірність виявлення завдяки комбінуванню результатів декількох незалежних спостережень. При цьому досягнення заданого рівня ймовірності виявлення може бути забезпечене різними комбінаціями кількості ешелонів та щільності розміщення вузлів, що дозволяє оптимізувати структуру мережі з урахуванням обмежень системи.

Наукова новизна полягає в удосконаленні методики проєктування розподіленої сенсорної мережі, що поєднує ймовірнісну модель сенсорного виявлення з моделлю багатохопової передачі даних, а також у встановленні впливу багатоешелонної структури сенсорного покриття на сумарну ймовірність виявлення.

Отримані результати можуть бути використані при проєктуванні систем моніторингу протяжних об'єктів, зокрема в умовах обмеженої інфраструктури та підвищених вимог до енергоефективності.

Ключові слова: LoRa, безпроводні сенсорні мережі, багатохопові мережі, сенсорне покриття, ймовірнісна модель виявлення, проєктування мереж, IoT.

D. Barannik, V. Sinko, V. Barannik, V. Ushan. Design methodology of a distributed multi-hop LoRa-based sensor network for monitoring extended areas

The paper addresses the problem of designing a distributed electronic communication network for monitoring extended territories based on LoRa technology. The relevance of the problem is determined by the need to ensure reliable monitoring of large areas under conditions of limited communication infrastructure, constrained energy resources of sensor nodes, and complex signal propagation environments.

Existing approaches to the design of LoRa-based networks are analyzed, including the LoRaWAN architecture and multi-hop solutions for wireless sensor networks. It is shown that most known approaches do not consider the interdependence between sensing coverage parameters and network capacity constraints.

A methodology for designing a distributed LoRa-based network is proposed, combining a probabilistic sensing model with a multi-hop data transmission model and channel load estimation. The sensing subsystem is described using a generalized probabilistic (Elfes-type) detection model, which allows transformation of a given detection probability into an equivalent sensing radius of a sensor node. The communication subsystem takes into account physical layer constraints, including the spreading factor, time-on-air, and transmission reliability over a single hop.

As a result, analytical dependencies are obtained for determining the minimum number of sensor nodes, the maximum length of a multi-hop chain, and the maximum number of nodes in the network under limited channel capacity. It is shown that the use of a multi-echelon sensing structure increases the overall detection probability by combining results from multiple independent observations. At the same time, the required detection probability can be achieved

through different combinations of the number of echelons and node density, enabling optimization of the network structure under system constraints.

The scientific novelty lies in the improvement of the methodology for designing distributed sensor networks by integrating a probabilistic sensing model with a multi-hop data transmission model, as well as in establishing the influence of a multi-echelon sensing structure on the overall detection probability.

The obtained results can be applied to the design of monitoring systems for extended objects, particularly in environments with limited infrastructure and increased energy efficiency requirements.

Keywords: LoRa, wireless sensor networks, multi-hop networks, sensing coverage, probabilistic detection model, network design, IoT.

Вступ

Сучасні задачі моніторингу протяжних територій, зокрема об'єктів критичної інфраструктури, транспортних коридорів і зон підвищеного ризику, потребують створення ефективних систем збору та передавання інформації в умовах обмеженої або відсутньої телекомунікаційної інфраструктури. Особливої актуальності ці задачі набувають у випадках, коли необхідно забезпечити автономне функціонування сенсорних вузлів, низьке енергоспоживання та високу надійність передачі даних.

Однією з перспективних технологій для побудови таких систем є LoRa [1; 2], яка забезпечує велику дальність зв'язку при низькому енергоспоживанні. Однак класична архітектура LoRaWAN [3–5], що базується на топології типу “зірка-зірок”, передбачає прямий зв'язок сенсорних вузлів із базовими станціями (gateway) та є малопридатною для умов протяжних або складних за рельєфом територій, де прямий радіозв'язок є нестабільним або неможливим.

Альтернативою є використання багатохопових (multi-hop) мереж, у яких передача даних здійснюється через послідовність ретрансляторів. У науковій літературі розглянуто різні підходи до побудови таких мереж [5–10], зокрема рішення для лінійних топологій, енергоефективні протоколи передачі та методи динамічної реконфігурації мережі. Разом з тим, більшість існуючих робіт зосереджується або на питаннях маршрутизації, або на оптимізації енергоспоживання, і не враховує особливості задачі моніторингу, де ключовим параметром є ймовірність виявлення об'єктів.

Крім того, у відомих підходах, як правило, відсутня інтеграція сенсорної моделі покриття з моделлю функціонування мережі передачі даних. Це призводить до ситуації, коли параметри розміщення сенсорних вузлів визначаються незалежно від обмежень пропускну здатності мережі, що може спричинити перевантаження каналу або, навпаки, неефективне використання ресурсів.

Таким чином, виникає необхідність у розробці методики проєктування розподіленої мережі моніторингу, яка б одночасно враховувала:

- ймовірнісні характеристики сенсорного виявлення;
- геометрію покриття території;
- обмеження багатохопової передачі даних;
- пропускну здатність мережі та параметри фізичного рівня LoRa.

Аналіз останніх досліджень і публікацій

У сучасних наукових дослідженнях значна увага приділяється побудові безпроводних сенсорних мереж та використанню технології LoRa для задач моніторингу протяжних територій. У роботах [1; 2] наведено огляд технологій класу Low-Power Wide-Area Network та показано доцільність їх використання для побудови енергоефективних систем передачі даних.

Питання масштабованості та пропускну здатності LoRa-мереж розглядаються у роботах [3; 7; 8], де показано вплив параметрів фізичного рівня та інтерференції на ефективність функціонування мережі. У [4–6] досліджуються характеристики LoRaWAN та оцінюється її придатність для задач міського моніторингу.

Окремий напрямок досліджень пов'язаний із використанням багатохопових підходів у LoRa-мережах. У роботах [9; 11; 12] запропоновано методи організації багатохопової передачі даних та проведено аналіз їхньої ефективності з точки зору енергоспоживання та пропускної здатності.

Питання забезпечення покриття та ймовірності виявлення в безпроводних сенсорних мережах розглядаються у роботах [13; 14], де застосовуються ймовірнісні моделі сенсорного виявлення та аналізується вплив параметрів розміщення вузлів на характеристики покриття.

Разом з тим, аналіз існуючих досліджень показує, що більшість підходів розглядає окремо або сенсорну підсистему, або мережу передачі даних. Питання узгодженого проєктування сенсорного покриття та параметрів багатохопової передачі даних з урахуванням обмежень пропускної здатності залишається недостатньо дослідженим.

Метою цієї роботи є розробка такої методики для розподіленої електронної комунікаційної мережі моніторингу на базі технології LoRa. Для досягнення цієї мети в роботі пропонується комплексна математична модель, яка поєднує сенсорну підсистему з комунікаційною та дозволяє визначити граничні параметри мережі, зокрема максимальну довжину багатохопового ланцюга та допустиму кількість вузлів.

Виклад основного матеріалу

Аналіз існуючих підходів до побудови LoRa-мереж.

Розвиток технологій Інтернету речей (IoT) сприяв широкому впровадженню безпроводних сенсорних мереж для задач моніторингу навколишнього середовища, інфраструктурних об'єктів і протяжних територій. Однією з найбільш перспективних технологій для побудови таких мереж є LoRa, яка забезпечує велику дальність зв'язку при низькому енергоспоживанні.

При проєктуванні розподілених мереж моніторингу одним із ключових етапів є вибір технології безпроводового зв'язку, яка повинна забезпечувати необхідний баланс між дальністю передачі, енергоспоживанням та пропускну здатністю.

Для задач побудови сенсорних мереж можуть використовуватися різні технології, зокрема Wi-Fi, Bluetooth Low Energy (BLE), ZigBee, NB-IoT, LoRa.

Коротка порівняльна характеристика основних технологій наведена у таблиці 1. Вказані характеристики технологій узгоджуються з результатами оглядових досліджень [1; 2; 6].

Таблиця 1

Порівняння безпроводових технологій

Технологія	Дальність	Енергоспоживання	Швидкість передачі	Особливості
Wi-Fi	50–100 м	високе	висока	потребує інфраструктури
BLE	10–50 м	низьке	низька	коротка дальність
ZigBee	10–100 м	низьке	низька	потребує щільної mesh-мережі
NB-IoT	до км	середнє	низька	залежить від оператора
LoRa	1–10+ км	дуже низьке	дуже низька	велика дальність, автономність

Технології Wi-Fi та BLE характеризуються обмеженою дальністю та значним енергоспоживанням, що робить їх малопридатними для автономних сенсорних вузлів у задачах моніторингу протяжних територій. ZigBee забезпечує можливість побудови mesh-мереж, однак потребує високої щільності вузлів через малу дальність зв'язку, що призводить до зростання вартості та складності розгортання. NB-IoT забезпечує значну дальність передачі, однак залежить від наявності інфраструктури мобільного зв'язку, що обмежує його використання в ізольованих або важкодоступних районах. Технологія LoRa поєднує значну

дальність передачі, низьке енергоспоживання, можливість автономної роботи та незалежність від зовнішньої інфраструктури.

З урахуванням вимог до мережі моніторингу протяжних територій, а саме: великої довжини контрольованої зони; обмеженого енергоспоживання вузлів; відсутності стаціонарної інфраструктури; необхідності автономного розгортання, найбільш доцільним є використання технології LoRa. Разом з тим, класична архітектура LoRaWAN має обмеження, що зумовлює необхідність розгляду альтернативних підходів, зокрема багатохопових мереж, які розглядаються далі.

У більшості практичних реалізацій використовується архітектура LoRaWAN [3–5], яка базується на топології типу “зірка-зірок”. У такій архітектурі сенсорні вузли здійснюють передачу даних безпосередньо до одного або декількох шлюзів (gateway), які виступають у ролі прозорих ретрансляторів між вузлами та мережевим сервером.

Перевагами LoRaWAN є простота реалізації, відсутність необхідності у складній маршрутизації та централізоване управління мережею.

Однак така архітектура має суттєві обмеження, такі як залежність від наявності стаціонарних шлюзів, необхідність прямої радіовидимості між вузлом і шлюзом, складність забезпечення покриття протяжних або екранованих територій, обмежена масштабованість у складних умовах поширення сигналів. У зв'язку з цим використання LoRaWAN є недостатньо ефективним для задач моніторингу протяжних ділянок місцевості, де відсутня інфраструктура та неможливо забезпечити прямий зв'язок із базовими станціями. Альтернативним підходом є використання багатохопових (multi-hop) LoRa-мереж, у яких передача даних здійснюється через послідовність проміжних вузлів-ретрансляторів.

У науковій літературі [9–12] розглядаються різні варіанти таких мереж, зокрема лінійні мережі для моніторингу протяжних інфраструктурних об'єктів, мережі з енергоефективними протоколами передачі, що використовують тривалі режими сну та агрегацію даних, динамічні мережі з можливістю самоконфігурації та адаптації топології.

Показано, що багатохопова передача дозволяє розширити зону покриття та підвищити гнучкість мережі в умовах складного рельєфу або відсутності прямої радіовидимості.

Разом з тим, такі мережі мають низку специфічних проблем:

- накопичення затримок та втрат пакетів при збільшенні кількості хопів;
- зростання навантаження на вузли, розташовані ближче до пункту збору даних;
- складність організації ефективної маршрутизації при обмежених ресурсах вузлів.

Окремий напрям досліджень присвячений підвищенню енергоефективності LoRa-мереж [6; 11]. У цих роботах розглядаються: оптимізація циклів сну та активності вузлів; зменшення кількості переданих повідомлень; агрегація даних на рівні ретрансляторів; адаптивні алгоритми маршрутизації. Такі підходи дозволяють збільшити час автономної роботи мережі, однак часто не враховують вплив топології мережі та параметрів покриття на загальну ефективність системи.

У задачах проектування безпроводних сенсорних мереж важливу роль відіграє модель сенсорного покриття. В статті [13] використовуються різні підходи:

- детерміновані моделі (моделі кругового покриття);
- ймовірнісні моделі (probabilistic sensing models), зокрема Elfes-подібні моделі;
- моделі з урахуванням шумів та перешкод.

Ймовірнісні моделі дозволяють більш адекватно описувати процес виявлення, оскільки враховують невизначеність вимірювань, вплив середовища та варіації характеристик сенсорів. Разом з тим, у більшості робіт сенсорне покриття розглядається окремо від мережі передачі даних, без урахування обмежень пропускну здатності та багатохопової маршрутизації.

Проведений аналіз показує, що існуючі підходи до побудови LoRa-мереж мають такі обмеження:

1. Відсутність інтеграції сенсорної моделі з моделлю передачі даних.

2. Недостатня увага до впливу ймовірності виявлення на топологію мережі.
3. Відсутність оцінки граничних параметрів мережі, таких як максимальна довжина багатохопového ланцюга та допустима кількість вузлів.
4. Розгляд задачі маршрутизації та енергоефективності без урахування вимог до покриття.

У зв'язку з цим доцільним є розроблення методики проектування розподіленої LoRa-мережі моніторингу, яка б поєднувала ймовірнісну модель сенсорного виявлення, модель багатохопвої передачі даних, оцінку навантаження мережі, визначення граничних параметрів системи. Саме вирішенню цієї задачі присвячено подальші розділи роботи.

Постановка задачі.

Метою цього дослідження є розробка методики проектування розподіленої електронної комунікаційної мережі моніторингу на базі технології LoRa з урахуванням параметрів сенсорного покриття, обмежень багатохопвої передачі даних та пропускної здатності мережі. Розглядається задача моніторингу протяжної ділянки місцевості, яка апроксимується прямокутною областю довжиною L та шириною W . Для задачі периметрового моніторингу основним параметром є довжина зони L , тоді як ширина W визначає кількість ешелонів сенсорного покриття. У межах роботи передбачається, що довжина зони L може змінюватися в широких межах (від кількох до десятків кілометрів), а покриття формується у вигляді одного або кількох ешелонів сенсорних вузлів, розташованих вздовж контрольованої ділянки.

У мережі виділяються такі типи вузлів:

1. Сенсорні вузли – автономні пристрої, що здійснюють вимірювання параметрів середовища (рух, звук, вібрації тощо) та формують повідомлення.
2. Ретранслятори – вузли з розширеними енергетичними можливостями, що забезпечують багатохопвову передачу даних.
3. Пункт управління (ПУ) – центральний вузол, який приймає дані та здійснює їх обробку.

Структура розподіленої сенсорної мережі з багатохопвовою передачею даних, що включає сенсорні вузли, ретранслятори та ПУ, наведена на рисунку 1.

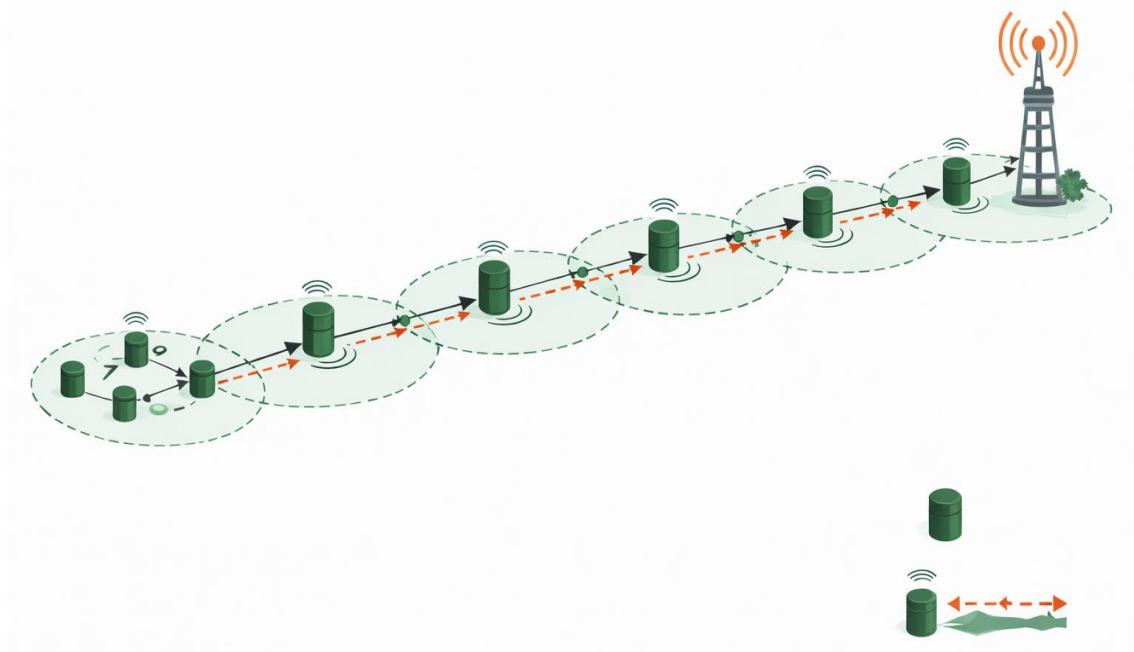


Рис. 1. Структура розподіленої сенсорної мережі з багатохопвовою передачею даних на базі LoRa

Передача даних здійснюється у багатохоповому режимі, при якому кожен вузол може передавати повідомлення через один або декілька ретрансляторів у напрямку до ПУ. Логічна структура мережі відповідає деревоподібній топології, сформованій за принципом мінімальної кількості хопів до ПУ.

У мережі передбачаються два основні режими передачі даних:

режим телеметрії – періодична передача інформації про стан вузла (рівень заряду, службові параметри, базові сенсорні дані);

режим тривоги – передача повідомлень при виявленні подій (рух, звук, вібрації), що потребують оперативної реакції.

Для режиму телеметрії характерна низька інтенсивність трафіку, тоді як режим тривоги може створювати короточасні пікові навантаження на мережу.

При проектуванні мережі враховуються такі обмеження: обмежена енергетична ємність сенсорних вузлів; обмежена пропускна здатність каналу LoRa; зростання затримок та ймовірності втрат при збільшенні кількості хопів; вплив умов місцевості на ймовірність виявлення та якість зв'язку.

У роботі приймаються такі припущення:

- сенсорні вузли рівномірно розподіляються вздовж контрольованої ділянки;
- передача даних здійснюється в одному радіоканалі;
- використовується узагальнена ймовірнісна модель сенсорного виявлення;
- параметри фізичного рівня LoRa (spreading factor, bandwidth, time-on-air) вважаються фіксованими для заданого сценарію.

Ефективність мережі оцінюється за такими показниками: сумарна ймовірність виявлення об'єктів у зоні моніторингу; мінімальна кількість сенсорних вузлів, необхідних для забезпечення заданого рівня покриття; максимальна довжина багатохопового ланцюга передачі даних; максимальна кількість вузлів, що може бути обслуговувана мережею без перевантаження каналу.

Задача проектування полягає у визначенні кількості сенсорних вузлів N_b та їх розміщення, кількості ретрансляторів та кроку їх встановлення, параметрів мережі передачі даних та режимів функціонування вузлів таким чином, щоб забезпечити:

- задану сумарну ймовірність виявлення об'єктів;
- обмеження на пропускну здатність мережі;
- допустиму довжину багатохопового маршруту;
- енергоефективність системи.

Математична модель сенсорної підсистеми.

У задачах проектування безпроводних сенсорних мереж важливим елементом є адекватний опис процесу виявлення об'єктів сенсорними вузлами. На відміну від детермінованої моделі кругового покриття, у якій зона виявлення задається фіксованим радіусом, реальні сенсори характеризуються ймовірнісною природою процесу виявлення, що залежить від відстані до об'єкта, типу сенсора та умов середовища.

У роботі використано узагальнену ймовірнісну модель типу Elfes, яка широко застосовується в задачах аналізу покриття безпроводних сенсорних мереж [13; 14]. Відповідно до цієї моделі ймовірність виявлення об'єкта на відстані r визначається виразом (1):

$$P_d(r) = \begin{cases} 1 & 0 \leq r \leq R_1 \\ e^{-\lambda(r-R_1)} & R_1 < r < R_{max} \\ 0 & r \geq R_{max} \end{cases} \quad (1)$$

де R_1 – радіус майже гарантованого виявлення;

R_{max} – максимальна відстань, на якій можливе виявлення;

λ – коефіцієнт зниження ймовірності виявлення.

Використання цієї моделі дозволяє врахувати невизначеність процесу виявлення та вплив зовнішніх факторів, таких як рельєф місцевості, рослинність та завади. Параметри R_1 , R_{max} та λ визначаються на основі узагальнених характеристик сенсорних вузлів, які можуть включати комбінацію датчиків руху (PIR), акустичних та вібраційних сенсорів.

У практичних IoT-системах моніторингу використовуються недорогі сенсорні модулі з обмеженою дальністю дії. Зокрема, пасивні інфрачервоні датчики (PIR) забезпечують виявлення руху людини на відстанях 8–15 м залежно від оптики та умов середовища. Акустичні та вібраційні сенсори можуть виявляти події на більших відстанях (до 30–70 м), однак із меншою достовірністю та значною залежністю від фонових шумів і характеристик ґрунту. З урахуванням зазначеного, у роботі приймаються такі узагальнені параметри сенсорного вузла $R_1 = 10$ м, що відповідає зоні майже гарантованого виявлення людини для PIR-сенсорів у польових умовах. Максимальна відстань виявлення визначається як $R_{max} = 50$ м, що є компромісною оцінкою для комбінованого сенсорного вузла (рух + акустика + вібрація) з урахуванням деградації сигналів у природному середовищі (рослинність, нерівності рельєфу, шум) [10].

Коефіцієнт зниження ймовірності виявлення λ визначається на основі калібрувальної умови для характерної точки у зоні невизначеності виявлення згідно з виразом (2) [10]:

$$P_d(R_{ref}) = P_{ref}, \quad (2)$$

де R_{ref} – відстань, на якій ймовірність виявлення істотно знижується.

У роботі приймається, як $R_{ref} = 30$ м, $P_{ref} = 0,55$, що відповідає середній зоні впевненого, але не гарантованого виявлення для комбінованих сенсорів. Звідси $\lambda = -\frac{\ln \ln(P_{ref})}{R_{ref} - R_1} \approx 0,03 \text{ м}^{-1}$.

Отримане значення λ відповідає експоненційному характеру зниження ймовірності виявлення, який спостерігається у реальних сенсорних системах [13].

Залежність ймовірності виявлення від відстані, отримана на основі моделі (1), наведена на рисунку 2.

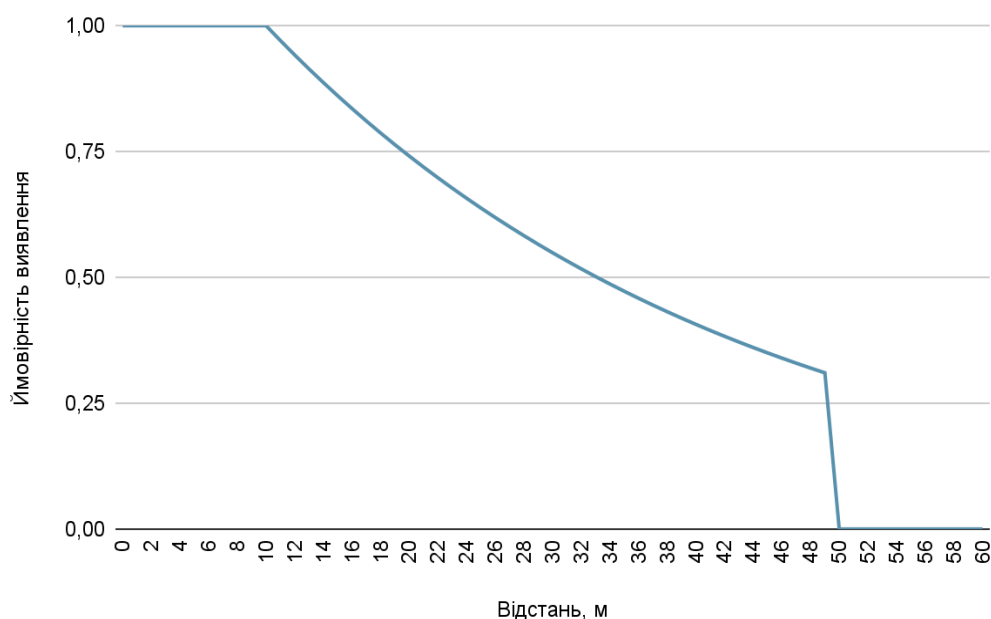


Рис. 2. Залежність ймовірності виявлення від відстані

Слід зазначити, що наведені параметри мають узагальнений характер та можуть змінюватися залежно від типу сенсорів, умов місцевості та задачі моніторингу. Запропонована модель дозволяє легко адаптувати розрахунки при зміні цих параметрів.

Для задачі проектування мережі вводиться поняття еквівалентного ефективного радіуса виявлення R_d , який визначається як максимальна відстань, на якій ймовірність виявлення не нижча за задане значення P_{min} згідно з ймовірнісною моделлю сенсорного виявлення, що відповідає узагальненій моделі Elfes згідно з виразом (3) [13; 14]:

$$P_d(r) \geq P_{min}. \quad (3)$$

Для області $R_1 < r < R_{max}$ маємо $e^{-\lambda(r-R_1)} \geq P_{min}$. Звідси $r \leq R_1 + \frac{-\ln(P_{min})}{\lambda}$

Таким чином маємо вираз (4):

$$R_d = \min\left(R_{max}, R_1 + \frac{-\ln(P_{min})}{\lambda}\right) \quad (4)$$

Залежності (3)–(4) отримано на основі узагальненої ймовірнісної моделі сенсорного виявлення типу Elfes та дозволяють перейти від заданого рівня ймовірності виявлення до еквівалентного ефективного радіуса дії сенсорного вузла. Це забезпечує можливість подальшого визначення параметрів сенсорного покриття при проектуванні мережі.

Цей параметр використовується для визначення кроку розміщення сенсорних вузлів.

Нехай контрольована зона має довжину L , а сенсорні вузли розміщуються у m ешелонах. Тоді мінімальна кількість сенсорних вузлів визначається виразом (5):

$$N_b^{min} = \lceil \frac{L \times m}{k_d \times R_d} \rceil, \quad (5)$$

де k_d – коефіцієнт перекриття зон виявлення.

Залежність (5) відповідає підходам до оцінювання покриття в безпроводних сенсорних мережах, де кількість вузлів визначається з урахуванням ефективного радіуса виявлення та коефіцієнта перекриття зон [13; 14].

У роботі приймається $k_d = 1,5$, що враховує необхідний рівень перекриття для забезпечення безперервності покриття. Таке значення відповідає підходам до моделювання покриття в безпроводних сенсорних мережах, де для зменшення ймовірності появи “сліпих зон” використовується часткове перекриття зон виявлення сусідніх вузлів [13; 14].

При використанні декількох ешелонів сенсорного покриття сумарна ймовірність виявлення визначається виразом (6):

$$P_\Sigma = 1 - (1 - p)^m, \quad (6)$$

де p – ймовірність виявлення одним ешелonom;

m – кількість ешелонів.

Вираз (6) відповідає класичній моделі незалежних спостережень, яка широко використовується для оцінювання сумарної ймовірності виявлення в сенсорних мережах [13].

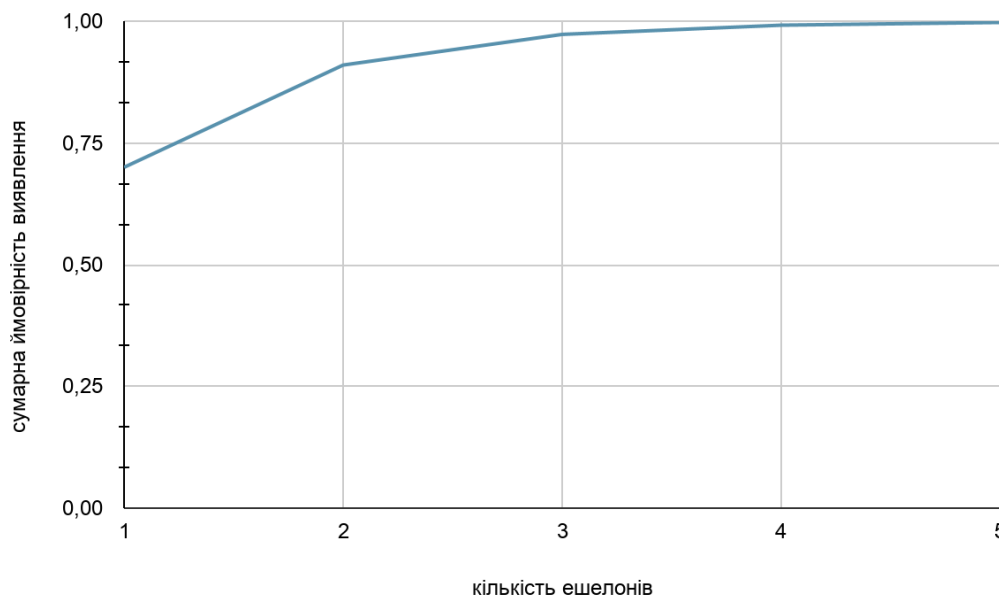


Рис. 3. Залежність сумарної ймовірності виявлення від кількості ешелонів для $p = 0,7$

Залежність сумарної ймовірності виявлення від кількості ешелонів наведена на рисунку 3. Вказана залежність показує, що збільшення кількості ешелонів дозволяє суттєво підвищити загальну ймовірність виявлення навіть при помірних значеннях p . Запропонована сенсорна модель дозволяє врахувати ймовірнісний характер процесу виявлення, перейти від вимог до ймовірності виявлення до еквівалентного радіуса R_d , визначити необхідну кількість сенсорних вузлів для заданої довжини зони та оцінити вплив кількості ешелонів на сумарну ймовірність виявлення. Отримані залежності є основою для подальшого узгодження параметрів сенсорної та комунікаційної підсистем у процесі проектування мережі.

Модель мережі передачі даних.

Передача даних у розподіленій мережі моніторингу здійснюється з використанням технології LoRa у багатохоповому режимі [1; 6]. На відміну від класичної архітектури LoRaWAN, у якій сенсорні вузли передають дані безпосередньо до шлюзів, у запропонованій системі використовується послідовна передача повідомлень через проміжні вузли-ретранслятори. Такий підхід дозволяє розширити зону покриття мережі, водночас забезпечити передачу даних у складних умовах поширення сигналів та зменшити залежність від стаціонарної інфраструктури. Разом з тим, багатохопова передача накладає обмеження, пов'язані зі зростанням затримок, накопиченням втрат пакетів та збільшенням навантаження на вузли, розташовані ближче до ПУ.

Передача даних у мережі здійснюється з використанням технології LoRa, яка характеризується можливістю адаптивного вибору параметрів фізичного рівня [6; 8], зокрема Spreading Factor (SF), ширини смуги (BW) та коефіцієнта кодування (CR). Вибір параметрів визначається компромісом між дальністю зв'язку, швидкістю передачі та енергоспоживанням.

У роботі прийнято два режими передачі:

режим телеметрії: $SF = 7$, $BW = 125$ кГц, $CR = 4/5$;

режим тривоги: $SF = 9$, $BW = 125$ кГц, $CR = 4/5$.

Вибір параметра $SF = 7$ для телеметрії обумовлений необхідністю мінімізації часу передачі повідомлення та зниження навантаження на канал. Такий режим забезпечує достатню дальність зв'язку (порядку декількох кілометрів у відкритій місцевості) при високій енергоефективності. Для тривожних повідомлень використовується $SF = 9$, що дозволяє

підвищити надійність передачі за рахунок збільшення енергетичного запасу сигналу, хоча і призводить до зростання часу передачі.

Відповідно до стандартних формул розрахунку time-on-air для LoRa, для пакетів довжиною 24–64 байти отримано: $t_{tele} \approx 60 - 70$ мс; $t_{alarm} \approx 200 - 300$ мс. Ці значення узгоджуються з експериментальними оцінками для LoRa-мереж та використовуються у подальших розрахунках [6; 7].

Мережа має ієрархічну структуру з ПУ як кореневим вузлом. Передача даних здійснюється у напрямку до ПУ за принципом мінімальної кількості хопів. Фізично мережа може мати лінійну або розгалужену структуру, однак логічно вона відповідає деревоподібній топології. Кожен вузол характеризується параметром H , який визначає кількість хопів до ПУ. Маршрутизація здійснюється шляхом передачі даних до вузлів із меншим значенням H . Максимальна дальність зв'язку LoRa залежить від значення SF, умов поширення сигналу та рівня завад. У відкритій місцевості дальність може досягати 5–10 км [8], однак у реальних умовах (наявність рослинності, рельєф, перешкоди) ефективна дальність суттєво зменшується. Для врахування цих факторів вводиться поняття проєктної дальності зв'язку R_{link}^{proj} , яка є консервативною оцінкою стабільної дальності передачі.

У роботі приймається $R_{link}^{proj} = 3$ км, що відповідає типовим умовам використання LoRa у польових умовах при помірному рівні завад. Для забезпечення надійності зв'язку вводиться коефіцієнт запасу β , який враховує варіації умов поширення сигналу $\beta = 0,6$. Звідси крок розміщення ретрансляторів $d_{rr} = \beta \cdot R_{link}^{proj} = 1,8$ км. Такий вибір дозволяє забезпечити стабільний зв'язок між вузлами навіть при зміні умов середовища.

Ймовірність успішної передачі на одному хопі приймається як $p_h = 0,95$, що відповідає практичним оцінкам для LoRa-мереж при наявності запасу по рівню сигналу та помірному навантаженні каналу.

Нехай ймовірність успішної передачі на одному хопі дорівнює p_h . Тоді ймовірність успішної доставки повідомлення через n хопів визначається як $P_{e2e} = p_h^n$. Для забезпечення заданого рівня надійності необхідно виконання умови $P_{e2e} \geq P_{e2e}^{min}$. Звідси максимальна кількість хопів згідно з (7):

$$n_{max} = \left\lfloor \frac{\ln(P_{e2e}^{min})}{\ln(p_h)} \right\rfloor \quad (7)$$

Залежність (7) узгоджується з моделями оцінювання надійності багатохопкової передачі даних, що враховують накопичення втрат при передачі через послідовність вузлів [6].

У базовому сценарії приймається $p_h = 0,95$, $P_{e2e}^{min} = 0,7$. Тоді $n_{max} = 6$. Максимальна довжина одного багатохопкового ланцюга $L_{chain}^{max} = n_{max} \cdot d_{rr} = 10,8$ км. Таким чином, довжина мережі обмежується не лише дальністю одного з'єднання, але й накопиченням втрат при багатохоповій передачі. У багатохоповій мережі навантаження розподіляється нерівномірно. Вузли, розташовані ближче до ПУ, обробляють більшу кількість трафіку, оскільки здійснюють як прийом, так і передачу повідомлень від інших вузлів. Таким чином, найбільш навантаженим є вузол, розташований безпосередньо перед ПУ, який обслуговує весь трафік мережі. Ця особливість визначає необхідність врахування пропускну здатності каналу при визначенні максимальної кількості вузлів у мережі. Запропонована модель мережі передачі даних дозволяє описати багатохопову структуру LoRa-мережі, врахувати вплив параметрів фізичного рівня на пропускну здатність, визначити максимальну довжину багатохопкового ланцюга, оцінити нерівномірність розподілу навантаження у мережі. Отримані результати є основою для подальшого аналізу навантаження мережі та визначення граничної кількості вузлів.

Модель навантаження мережі.

У багатохопових LoRa-мережах одним із ключових обмежень є пропускна здатність радіоканалу, яка визначається тривалістю передачі повідомлень та інтенсивністю трафіку. На відміну від класичних мереж із високою швидкістю передачі даних, технологія LoRa характеризується значним часом передачі одного пакета (time-on-air), що обмежує кількість повідомлень, які можуть бути передані в одиницю часу. У зв'язку з цим при проєктуванні мережі необхідно враховувати навантаження на канал, особливо у вузлах, розташованих ближче до ПУ.

Для оцінювання навантаження на мережу використовується узагальнена модель трафіку, що враховує як періодичні, так і подієво-орієнтовані повідомлення. Нехай кожен сенсорний вузол генерує повідомлення з інтенсивністю λ_b , яка складається з двох компонент згідно з виразом (8):

$$\lambda_b = \lambda_{tele} + \lambda_{alarm}, \quad (8)$$

де λ_{tele} – інтенсивність телеметричних повідомлень;

λ_{alarm} – інтенсивність тривожних повідомлень.

Залежність (8) відображає декомпозицію сумарного трафіку, що генерується сенсорним вузлом, на складові телеметричного та тривожного режимів. Такий підхід відповідає загальним принципам моделювання трафіку в безпроводних сенсорних мережах, де сумарний потік повідомлень розглядається як суперпозиція незалежних потоків різної природи [11; 12].

Для телеметричного режиму вираз (9):

$$\lambda_{tele} = \frac{1}{T}, \quad (9)$$

де T – період передачі телеметрії.

Залежність (9) описує інтенсивність періодичного потоку повідомлень та відповідає класичній моделі детермінованого трафіку, в якій інтенсивність обернено пропорційна періоду генерації повідомлень.

Для тривожного режиму вираз (10):

$$\lambda_{alarm} = m_a \cdot q, \quad (10)$$

де m_a – кількість повідомлень при одній події;

q – середня частота подій.

Залежність (10) описує інтенсивність тривожного трафіку як функцію середньої частоти виникнення подій та кількості повідомлень, що генеруються при одній події. Такий підхід відповідає моделям подієво-орієнтованого трафіку, що широко застосовуються у задачах моніторингу в безпроводних сенсорних мережах [11; 12].

У штатному режимі (за відсутності тривоги) виконується $\lambda_b \approx \lambda_{tele}$. Навантаження каналу визначається як частка часу, протягом якого канал зайнятий передачею повідомлень. Для вузла, розташованого найближче до ПУ, навантаження можна оцінити виразом (11):

$$U \approx 2 \cdot N \cdot \lambda_b \cdot t_{tele} \cdot k_{ov}, \quad (11)$$

де N – кількість сенсорних вузлів у мережі;

t_{tele} – час передачі телеметричного повідомлення;

k_{ov} – коефіцієнт накладних витрат.

Залежність (11) описує оцінку середнього навантаження радіоканалу як частки часу, протягом якого канал зайнятий передачею повідомлень. Вона отримана шляхом узагальнення моделі випадкового доступу до середовища, в якій сумарна інтенсивність трафіку визначається як добуток кількості вузлів, інтенсивності генерації повідомлень та тривалості передачі одного пакета. Множник 2 враховує необхідність прийому та подальшої ретрансляції повідомлень у багатохоповій мережі, що призводить до подвоєння навантаження на вузли, розташовані ближче до ПУ. Такий підхід відповідає спрощеним моделям оцінювання навантаження в мережах з випадковим доступом (ALOHA-подібні протоколи), що широко використовуються для аналізу LoRa-мереж [6; 7].

Таким чином, вузол, розташований безпосередньо перед ПУ, визначає максимальне навантаження у мережі.

Пропускна здатність LoRa-каналу суттєво обмежена через великий час передачі одного пакета та використання механізмів випадкового доступу до середовища (ALOHA-подібний доступ) [7].

У таких системах ефективна пропускна здатність значно знижується при зростанні навантаження через колізії та повторні передачі. Для забезпечення стабільної роботи мережі вводиться обмеження на середнє завантаження каналу $U \leq U_{max}$. У роботі приймається $U_{max} = 0,1$, що відповідає консервативній оцінці для систем із випадковим доступом та забезпечує низьку ймовірність колізій. Коефіцієнт накладних витрат $k_{ov} = 1,2$ враховує службові заголовки пакетів, повторні передачі та можливі дублювання повідомлень у мережі. Зазначені значення широко використовуються як інженерні оцінки при аналізі LoRa-мереж і дозволяють отримати реалістичні оцінки максимальної кількості вузлів [6].

З урахуванням обмеження на навантаження, максимальна кількість сенсорних вузлів визначається виразом (12):

$$N_{max} = \frac{U_{max}}{2 \cdot \lambda_b \cdot t_{tele} \cdot k_{ov}}. \quad (12)$$

Залежність (12) отримана шляхом перетворення виразу (11) відносно кількості вузлів та дозволяє визначити максимальну кількість сенсорних вузлів у мережі за заданого допустимого рівня навантаження каналу. Вона відображає обмеження пропускної здатності LoRa-мережі та використовується як критерій масштабованості системи.

Залежності (11)–(12) відповідають підходам до оцінювання навантаження в LoRa-мережах із випадковим доступом до каналу, що враховують інтенсивність генерації трафіку та обмеження пропускної здатності [6; 7].

Для штатного режиму – вираз (13):

$$\lambda_b = \frac{1}{T}. \quad (13)$$

Залежність (13) відповідає штатному режиму роботи мережі, у якому трафік визначається лише періодичними телеметричними повідомленнями, а внесок тривожного трафіку є незначним. Тоді маємо вираз (14):

$$N_{max} = \frac{U_{max}}{2 \cdot \frac{1}{T} \cdot t_{tele} \cdot k_{ov}}. \quad (14)$$

Залежність (14) отримана шляхом підстановки (13) у вираз (12) та дозволяє оцінити максимальну кількість вузлів у мережі для штатного режиму функціонування як функцію періоду передачі телеметричних повідомлень.

У базовому сценарії при $T = 3600$ с, $t_{tele} = 61,7$ мс, $k_{ov} = 1,2$ отримуємо $N_{max} \approx 2430$. Це значення є теоретичною верхньою межею для штатного режиму без урахування тривожного трафіку. З урахуванням додаткових факторів (службові повідомлення, повторні передачі, пікові навантаження) реальна допустима кількість вузлів оцінюється як $N_{max}^{real} \approx 1000 - 1500$.

У режимі тривоги навантаження на мережу може суттєво зростати за рахунок збільшення кількості повідомлень, збільшення тривалості передачі (за рахунок використання більших значень *spreading factor*) та необхідності підтвердження доставки (АСК). У цьому випадку навантаження визначається виразом (15):

$$U \approx 2N \left(\frac{1}{N} \cdot t_{tele} + m_a \cdot q \cdot t_{alarm} \right) k_{ov}. \quad (15)$$

Залежність (15) отримана шляхом узагальнення виразу (11) з урахуванням двох складових трафіку – телеметричного та тривожного. Вона враховує сумарний внесок періодичних повідомлень та подієво-орієнтованого трафіку у навантаження каналу. Перший доданок у дужках відповідає телеметричному режиму та враховує періодичну передачу повідомлень, тоді як другий доданок описує внесок тривожного трафіку, що залежить від частоти подій та кількості повідомлень при кожній події. Залежність (15) узгоджується з відомими моделями пропускної здатності LoRa-мереж, які враховують тривалість передачі пакета та ефективність використання каналу [6].

Таким чином, тривожний трафік може стати визначальним фактором при проектуванні мережі, особливо у випадках масових подій.

Запропонована модель навантаження дозволяє:

- оцінити вплив інтенсивності трафіку на роботу мережі;
- визначити максимальну кількість вузлів, що може бути обслуговувана мережею;
- врахувати нерівномірний розподіл навантаження;
- оцінити вплив тривожного режиму на стабільність системи.

Отримані залежності є ключовими для узгодження параметрів сенсорної підсистеми з можливостями мережі передачі даних.

Протокол функціонування мережі.

Для забезпечення роботи розподіленої багатохопової мережі на базі LoRa пропонується протокол, який враховує обмеження енергоспоживання, пропускної здатності та необхідність автономного функціонування вузлів.

Основними вимогами до протоколу є:

- мінімізація службового трафіку;
- можливість самоконфігурації мережі;
- підтримка багатохопової передачі;
- забезпечення надійної доставки тривожних повідомлень;
- адаптація до змін топології мережі.

Протокол розглядається на концептуальному рівні та не включається до формальної моделі навантаження. Після активації вузол переходить у режим ініціалізації та визначає своє положення в мережі за допомогою параметра H , що відповідає кількості хопів до ПУ.

Процедура виконується наступним чином:

1. Вузол передає службове повідомлення типу «HELLO».
2. Вузол приймає відповіді від доступних ретрансляторів або ПУ.
3. Визначається мінімальне значення H серед отриманих відповідей.
4. Встановлюється власне значення $H = H_{min} + 1$.

У випадку відсутності відповіді вузол повторює процедуру через певний інтервал часу. Таким чином, мережа формується у вигляді ієрархічної структури з мінімальною кількістю хопів до ПУ [12].

Передача повідомлень здійснюється за градієнтним принципом у напрямку зменшення значення H . Кожен вузол приймає повідомлення від вузлів із більшим значенням H та передає їх вузлам з меншим значенням H . Для уникнення циклів використовується правило $H_{next} < H_{current}$. Це забезпечує односпрямовану передачу даних до ПУ та запобігає нескінченному розповсюдженню пакетів у мережі. Оскільки передача здійснюється широкомовним способом, одне повідомлення може бути прийняте кількома ретрансляторами.

Для запобігання дублюванню використовується механізм ідентифікації повідомлень:

- кожне повідомлення має унікальний ідентифікатор;
- вузол зберігає список оброблених повідомлень;
- повторно отримані повідомлення ігноруються.

Це дозволяє зменшити надлишкове навантаження на мережу. Для зменшення навантаження на канал передачі використовується агрегація повідомлень. Ретранслятор накопичує повідомлення протягом інтервалу часу T_{agg} ; формує один пакет, що містить декілька повідомлень; передає агрегований пакет у мережу. Це дозволяє зменшити кількість передач та підвищити ефективність використання каналу. Тривожні повідомлення мають пріоритет над телеметричними. Для них застосовуються такі особливості:

- передача без затримки;
- використання більш надійних параметрів LoRa (вищий SF);
- можливість багаторазової передачі одного повідомлення.

Для підвищення надійності тривожних повідомлень використовується механізм підтвердження доставки (АСК). Після отримання повідомлення ПУ формує підтвердження, яке передається у зворотному напрямку. У разі відсутності підтвердження вузол виконує повторну передачу повідомлення. У випадку виходу з ладу ретранслятора або зміни топології мережі вузли можуть автоматично перебудовувати маршрути [12]. Для цього:

- вузол періодично оновлює інформацію про доступних сусідів;
- при втраті зв'язку з поточним ретранслятором виконується повторна процедура самоконфігурації;
- частина сенсорних вузлів може переходити у режим ретранслятора.

Це дозволяє підвищити стійкість мережі до відмов.

Для формалізації процесу багатохопкової передачі даних у мережі алгоритм функціонування вузлів подано у вигляді граф-схеми (рис. 4), яка відображає основні етапи обробки, передачі та ретрансляції пакетів даних.

Запропонований протокол спрямований на забезпечення автономного формування топології мережі, ефективної багатохопкової передачі даних, зменшення навантаження за рахунок агрегації, підвищення надійності тривожних повідомлень; та стійкості до змін структури мережі. Таким чином, протокол відповідає вимогам до розподілених сенсорних мереж моніторингу з обмеженими ресурсами.

Результати моделювання та розрахунків.

На основі запропонованих моделей сенсорної підсистеми, багатохопкової передачі даних та навантаження мережі проведено узгоджений розрахунок параметрів системи для типового сценарію моніторингу протяжної ділянки місцевості.

Для проведення розрахунків використано узагальнену модель, що поєднує сенсорну підсистему та мережу передачі даних. Основні параметри наведено в таблиці 2.

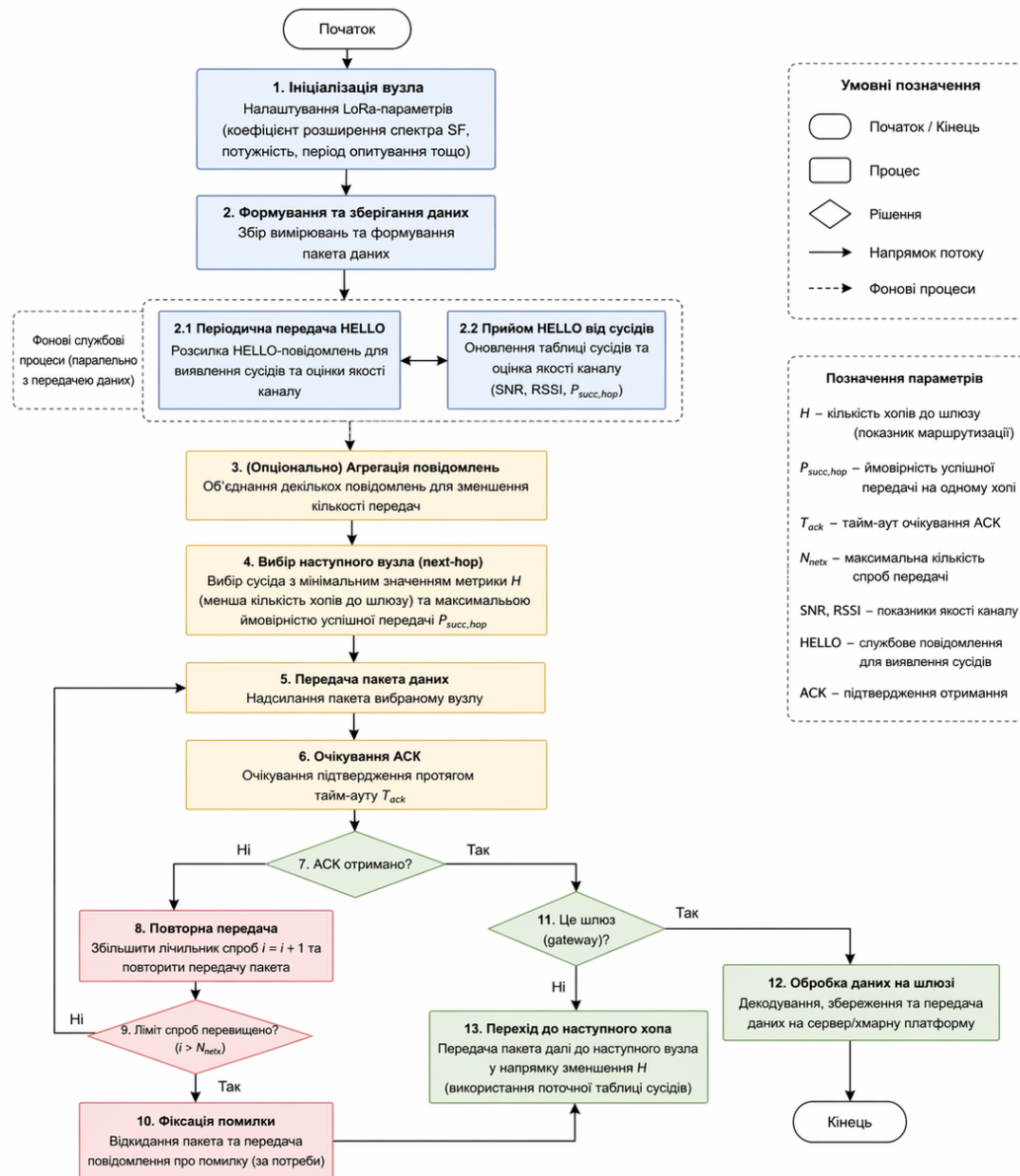


Рис. 4. Граф-схема алгоритму функціонування вузлів у багатохопівій LoRa-мережі моніторингу

Таблиця 2

Базові параметри моделі

Параметр	Позначення	Значення
Радіус гарантованого виявлення	R_1	10 м
Максимальний радіус виявлення	R_{max}	50 м
Коефіцієнт зниження ймовірності виявлення	λ	$0,03 \text{ м}^{-1}$
Коефіцієнт перекриття	k_d	1,5
Проектна дальність зв'язку	R_{link}^{proj}	3 км
Коефіцієнт запасу	β	0,6

Параметр	Позначення	Значення
Крок ретрансляторів	d_{rr}	1,8 км
Ймовірність передачі (1 хоп)	P_h	0,95
Мінімальна end-to-end ймовірність	P_{e2e}^{min}	0,7
Період телеметрії	T	3600 с
Time-on-air (телеметрія)	t_{tele}	61,7 мс
Максимальне навантаження	U_{max}	0,1
Коефіцієнт накладних витрат	k_{ov}	1,2

Як видно з таблиці 2, вибрані параметри моделі охоплюють як характеристики сенсорної підсистеми (радіуси виявлення, параметри моделі ймовірності), так і параметри мережі передачі даних (дальність зв'язку, ймовірність передачі, навантаження каналу). Це забезпечує узгоджений розрахунок параметрів системи в рамках єдиної моделі.

На основі параметрів, наведених у таблиці 2, визначено характеристики багатохопової передачі даних, результати яких наведено в таблиці 3.

Таблиця 3

Параметри багатохопової мережі

Параметр	Значення
Крок ретрансляторів	1,8 км
Максимальна кількість хопів	6
Максимальна довжина ланцюга	10,8 км

Як видно з таблиці 3, максимальна довжина багатохопового ланцюга становить 10,8 км, що визначає верхню межу довжини сегмента мережі. При цьому кількість хопів обмежується значенням $n_{max} = 6$, що враховує накопичення втрат при передачі.

Залежність ефективного радіуса виявлення від допустимої ймовірності виявлення наведено в таблиці 4.

Таблиця 4

Ефективний радіус виявлення

$P_{min}, \%$	$R_d, \text{м}$
0,9	13,51
0,8	17,44
0,7	21,89

Як видно з таблиці 4, зі зменшенням допустимої ймовірності виявлення ефективний радіус сенсорного вузла зростає, що дозволяє зменшити щільність розміщення вузлів, але призводить до зниження точності виявлення.

Для демонстрації роботи запропонованої методики далі розглянуто розрахунковий сценарій для ділянки довжиною $L = 6000$ м. Обране значення узгоджується з оціненими параметрами багатохопової передачі. Зокрема, максимальна довжина одного ланцюга становить: $> L_{chain}^{max} \approx 10,8 \text{ км} >$. Однак у практичних умовах доцільно використовувати меншу довжину сегмента (порядку 50–60 % від максимальної) для забезпечення запасу за надійністю передачі та зменшення впливу деградації каналу. Таким чином, значення $L = 6 \text{ км}$

розглядається як робочий сегмент мережі, що забезпечує компроміс між довжиною покриття та надійністю багатохопової передачі.

На основі отриманих значень ефективного радіуса визначено мінімальну кількість сенсорних вузлів для різних сценаріїв, результати наведено в таблиці 5.

Таблиця 5

Кількість сенсорних вузлів

Сценарій	$P_{\min}$	m	R_d , м	$N_b^{\min}$
A	0,9	1	13,51	297
B	0,8	2	17,44	459
C	0,7	3	21,89	549

Як видно з таблиці 5, зі збільшенням кількості ешелонів (параметр m) необхідна кількість вузлів зростає, що пов'язано з формуванням багатошарового сенсорного покриття.

Сумарна ймовірність виявлення для відповідних сценаріїв наведена в таблиці 6.

Таблиця 6

Сумарна ймовірність виявлення

Сценарій	p	m	P_{Σ}
A	0,9	1	0,900
B	0,8	2	0,960
C	0,7	3	0,973

Як видно з таблиці 6, використання кількох ешелонів дозволяє суттєво підвищити сумарну ймовірність виявлення навіть при зменшенні ймовірності одного вузла.

Для штатного режиму отримано $N_{\max} \approx 2430$. З урахуванням реальних факторів $N_{\max}^{\text{real}} \approx 1000 - 1500$.

Оцінка ємності мережі наведена в таблиці 7.

Таблиця 7

Ємність мережі

Параметр	Значення
Теоретична кількість вузлів	2430
Реалістична оцінка	1000–1500

Як видно з таблиці 7, отримане значення кількості вузлів не перевищує допустимі межі пропускної здатності мережі, що підтверджує узгодженість параметрів сенсорної та комунікаційної підсистем.

Отримані результати (табл. 5–7) показують, що для розглянутого сценарію з довжиною ділянки $L = 6$ км та використанням трьох ешелонів сенсорного покриття необхідна кількість вузлів становить $N_b = 549$. При цьому сумарна ймовірність виявлення досягає $P_{\Sigma} \approx 0,973$.

З урахуванням оціненої пропускної здатності мережі (табл. 7) отримане значення кількості вузлів не перевищує допустимі межі ($N_{\max}^{\text{real}} \approx 1000-1500$), що свідчить про узгодженість параметрів сенсорної та комунікаційної підсистем.

Структура запропонованої розподіленої сенсорної мережі з багатохоповою передачею даних, що включає сенсорні вузли, ретранслятори та пункт збору інформації, наведена на рисунку 5.

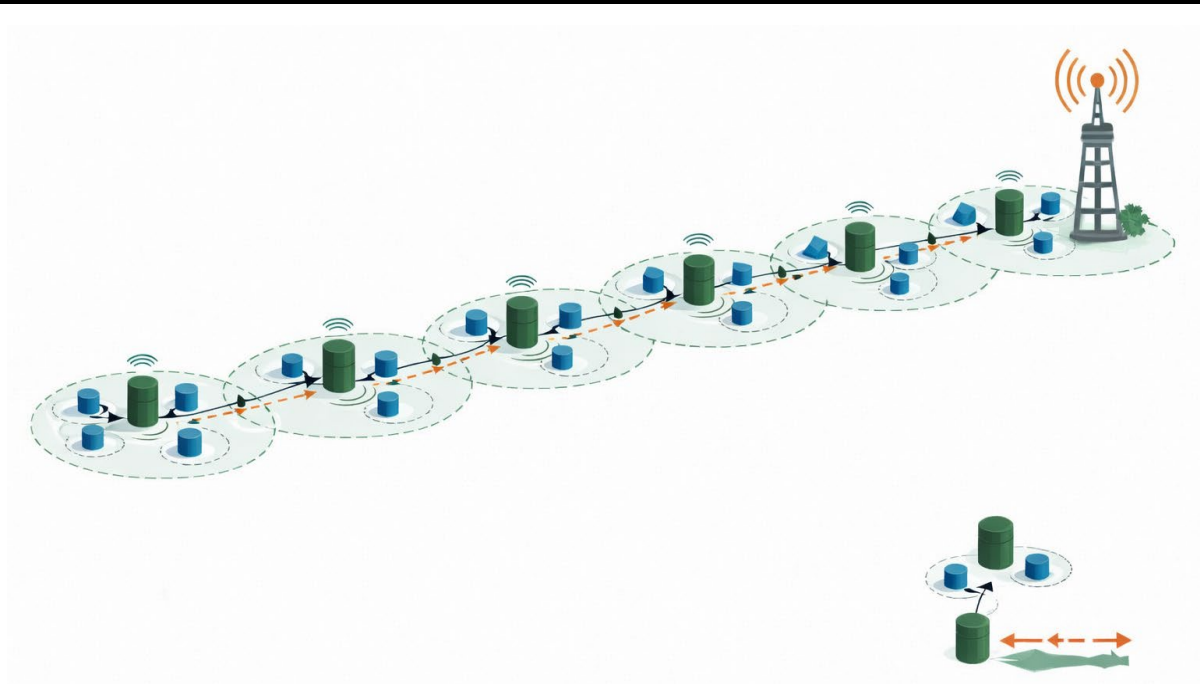


Рис. 5. Структура тришелевної розподіленої сенсорної мережі з багатохопковою передачею даних на базі LoRa

Таким чином, у цьому сценарії обмеження мережі передачі даних не є визначальним фактором, і вимоги до системи визначаються переважно параметрами сенсорного покриття.

Результати моделювання дозволяють встановити наступні ключові закономірності: ефективний радіус сенсорного вузла визначається заданою ймовірністю виявлення; кількість сенсорних вузлів зростає при підвищенні вимог до ймовірності виявлення; використання багатохопкової передачі обмежується накопиченням втрат; пропускна здатність мережі визначає верхню межу кількості вузлів; сенсорна та комунікаційна підсистеми повинні проектуватися спільно.

Наукова новизна.

Наукова новизна роботи полягає у наступному:

- удосконалено методику проектування розподіленої сенсорної мережі, яка поєднує ймовірнісну модель сенсорного виявлення з моделлю багатохопкової передачі даних;
- показано вплив багатешелевної структури сенсорного покриття на сумарну ймовірність виявлення за рахунок об'єднання результатів незалежних спостережень.

Висновки та перспективи подальших досліджень.

Розроблена методика проектування розподіленої сенсорної мережі моніторингу на базі технології LoRa забезпечує узгоджене врахування параметрів сенсорної підсистеми, багатохопкової передачі даних та обмежень пропускної здатності мережі.

Встановлено, що використання багатешелевної структури сенсорного покриття дозволяє підвищити сумарну ймовірність виявлення за рахунок об'єднання результатів незалежних спостережень та забезпечує гнучкість при виборі параметрів мережі.

Отримані результати можуть бути використані як основа для інженерного проектування систем моніторингу протяжних територій в умовах обмежених ресурсів і складних умов поширення сигналів.

Перспективи подальших досліджень пов'язані з уточненням параметрів сенсорної моделі на основі експериментальних даних та дослідженням впливу реальних умов середовища на ефективність функціонування мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Raza U., Kulkarni P., Sooriyabandara M. Low Power Wide Area Networks: An Overview // IEEE Communications Surveys & Tutorials. 2017. Vol. 19, No. 2. P. 855–873. DOI: 10.1109/COMST.2017.2652320.
2. Lavric A., Popa V. Internet of Things and LoRa™ Low-Power Wide-Area Networks: A Survey. 2017 International Symposium on Signals, Circuits and Systems (ISSCS). 2017. P. 1–5. DOI: 10.1109/ISSCS.2017.8034915.
3. Georgiou O., Raza U. Low Power Wide Area Network Analysis: Can LoRa Scale? // IEEE Wireless Communications Letters. 2017. Vol. 6, No. 2. P. 162–165. DOI: 10.1109/LWC.2016.2647247.
4. Marini R., Mikhaylov K., Pasolini G., Buratti C. LoRaWANSim: A Flexible Simulator for LoRaWAN Networks // Sensors. 2021. Vol. 21, No. 3. Article 695. DOI: 10.3390/s21030695.
5. Basford P. J., Bulot F. M. J., Apetroaie-Cristea M., Cox S. J., Ossont S. J. LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation // Sensors. 2020. Vol. 20, No. 3. Article 648. DOI: 10.3390/s20030648.
6. Augustin A., Yi J., Clausen T., Townsley W. M. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things // Sensors. 2016. Vol. 16, No. 9. Article 1466. DOI: 10.3390/s16091466.
7. Haxhibeqiri J., Van den Abeele F., Moerman I., Hoebeke J. LoRa Scalability: A Simulation Model Based on Interference Measurements // Sensors. 2017. Vol. 17, No. 6. Article 1193. DOI: 10.3390/s17061193.
8. Reynders B., Meert W., Pollin S. Range and Coexistence Analysis of Long Range Unlicensed Communication. 2016 23rd International Conference on Telecommunications (ICT). 2016. P. 1–6. DOI: 10.1109/ICT.2016.7500415.
9. Tran H. P., Jung W.-S., Yoo D.-S., Oh H. Design and Implementation of a Multi-Hop Real-Time LoRa Protocol for Dynamic LoRa Networks // Sensors. 2022. Vol. 22, No. 9. Article 3518. DOI: 10.3390/s22093518.
10. Tomic I., McCann J. A. A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols // IEEE Internet of Things Journal. 2017. Vol. 4, No. 6. P. 1910–1923. DOI: 10.1109/JIOT.2017.2749883.
11. Leenders G., Plets D., Hoebeke J., Martens L., Joseph W. An Energy-Efficient LoRa Multi-Hop Protocol through Preamble Sampling for Remote Sensing // Sensors. 2023. Vol. 23, No. 11. Article 4994. DOI: 10.3390/s23114994.
12. Alhomyani H., Fadel M., Dimitriou N., Bakhsh H., Aldabbagh G. Modeling the Performance of a Multi-Hop LoRaWAN Linear Sensor Network for Energy-Efficient Pipeline Monitoring Systems // Applied Sciences. 2024. Vol. 14, No. 20. Article 9391. DOI: 10.3390/app14209391.
13. Shan A., Xu X., Cheng Z. Target Coverage in Wireless Sensor Networks with Probabilistic Sensors // Sensors. 2016. Vol. 16, No. 9. Article 1372. DOI: 10.3390/s16091372.
14. Pyrih Ya., Pyrih Yu. Investigation of Sensor Node Placement on a Plane Using a Genetic Algorithm // Infocommunications Technologies and Electronic Engineering. 2025. Vol. 5, No. 1. DOI: 10.23939/ict2025.01.082.

Надійшла до редколегії 28.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 355.6:623.4:001.891.57:658.512.2

д-р філософії Бернацький А. П. ORCID: 0000-0003-0379-075X (ВІТІ ім. Героїв Крут)

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЦЕНТРУ ПЕРСПЕКТИВНИХ ТЕХНОЛОГІЙ ЯК АДАПТИВНОГО БАГАТОКОНТУРНОГО ЦИКЛУ ФОРМУВАННЯ ОБОРОННО-ТЕХНОЛОГІЧНОЇ СПРОМОЖНОСТІ НА ОСНОВІ ОПЕРАТИВНОГО ДОСВІДУ

У статті розглянуто концептуальну модель центру перспективних технологій ADM як адаптивну багатоконтурну систему, призначеної для формування оборонно-технологічної спроможності на основі реального оперативного досвіду. Необхідність такого підходу зумовлена тим, що сучасні умови воєнного часу вимагають не лише швидкого реагування на окремі технічні проблеми, а й створення цілісного механізму, здатного перетворювати бойові потреби, дефіцит комплектуючих, пошкодження озброєння і військової техніки, а також нові вимоги практики на перевірені інженерні рішення. У межах дослідження ADM пропонується розглядати не тільки як виробничий, ремонтний або дослідно-конструкторський осередок, а як цілісну соціотехнічну систему, у якій взаємопов'язані кілька функціональних контурів. До них належать контури: виявлення та формалізації оперативної потреби, аналітичного й наукового осмислення проблеми, R&D та інженерного опрацювання, реверс-інжинірингу, технологічної реалізації, випробувань і верифікації, впровадження, підготовки персоналу, документування та оновлення бази знань.

У роботі запропоновано формалізований опис: стану ADM, індексу оборонно-технологічної спроможності, невизначеності технічної проблеми, верифікованої придатності рішення, освітньо-кадрових контурів, умов допуску до впровадження та показників економічної ефективності. Окремо розкрито механізм керування, який забезпечує відбір і пріоритезацію кейсів, визначення траєкторії їх проходження через основні стадії, повернення на доопрацювання у разі невідповідності вимогам, а також адаптивне коригування дій залежно від ризиків, ресурсних обмежень і зміни оперативної ситуації. Прикладний сценарій відновлення дефіцитної деталі озброєння, що була пошкоджена в бойових умовах і не може бути швидко замінена штатним способом, демонструє практичну придатність запропонованої моделі. У висновках показано, що ADM здатний забезпечити контрольований перехід від початкової проблеми до верифікованого технічного рішення, навчального кейсу, цифрового сліду та елементу інституційної пам'яті. Окреслено подальші напрями розвитку моделі, зокрема її математичну деталізацію, кількісне оцінювання ефективності та прикладну апробацію в різних сценаріях оборонно-технологічного реагування.

Ключові слова: ADM, перспективні технології, оборонно-технологічна спроможність, оперативний досвід, багатоконтурний цикл, адаптивне виробництво, верифікація технічних рішень, управління знаннями, підготовка персоналу, оборонні технології, невизначеність, економічна ефективність, ремонт і відновлення озброєння, логістична стійкість.

A. Bernatskyi. Conceptual model of a centre for advanced technologies as an adaptive, multi-loop cycle for building defence and technological capabilities based on operational experience

This paper considers a conceptual model of the ADM Centre for Advanced Technologies as an adaptive multi-loop system designed to build defence and technological capabilities based on real-world operational experience. The need for such an approach stems from the fact that modern wartime conditions require not only a rapid response to individual technical problems, but also the creation of a comprehensive mechanism capable of transforming combat requirements, shortages of components, damage to weapons and military equipment, as well as new practical demands, into proven engineering solutions. Within the scope of this study, the ADM is proposed to be viewed not merely as a production, repair or research and development centre, but as a holistic socio-technical system in which several functional loops are interconnected. These include the loop for identifying and formalising operational requirements, analytical and scientific understanding of the problem, R&D and engineering development, reverse engineering, technological implementation, testing and verification, deployment, personnel training, documentation, and updating the knowledge base.

The paper proposes a formalised description of the ADM state, the defence-technology capability index, the uncertainty of the technical problem, the verified suitability of the solution, knowledge and personnel frameworks, conditions for approval for implementation, and economic efficiency indicators. Separately, the paper details a management mechanism that ensures the selection and prioritisation of cases, the determination of their progression through the main stages, their return for further refinement in the event of non-compliance with requirements, as well as the adaptive adjustment of actions depending on risks, resource constraints and changes in the operational situation. An applied scenario involving the restoration of a scarce weapon component, which was damaged in combat conditions and cannot be quickly replaced through standard procedures, demonstrates the practical suitability of the proposed model. The conclusions show that ADM is capable of ensuring a controlled transition from the initial problem to a verified

technical solution, a training case, a digital trail and an element of institutional memory. Further directions for the model's development are outlined, in particular its mathematical refinement, quantitative assessment of effectiveness, and applied testing in various defence-technology response scenarios.

Keywords: *ADM, promising technologies, defence technology capability, operational experience, multi-loop cycle, additive manufacturing, verification of technical solutions, knowledge management, personnel training, defence technologies, uncertainty, cost-effectiveness, repair and refurbishment of weaponry, logistical resilience.*

Постановка проблеми. Повномасштабна війна докорінно змінила вимоги до системи забезпечення військ, ремонту, адаптації озброєння та військової техніки, а також до швидкості розроблення й впровадження нових технічних рішень. Ключовими ознаками сучасного середовища стали висока динаміка бойових умов, нестабільність ланцюгів постачання, дефіцит окремих комплектуючих, потреба в оперативному відновленні техніки, швидкому масштабуванні виробництва та переході від тривалого мирного циклу інженерного погодження до воєнного циклу швидкого технічного реагування. У документах НАТО та Європейського Союзу 2025 року посилено акцентується значення швидкості, адаптивності, інноваційного оборонного виробництва, стійких ланцюгів постачання, підготовки персоналу та прискореного впровадження нових технологій у формування сучасної оборонної готовності [1]. Україна вже володіє не лише унікальним бойовим, а й вагомим логістичним, технічним та організаційним досвідом функціонування в умовах тривалої війни проти російської агресії. НАТО окремо наголошує на значущості системного вивчення й поширення уроків війни України, а українські державні інституції підкреслюють, що безперервний зворотний зв'язок між виробниками та фронтом дає змогу швидко адаптувати технології до реальних потреб поля бою [2]. Показовим є й зростання частки українських виробників у закупівлях товарів військового призначення до 82 % у 2025 році [3], що свідчить про посилення ролі внутрішнього оборонно-промислового потенціалу та поступове формування більш зрілого інноваційного середовища.

Отже, наукова проблема полягає у відсутності цілісної концептуальної моделі, яка б описувала центр перспективних технологій як адаптивну багатоконтурну систему перетворення оперативного досвіду на оборонно-технологічну спроможність. Наявна практика воєнного часу вже демонструє високу швидкість технічного реагування, однак здебільшого залишається фрагментарною з погляду формалізації зв'язків між оперативною потребою, інженерним опрацюванням, верифікацією, підготовкою персоналу та накопиченням знань. Саме тому виникає потреба в моделі, що пояснює логіку замкненого циклу розвитку такої спроможності та створює підґрунтя для переходу від частково імпровізаційної практики до системно організованої архітектури.

Аналіз останніх досліджень і публікацій. Проблематика формування оборонно-технологічних спроможностей Сил оборони України та партнерів перебуває на перетині кількох взаємопов'язаних дослідницьких напрямів, серед яких найбільш близькими до теми цієї роботи є застосування адитивного виробництва в умовах критичних операцій, управління запасними частинами та стійкістю ланцюгів постачання, а також реверс-інжиніринг і перепроєктування деталей для швидкого технологічного відтворення. Саме в межах цих напрямів упродовж останніх років сформовано важливе теоретичне і прикладне підґрунтя для осмислення ролі центрів перспективних технологій у секторі безпеки й оборони. Так, у роботі [4] Dey A. та співавтори адитивне виробництво розглядають як перспективний інструмент для місійно-критичних застосувань завдяки скороченню строків виготовлення, можливості виробництва на вимогу, створенню складних індивідуалізованих конструкцій і дистанційному обміну цифровими моделями; водночас автори наголошують, що ширше використання таких рішень стримується вимогами до якості, надійності та стандартизації. Систематичний огляд [5] Alzahmi W., Shamayleh A., Stefancich M., виконаний за PRISMA-підходом на основі 77 публікацій, показує, що адитивне виробництво здатне забезпечити виготовлення запасних частин на вимогу, зменшення складських запасів, скорочення строків постачання, підвищення

гнучкості та зниження простоїв у процесах технічного обслуговування. У свою чергу, Peron M. зі співавторами у Delphi-дослідженні [6] доводять, що адитивне виробництво загалом позитивно впливає на стійкість ланцюгів постачання, передусім через зростання адаптивності та ефективності, однак його ефект не є універсально позитивним, оскільки одночасно виникають нові ресурсні та організаційні обмеження.

Окрему групу становлять сучасні дослідження, у яких увагу зосереджено не лише на друці деталей, а на повному переході від дефіцитного або пошкодженого компонента до нового інженерно обґрунтованого рішення, вони ґрунтуються на застосуванні реверс-інжинірингу та перепроєктування деталей, що є особливо важливим для концепції ADM. Rešetar M. та співавтори у дослідженні [7] пропонують підхід, який поєднує 3D-сканування, реверс-інжиніринг, функціональний аналіз і Design for Additive Manufacturing для виготовлення запасних частин; при цьому автори переконливо показують, що простого копіювання геометрії недостатньо, а відновлення деталі має враховувати її функціональне призначення, сумісність із системою та доцільність перепроєктування під нову технологію виготовлення. У вітчизняному науковому полі важливими є праці, що розкривають інституційний та логістичний вимір оборонно-технологічного розвитку. Так Давимука С. А. в роботі [8] обґрунтовує необхідність формування багаторівневої інноваційної екосистеми оборонної промисловості України, у якій поєднуються наукові знання, технології, інституційні механізми та учасники сектору Defense Tech. Натомість Бурдейна Н., Федченко О. та Венцюк А. акцентують [9] увагу на сучасних викликах військової логістики України, пов'язаних із координацією, ефективністю управління ресурсами, постачанням, транспортуванням, зберіганням і розподілом матеріально-технічних засобів, а серед практичних напрямів удосконалення виділяють централізоване управління та єдиний координаційний контур логістичних процесів. У цьому ж контексті інтерес становлять роботи норвезького FFI [10], де адитивне виробництво розглядається як засіб швидкого виготовлення, ремонту та використання нових матеріалів у військових умовах, а польові експерименти демонструють можливість розподіленого виробництва прототипів і запасних частин безпосередньо близько до місця потреби, зокрема у контейнеризованому форматі.

Поряд із науковими працями дедалі більшого значення набувають офіційні документи НАТО, Європейського Союзу та Європейського оборонного агентства, які задають інституційну рамку для осмислення оборонно-технологічної спроможності. Оновлений Defence Production Action Plan НАТО, Секретарський річний звіт за 2025 рік, а також документи НАТО STO засвідчують зростання уваги до оборонного виробництва, стійкості логістики, багатонаціонального обслуговування та впровадження адитивного виробництва для підвищення взаємосумісності й логістичної ефективності. На рівні ЄС аналогічна логіка простежується в European Defence Industrial Strategy та White Paper for European Defence, де акцент зроблено на переході до defence industrial readiness, прискоренні виробництва, посиленні досліджень і формуванні більш цілісної європейської оборонно-технологічної бази. Водночас European Defence Agency у звіті за 2025 рік прямо фіксує розвиток проєкту Additive Manufacturing for Logistic Support, спрямованого на вироблення спільних стандартів і підвищення взаємозамінності запасних частин між державами, причому до цього проєкту вже долучено десять країн ЄС і Норвегію.

Отже, наявні дослідження достатньо ґрунтовно розкривають окремі технологічні, логістичні та організаційні аспекти оборонно-технологічного реагування, зокрема адитивне виробництво, виготовлення запасних частин на вимогу, реверс-інжиніринг, перепроєктування та інституційні механізми зміцнення оборонно-промислової стійкості. Водночас у доступному науковому полі практично відсутня цілісна концептуальна модель, яка б інтегрувала ці елементи в єдиний адаптивний багатоконтурний цикл формування оборонно-технологічної спроможності на основі оперативного досвіду.

Мета дослідження. Метою дослідження є теоретичне обґрунтування та концептуальне моделювання центру перспективних технологій ADM, як адаптивного багатоконтурного циклу формування оборонно-технологічної спроможності на основі оперативного досвіду.

Виклад основного матеріалу. У сучасних умовах воєнного часу центр перспективних технологій доцільно розглядати не як сукупність ізольованих функцій, а як цілісну адаптивну соціотехнічну систему, у межах якої інтегруються оперативний досвід, технічний аналіз, наукове осмислення, інженерне опрацювання, технологічна реалізація, верифікація, підготовка персоналу, документування та накопичення знань. У такому підході ключовим результатом діяльності центру стає не окремий виріб чи разове розв'язання локальної технічної проблеми, а формування стійкої оборонно-технологічної спроможності, здатної до відтворення, масштабування, адаптації та подальшого розвитку. Отже, ADM слід інтерпретувати як інституційний механізм перетворення практичного досвіду на керовану систему рішень, знань, технологій і підготовлених фахівців. Теоретичною передумовою такого підходу є те, що у воєнному середовищі формування спроможності не відбувається лінійно. На відміну від класичних мирних моделей, де між виявленням потреби та реалізацією рішення існує відносно стабільний і послідовний ланцюг погоджень, у середовищі високої невизначеності, часових обмежень, дефіциту комплектуючих, ризиків логістичного зриву та швидкої зміни вимог ефективна система повинна функціонувати як замкнений цикл із багатьма внутрішніми поверненнями. Саме тому ADM доцільно описувати як адаптивний багатоконтурний цикл, у якому кожен завершений результат не лише вирішує поточну проблему, а й зменшує невизначеність майбутніх рішень, збагачує систему знаннями і підсилює її кадрову та технологічну готовність.

У межах запропонованого підходу загальна логіка функціонування ADM може бути представлена як великий зовнішній цикл (рис. 1), який включає такі стадії, як виникнення оперативної потреби, формалізація проблеми, наукове осмислення, R&D та інженерне опрацювання, технологічна реалізація, верифікація, впровадження, підготовка особового складу, документування, оновлення знань і перехід до нового циклу розвитку. Ця послідовність є принципово важливою, оскільки вона демонструє, що центр перспективних технологій не зводиться до виробничого майданчика чи ремонтного вузла, а функціонує як механізм постійного перетворення бойового досвіду на інституційно закріплену оборонно-технологічну спроможність.

Перша стадія циклу пов'язана з виникненням оперативної потреби. Під нею слід розуміти не будь-який абстрактний запит, а реальну проблему, що виникає внаслідок пошкодження виробу, дефіциту запасних частин, необхідності адаптації техніки до нових умов, появи нових засобів ураження або потреби у швидкому технологічному реагуванні. На цьому етапі система отримує первинний імпульс від практики. Проте емпіричний характер такого запиту є недостатнім для побудови відтворюваного рішення, а тому наступною стадією є формалізація проблеми, у межах якої визначаються її технічна сутність, функціональні вимоги, критичність, обмеження, граничні часові параметри, ризики та критерії допустимого результату. Після формалізації, проблема переходить у стадію наукового осмислення, де початковий практичний запит переводиться в аналітичну площину, а саме з'ясовуються причини відмови або дефіциту, аналізуються закономірності виникнення проблеми, формуються гіпотези щодо шляхів її розв'язання, визначаються можливі технічні, матеріалознавчі, конструктивні чи організаційні альтернативи. Саме на цьому етапі ADM перестає бути лише інструментом швидкої реакції, а набуває якостей дослідницько-аналітичного осередку, який здатний не тільки виконати завдання, а й пояснити проблему, узагальнити її та підготувати основу для повторного використання знання в майбутньому.

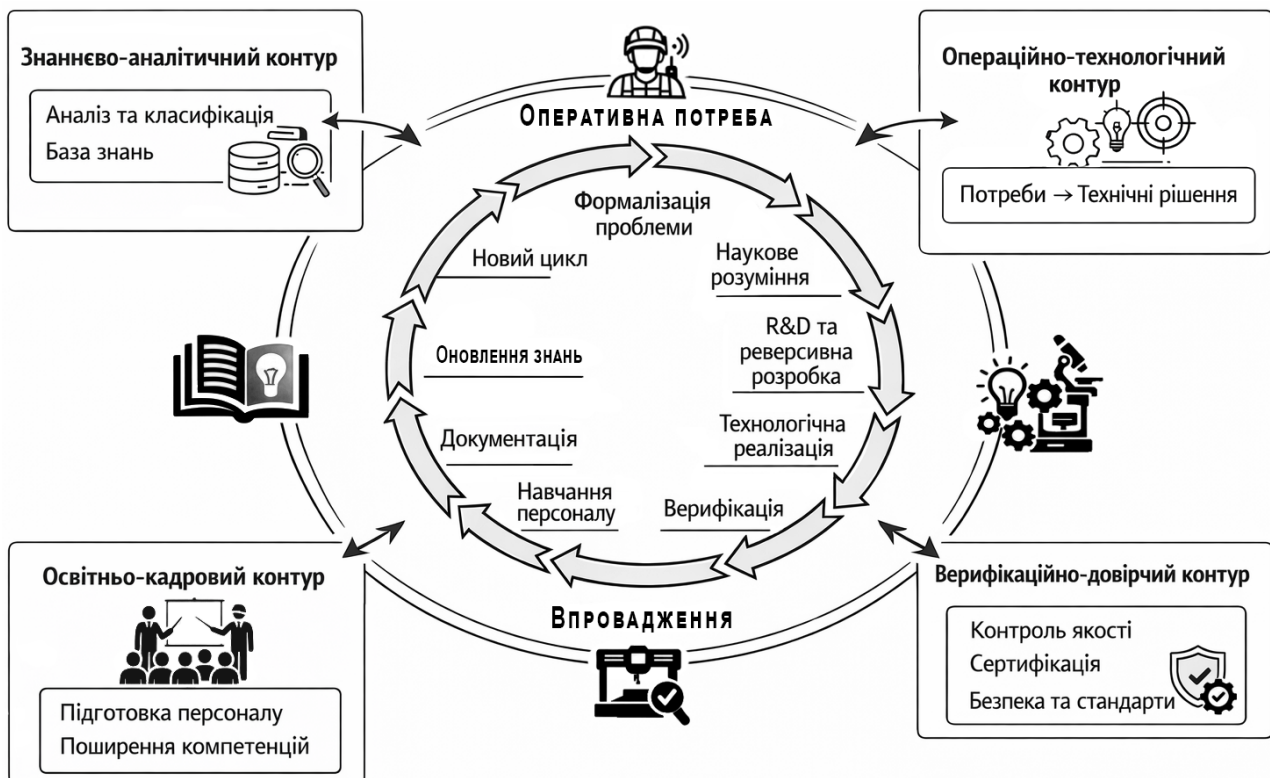


Рис. 1. Концептуальна модель адаптивного багатоконтурного циклу ADM формування оборонно-технологічної спроможності

Центральною ланкою моделі виступає стадія R&D та інженерного опрацювання. У її межах здійснюються реверс-інжиніринг, перепроєктування, адаптація конструкції до доступних технологічних можливостей, підбір матеріалів, цифрове моделювання, виготовлення прототипів, випробувальне уточнення параметрів та інші інженерні дії, спрямовані на перехід від аналітичного розуміння проблеми до конкретного технічного рішення. Саме тут відбувається найінтенсивніша трансформація знання в артефакт, вузол, деталь, модуль, технологічну карту, методику або новий виробничий процес. При цьому R&D-стадія не є одноразовою, оскільки для досягнення прийнятного рівня функціональності, сумісності та технологічної здійсненості зазвичай потрібні багаторазові мікроітерації між моделюванням, прототипуванням, перевіркою та коригуванням.

Наступною стадією виступає технологічна реалізація, яка охоплює виготовлення або відновлення виробу, цифрове відтворення геометрії, адитивне чи субтрактивне виробництво, постобробку, складання, доведення та підготовку об'єкта до практичного застосування. Однак технологічна реалізація сама по собі ще не означає завершення циклу, оскільки будь-який отриманий результат повинен бути перевірений на відповідність функціональним, безпековим і експлуатаційним вимогам. Саме тому верифікація в моделі ADM має системоутворювальний характер. Вона включає контроль якості, випробування, технічний допуск, перевірку повторюваності результату, оцінку ризику відмови, формування технічної довіри до рішення та ухвалення рішення щодо допуску до впровадження.

У межах концептуальної моделі верифікацію доцільно розглядати не як допоміжну процедуру, а як формальний фільтр між експериментальним рішенням і рішенням, що допускає до практичного використання. Це означає, що до впровадження буде допущений результат, який задовольняє мінімальні порогові значення функціональної придатності, безпекової відповідності та економічної доцільності. Тим самим ADM вбудовує в свою логіку не лише прискорення технічного циклу, а й механізм запобігання помилковому або

передчасному впровадженню. І після верифікації система переходить до стадії впровадження. У контексті ADM це означає не просто передання готового виробу, а включення результату в реальний контекст експлуатації, де він взаємодіє з технікою, операторами, інженерами, логістичними ланцюгами та організаційними процедурами. Лише на цьому рівні стає остаточно зрозуміло, наскільки рішення є не тільки технічно працездатним, а й експлуатаційно доцільним, зручним, масштабованим і виправданим з погляду часу та ресурсів. Отже, впровадження виконує роль переходу від внутрішнього циклу центру до зовнішнього середовища оборонної практики.

Жодне технологічне рішення не здатне забезпечити довготривалий ефект, якщо не сформовано людський ресурс, який може його відтворювати, застосовувати, супроводжувати, удосконалювати та передавати далі. Тож у концептуальній моделі ADM особливе місце посідає підготовка особового складу. На відміну від класичних виробничих схем, у яких навчання часто розглядається як зовнішній або другорядний процес, у запропонованому підході кадровий контур є невід'ємною частиною формування спроможності. Саме тому підготовка операторів, інженерів, техніків, інструкторів і майбутніх фахівців має ґрунтуватися не на абстрактних програмах, а на реальних кейсах, сформованих у попередніх стадіях великого циклу. У цьому сенсі ADM виступає також середовищем безперервного кадрового відтворення технологічної культури.

Завершальними стадіями великого циклу є документування та оновлення знань. Документування включає фіксацію конструктивних рішень, параметрів виготовлення, результатів випробувань, типових дефектів, обміну досвідом, технологічних карт, цифрових моделей, навчальних кейсів і методичних матеріалів. Оновлення знань означає включення цього досвіду до бази знань центру, перегляд методик, уточнення стандартів, розроблення нових навчальних модулів і формування наступних технічних задач. Саме через ці стадії ADM набуває замкнутого характеру, коли результат не зникає після виконання окремого завдання, а повертається в систему як ресурс нового циклу розвитку.

Проведемо формалізований опис запропонованої моделі ADM. Нехай стан ADM у дискретний момент часу k визначається вектором (1):

$$X_k = (H_k, Z_k, V_k, P_k, K_k, L_k), \quad (1)$$

де H_k – рівень невизначеності щодо технічної проблеми; Z_k – рівень технічної зрілості рішення; V_k – рівень верифікованої придатності; P_k – кадрова готовність; K_k – обсяг формалізованого знання; L_k – рівень логістично-виробничої забезпеченості. Тоді загальна динаміка системи може бути подана як формула (2):

$$X_{k+1} = F(X_k, U_k, E_k), \quad (2)$$

де U_k – керуючі дії системи; E_k – зовнішні впливи середовища, серед яких часовий тиск, дефіцит ресурсів, зміна бойових вимог, ризики порушення постачання та інтенсивність зворотного зв'язку з практики.

Інтегральний результат функціонування ADM опишемо через індекс оборонно-технологічної спроможності (3):

$$C_k = \alpha_1 \left(1 - \frac{H_k}{H_{max}}\right) + \alpha_2 Z_k + \alpha_3 V_k + \alpha_4 P_k + \alpha_5 K_k + \alpha_6 L_k, \quad (3)$$

де $\alpha_i \geq 0$, $\sum_{i=1}^6 \alpha_i = 1$. Розуміємо, що (2) демонструє зростання спроможності не лише через факт виготовлення рішення, а як результат одночасного зменшення невизначеності, зростання

технічної зрілості, проходження верифікації, підготовки кадрів, накопичення знань і підсилення виробничо-логістичної готовності.

Формалізуємо невизначеність технічної проблеми з урахуванням ентропії (4):

$$H_k = -\sum_{i=1}^m p_i^{(k)} \ln p_i^{(k)}, \quad (4)$$

де $p_i^{(k)}$ – імовірність того, що i -та гіпотеза розв'язання є правильною на етапі k . Це свідчить про те, що на ранніх стадіях циклу система має кілька конкуруючих пояснень і варіантів рішення, а отже невизначеність є високою. У міру формалізації, аналізу, R&D та верифікації правильний варіант поступово уточнюється, а ентропія зменшується. Таким чином, ключовий ефект ADM полягає не лише у виготовленні виробу, а в системному зменшенні невизначеності майбутніх технічних рішень.

Проведемо опис верифікованої придатності, як інтегральної функції якості, відповідності вимогам, повторюваності результату та ризику (5):

$$V_k = \sigma(\beta_1 q_k + \beta_2 s_k + \beta_3 r_k - \beta_4 \rho_k), \quad (5)$$

де q_k – функціональна якість рішення; s_k – рівень відповідності технічним вимогам і стандартам; r_k – повторюваність результату; ρ_k – ризик відмови або небезпечного застосування; $\sigma(\cdot)$ – нормувальна функція. За такого підходу довіра до виробу або технології вже не є інтуїтивною оцінкою виконавця, а виступає наслідком формалізованих та виконаних процедур контролю, випробувань і підтвердження відповідності.

Контури знань і кадрів також доцільно подати у вигляді динамічних залежностей (6), (7):

$$K_{k+1} = (1 - \mu)K_k + \gamma_1 D_k + \gamma_2 LL_k, \quad (6)$$

$$P_{k+1} = (1 - \nu)P_k + \delta_1 T_k + \delta_2 Pr_k, \quad (7)$$

де D_k – інтенсивність документування LL_k – обсяг обміну досвідом; T_k – інтенсивність навчання; Pr_k – обсяг практичної участі персоналу в реальних кейсах; μ і ν – коефіцієнти старіння знання та деградації компетенцій без практичного застосування. В такому вигляді, знання і кадри в ADM не є периферійними продуктами діяльності, а належать до базових змінних системного розвитку.

Багатоконтурність ADM передбачає наявність мінімум чотирьох локальних мікроциклів поряд із великим зовнішнім циклом. Де перший, це *дослідницько-інженерний мікроцикл*, який функціонує в зоні R&D та забезпечує повторюваний перехід між аналізом, моделюванням, перепроєктуванням, прототипуванням і технічним уточненням до досягнення прийнятного рівня здійсненності. Другий, це *верифікаційно-довірчий мікроцикл*, він локалізується в зоні випробувань і контролю якості та забезпечує коригування рішення на основі результатів тестування, уточнення критеріїв допуску та зниження ризику помилкового впровадження. Третій, *освітньо-кадровий мікроцикл*, що забезпечує взаємний перехід між реальним практичним кейсом, навчальним модулем, формуванням компетенцій і поверненням підготовлених фахівців у контур практичної діяльності. І четвертий, *мікроцикл освітньо-аналітичний*, якій охоплює документування, класифікацію, накопичення та повторне використання технічного досвіду, перетворюючи одиничний результат на колективний ресурс системи.

Розширимо модель за рахунок введення умови допуску рішення до впровадження. Нехай рішення може бути передане до практичної реалізації лише тоді, коли виконується система умов (8):

$$V_k \geq V_{min}, \rho_k \leq \rho_{max}, \eta_k > 0, \quad (8)$$

де V_{min} – мінімально допустимий рівень верифікованої придатності, ρ_{max} – гранично допустимий ризик, η_k – показник економічної доцільності. Це дозволить відмежувати просто технічно можливе рішення від рішення, яке є обґрунтовано допустимим до реального оборонного застосування.

Важливо зазначити, що економічний зміст ADM полягає в тому, що він функціонує не лише як центр виготовлення чи відновлення окремих технічних об'єктів, а як механізм зниження сукупних витрат оборонної системи в умовах високої невизначеності. При цьому в традиційній лінійній моделі втрати зазвичай формуються за рахунок тривалих строків постачання, простоїв техніки, імпортої залежності, повторюваних інженерних помилок, браку стандартизованого знання, дефіциту підготовленого персоналу тощо. Тоді як у моделі ADM частина цих витрат трансформується в інвестиції у знання, інженерну спроможність, підготовку кадрів і повторне використання цифрових рішень.

Сукупні витрати функціонування ADM можна подати як (9):

$$J = \sum_{k=0}^T (c_k^{R\&D} + c_k^{prod} + c_k^{ver} + c_k^{train} + c_k^{log} + c_k^{delay} + c_k^{fail}), \quad (9)$$

де $c_k^{R\&D}$ – витрати на інженерне опрацювання; c_k^{prod} – витрати на виготовлення або відновлення; c_k^{ver} – витрати на випробування; c_k^{train} – витрати на навчання; c_k^{log} – логістичні витрати; c_k^{delay} – втрати від затримки забезпечення; c_k^{fail} – втрати від браку або помилкового впровадження. Водночас інтегральний ефект функціонування системи може бути представлений як (10):

$$E = \sum_{k=0}^T (b_k^{time} + b_k^{import} + b_k^{uptime} + b_k^{reuse} + b_k^{knowledge}) - J, \quad (10)$$

де b_k^{time} – вигрaш від скорочення часу до отримання рішення; b_k^{import} – вигрaш від зменшення імпортої залежності; b_k^{uptime} – вигрaш від скорочення простоїв техніки; b_k^{reuse} – вигрaш від повторного використання моделей і рішень; $b_k^{knowledge}$ – довгостроковий вигрaш від накопичення знань і кадрового відтворення. Якщо $E > 0$, система демонструє не лише технологічну, а й економічну доцільність.

Для порівняння окремих кейсів доцільно також використовувати питомий показник ефективності (11):

$$\eta_k = \frac{\lambda_1 \Delta t_k + \lambda_2 \Delta d_k + \lambda_3 \Delta i_k + \lambda_4 \Delta u_k}{J_k}, \quad (11)$$

де Δt_k – скорочення часу виготовлення або відновлення; Δd_k – зменшення простою техніки; Δi_k – зменшення імпортої залежності; Δu_k – приріст повторного використання напрацьованих рішень; J_k – витрати поточного циклу; λ_i – вагові коефіцієнти. Саме цей показник дає змогу переходити від загальних тверджень про корисність ADM до вимірюваного аналізу його результативності.

Для завершеного опису концептуальної моделі ADM недостатньо його подати лише як послідовність стадій великого адаптивного циклу та сукупність локальних мікроциклів. Не менш важливо визначити внутрішню структурно-функціональну архітектуру центру, тобто ті підсистеми, організаційні вузли та функціональні модулі, через які забезпечується проходження оперативного запиту від стадії виявлення потреби до стадії верифікованого впровадження, навчального відтворення та закріплення знань. Саме така архітектура

дозволяє перейти від опису процесу до моделі інституційно організованого середовища, здатного стабільно відтворювати оборонно-технологічну спроможність у воєнних умовах.

З позицій системного аналізу запропоновану архітектуру доцільно інтерпретувати як поєднання трьох взаємопов'язаних рівнів. Перший рівень становить рівень оперативного входу, до якого належать виявлення потреби, її постановка та пріоритезація. Другий рівень є рівнем інженерно-технологічного перетворення, де здійснюються дослідження, R&D, виготовлення, випробування та допуск. Третій рівень утворює рівень інституційного відтворення, який охоплює навчання, документування, накопичення знань, кадрове забезпечення та підготовку основи для нового циклу розвитку. Така трирівнева інтерпретація дозволяє показати, що ADM є не лише технічним, а й організаційно-знансвим механізмом, де результати кожного циклу працюють одночасно на поточне розв'язання проблеми та на довгострокове нарощування спроможності.

Проведемо формалізацію механізму керування запропонованої моделі. У загальному вигляді керування ADM доцільно інтерпретувати як процес цілеспрямованого впливу координаційно-управлінського ядра на стан функціональних підсистем центру з метою досягнення прийняттого поєднання чотирьох базових результатів, таких як, скорочення часу реакції на оперативну потребу, забезпечення технічної та безпекової придатності рішення, мінімізації ризику помилкового впровадження та формування довготривалого освітньо-кадрового ефекту. У такій постановці ADM прагне не лише до швидкого проходження циклу, а прагне до оптимального балансу між швидкістю, якістю, ризиком і накопиченням спроможності.

Для формалізації механізму керування введемо вектор керуючих дій системи (12):

$$U_k = (u_k^p, u_k^a, u_k^r, u_k^t, u_k^v, u_k^i, u_k^e, u_k^d), \quad (12)$$

де u_k^p – інтенсивність постановки та формалізації задачі; u_k^a – аналітичне опрацювання; u_k^r – R&D та конструкторсько-інженерні дії; u_k^t – технологічна реалізація; u_k^v – верифікаційно-випробувальні процедури; u_k^i – дії з впровадження та супроводу; u_k^e – освітньо-кадрові дії; u_k^d – документування та інтеграція результату до бази знань. У цьому вигляді керування набуває змісту розподілу інституційної уваги, ресурсів і часу між ключовими контурами системи залежно від характеру запиту та поточного стану ADM.

Зазначимо, що вхідним об'єктом керування є оперативний кейс або технічний запит R_j , що надходить із зовнішнього середовища практичного застосування. Для кожного такого запиту доцільно формувати картку первинної постановки, яку можна подати у вигляді вектора (13):

$$R_j = (q_j, \tau_j, \kappa_j, \chi_j, \psi_j), \quad (13)$$

де q_j – критичність потреби; τ_j – допустимий часовий горизонт реагування; κ_j – технічна складність; χ_j – ресурсомісткість; ψ_j – очікуваний ефект від розв'язання. Саме на основі цих параметрів координаційно-керуючий блок приймає рішення щодо пріоритетності кейсу, вибору траєкторії його проходження через контури ADM та допустимого режиму використання ресурсів.

Для впорядкування потоку запитів введемо інтегральний показник пріоритету (14):

$$П_j = \omega_1 q_j + \omega_2 \frac{1}{\tau_j} + \omega_3 \kappa_j + \omega_4 \psi_j - \omega_5 \chi_j, \quad (14)$$

де ω_i – вагові коефіцієнти, що відображають управлінські пріоритети центру. Така функція означає, що перевага надається задачам із високою критичністю, коротким допустимим часом

реагування, значним очікуваним ефектом і прийнятною ресурсною вартістю. У разі дефіциту потужностей саме значення P_j дозволяє не інтуїтивно, а формалізовано визначати черговість опрацювання кейсів. Це особливо важливо для воєнного середовища, де одночасно можуть надходити кілька конкурентних запитів із різною глибиною наслідків.

Після прийняття кейсу до опрацювання система переходить у режим керованого просування між контурами. Для цього доцільно ввести дискретну змінну стадії (15):

$$s_k \in \{S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9, S_{10}\}, \quad (15)$$

де S_1 – оперативна потреба; S_2 – формалізація; S_3 – наукове осмислення; S_4 – R&D; S_5 – технологічна реалізація; S_6 – верифікація; S_7 – впровадження; S_8 – підготовка персоналу; S_9 – документування; S_{10} – оновлення знань. Тоді рух кейсу через систему можна подати як (16):

$$s_{k+1} = \mathcal{T}(s_k, \mathcal{E}_k), \quad (16)$$

де $\mathcal{T}$ – функція переходу, а $\mathcal{E}_k$ – сукупність умов переходу, що включає поточні значення технічної зрілості, рівня верифікованої придатності, ризику, економічної доцільності, кадрової готовності й повноти документування.

Перехід від стадії оперативної потреби до формалізації доцільно дозволяти лише за умови наявності мінімально достатньої вхідної інформації, тобто коли показник повноти постановки I_k задовольняє умову $I_k \geq I_{min}$. Це означає, що кейс не може бути переданий у поглиблене технічне опрацювання, доки не визначено його функціональний контекст, обмеження, критичність і хоча б базові критерії успішності. Якщо ж $I_k \geq I_{min}$, система не рухає кейс уперед, а повертає його в контур додаткового уточнення. Такий підхід запобігає ситуації, коли інженерний або виробничий контур починає працювати з частково поставленою задачею.

Також перехід від аналітичного осмислення до R&D та конструкторського опрацювання доцільно здійснювати тільки тоді, коли сформовано хоча б одну технічно несуперечливу гіпотезу розв'язання та визначено множину допустимих обмежень. Формально це може бути задано умовами $n_h \geq 1$, $\Omega_k = \emptyset$, де n_h – кількість сформованих робочих гіпотез, а Ω_k – множина допустимих конструктивно-технологічних рішень. Якщо ж аналітичний блок не спромігся виділити реалістичну траєкторію розв'язання, кейс не переходить у R&D, а або повертається на доуточнення постановки, або переводиться в режим відкладеного опрацювання до появи додаткових даних чи ресурсів.

Критично важливим є перехід від R&D до технологічної реалізації. У межах ADM його доцільно дозволяти лише за умови досягнення мінімального рівня технічної зрілості рішення Z_k та технологічної здійсненності M_k , тобто $Z_k \geq Z_{min}$, $M_k \geq M_{min}$. При цьому тут Z_k відображає ступінь інженерної пропрацьованості рішення, а M_k – його сумісність із наявними технологічними засобами, матеріалами, обладнанням і часовими обмеженнями центру. Якщо хоча б одна з цих умов не виконується, кейс повертається в R&D-контур на доопрацювання. Саме цей механізм запобігає надходженню у виробничо-технологічний блок тільки рішення, що доведені до стану реальної матеріалізації, а не будь-які конструкторські гіпотези. Завершення технологічної реалізації, направляє кейс у верифікаційно-випробувальний контур. Такий перехід доцільно здійснювати лише за умови досягнення базової функціональної завершеності прототипу або виробу, $G_k \geq G_{min}$, де G_k – показник готовності об'єкта до випробувань. Його зміст полягає в тому, що результат має бути достатньо цілісним, аби його випробування мало сенс з інженерної точки зору. У протилежному випадку верифікація буде фіксувати не властивості рішення, а лише факт його незавершеності, що

створює зайве навантаження на контрольний контур і спотворює управлінський зворотний зв'язок.

Найважливішим у структурі керування ADM є механізм прийняття рішення про допуск до впровадження. В межах запропонованої моделі він має бути не ситуативним, а формалізованим і узгодженим. Тому рішення може бути передане в практичне середовище лише тоді, коли одночасно виконуються умови $V_k \geq V_{min}$, $\rho_k \leq \rho_{max}$, $\eta_k > 0$. Тут V_k – інтегральний рівень верифікованої придатності, ρ_k – ризик відмови або небажаного ефекту при застосуванні, η_k – показник економічної доцільності. Ця система умов означає, що ADM не розглядає технічно можливе рішення як автоматично придатне до впровадження. Для практичного допуску воно має бути перевіреним, достатньо безпечним і виправданим не лише функціонально, а й з позицій часу, ресурсів і повторюваності. У випадках, коли хоча б одна з умов допуску не виконується, система повинна визначати не просто факт відмови, а й контур повернення (табл. 1).

Таблиця 1

Контур повернення

Логіка	Пункт повернення
Недостатня якість	повернення в R&D або технологічний блок
Невідповідність вимогам	повернення в R&D або технологічний блок
Надмірний ризик	направлення в поглиблену верифікацію
Відсутня економічна доцільність	координаційно-керуючий блок зупиняє проєкт, або зміна режиму у відкладений розвиток

Таким чином, зворотний хід у моделі ADM є частиною адаптивного циклу, що зменшує ймовірність помилкового впровадження та підвищує якість майбутніх рішень.

Окремо слід підкреслити роль освітньо-кадрового та знаннєво-аналітичного контурів у механізмі керування. У межах ADM вони не мають активуватися лише наприкінці циклу як завершальний додаток до технічного результату. Навпаки, рішення про підключення освітнього або знаннєвого контуру має прийматися ще на етапі проходження кейсу через основні стадії. Якщо кейс має високу повторюваність, навчальний потенціал або значення для формування стандарту, координаційно-керуючий блок повинен ініціювати паралельне формування документації, шаблонів, інструкцій, навчальних модулів і матеріалів супроводу. Це дозволяє відразу перетворювати одиничний результат на інституційний ресурс, не відкладаючи його формалізацію до завершення проєкту.

З позицій системної оптимізації мету керування ADM доцільно розглянути через цільову функцію (17):

$$\max \Phi_k = \theta_1 C_k - \theta_2 T_k - \theta_3 J_k - \theta_4 \rho_k + \theta_5 K_k + \theta_6 P_k, \quad (17)$$

де C_k – інтегральна оборонно-технологічна спроможність; T_k – тривалість проходження циклу; J_k – сукупні витрати; ρ_k – ризик; K_k – знаннєвий приріст; P_k – кадровий приріст; θ_i – вагові коефіцієнти. Така форма показує, що ADM керується не однією метою, наприклад, мінімізацією часу, а багатокритеріальною логікою, у якій швидкість, безпека, ефективність, знання та кадрове відтворення повинні перебувати у збалансованому співвідношенні.

У практичному розумінні це означає, що координаційно-керуючий блок ADM виконує три базові функції:

а) функцію відбору та пріоритетності кейсів;

б) функцію маршрутизації, тобто визначення послідовності проходження кейсу через контури та рішення про повернення;

в) функцію адаптивної корекції, коли на основі результатів верифікації, експлуатаційного зворотного зв'язку або ресурсних змін система змінює інтенсивність керуючих дій U_k та фактично перебудовує траєкторію проходження кейсу.

А отже, бачимо, що механізм керування ADM доцільно визначати як формалізовану систему пріоритетності, маршрутизації, допуску, повернення та адаптивної корекції кейсів у межах структурно-функціональної архітектури центру. У такому підході кожний перехід між контурами спирається на визначені критерії стану, а кожне повернення має не випадковий, а функціонально обґрунтований характер. Саме це забезпечує цілісність ADM як керованої системи, здатної працювати в умовах невизначеності, часового тиску, ресурсних обмежень і високої ціни помилки. У подальшому така формалізація створює підґрунтя для сценарного опису проходження кейсу через центр і для побудови системи показників оцінювання результативності ADM.

Сценарій функціонування ADM та система показників ефективності. Для прикладної інтерпретації запропонованої концептуальної моделі розглянемо типовий для воєнного часу сценарій, у якому об'єктом втручання виступає дефіцитна деталь озброєння, що вже не випускається серійно, але є критично важливою для відновлення працездатності пошкодженого вузла після бойового застосування. Вибір саме такого кейсу є методично виправданим, оскільки він поєднує одразу кілька характерних ознак середовища, описаного в моделі ADM, таких як дефіцит постачання, пошкодження виробу, часовий тиск, невизначеність технічного стану, потребу в інженерній адаптації та необхідність швидкого переходу від емпіричної проблеми до верифікованого рішення. Саме такі умови визначимо як базові для виникнення оперативної потреби та запуску великого адаптивного циклу ADM.

Нехай унаслідок бойового впливу пошкоджено вузол певного зразка озброєння, а його ключова деталь D^* більше не виробляється серійно, в зв'язку з чим відсутня в доступному ланцюгу постачання та не може бути оперативно замінена штатним способом. У такому випадку оперативний запит до ADM формується не як абстрактне технічне завдання, а як критичний кейс відновлення бойової спроможності конкретного виробу в обмеженому часовому інтервалі. Формалізуємо такий кейс у виразі (18):

$$R^* = (q^*, \tau^*, \kappa^*, \chi^*, \psi^*), \quad (18)$$

де q^* – критичність деталі для функціонування вузла; τ^* – максимально допустимий час реагування; κ^* – технічна складність відтворення; χ^* – ресурсомісткість рішення; ψ^* – очікуваний ефект від відновлення. Для обраного сценарію природно припустити, що q^* є високим, τ^* – малим, κ^* – середнім або високим, а ψ^* – істотним, оскільки відновлення деталі повертає в дію не окремий компонент, а цілий функціональний вузол.

На першій стадії запропонованого циклу ADM відбувається фіксація оперативної потреби. Джерелом запиту виступає факт бойового пошкодження та неможливість штатної заміни деталі. Оскільки запит поєднує високу функціональну значущість, дефіцитність і прямий вплив на відновлення спроможності, координаційно-керуючий блок маркує кейс як пріоритетний. В форматі ADM це є первинний контакт системи з практичною складовою, коли емпіричний факт відмови стає джерелом постановки задачі.

Наступна фаза, це стадія формалізації проблеми, де здійснюється ідентифікація пошкодженого вузла, збір залишків або уламків деталі, аналіз місця її розташування в системі, уточнення функціонального призначення, навантажень, допусків, умов взаємодії з суміжними елементами та можливих обмежень щодо матеріалу. Якщо повна технічна документація відсутня, формується неповна, але достатня для старту інженерного аналізу постановка завдання. На цій стадії ключовим результатом є технічно придатний опис задачі, який дозволяє перейти від запиту “потрібно відновити деталь” до задачі типу “потрібно відтворити або перепроєктувати функціональний елемент із заданими механічними, геометричними та

посадковими характеристиками”, а не саме рішення проблеми. Саме такий перехід від емпіричного випадку до формалізованої проблеми є обов'язковою умовою запуску подальших контурів ADM.

Після цього кейс входить у дослідницько-аналітичний контур. На цій стадії встановлюється, що пряме копіювання залишків пошкодженої деталі може бути недостатнім, оскільки її геометрія вже спотворена бойовим ушкодженням, а первинний матеріал або технологія виробництва можуть бути недоступними. Тому аналітичне осмислення включає не лише відновлення форми, а й реконструкцію функції деталі в межах цілого вузла. У результаті формується одна або кілька інженерних гіпотез, таких як точне відтворення, функціонально еквівалентне перепроєктування або посилене перепроєктування з адаптацією до доступної технології виготовлення та тимчасове польове рішення з подальшим доопрацюванням.

Саме на цьому етапі невизначеність H_k є найбільшою, оскільки існує кілька конкуруючих траєкторій розв'язання. У міру відбору гіпотез і накопичення технічних даних ентропія проблеми зменшується, що і становить один із головних системних ефектів ADM.

Центральною фазою сценарію виступає R&D та інженерне опрацювання. У цьому контурі здійснюються 3D-сканування уламків, побудова цифрової моделі, реверс-інжиніринг, обчислювальна реконструкція відсутніх фрагментів, визначення функціонально критичних поверхонь, підбір доступного матеріалу та коригування геометрії під наявну технологію виготовлення. Якщо оригінальна технологія була недосяжною або економічно не виправданою, модель переходить до перепроєктування деталі під адитивне або гібридне виробництво. Це повністю узгоджується з роллю R&D-контурів, описаних у запропонованій моделі як ядра інженерної трансформації оперативного досвіду в придатний до реалізації продукт.

Після досягнення мінімального рівня технічної зрілості $Z_k \geq Z_{min}$ кейс переходить у виробничо-технологічний контур. Тут відбувається фізичне виготовлення деталі D_{new}^* , яке може включати адитивний друк, механічну дообробку, термічну або поверхневу постобробку, контроль посадкових розмірів і складання з суміжним вузлом. Якщо в процесі виготовлення виявляються технологічні обмеження, кейс повертається в R&D-контур для корекції цифрової моделі або відбору іншого матеріалу. Таким чином, технологічна реалізація виступає не просто етапом виготовлення, а активним елементом адаптації рішення до ресурсних і часових умов.

Стадія верифікації для даного сценарію є критичною, оскільки деталь стосується озброєння, а отже помилка впровадження може мати неприйнятні наслідки. Верифікація включає геометричний контроль, функціональні випробування у складі вузла, оцінку стійкості до робочих навантажень, перевірку сумісності, аналіз поведінки після циклу роботи та, за потреби, прискорені ресурсні тести. У межах моделі ADM рішення може бути допущене до впровадження лише тоді, коли виконується система умов $V_k \geq V_{min}$, $\rho_k \leq \rho_{max}$, $\eta_k > 0$, де V_k – інтегральна верифікована придатність, ρ_k – ризик відмови, η_k – економічна доцільність. Якщо хоча б одна з умов не виконується, кейс не вважається завершеним, а повертається в контур доопрацювання. Саме в такій процедурі реалізується верифікаційно-довірчий мікроцикл, у якому довіра до рішення є не інтуїцією, а результатом багатокрокового підтвердження.

Після успішної верифікації деталь передається на стадію впровадження. У межах сценарію це означає не лише встановлення нової деталі у вузол, а фактичне відновлення функціональної готовності конкретного зразка озброєння. Однак на цьому практична цінність кейсу не завершується. На відміну від лінійної ремонтної моделі, ADM розглядає впровадження як точку виходу рішення в експлуатаційне середовище, з якого надходить новий зворотний зв'язок: чи була деталь зручною в монтажі, чи не виявилися додаткові вібраційні або теплові ефекти, чи не виникли нові обмеження під час бойового застосування,

чи можна стандартизувати таке рішення для інших аналогічних випадків. Таким чином, кейс не “закривається” впровадженням, а переходить у фазу експлуатаційного навчання системи.

Особливе значення в цьому сценарії має освітньо-кадровий контур. Якщо відновлення дефіцитної деталі виявилося успішним, результат повинен бути використаний для формування навчального кейсу: як ідентифікувати критичні пошкодження такого типу, як правильно збирати залишки геометрії, як будувати цифрову модель, які параметри є функціонально визначальними, які технологічні ризики супроводжують виготовлення, які критерії допуску є обов'язковими. У такий спосіб одиничне технічне рішення трансформується в навчальний модуль для інженерів, техніків, операторів ремонтних підрозділів або курсантів. Саме тут ADM проявляє себе не просто як центр виготовлення, а як середовище кадрового відтворення технологічної компетентності.

Останнім, але не менш важливим етапом виступає документування та оновлення знань. Для розглянутого кейсу це означає створення цифрового паспорту рішення, який включає 3D-модель відновленої деталі, опис вихідної проблеми, параметри сканування та реконструкції, вибір матеріалу, технологічну карту виготовлення, результати випробувань, зафіксовані ризики, часові витрати, обмін досвідом, що були отримані під час процесу, і рекомендації для аналогічних випадків. Після цього кейс повинен бути включений у бібліотеку реверсованих деталей, базу обміну досвідом і, за потреби, у каталог допустимих тимчасових або серійно відтворюваних рішень. Завдяки цьому ADM зменшує витрати майбутніх циклів: наступний випадок аналогічного пошкодження вже не стартує з нульової невизначеності, а використовує накопичений знаннявий капітал. Саме така логіка повернення результату в систему як ресурсу нового циклу і становить одну з головних відмінностей ADM від звичайного ремонтного ланцюга.

З позицій формалізації підсумковий ефект розглянутого сценарію доцільно описувати не одним результатом, а вектором виходу (19):

$$Y^* = (D_{new}^*, V^*, \Delta T^*, \Delta U^*, K_{add}^*, P_{add}^*), \quad (19)$$

де D_{new}^* – відновлена або перепроєктована деталь; V^* – досягнутий рівень верифікованої придатності; ΔT^* – скорочення часу відновлення порівняно з альтернативним способом; ΔU^* – приріст відновленої бойової спроможності вузла або системи; K_{add}^* – приріст ресурсу знання; P_{add}^* – приріст кадрової готовності. Такий підхід дозволяє показати, що результатом роботи ADM є не лише фізична деталь, а складний багатокомпонентний ефект відновлення.

Для оцінювання результативності ADM у розглянутому сценарії введемо систему показників ефективності.

Першою групою визначимо часові показники, такі як, час від надходження запиту до формалізації проблеми t_1 , час аналітичного опрацювання t_2 , час R&D t_3 , час виготовлення t_4 , час верифікації t_5 та час до фактичного впровадження t_6 . Тож сукупний час проходження кейсу дорівнює виразу (20):

$$T_{ADM} = t_1 + t_2 + t_3 + t_4 + t_5 + t_6. \quad (20)$$

Розуміємо, щодо доцільності порівняння T_{ADM} з умовним альтернативним часом відновлення T_{alt} , який був би потрібен у разі зовнішнього пошуку аналога, імпортного замовлення, канібалізації іншого зразка або відкладеного ремонту, отримаємо часовий вииграш (20):

$$\Delta T = T_{alt} - T_{ADM}. \quad (21)$$

Другою групою розглянемо техніко-функціональні показники. До них належать рівень верифікованої придатності V^* і коефіцієнт функціонального відновлення вузла (21):

$$\Gamma = \frac{F_{after}}{F_{nom}}, \quad (22)$$

де F_{after} – фактична функціональність вузла після впровадження рішення, а F_{nom} – його номінальна функціональність, а також показник повторюваності виготовлення R_{rep} , який показує, чи може це рішення бути стабільно відтворене повторно без втрати якості.

Третьою групою є ризикові показники. Базовим серед них є ρ^* – оцінений ризик відмови після впровадження. Для прикладного аналізу його можна доповнювати частотою виявлених критичних дефектів на етапі випробувань, коефіцієнтом повернення кейсу на доопрацювання та середньою кількістю ітерацій у верифікаційно-довірчому мікроциклі. Чим нижчим є ρ^* від прийнятного T_{ADM} , тим вищою є якість роботи ADM саме як керованої системи, а не лише як швидкого виробничого майданчика.

Четверту групу становлять економічні показники. Витрати на проходження кейсу доцільно розглядати як (23):

$$J^* = c^{anal} + c^{R\&D} + c^{prod} + c^{ver} + c^{train} + c^{doc}, \quad (23)$$

де окремі доданки відображають витрати на аналіз, інженерне опрацювання, виготовлення, випробування, навчання та документування. Водночас економічний ефект кейсу може бути поданий у вигляді (24):

$$E^* = b^{uptime} + b^{import} + b^{reuse} + b^{knowledge} - J^*, \quad (24)$$

де b^{uptime} – виграш від скорочення простою озброєння; b^{import} – виграш від уникнення зовнішньої закупівлі або пошуку аналога; b^{reuse} – виграш від можливості повторно використовувати модель і технологічну карту; $b^{knowledge}$ – довгостроковий виграш від включення кейсу до бази знань і навчальної системи. Якщо $E^* > 0$, кейс є не лише технічно успішним, а й економічно виправданим.

П'ята група показників призначена відображати освітньо-кадровий результат, без якого ADM втрачає свою концептуальну відмінність. До неї доцільно віднести приріст формалізованого знання ΔK (25):

$$\Delta K = K_{after} - K_{before}, \quad (25)$$

про кількість створених або оновлених документів, число підготовлених фахівців, що пройшли кейс як навчальний модуль, а також коефіцієнт повторного використання знання Λ_K (26):

$$\Lambda_K = \frac{N_{reuse}}{N_{cases}}, \quad (26)$$

де N_{reuse} – кількість наступних кейсів, у яких використано напрацювання даного сценарію, а N_{cases} – загальна кількість кейсів відповідного типу. Саме цей показник особливо важливий, оскільки він демонструє, чи справді ADM переводить одиничне технічне рішення в режим інституційної пам'яті.

Отже, розглянутий сценарій з дефіцитною деталлю озброєння, що вже не випускається і була пошкоджена в бойових умовах, наочно демонструє прикладну працездатність

концептуальній моделі ADM. Узагальнюючи викладене, слід підкреслити, що прикладна цінність концептуальної моделі ADM полягає не в описі окремого технічного процесу, а у формуванні цілісного механізму перетворення оперативного досвіду на відтворювану оборонно-технологічну спроможність. Саме в цьому полягає принципова відмінність запропонованого підходу від лінійних схем ремонту, локального реверс-інжинірингу або разового технологічного реагування. У моделі ADM кожен окремий кейс, зокрема такий, як відновлення дефіцитної деталі озброєння, що вже не випускається, розглядається не як ізольований епізод технічної допомоги, а як елемент ширшого інституційного циклу, в якому матеріальний результат поєднується зі знанням, кадровим, організаційним та економічним ефектом. Запропонована модель демонструє, що ефективність ADM визначається не тільки здатністю виготовити або відновити потрібний компонент у стислий строк. Її справжня результативність проявляється в тому, що центр одночасно виконує кілька функцій, скорочує час реагування на критичну потребу, знижує невизначеність технічного рішення, фільтрує ризик через верифікаційно-довірчий контур, формує документально зафіксоване знання, створює основу для навчання персоналу та зменшує витрати майбутніх циклів за рахунок повторного використання напрацьованих рішень. Таким чином, ADM виступає не лише засобом технічного відновлення, а механізмом накопичення оборонно-технологічного капіталу, що зростає з кожним завершеним кейсом.

У процесі дослідження отримані значення переваг моделі ADM порівняно з лінійним підходом воєнно-технічного реагування, наведені у нормованому концептуально-аналітичному вигляді для зручної ілюстрації системної відмінності запропонованої концепції ADM (табл. 2). На основі чого побудований нормований порівняльний профіль ефективності моделі ADM та класичного лінійного підходу, що показаний на рисунку 2.

Таблиця 2

Порівняльний профіль ефективності моделі ADM за ключовими функціональними вимірами

КРІ	Класична модель	ADM модель
Швидкість реагування	0,45	0,8
Технічна придатність	0,55	0,82
Верифікаційна надійність	0,4	0,85
Економічна доцільність	0,5	0,78
Накопичення знань	0,2	0,92
Кадрове відтворення	0,25	0,88
Масштабованість	0,35	0,76

Особливе значення має те, що в межах запропонованої моделі архітектура центру, механізм керування, сценарій проходження кейсу та система показників ефективності не існують відокремлено. Вони утворюють єдину логіку. Архітектура визначає, які саме підсистеми забезпечують цикл. Механізм керування встановлює правила переходу, повернення й допуску. Сценарій показує, як ця логіка працює на реальному прикладі.

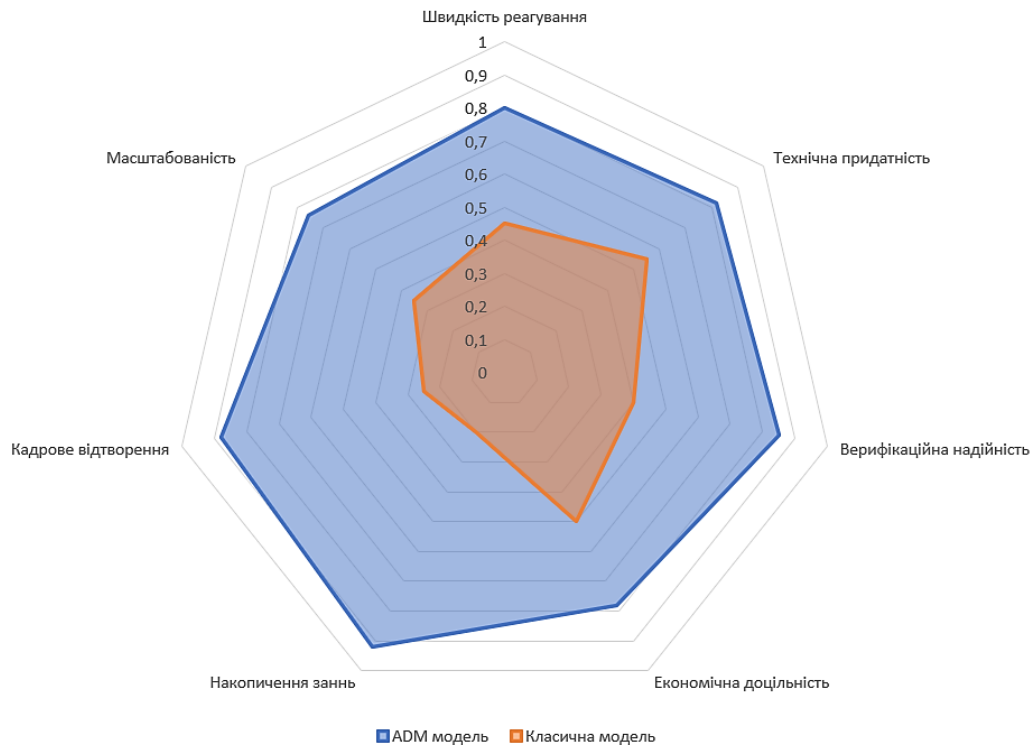


Рис. 2. Нормований порівняльний профіль ефективності моделі ADM та класичного лінійного підходу

Система показників переводить результат з рівня якісного опису у площину оцінювання й порівняння. Саме тому модель ADM може бути використана не лише як теоретичне пояснення, а як рамка для побудови практичних організаційних рішень, для внутрішнього аудиту роботи центру, для порівняння альтернативних конфігурацій і для подальшого математичного або цифрового моделювання. З прикладного погляду це означає, що ADM має цінність одразу на трьох рівнях. На оперативному рівні він дозволяє швидше повертати в дію техніку, вузли та системи, критичні для бойового застосування. На організаційному рівні він переводить імпровізаційні або ситуативні практики в керований та повторюваний цикл. На стратегічному рівні він створює передумови для поступового накопичення внутрішнього оборонно-технологічного потенціалу через знання, кадри, стандартизовані рішення та зменшення залежності від зовнішніх джерел постачання. Саме в сукупності цих рівнів і проявляється реальна прикладна цінність моделі центру перспективних технологій ADM.

Отже, запропонована концептуальна модель ADM має прикладну значущість не лише як спосіб опису воєнно-технічного реагування, а як інструмент системної організації оборонно-технологічного розвитку в умовах невизначеності, дефіциту та високої ціни помилки. Її сильна сторона полягає в тому, що вона поєднує практику, наукове осмислення, інженерію, верифікацію, навчання, документування та економічну доцільність у межах єдиного багатоконтурного циклу, де кожен завершений результат стає основою для наступного етапу розвитку. Саме така побудова створює логічно завершене підґрунтя для формулювання висновків і визначення напрямів подальших досліджень.

Висновки та напрями подальших досліджень

У роботі здійснено теоретичне обґрунтування та концептуальне моделювання центру перспективних технологій ADM як адаптивного багатоконтурного циклу формування оборонно-технологічної спроможності на основі оперативного досвіду. На відміну від підходів, у яких технічне реагування зводиться до окремих виробничих, ремонтних або дослідницьких дій, запропонована модель дозволяє інтерпретувати ADM як цілісне

соціотехнічне та інституційне середовище воєнного часу, у межах якого оперативна потреба послідовно проходить стадії формалізації, наукового осмислення, R&D та інженерного опрацювання, технологічної реалізації, верифікації, впровадження, підготовки персоналу, документування та оновлення знань. Саме така логіка дала змогу показати, що ключовим результатом функціонування ADM є не лише окреме технічне рішення, а відтворювана оборонно-технологічна спроможність, здатна до накопичення, масштабування та подальшого розвитку.

У ході дослідження доведено, що концептуальна модель ADM має багатоконтурний характер і поєднує макрологіку великого циклу з мікрологікою локальних контурів адаптації, верифікації, кадрового відтворення та накопичення знань. Це дало підстави обґрунтувати ADM не як суто функціональну схему центру, а як замкнений механізм нарощування спроможності, у якому практичний досвід, інженерне рішення, верифікація, навчання і документування не існують окремо, а взаємно підсилюють одне одного. Розроблені в межах роботи структурно-функціональна архітектура центру, механізм керування переходами між контурами, а також сценарій проходження типового кейсу показали, що запропонований підхід має не лише теоретичну цілісність, а й прикладну придатність до організації реального процесу воєнно-технічного реагування.

Розгляд прикладного сценарію з відновлення дефіцитної деталі озброєння, що вже не випускається і була пошкоджена в бойових умовах, підтвердив, що ADM може бути інтерпретований як механізм, який перетворює одиничну критичну проблему не лише на верифіковане технічне рішення, а й на навчальний кейс, елемент бази знань, підставу для майбутнього повторного використання та джерело зменшення витрат наступних циклів. Саме в цьому виявляється одна з головних сильних сторін моделі, що описує не тільки відновлення окремого вузла, а процес накопичення оборонно-технологічного капіталу через знання, кадри, стандартизовані рішення та інституційно організований досвід.

До напрямів подальших досліджень доцільно віднести, насамперед, поглиблення математичної формалізації моделі ADM через побудову системи динамічних змінних, функції цілі та критеріїв оптимального керування багатоконтурним циклом; розроблення методики кількісного оцінювання ефективності центру на основі часових, техніко-функціональних, ризикових, економічних і освітньо-кадрових показників; побудову цифрового двійника функціонування ADM для імітаційного дослідження різних типів кейсів і режимів навантаження; апробацію моделі на ширшому спектрі практичних сценаріїв, зокрема для задач бойового ремонту, адаптації вузлів, прискореного виготовлення компонентів, підготовки персоналу та відновлення логістичних критичних елементів; а також дослідження можливостей інтеграції ADM із системами управління знаннями, цифровими бібліотеками моделей, платформами верифікації та освітніми траєкторіями підготовки фахівців. Перспективним є і окремий напрям економічного аналізу, пов'язаний із оцінюванням довгострокового ефекту від функціонування ADM через скорочення простоїв техніки, зниження імпортої залежності, повторне використання інженерних рішень і накопичення внутрішнього технологічного потенціалу. Саме ці напрями можуть стати підґрунтям для переходу від концептуальної моделі до її подальшої методичної, організаційної та прикладної реалізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Updated Defence Production Action Plan // NATO. 13 February 2025. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/updated-defence-production-action-plan>.

2. Ukraine directed over 70% of weapon procurement spending to its own defense industry // National Security and Defense Council of Ukraine. 21.01.2026. URL: <https://www.rnbo.gov.ua/en/Dialnist/7364.html> (дата звернення: 17.04.2026).

3. Share of Ukrainian manufacturers in military procurement rises to 82% // Ministry of Defence of Ukraine. 23.01.2026. URL: <https://mod.gov.ua/en/news/share-of-ukrainian-manufacturers-in-military-procurement-rises-to-82> (дата звернення: 17.04.2026).
4. Dey A., Olusanmi A., Monsuru R., Nita Y., Weilong C. Additive Manufacturing Applications in Mission-Critical Operations: A Review // Journal of Manufacturing and Materials. 2025. Proc. 9, no.3. P. 70. URL: <https://doi.org/10.3390/jmmp9030070>.
5. Alzahmi W., Shamayleh A., Stefanchik M. The role of additive manufacturing in spare parts management: A systematic review // Cleaner Engineering and Technology. 2025. Vol. 27. P. 101029. URL: <https://doi.org/10.1016/j.clet.2025.101029>.
6. Peron M., Saporiti N., Coruzzolo A.M., Lolli F., Holmström J. The impact of Additive Manufacturing on supply chain resilience: a Delphi study // Technological Forecasting and Social Change. 2025. Vol. 219. P. 124231. URL: <https://doi.org/10.1016/j.techfore.2025.124231>.
7. Rešetar M., Valjak F., Branilović M., Šercer M., Bojčetić N. An approach for reverse engineering and redesign of additive manufactured spare parts // Proceedings of the Design Society. 2024. No. 4. P. 703–712. URL: <https://doi.org/10.1017/pds.2024.73>.
8. Давимука С. А. Інноваційна екосистема оборонної промисловості України: концептуальні засади та практика формування // О.В. Регіональна економіка – Регіональна економіка. 2024. № 111 (1). С. 65–80. DOI: <https://doi.org/10.36818/1562-0905-2024-1-7>.
9. Бурдейна Н., Федченко О., Венцюк А. Сучасні виклики військової логістики: аналіз забезпечення Збройних сил України в умовах війни з РФ. // Journal of Scientific Papers Social development & Security. 2025. № 15. С. 83–91. URL: <https://doi.org/10.33445/sds.2025.15.3.9>.
10. Research and development plan. 2021–2024. Part 1. Outlook // Norwegian Defence Research Establishment (FFI). 2021. 36 p. URL: <https://www.ffi.no/en/documents/> (date of access: 17.04.2026).
11. The Secretary General's Annual Report 2025 // NATO. 2026. URL: <https://www.nato.int/> (date of access: 17.04.2026).
12. 2024 NATO STO Highlights // NATO Science & Technology Organization (STO). 31.03.2025. URL: <https://www.sto.nato.int/> (date of access: 17.04.2026).
13. NATO Science and Technology Organization 2025 Collaborative Programme of Work // NATO Science & Technology Organization (STO). 10.02.2025. URL: <https://www.sto.nato.int/> (date of access: 17.04.2026).
14. First ever defence industrial strategy and a new defence industry programme to enhance Europe's readiness and security // European Commission, Directorate-General for Defence Industry and Space. 05.03.2024. URL: <https://defence-industry-space.ec.europa.eu/> (date of access: 17.04.2026).
15. Joint White Paper for European Defence Readiness 2030 // European Commission, High Representative of the Union for Foreign Affairs and Security Policy. 19.03.2025. URL: <https://defence-industry-space.ec.europa.eu/document/> (date of access: 17.04.2026).
16. Annual report 2025 // European Defence Agency. 2026. 36 p. URL: <https://eda.europa.eu/docs/> (date of access: 17.04.2026).

Надійшла до редколегії 27.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.396

канд. техн. наук Бовда Е. М. ORCID: 0000-0002-8267-2120 (ВІТІ ім. Героїв Крут)
д-р техн. наук Самохвалов Ю. Я. ORCID: 0000-0001-5123-1288 (КНУ ім. Т. Шевченка)
Клименко В. М. ORCID: 0000-0001-7834-7213 (ВІТІ ім. Героїв Крут)

ДЕЯКІ АСПЕКТИ КОНЦЕПТУАЛЬНОГО ПРОЄКТУВАННЯ ІНФОКОМУНІКАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Розглянуто питання концептуального проєктування інфокомунікаційних систем військового призначення. Проєктування таких систем передбачає поетапне створення технічної та організаційної моделі майбутньої системи, здатної ефективно виконувати задані функції. Запропоновано декларативно-процедурну структурування розробки концепції таких систем. Концепція системи виступає в якості керівного і організуючого початку при формуванні проєкту системи, обґрунтуванні її технічного вигляду і тактико-технічних вимог, що пред'являються до системи. Запропоновано механізм формування варіантів концепції на основі морфологічного методу Цвікі. Властивістю морфологічного підходу є спрямованість на пошук повноти і спільності варіантів побудови системи. Це дозволяє систематично виявити всю сукупність можливих варіантів, проаналізувати наслідки прийнятих рішень і врахувати наявність декількох цілей, для досягнення яких призначається проєктована система. Обґрунтовано застосування методу аналізу ієрархій для вибору варіанту, який найбільше відповідає вимогам зацікавлених осіб. Розглянуто питання визначення очікуваних результатів реалізації обраного варіанту концепції та їх методи. На основі отриманих оцінок глобального домінування альтернатив визначається відносна оцінка ефективності концепції за обраним показником. Якщо задано кілька показників, то в цьому випадку отримують інтегральну оцінку ефективності за цими показниками. В цілому розглянутий підхід не претендує на завершеність і може бути використаний в якості пілотажу для розробки відповідних методик концептуального проєктування інфокомунікаційних систем.

Ключові слова: концептуальне проєктування, концепція, інфокомунікаційні системи військового призначення, метод морфологічного аналізу, функціональна ефективність, техніко-економічні показники.

E. Bovda, Y. Samokhvalov, V. Klymenko. Some aspects of conceptual design of military information and communication systems

The article considers the issues of conceptual design of military information and communication systems. The design of such systems involves the phased creation of a technical and organizational model of the future system capable of effectively performing the specified functions. A declarative-procedural structuring of the development of the concept of such systems is proposed. The concept of the system acts as a guiding and organizing principle in the formation of the system design, the justification of its technical appearance, and the tactical and technical requirements imposed on the system. A mechanism for forming concept options based on Zwicky's morphological method is proposed. A feature of the morphological approach is its focus on finding the completeness and commonality of system design options. This allows for the systematic identification of all possible options, analysis of the consequences of decisions made, and consideration of the multiple goals for which the designed system is intended. The application of the hierarchy analysis method for selecting the option that best meets the requirements of interested parties is justified. The issues of determining the expected results of implementing the selected concept option and their methods are considered. Based on the obtained estimates of global dominance of alternatives, a relative assessment of the concept's effectiveness is determined for the selected indicator. If several indicators are specified, an integral assessment of effectiveness for these indicators is obtained. In general, the approach considered does not claim to be complete and can be used as a pilot for the development of appropriate methods for the conceptual design of information and communication systems.

Keywords: conceptual design, concept, military information and communication systems, morphological analysis method, functional effectiveness, technical and economic indicators.

Постановка завдання та актуальність дослідження. Інфокомунікаційна система (ІКС) – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1].

У Збройних Сил України інфокомунікаційні системи виконують роль базової інфраструктури, яка забезпечує оперативний та надійний обмін інформацією, підтримку цифрових сервісів, автоматизацію управлінських і виробничих процесів, інтеграцію різних галузей (економіки, науки, освіти, оборони) у єдиний інформаційний простір для потреб оборони.

У загальному вигляді інфокомунікаційна система військового призначення за своєю організаційною побудовою є ієрархічною і в залежності від задач, що вирішуються, може бути системою стратегічного, оперативного, або тактичного рівня (рис. 1). Основним елементом ІКС є система управління, яка виконує основні функції:

мережевого управління, що складається з завдань: управління конфігурацією; управління безпекою; управління за відмов; управління послугами; управління робочими характеристиками;

управління розподіленими застосуваннями;

моніторинг технічного програмного забезпечення;

підтримання прийняття рішень щодо функціонування мережі;

управління модернізацією;

моделювання мереж;

тренування та злагодження особового складу пунктів управління.

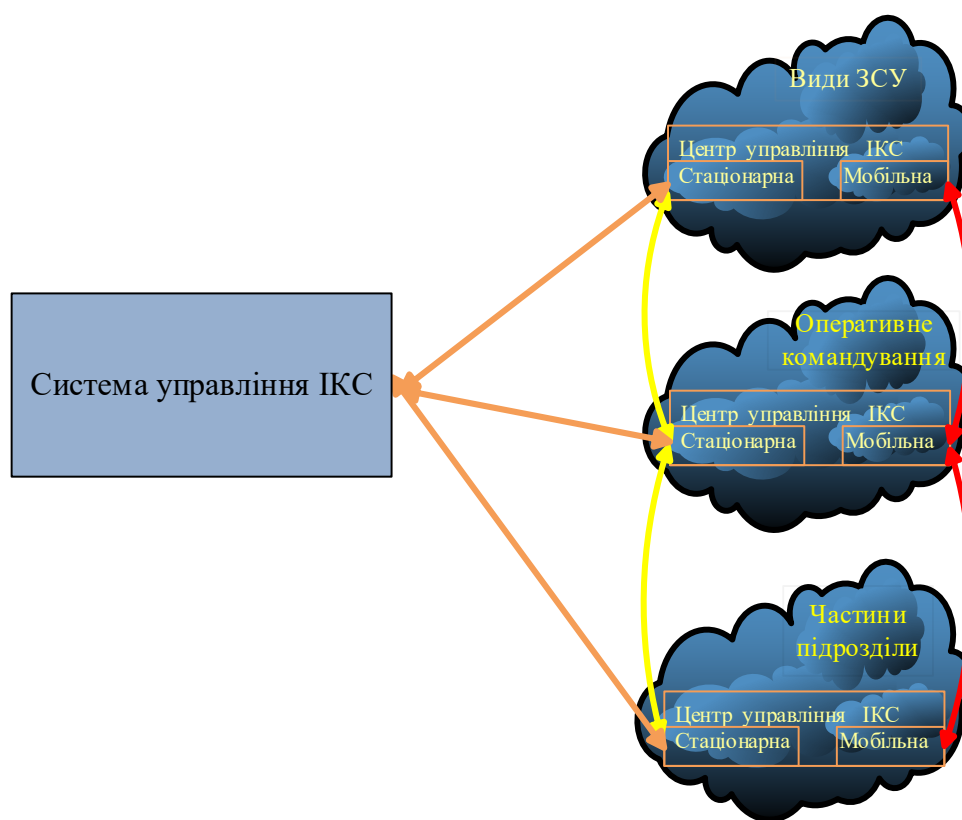


Рис. 1. Загальна схема інфокомунікаційної системи військового призначення

Проектування інфокомунікаційних систем військового призначення передбачає поетапне створення технічної та організаційної моделі майбутньої системи, здатної ефективно виконувати задані функції. Особливістю проектування є необхідність інтеграції різномірних технологій (мережових, обчислювальних, програмних), забезпечення масштабованості, сумісності та кіберзахисту, а також урахування швидких темпів розвитку інфокомунікаційних технологій, що потребує гнучких та адаптивних рішень.

Аналіз останніх досліджень та публікацій. Концептуальне проектування ІКС здійснюється на початковій стадії її проектування, результатом якої є концепція системи. Вона є стратегічним документом, в якому втілений генеральний задум (керівна ідея) її побудови та функціонування [2; 3].

Незважаючи на практичну важливість результатів концептуального проектування, у вітчизняних програмах етапу «формулювання концепції» незаслужено мало приділяється уваги. У зв'язку з цим практично не опрацьовуються в достатній мірі фундаментальні питання системної побудови системи та її функціонування. У зарубіжній же практиці цьому етапу приділяється значно більше уваги. Так, ще в 1965 р. в Міністерстві оборони США було прийнято рішення, що без етапу «формулювання концепції» пропозиції про контракти на розробку військової техніки просто не розглядаються [2].

На сьогодні відсутня будь-яка цілісна і апробована методологія, що дозволяє розглядати процес концептуального проектування комплексно, з системних позицій. Тому концептуальні рішення щодо створення автоматизованих систем військового призначення приймаються на основі евристики, інтуїтивних міркувань і досвіду вирішення аналогічних завдань. І, як наслідок, питання концептуального проектування в більшості своїй висвітлені тільки на понятійному та декларативному рівнях [2]. Таке становище в області концептуального проектування ІКС не дозволяє приймати проєктні рішення з гарантованим досягненням мети і не відповідає умовам результативності. У підсумку це призводить до порушення термінів реалізації проєктів, перевитрат коштів і невиконання вимог показників до кінцевого результату. Тому в даний час ці питання вимагають інтенсивного обговорення і розвитку.

У галузі конструктивної методології розробки концепції ІКС можна відзначити роботи [3–8], в яких розглядаються питання формування технічного обриса перспективних зразків озброєння та військової техніки, проектування інформаційних систем, системно-концептуальні основи і елементи методології формування оперативно-тактичних і тактико-технічних вимог, що пред'являються до перспективних зразків озброєння і військової техніки та зразків, що модернізуються, формування концептуальних проєктних моделей перспективних складних зразків озброєння і військової техніки, методичні аспекти концептуального проектування автоматизованих систем, передпроєктного проектування ІКС.

У даній роботі отримав подальший розвиток підхід до структурування і формалізації процесу концептуального проектування, запропонованого в [7]. Запропонований підхід базується на методі морфологічного аналізу Ф. Цвіккі, що дозволяє виявити, систематизувати і вивчити всі можливі варіанти побудови системи, призначеної для реалізації заданих функцій, вибрати найбільш раціональний, оцінити його функціональну ефективність і техніко-економічні показники.

Метою статті є дослідження шляхів концептуального проектування інфокомунікаційних систем військового призначення

Основна частина. Декларативно-процедурне структурування розробки концепції. З точки зору семантики, термін «концепт» відображає зміст поняття, його сенс, тому проектування на концептуальному рівні – це проектування на рівні сенсу або змісту поняття систем. З огляду на цю тезу, процес розробки концепції можна представити як синтез можливостей засобів обчислювальної техніки (ЗОТ), концептуальних ідей їх використання для досягнення максимуму ефекту системи, а також вимог користувача [2]. Це творчий процес, і, по суті, є сумішшю науки і мистецтва.

Концептуальні ідеї використання можливостей ЗОТ формуються на основі досвіду, знань та інтуїції і представляють відкриту множину, оскільки під впливом розвитку науки, практики та запитів користувачів ідеї виникають і зникають. Ці ідеї можна згрупувати в чотири групи [2]: інформатизація, інтелектуалізація, інтеграція та індивідуалізація. З урахуванням сказаного, процес формування концепції ІКС в загальному вигляді можна представити наступною схемою [7] (Рис. 2).

На основі даної схеми формується концепція системи, яка виступає в якості керівного і організуючого початку при формуванні проєкту системи, обґрунтуванні її технічного вигляду і тактико-технічних вимог, що висувають до системи. Вона в найбільш концентрованому вигляді з позицій найголовніших функціональних властивостей і ключових характеристик

представляє ІКС, об'єднує в єдине ціле потреби, можливості, ресурси та обмеження при розробці, виробництві, експлуатації та застосуванні за функціональним призначенням системи.

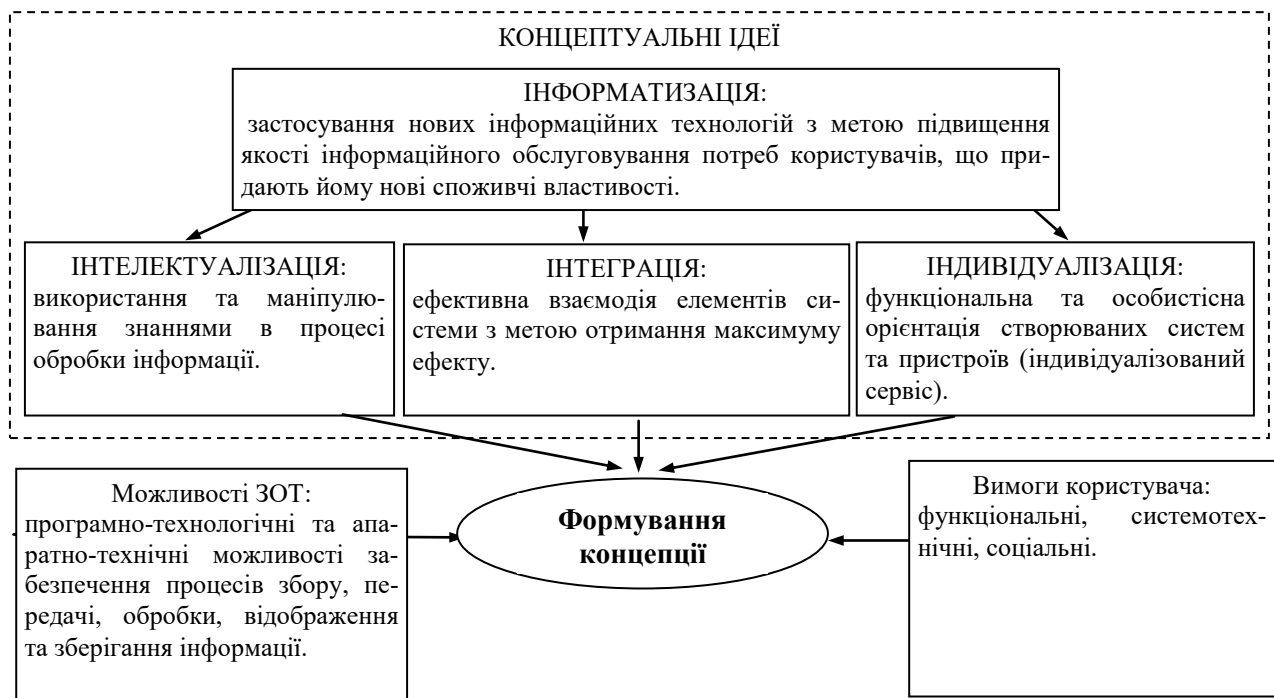


Рис. 2. Загальна системно-логічна схема розробки ІКС

Основоположними складовими частинами концепції ІКС військового призначення є: оперативно-тактична концепція; науково-технічна концепція; виробничо-економічна концепція [6] (рис. 3).



Рис. 3. Складові частини концепції ІКС

Оперативно-тактична концепція ІКС характеризує призначення системи, покладені на неї завдання, умови їх виконання та оперативно-тактичні вимоги, що впливають з них і пред'являються до системи. Ключовими компонентами оперативно-тактичної концепції ІКС

є її функціональні властивості, наприклад, такі, як мобільність, безперервність, застосовність, стійкість тощо.

Науково-технічна концепція ІКС відображає науково-технічні можливості, матеріально-технічну основу можливого створення ІКС і визначає технічні шляхи та засоби реалізації оперативно-тактичних вимог, що пред'являються до системи.

Виробничо-економічна концепція ІКС визначає наявні та прогнозовані необхідні ресурси, можливості та обмеження виробничо-технологічного характеру при розробці та виробництві системи.

Вимоги, що пред'являються до ІКС – це вимоги до бойових (функціональних) можливостей та ефективності застосування системи для виконання покладених на неї завдань у складі системи управління. Вони впливають з ролі та місця ІКС в системі управління. Вимоги представляються сукупністю найбільш важливих (істотних) бойових (функціональних) властивостей, якими повинна володіти ІКС, і виражаються у формі вимог до рівневих значень кількісно-якісних показників, за допомогою яких оцінюється ступінь прояву кожної з цих властивостей. Вимоги до ІКС повинні відображати: призначення і область застосування (просторово-часові характеристики); завдання, покладені на зразок; вимоги до основних бойових (функціональних) властивостей ІКС; умови застосування за призначенням тощо. За своєю суттю вимоги до ІКС – це вимоги, що виконують роль системно об'єднуючої основи тактико-технічних вимог, відповідно до яких формуються інші їх компоненти.

На основі загальних вихідних даних, отриманих в результаті обстеження об'єкту автоматизації (ОА), визначаються фактори, що зумовлюють дефіцит ефективності функціонування ОА, а також завдання ІКС та умови їх вирішення. В результаті всебічного аналізу шляхів удосконалення системи для забезпечення вирішення завдань у заданих умовах з необхідним рівнем ефективності формується оперативно-тактична концепція ІКС, яка відіграє роль інформаційної основи для обґрунтування оперативно-тактичних вимог до функціонування системи.

Дослідження науково-технічних можливостей створення ІКС з урахуванням реалізації оперативно-тактичної концепції призводять до формування науково-технічної концепції системи, яка в комплексі з оперативно-тактичними вимогами виступає базою для обґрунтування тактико-технічних вимог. Виробничо-економічний аналіз можливості створення ІКС, яка б реалізувала її науково-технічну концепцію, призводить до формування виробничо-економічної концепції системи.

Формування варіантів концепції. Як було зазначено вище, концепція ІКС являє собою сукупність поглядів (ідей) на принципи розробки та функціонування системи та її архітектуру. Згідно зі стандартом IEEE 1471-2000 архітектура – це базова організація системи, втілена в її компонентах, їхніх відносинах між собою та з оточенням [9]. Під компонентом розуміється модульна частина системи, яка інкапсулює її вміст. В якості компонент базової організації ІКС виступає організаційно-функціональна структура системи, її функції та режими функціонування, а також склад видів забезпечення [10].

У процесі формування концепції, як правило, розглядаються різні концептуальні ідеї та інформаційні технології, що дозволяє сформувати альтернативні її варіанти. Цей процес пропонується реалізувати в рамках морфологічного підходу Цвікі [11], який є досить ефективним засобом для вирішення завдання формування варіантів різноманітних систем. Найбільш характерною і суттєвою властивістю морфологічного підходу є його спрямованість на пошук повноти і спільності варіантів побудови системи. Він дозволяє систематично виявити всю сукупність можливих варіантів, проаналізувати наслідки прийнятих рішень і врахувати наявність декількох цілей, для досягнення яких призначається проєктована система.

В основі морфологічного підходу лежать три розвинені Ф. Цвіккі морфологічні методи: метод систематичного покриття поля, метод заперечення і конструювання та метод морфологічного аналізу. Останній застосовується найчастіше, оскільки є досить простим.

Згідно з цим методом спочатку визначаються компоненти концепції системи, які відображають її архітектуру, функції та види забезпечення. Потім для кожної компоненти визначаються способи її реалізації. В результаті формується морфологічна таблиця. Фрагмент цієї таблиці, що відображає можливі варіанти реалізації функцій системи, наведено на рисунку 4.

Функції системи	Можливі способи реалізації функції					Число способів
F_1	c_{11}	c_{12}	c_{13}	$\dots$	c_{1k_1}	k_1
F_2	c_{21}	c_{22}	c_{23}	$\dots$	c_{2k_2}	k_2
$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	
F_l	c_{l1}	c_{l2}	c_{l3}	$\dots$	c_{lk_l}	k_l
$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	
F_L	c_{L1}	c_{L2}	c_{L3}	$\dots$	c_{Lk_L}	k_L

Рис. 4. Можливі варіанти реалізації функцій системи

У цій таблиці ланцюжок пов'язаних шляхів показує один із варіантів реалізації функцій системи, а кожен рядок таблиці визначає відповідний морфологічний клас, тобто рядок $F_l = (c_{l1}, \dots, c_{lk_l})$ визначає l -й морфологічний клас.

При використанні методу морфологічного аналізу виникає проблема розмірності, яка пов'язана з великою кількістю різноманітних варіантів системи навіть при вирішенні відносно невеликої за складністю задачі. Тому особливого значення набуває дослідження можливої локалізації областей досліджуваних варіантів системи. Ці області повинні включати в себе варіанти, кращі в певному сенсі, причому їх кількість повинна бути в розумних межах. Один із способів, що дозволяє здійснити таку локалізацію, був запропонований Р. Ейресом [12].

В основі способу Ейреса лежить поняття «відстані» для морфологічних варіантів.

Введемо наступні поняття.

Морфологічний простір (Λ) – це сукупність дискретних точок, де кожна точка представляє конкретну комбінацію способів реалізації функцій системи.

Морфологічний варіант – це точка в морфологічному просторі.

Морфологічна відстань – це кількість функцій, для яких два варіанти мають неспівпадаючі елементи.

Нехай $x = (x_1, \dots, x_L)$, $x_l \in F_l$ – морфологічний варіант. Тоді морфологічна відстань $\rho(x, y)$ між варіантами x і y обчислюється наступним чином:

$$\rho(x, y) = \sum_{l=1}^L (1 - \delta_{x_l y_l}),$$

де $\delta_{x_l y_l}$ є символ дельта Кронекера: $\delta_{x_l y_l} = \begin{cases} 1, & \text{якщо } x_l = y_l, \\ 0, & \text{в протилежному випадку.} \end{cases}$

Сферичною околицею $u_{\rho, L}(x)$ радіуса ρ з центром у точці $x \in \Lambda$ називається підмножина точок у метризованого простору Λ , віддалених від точки x на відстані ρ :

$$u_{\rho, L}(x) = \{y \mid \rho(x, y) = \rho; x, y \in \Lambda\}.$$

Кульовою околицею $w_{r,L}(x)$ радіуса ρ з центром у точці $x \in \Lambda$ називається підмножина точок у метризованого простору Λ , віддалених від точки x на відстані, не більший за r :

$$w_{\rho,L}(x) = \{y \mid \rho(x, y) \leq r; x, y \in \Lambda\}.$$

В якості локалізації областей досліджуваних варіантів системи можна використовувати обидві околиці, проте, на наш погляд, більш інформативною є кульова околиця.

На ранніх стадіях морфологічного аналізу бажано виключати з розгляду завідомо нереалізовані варіанти, тобто варіанти, які містять несумісні елементи різних класів. У морфологічному просторі таким варіантам будуть відповідати заборонені точки, які слід виключити з числа точок околиці, яка розглядається.

Будемо вважати, що морфологічний варіант є допустимим тоді і тільки тоді, коли всі елементи, що входять до нього, попарно сумісні. Поставимо кожній парі елементів x_i і x_k вектору $x \in \Lambda$ у відповідність індикатор $b(c_i, c_k)$ сумісності елементів c_i і c_k векторів x_i і x_k , тобто:

$$b(c_i, c_k) = \begin{cases} 1, & \text{якщо } c_i \text{ та } c_k \text{ сумісні,} \\ 0, & \text{в протилежному випадку} \end{cases}$$

Тоді кількість варіантів, всі елементи яких попарно сумісні, буде дорівнювати:

$$N(x) = \prod_{i \geq k} b(c_i, c_k) = 1,$$

а число всіх допустимих варіантів буде дорівнювати:

$$N = \sum_{x \in \Lambda} N(x).$$

Наведені вище результати дають можливість формувати і досліджувати тільки ті варіанти системи, які знаходяться в деякій околиці заданої точки морфологічного простору. Вибір цієї «базової» точки, як правило, визначається змістовною постановкою задачі. В якості базової точки може виступати, наприклад, вже існуючий варіант системи або ж деякий гіпотетичний варіант, що має досить високі оцінки за критеріями, але неприпустимий через попарну несумісність його елементів.

Якщо базових варіантів декілька, то можна виділити такі точки морфологічного простору, сумарна відстань від яких до всіх базових варіантів мінімальна. Іншими словами, виникає завдання визначення варіантів, які в середньому найбільш наближені до множини базових варіантів. При цьому передбачається, що реалізувати такі проміжні варіанти буде простіше, оскільки значною мірою можна буде використовувати досвід, отриманий при розробці та застосуванні базових варіантів.

Медіаною множини точок Y метризованого морфологічного простору Λ називається будь-яка точка $x \in \Lambda$, сумарна відстань від якої до всіх точок множини Y мінімальна. Медіана M множини Y обчислюється наступним чином:

$$M = \underset{x \in \Lambda}{\operatorname{Argmin}} \frac{1}{|Y|} \sum_{y \in Y} p(x, y).$$

Аналогічно будуються морфологічні таблиці для інших компонентів концепції (рис. 5).

Концепція ІКС	Компоненти		Елементи	Принципи	Способи реалізації				
	Організаційно-функціональна структура			Принципи побудови організаційно-функціональної структури	c_1^S	c_2^S	c_3^S	...	$c_{k_S}^S$
	Функції		F_1	Принципи реалізації функцій	$c_1^{F_1}$	$c_2^{F_1}$	$c_3^{F_1}$	...	$c_{k_{F_1}}^{F_1}$
			$\vdots$		$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
			F_{n_F}		$c_1^{F_{n_F}}$	$c_2^{F_{n_F}}$	$c_3^{F_{n_F}}$	...	$c_{k_{F_{n_F}}}^{F_{n_F}}$
	Режими функціонування		R_1	Принципи функціонування	$c_1^{R_1}$	$c_2^{R_1}$	$c_3^{R_1}$	...	$c_{k_{R_1}}^{R_1}$
			$\vdots$		$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
			R_{n_R}		$c_1^{R_{n_R}}$	$c_2^{R_{n_R}}$	$c_3^{R_{n_R}}$	...	$c_{k_{R_{n_R}}}^{R_{n_R}}$
	Види забезпечення	Компоненти математичного забезпечення	M_1	Принципи розробки математичного забезпечення	$c_1^{M_1}$	$c_2^{M_1}$	$c_3^{M_1}$	...	$c_{k_{M_1}}^{M_1}$
			$\vdots$		$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
			M_{n_M}		$c_1^{M_{n_M}}$	$c_2^{M_{n_M}}$	$c_3^{M_{n_M}}$	...	$c_{k_{M_{n_M}}}^{M_{n_M}}$
		Компоненти інформаційного забезпечення	I_1	Принципи розробки інформаційного забезпечення	$c_1^{I_1}$	$c_2^{I_1}$	$c_3^{I_1}$	...	$c_{k_{I_1}}^{I_1}$
			$\vdots$		$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
			I_{n_I}		$c_1^{I_{n_I}}$	$c_2^{I_{n_I}}$	$c_3^{I_{n_I}}$	...	$c_{k_{I_{n_I}}}^{I_{n_I}}$
		Компоненти програмного забезпечення	P_1	Принципи розробки програмного забезпечення	$c_1^{P_1}$	$c_2^{P_1}$	$c_3^{P_1}$	...	$c_{k_{P_1}}^{P_1}$
			$\vdots$		$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
			P_{n_P}		$c_1^{P_{n_P}}$	$c_2^{P_{n_P}}$	$c_3^{P_{n_P}}$	...	$c_{k_{P_{n_P}}}^{P_{n_P}}$
		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
		Компоненти технічного забезпечення	T_1	Принципи розробки технічного забезпечення	$c_1^{T_1}$	$c_2^{T_1}$	$c_3^{T_1}$	...	$c_{k_T}^{T_1}$
			$\vdots$		$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
			T_{n_T}		$c_1^{T_{n_T}}$	$c_2^{T_{n_T}}$	$c_3^{T_{n_T}}$	...	$c_{k_{T_{n_T}}}^{T_{n_T}}$

Рис. 5. Морфологічна таблиця концепції інфокомунікаційної системи

У цій таблиці ланцюжок пов'язаних способів показує варіант концепції системи.

Вибір варіанту концепції. Для стадії концептуального проектування ІКС характерна низька структурованість предметних областей, багатоаспектність процесів, що відбуваються, відсутність достатньої кількісної інформації про їх динаміку, неповнота і неточність вихідних даних, що обумовлює велику невизначеність у прийнятті рішень [13]. Тому найбільш ефективними, а в деяких випадках і єдино можливими методами, які можуть бути використані для вирішення даного завдання, є методи експертних оцінок, зокрема, метод аналізу ієрархій (МАІ) [14; 15]. При цьому, в умовах, коли висувуються підвищені вимоги до точності результатів, можна використовувати підхід [17], який дозволить підвищити узгодженість парних порівнянь.

Ми не будемо наводити всі механізми цього методу, а розглянемо тільки його основний етап, що полягає в структуруванні завдання у вигляді домінантної ієрархії.

Вершина ієрархії визначає мету завдання – вибір варіанту концепції ІКС. Потім формується рівень так званих акторів, які здатні впливати на створення і функціонування ІКС. Наступний рівень складають вимоги (цілі) акторів, які мотивують вибір. Можливий перелік акторів та їх вимог наведено в таблиці 1.

Таблиця 1

Перелік акторів та їх вимог

Актори	Вимоги (цілі)
Керівництво об'єкта автоматизації (замовник – головний центр управління ІКС)	Передбачуваність ходу проєктування, продуктивне використання ресурсів та бюджету; виконання функціональних вимог до ІКС
Кінцевий користувач (центр управління ІКС різного рівня)	Інтуїтивно зрозуміле та коректне функціонування ІКС, продуктивність, надійність, зручність використання, доступність та безпека
Системний адміністратор ІКС	Інтуїтивно зрозуміле функціонування та управління ІКС, наявність інструментів моніторингу
Фахівець із супроводу ІКС	Зрозумілий, несуперечливий та документований принцип функціонування ІКС, легкість внесення змін
Розробник ІКС	Прості та несуперечливі принципи проєктування

У таблиці 2 наведено функціональні вимоги, які, як правило, висуваються до ІКС, та показники їх функціонування [6; 7].

Таблиця 2

Функціональні вимоги, які висуваються до ІКС

Вимога	Показник
Оперативність (швидкість)	Час на збирання, обробку та видачу інформації
	Час прийняття рішення, постановку і доведення завдань до виконавців
	Час вирішення завдань
Розмах	Дальність передачі
	Площа збору інформації
Безперервність	Математичне очікування часу максимальної перерви функціонування
	Математичне очікування часу на мінімальну тривалість безперебійної роботи
Стійкість (живучість, завадостійкість, надійність, електромагнітна сумісність)	Коефіцієнт стійкості
	Ймовірність своєчасного збирання інформації
	Ймовірність своєчасної передачі
	Коефіцієнт живучості
	Коефіцієнт збереження працездатності
	Коефіцієнт завадостійкості
	Коефіцієнт готовності
	Середній час безвідмовної роботи
	Ймовірність безвідмовної роботи за заданий час
	Коефіцієнт електромагнітної сумісності
Пропускна спроможність	Коефіцієнт інформаційного заповнення системи
	Коефіцієнт обробки (переробки) інформації
	Коефіцієнт споживання інформації
	Сумарний показник пропускної спроможності
	Максимальна пропускна спроможність каналу, маршруту, напрямку
	Мінімальний час доставки пакетів
	Ефективна пропускна спроможність

Вимога	Показник
Точність	Середня пропускна спроможність мережі
	Пікова пропускна спроможність
	Точність формування, збору, обробки та видачі інформації, а також її давність
	Сумарний коефіцієнт спотворення інформації (час давності інформації; час старіння)
	Середньоквадратичні помилки результатів розв'язання задач

I, нарешті, елементами нижнього рівня ієрархії є варіанти концепції системи, які представляються відповідними компонентами її архітектури, що відображають систему поглядів на побудову системи відповідним варіантом. Таку ієрархію можна представити у вигляді наступного дерева (рис. 6).

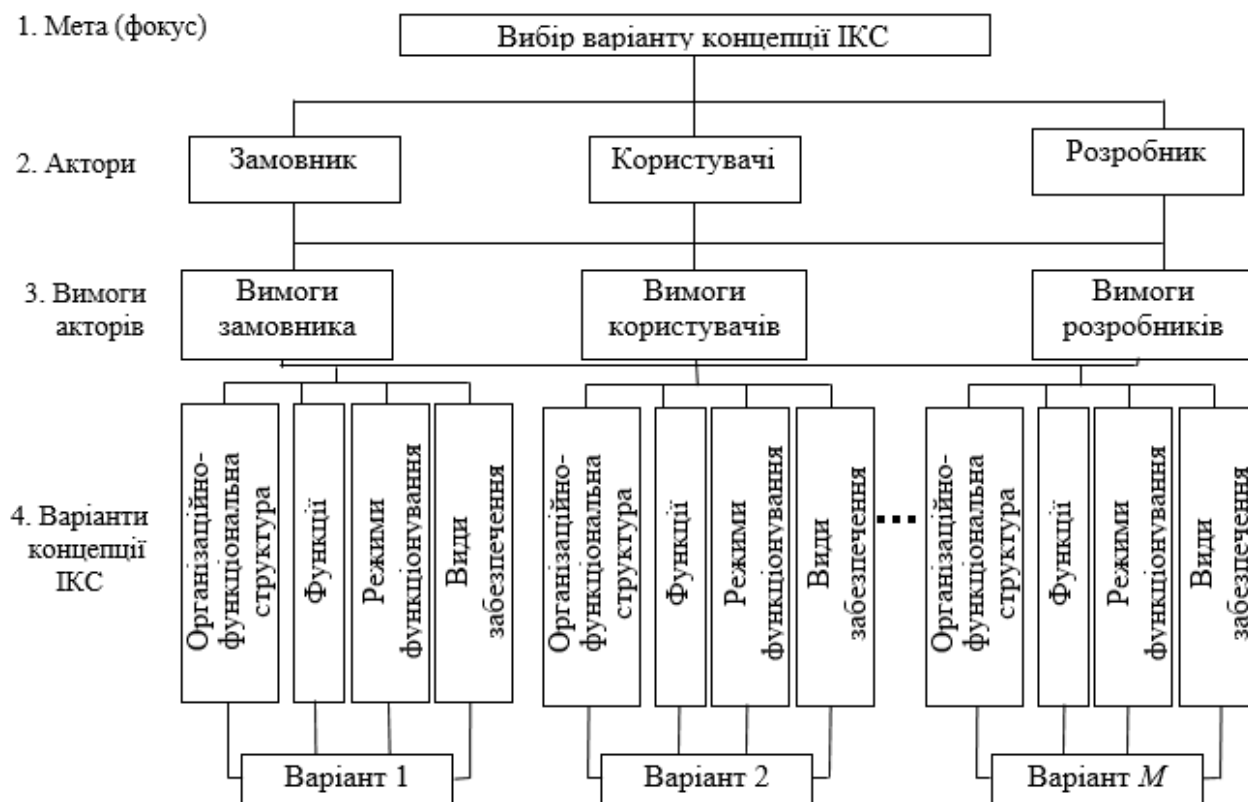


Рис. 6. Ієрархія завдання вибору варіанту концепції ІКС

Далі здійснюється побудова матриць домінування елементів рівнів ієрархії та послідовне обчислення локальних і глобальних пріоритетів. Варіант з найбільшим глобальним пріоритетом визначатиме концепцію системи.

Визначення очікуваних результатів реалізації концепції. Під очікуваними результатами реалізації концепції, згідно з [16], розуміється функціональна ефективність створюваної ІКС та її техніко-економічні показники.

Оцінювання функціональної ефективності ІКС. Функціональна ефективність ІКС – це властивість системи реалізовувати свої функції в заданих умовах функціонування та з певною якістю [9]. Суть оцінювання функціональної ефективності ІКС полягає у визначенні відносних оцінок прогнозованих показників функціонування системи з поточними, які визначаються в процесі обстеження ОА.

Для стадії концептуального проєктування ІКС характерна низька структурованість предметних областей, багатоаспектність процесів, що відбуваються, відсутність достатньої кількісної інформації про їх динаміку, неповнота і неточність вихідних даних, що обумовлює велику невизначеність у прийнятті рішень [13]. Тому для вирішення даного завдання також будемо використовувати метод аналізу ієрархій (МАІ). На рисунку 7 представлена в загальному випадку ієрархія завдання оцінки функціональної ефективності концепції.

На основі отриманих оцінок глобального домінування альтернатив визначається відносна оцінка ефективності концепції за обраним показником. Необхідно зауважити, що якщо задано кілька показників, то в цьому випадку буде отримано інтегральну оцінку ефективності за цими показниками.

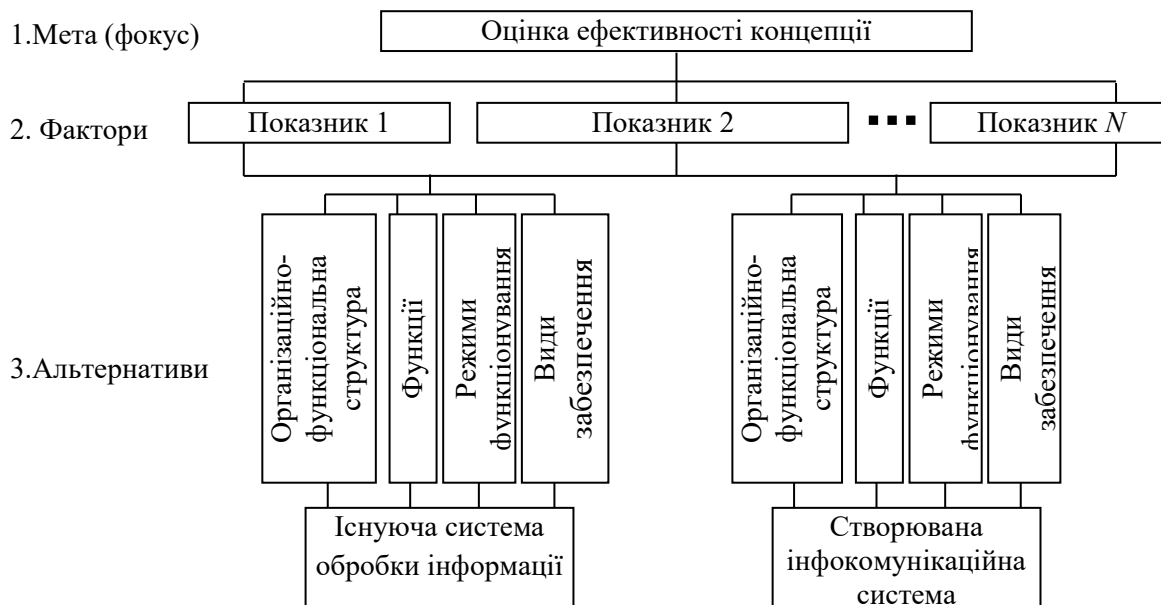


Рис. 7. Ієрархія завдання оцінювання функціональної ефективності концепції ІКС

Нехай, наприклад, необхідно оцінити ефективність концепції створюваної ІКС за показником «Час збору інформації». Далі, нехай $(0,4; 0,6)$ – вектор глобального домінування альтернатив щодо цього показника, а час збору інформації за допомогою існуючих засобів становить 10 хвилин. Тоді можна очікувати, що ІКС, побудована відповідно до оцінюваної концепції, дозволить скоротити цей час у 1,5 рази.

Оцінювання техніко-економічних показників. До техніко-економічних показників концепції належать час і вартість її реалізації. Для оцінки цих показників концепція сама по собі мало інформативна, оскільки досить складно з необхідною для практики точністю оцінити час і вартість реалізації загальних поглядів на побудову системи. Тому для отримання достатніх вихідних даних для оцінювання техніко-економічних показників ІКС академіком В. І. Скуріхіним [3] запропоновано на основі концепції системи формувати її вигляд, який є конкретним втіленням концептуальних ідей. Разом з тим, на етапі концептуального проєктування все ж можна отримати наближені оцінки цих показників, використовуючи механізми нечіткого прогнозування. З цією метою можна використовувати підхід, який дозволяє отримати прогнозні оцінки часу і вартості проєктів на основі нечітких лінгвістичних оцінок робіт, що входять до цих проєктів [17].

Висновки. Розглянуто питання концептуального проєктування інфокомунікаційних систем військового призначення. Запропоновано декларативно-процедурну структуру розробки концепції таких систем та механізм формування варіантів концепції на основі морфологічного методу Цвікі. Обґрунтовано застосування МАІ для вибору варіанту, який

найбільше відповідає вимогам зацікавлених осіб. Розглянуто питання визначення очікуваних результатів реалізації обраного варіанту концепції та їх методи. В цілому розглянутий підхід не претендує на завершеність і може бути використаний в якості пілотажу для розробки відповідних методик концептуального проєктування інфокомунікаційних систем військового призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakononline.com.ua/documents/show/162730_594986.
2. Скурихин В. И. О формулировании концепций. Концепция “четырёх И” / В. И. Скурихин // Управляющие системы и машины. 1989. № 2. С. 7–12.
3. Гриб Д. А. Методологічний підхід до формування технічного обрису перспективних зразків озброєння та військової техніки / Д. А. Гриб, Б. О. Демідов, М. В. Науменко // Наука і оборона. 2009. Вип. 4. С. 30–34.
4. Воробович Н. П. Проектирование информационных систем. Электронный учебно-методический комплекс / Н. П. Воробович. URL: <http://www.kgau.ru/istiki/umk/pis/18.htm>.
5. Гриб Д. А. Системно-концептуальні основи і елементи методології формування оперативно-тактичних і тактико-технічних вимог, що пред'являються до перспективних зразків озброєння і військової техніки та зразків, що модернізуються / Д. А. Гриб, Б. О. Демідов, М. В. Науменко // Системи озброєння та військова техніка. 2009. Вип. 2 (18). С. 65–73.
6. Демидов Б. А. Системна методология формирования концептуальных проектных моделей перспективных сложных образцов вооружения и военной техники / Б. А. Демидов, М. В. Науменко // Збірник наукових праць Харківського університету Повітряних Сил. 2010. Вип. 1 (23). С. 116–123.
7. Самохвалов Ю., Науменко Е., Бурба О. Методические аспекты концептуального проектирования автоматизированных систем // Регистрация, зберігання і обробка даних. 2012. Т. 14, № 4. С. 73–80.
8. Самохвалов Ю., Бурба О. Предпроектное проектирование АС. Киев, 2013. 289 с.
9. ANSI/IEEE Std 1471-2000, Recommended Practice for Architectural Description of SoftwareIntensive Systems. URL: <http://www.iso-architecture.org/ieee-1471/>.
10. Software Engineering Institute. Community Software Architecture Definitions. URL: <http://www.sei.cmu.edu/architecture/start/glossary/community.cfm>.
11. Zwicky F. Discovery invention, research through the morphological approach. New York: McMillan & Co., 1969. 106 с.
12. Эйрес Р. Научно-техническое прогнозирование и долгосрочное планирование / Р. Эйрес. М.: Мир, 1971. 296 с.
13. Герасимов Б. М. Нечеткие множества в задачах проектирования, управления и обработки информации / Б. М. Герасимов, Г. Г. Грабочевский, Н. А. Рюмшин. К.: Промінь, 2002. 137 с.
14. Саати Т. Принятие решений. Метод анализа иерархий. / Т. Саати. М.: Радио и связь, 1993. 314 с.
15. Samokhvalov Y. Y. Developing the Analytic Hierarchy Process Under Collective Decision-Making Based on Aggregated Matrices of Pairwise Comparisons // Cybern Syst Anal. 2022. № 58. P. 758–763. URL: <https://doi.org/10.1007/s10559-022-00509-3>.
16. Настанова “Інформаційні та автоматизовані системи управління”. ВКДП 6-26(01).01. 2020. 44 с. URL: https://sprotyvg7.com.ua/wp-content/uploads/2024/02/2_%D0%92%D0%9A%D0%94%D0%9F-6-2601.01-%D0%9D%D0%90%D0%A1-%D0%86%D0%9D%D0%A4-%D1%82%D0%B0-%D0%90%D0%A1%D0%A3.pdf.

17. Y. Samokhvalov. Forecasting Time and Cost of the Jobs in Network Models Based on Fuzzy Linguistic Estimates. *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2019, pp. 1–4, DOI: 10.1109/ATIT49449.2019.9030480.

Надійшла до редколегії 08.01.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.94:004.056:519.87

канд. техн. наук, доцент Грінков В. О. ORCID: 0000-0002-9574-3792 (ВІТІ ім. Героїв Крут)

Грінкова Г. В. ORCID: 0009-0003-4896-364X (НДІ ВР)

Слюсар П. П. ORCID: 0009-0007-3738-2523 (НДІ ВР)

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗАЛЕЖНО ВІД ТОПОЛОГІЇ ПОБУДОВИ НА ОСНОВІ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

У сучасних умовах ведення військових дій та зростання кіберзагроз забезпечення кіберстійкості інформаційних систем військового призначення набуває критичного значення. Одним із ключових факторів, що впливають на рівень кіберстійкості, є топологія побудови мережі, яка визначає її здатність протистояти відмовам, атакам і деградації функціонування.

Існуючі підходи до оцінювання кіберстійкості інформаційних систем, як правило, не враховують комплексного впливу структурних характеристик мережі або не забезпечують формалізованого багатокритеріального аналізу. Відсутність універсальної математичної моделі, яка дозволяє інтегрувати різноманітні топологічні показники та враховувати їхню відносну важливість, ускладнює обґрунтований вибір оптимальної структури мережі.

Метою статті є розроблення математичної моделі оцінювання кіберстійкості інформаційних систем залежно від топології їхньої побудови на основі методу аналізу ієрархій *Analytic Hierarchy Process*, що дозволяє визначати пріоритетність альтернативних топологічних рішень.

У роботі використано метод аналізу ієрархій для визначення вагових коефіцієнтів критеріїв кіберстійкості, зокрема робастності, алгебраїчної зв'язності, вершинної зв'язності, централізації та середньої довжини шляхів. Як альтернативи розглядаються типові мережеві топології (кільцева, подвійне кільце, дерево, часткова *mesh*-структура). Проведено формування матриць парних порівнянь критеріїв, альтернатив по кожному критерію, перевірку узгодженості суджень і розрахунок векторів пріоритетів.

Запропоновано математичну модель, яка дозволяє здійснювати інтегральну оцінку кіберстійкості інформаційних систем на основі агрегування зважених критеріїв. Отримано ранжування мережевих топологій за рівнем кіберстійкості та визначено найбільш ефективні структурні рішення для умов підвищених кіберзагроз. Показано, що використання методу аналізу ієрархій забезпечує обґрунтованість прийняття рішень за умов багатокритеріальності та невизначеності.

Розроблена модель дозволяє формалізувати процес оцінювання кіберстійкості інформаційних систем і враховувати вплив топологічних характеристик мережі. Отримані результати можуть бути використані при проектуванні та модернізації інформаційно-телекомунікаційних систем військового призначення. Подальші дослідження доцільно спрямувати на розширення моделі за рахунок використання нечітких, нейтрософських підходів та методу аналітичного мережевого процесу *Analytic Hierarchy Process* для підвищення точності і адекватності моделі.

Ключові слова: кіберстійкість, інформаційні системи, топологія мережі, метод аналізу ієрархій, АНР, ФАНР, багатокритеріальний аналіз, структурна зв'язність, робастність, оцінювання ефективності.

V. Hrinkov, H. Hrinkova, P. Sliusar. Mathematical model for assessing cyber resilience of information systems depending on the topology of the structure based on the hierarchy analysis method

In today's conditions of military operations and the growth of cyber threats, ensuring the cyber resilience of military information systems is becoming critical. One of the key factors affecting the level of cyber resilience is the topology of the network, which determines its ability to withstand failures, attacks, and degradation of functioning.

Existing approaches to assessing the cyber resilience of information systems, as a rule, do not take into account the complex impact of network structural characteristics or do not provide for formalized multi-criteria analysis. The lack of a universal mathematical model that allows integrating heterogeneous topological indicators and taking into account their relative importance complicates the informed choice of the optimal network structure.

The purpose of the article is to develop a mathematical model for assessing the cyber resilience of information systems depending on the topology of their construction based on the method of hierarchy analysis, which allows determining the priority of alternative topological solutions.

The paper uses the analysis of hierarchies method to determine the weighting coefficients of cyber resilience criteria, in particular robustness, algebraic connectivity, vertex connectivity, centralization, and average path length. Typical network topologies (ring, double ring, tree, partial mesh-structure) are considered as alternatives. Matrices of pairwise comparisons of criteria, alternatives for each criterion, verification of the consistency of judgments and calculation of priority vectors are formed.

A mathematical model is proposed that allows for an integrated assessment of cyber resilience of information systems based on the aggregation of weighted criteria. A ranking of network topologies by the level of cyber resilience is obtained and the most effective structural solutions for conditions of increased cyber threats are determined. It is shown that the use of the method of hierarchy analysis ensures the validity of decision-making under conditions of multi-criteria and uncertainty.

The developed model allows to formalize the process of assessing the cyber resilience of information systems and take into account the influence of topological characteristics of the network. The results obtained can be used in the design and modernization of military information and telecommunication systems. Further research should be directed at expanding the model by using fuzzy, neutrosophic approaches and the analytical network process method to increase the accuracy and adequacy of the model.

Keywords: *cyber resilience, information systems, network topology, analytic hierarchy process, AHP, FAHP, multi-criteria analysis, structural connectivity, robustness, efficiency assessment.*

Актуальність та постановка завдання в загальному вигляді. У сучасних умовах цифровізації сектору безпеки та оборони, а також зростання інтенсивності кіберзагроз, забезпечення кіберстійкості інформаційних систем (ІС) військового призначення стає одним із ключових чинників ефективного управління військами та функціонування систем зв'язку. Особливу роль у цьому контексті відіграє структура мережі, зокрема її топологія, яка визначає здатність системи зберігати працездатність у разі відмов окремих елементів, кібератак або порушення каналів зв'язку.

Аналіз сучасних наукових підходів показує, що оцінювання кіберстійкості часто здійснюється або на основі окремих показників (надійності, зв'язності, живучості), або з використанням складних моделей, які не враховують системну взаємодію структурних характеристик мережі. При цьому недостатньо досліджено вплив топології побудови ІС на її кіберстійкість у рамках формалізованого багатокритеріального підходу.

У зв'язку з цим актуальним є розроблення математичних моделей, що дозволяють інтегрувати різноманітні критерії оцінювання, враховувати їхню відносну важливість та забезпечувати обґрунтований вибір оптимальної топології мережі в умовах невизначеності та обмеженості ресурсів.

Аналіз попередніх досліджень. Поняття кіберстійкості в сучасних дослідженнях трактується не лише як здатність системи протистояти кібератакам, а також як спроможність передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, атак чи компрометації. Саме таке трактування закріплене у підходах Національного інституту технологій і стандартів США *National Institute of Standards and Technology* (NIST) [1], де кіберстійкість розглядається як властивість системи, критична для досягнення функціональних цілей у конфліктному кіберсередовищі.

Теоретичною основою багатокритеріального вибору в задачах оцінювання складних систем є метод аналізу ієрархій Т. Сааті [2]. У праці сформовано базові положення: ієрархічне структурування задачі, побудова матриць парних порівнянь, визначення локальних пріоритетів та перевірка узгодженості експертних суджень. Це робить метод придатним для задач, у яких необхідно інтегрувати кілька різноманітних критеріїв в один інтегральний показник.

Окремий напрям досліджень стосується використання спектральних характеристик графа для оцінювання стійкості мережевих структур. У роботі [3] показано, що алгебраїчна зв'язність — друге найменше власне значення матриці Лапласа — має важливе значення для аналізу робастності мережі, оскільки характеризує складність роз'єднання графа на незалежні компоненти. Автори також показують, що зі зростанням алгебраїчної зв'язності зростає і стійкість мережі до вузлових і каналних відмов.

У роботі [4] досліджується зв'язок між алгебраїчною зв'язністю та класичними показниками робастності графа — вершинною і реберною зв'язністю. У ній обґрунтовується, що спектральні характеристики можуть бути корисними індикаторами здатності мережі зберігати цілісність при відмовах вузлів і ліній зв'язку. Це особливо важливо для задач оцінювання кіберстійкості топологій ІС.

У роботі [5] виконано порівняння поширених метрик робастності для прогнозування стійкості мереж до атак. Автори доводять, що жодна окрема метрика не є універсально найкращою для всіх типів графів, натомість ефективність метрики залежить від структури мережі та сценарію впливу. Цей висновок є важливим для нашого дослідження, оскільки підтверджує доцільність не однокритеріального, а багатокритеріального оцінювання кіберстійкості.

Аналогічний висновок наведено у праці [6], де здійснено порівняльний аналіз різних показників мережевої робастності. Дослідження підтверджує, що окремі метрики відображають різні аспекти стійкості мережі, а тому для комплексного оцінювання доцільно поєднувати кілька показників у межах єдиної моделі.

У статті [7] показано, що топологічні атрибути суттєво впливають на стійкість мереж, однак самих топологічних індикаторів недостатньо для обґрунтованого проєктування системи, оскільки між різними аспектами стійкості можуть існувати компроміси. Це прямо підтримує ідею побудови інтегральної моделі на основі кількох критеріїв.

Щодо застосування *Analytic Hierarchy Process* (АНР) саме у сфері кібербезпеки, варто зазначити працю [8], де метод аналізу ієрархій використано для оцінювання стану мережевої безпеки для промислового інтернету речей. Автори демонструють, що АНР є придатним інструментом для визначення ваг окремих факторів безпеки та формування інтегральної оцінки. Водночас, такі роботи переважно орієнтовані на ситуаційне оцінювання безпеки, а не на аналіз впливу топології мережі на кіберстійкість.

Отже, аналіз літератури показує, що: по-перше, кіберстійкість доцільно трактувати як комплексну властивість системи, що охоплює протидію, відновлення та адаптацію; по-друге, графові та спектральні метрики дійсно є інформативними для аналізу стійкості топології; по-третє, жоден окремий показник не забезпечує повного опису кіберстійкості; по-четверте, АНР є придатним інструментом для агрегування різномірних критеріїв.

Водночас у виявлених джерелах недостатньо опрацьованим залишається питання інтегрального оцінювання кіберстійкості ІС саме залежно від топології їхньої побудови на основі поєднання характеристик графів. Саме ця прогалина і зумовлює доцільність подальшого дослідження.

Метою статті є розробка математичної моделі оцінювання кіберстійкості ІС залежно від топології їхньої побудови на основі методу аналізу ієрархій, яка забезпечує інтеграцію структурних і топологічних характеристик мережі, визначення їхньої вагомості та обґрунтоване ранжування альтернатив з урахуванням принципів кіберстійкості, сформульованих у рекомендаціях NIST.

Виклад основного матеріалу. Під кіберстійкістю ІС розумітимемо здатність системи зберігати працездатність, структурну цілісність і функціональність в умовах деструктивних впливів, зокрема кібератак, відмов елементів та порушень зв'язності.

Кіберстійкість ІС значною мірою визначається її топологією побудови, оскільки саме структура зв'язків між вузлами впливає на здатність мережі до відновлення після пошкоджень, наявність альтернативних маршрутів передачі даних, ступінь централізації та вразливість до атак на критичні вузли, ефективність функціонування в умовах деградації.

Таким чином, задача оцінювання кіберстійкості може бути зведена до аналізу та порівняння різних варіантів топологічної структури ІС.

Нехай задано множину альтернативних топологій ІС:

$$T = \{T_1, T_2, \dots, T_n\},$$

де кожна топологія T_i описується графом $G_i = (V_i, E_i)$;

V_i – множина вузлів; E_i – множина каналів зв'язку.

Для оцінювання кіберстійкості вводиться множина критеріїв:

$$C = \{C_1, C_2, \dots, C_m\},$$

які характеризують структурні та функціональні властивості мережі.

Кожній топології T_i за кожним критерієм C_j відповідає значення показника:

$$x_{ij} = f_j(T_i),$$

де x_{ij} – значення показника i топології та j критерію.

На основі значень показників x_{ij} для кожного критерію C_j сформовано вектор локальних пріоритетів альтернатив, отриманий через матрицю парних порівнянь альтернатив за критерієм C_j :

$$P^{(j)} = \{p_{1j}, p_{2j}, \dots, p_{nj}\},$$

де p_{ij} – відносна перевага (вага) альтернативи T_i за критерієм C_j і виконується умова

нормування: $\sum_{i=1}^n p_{ij} = 1, p_{ij} \geq 0$.

За методом аналізу ієрархій визначено ваги критеріїв:

$$W = \{w_1, w_2, \dots, w_m\}, \sum_{j=1}^m w_j = 1.$$

Задача полягає у визначенні інтегральної оцінки кіберстійкості для кожної топології T_i , визначеної як зважена сума локальних пріоритетів, згідно з виразом (1):

$$S_i = \sum_{j=1}^m w_j \cdot p_{ij}. \quad (1)$$

Оптимальна топологія визначається як:

$$T^* = \arg \max_{T_i \in T} S_i.$$

Таким чином, практична реалізація запропонованої моделі потребує уточнення двох ключових складових: множини альтернатив, що визначають простір можливих топологічних рішень; системи критеріїв, які адекватно відображають кіберстійкість з урахуванням структурних властивостей мережі.

З огляду на те, що вибір критеріїв безпосередньо залежить від типу досліджуваних альтернатив, доцільним є попереднє обґрунтування набору топологій, що підлягають аналізу.

Для аналізу оцінки кіберстійкості ІС обрано наступну множину топологій (рис. 1):

$$T = \{T_1, T_2, T_3, T_4, T_5\},$$

де T_1 – деревоподібна топологія (*Tree*);

- T_2 – кільцева топологія (*Ring*);
 T_3 – подвійне кільце (*Dual Ring*);
 T_4 – кільце з центральним вузлом (*Ring + Hub*);
 T_5 – частково-зв'язна мережа (*Partial Mesh*).

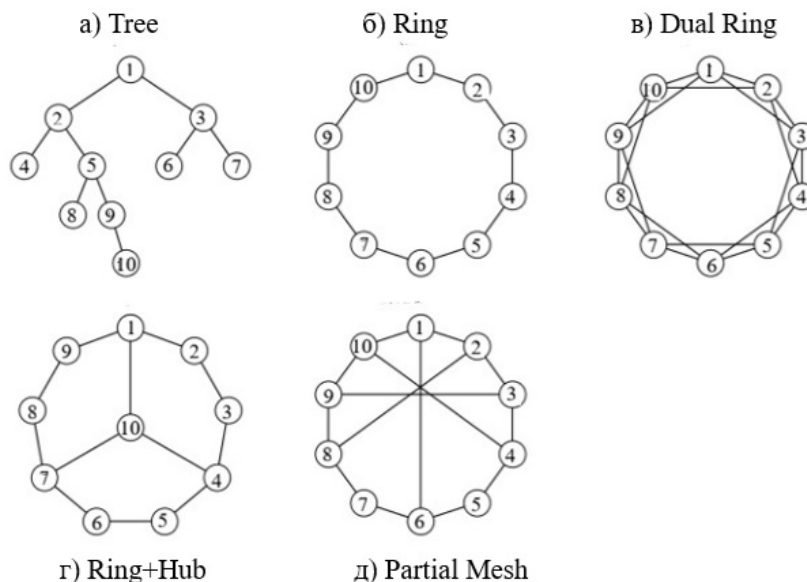


Рис. 1. Альтернативні топології мережі

Вибір топології *Tree*, *Ring*, *Dual Ring*, *Ring + Hub*, *Partial Mesh*, на наш погляд, є обґрунтованим, оскільки вони утворюють репрезентативну множину альтернатив, що відрізняються за рівнем централізації, резервування, зв'язності та наявністю альтернативних маршрутів передавання інформації. Це дозволяє всебічно дослідити вплив структурної організації мережі на кіберстійкість ІС. Використання однакової кількості вузлів $n = 10$ забезпечує коректність порівняння альтернатив і дає можливість зосередити аналіз саме на топологічних особливостях мережевої побудови.

Обрана множина топологій визначає простір альтернатив для оцінювання кіберстійкості та характеризується різними структурними властивостями, зокрема рівнем зв'язності, надмірності та централізації. Для їх коректного порівняння необхідно ввести систему критеріїв, що дозволяє кількісно оцінити вплив цих властивостей на стійкість мережі до деструктивних впливів. У зв'язку з цим наступним етапом є формування та обґрунтування критеріїв оцінювання кіберстійкості.

Для оцінювання кіберстійкості обраних топологічних структур введемо множину наступних критеріїв: робастність, алгебраїчна зв'язність, вершинна зв'язність, централізація графа, середня довжину шляхів.

У теорії графів робастність — це здатність графа зберігати зв'язність при видаленні вузлів або ребер. Робастність мережевої топології визначається її здатністю зберігати зв'язність та функціональну цілісність при частковому видаленні вузлів або каналів зв'язку та є структурною складовою кіберстійкості ІС [9].

Робастність мережевої структури є безрозмірним показником, що відображає частку збереженої зв'язності системи при поступовому видаленні її елементів та набуває значень у межах $[0; 1]$. Цей показник будемо визначати з урахуванням двох типів дестабілізуючих впливів: порушень вузлів (компрометація/відмова мережевих елементів) та порушень каналів зв'язку (блокування/перехоплення/порушення маршрутизації), що моделюються відповідно як видалення вершин і ребер графа. Для розрахунку робастності для всіх топологічних структур застосуємо формулу (2) [10]:

$$R = \frac{1}{k} \sum_{q=1}^k S(q), \quad (2)$$

де k – кількість вузлів; $S(q)$ – частка вузлів у найбільшій компоненті після видалення q вузлів, причому на кожному кроці вибирається така множина вилучених вузлів, яка мінімізує найбільшу компоненту, що відповідає імітації цільової атаки.

Робастність деревоподібної топології при цільовій атаці становить $R_{Tree} = 0,16$, що свідчить про високу вразливість ієрархічної структури до атак на вузли з найбільшим ступенем.

Для кільцевої топології робастність становить $R_{Ring} = 0,23$, що перевищує відповідний показник деревоподібної структури. Це пояснюється відсутністю центральних вузлів і більш рівномірним розподілом зв'язків.

Робастність кільця з центральним вузлом дорівнюється $R_{Ring + Hub} = 0,25$. Додавання hub-вузла не завжди знижує кіберстійкість, у деяких випадках воно підвищує робастність завдяки резервним шляхам.

Робастність подвійного кільця становить $R_{Dual Ring} = 0,41$, бо подвійне кільце має більше альтернативних шляхів, не містить жодного критичного вузла, довше зберігає зв'язність при видаленні вузлів.

Для частково зв'язаної топології при цільовій атаці на вузли отримано значення робастності $R_{Partial Mesh} = 0,28$, що перевищує відповідні показники для кільцевої та деревоподібної структур. Це пояснюється наявністю додаткових каналів, які забезпечують збереження альтернативних маршрутів після видалення критичних вузлів.

Алгебраїчна зв'язність графа λ_2 визначається як друге найменше власне значення лапласіана графа та використовується як показник структурної зв'язаності мережі [11; 12].

Для кільцевої топології алгебраїчна зв'язність визначалась за аналітичними формулами (3), (4) спектра циклічного графа [11; 12]:

$$\lambda_{2_{Ring}} = 2(1 - \cos \frac{2\pi}{k}), \quad (3)$$

$$\lambda_{2_{Dual Ring}} = 2(1 - \cos \frac{4\pi}{k} - \cos \frac{8\pi}{k}), \quad (4)$$

де k – кількість вузлів графа. Для топології *Tree*, *Ring + Hub*, *Partial Mesh* значення λ_2 визначалися зі спектрів матриць лапласіанів графів. Отримані значення алгебраїчної зв'язності для аналізованих топологій представлені в таблиці 1.

Таблиця 1

Значення алгебраїчної зв'язності

Топологія	Алгебраїчна зв'язність λ_2
<i>Tree</i>	0,154
<i>Ring</i>	0,382
<i>Dual Ring</i>	1,764
<i>Ring + Hub</i>	0,697
<i>Partial Mesh</i>	1,121

Для оцінювання мінімального рівня руйнування мережевої структури використано показник вершинної зв'язності графа $k(G)$, який визначає мінімальну кількість вузлів, видалення яких призводить до втрати зв'язності мережі. За критерієм вершинної зв'язності найбільш стійкою є двокільцева топологія $k_{Dual\ Ring} = 4$, тоді як деревоподібна структура має мінімальну стійкість $k_{Tree} = 1$. Кільцева, гібридна та частково зв'язана топології мають однакове значення вершинної зв'язності $k_{Ring} = k_{Ring+Hub} = k_{Partial\ Mesh} = 2$.

Централізація показує, наскільки мережа залежить від одного або кількох вузлів. Якщо більшість маршрутів проходить через один вузол, мережа високо централізована, що знижує її кіберстійкість. Це безрозмірна величина. Для оцінювання централізації топології використано ступеневу централізацію, що визначається через відхилення ступенів вершин від максимального значення. Такий підхід дозволяє виявити наявність структурно домінуючих вузлів у мережі і визначається за формулою (5) [13]:

$$C_D = \frac{\sum_{i=1}^k (d_{\max} - d(v_i))}{(k-1)(k-2)}, \quad (5)$$

де $d(v_i)$ – ступінь i вузла; $d_{\max}$ – максимальна ступінь у графі; k – кількість вузлів графа.

У таблиці 2 приведені отримані значення централізації альтернативних топологій.

Таблиця 2

Значення централізації C_D

Топологія	Централізація C_D	Інтерпретація значень
<i>Tree</i>	0,167	Помірна централізація
<i>Ring</i>	0,000	Децентралізація
<i>Dual Ring</i>	0,000	Децентралізація
<i>Ring + Hub</i>	0,083	Низька централізація
<i>Partial Mesh</i>	0,083	Низька централізація

Отримані результати показують, що кільцеві топології мають нульову централізацію, тоді як ієрархічна деревоподібна структура характеризується більшою залежністю від окремих вузлів.

Середня довжина шляху у мережевій структурі – це середня кількість кроків, необхідних для з'єднання будь-яких двох випадкових вузлів мережі. Вона вимірює ефективність передачі інформації або взаємодії в мережі: чим менше це значення, тим швидше та ефективніше вузли. Середня довжина найкоротших шляхів характеризує компактність мережевої топології та визначає ефективність маршрутизації в умовах порушення зв'язності. Менші значення цього показника свідчать про наявність коротких альтернативних маршрутів, що підвищує здатність мережі зберігати функціональність після атак або відмов. Зростання середньої довжини шляхів призводить до підвищення залежності мережі від проміжних вузлів, збільшення затримок та ускладнення відновлення маршрутизації, що негативно впливає на кіберстійкість ІС. Для неорієнтованого графа середня довжина шляхів визначається за формулою (6) [14]:

$$L = \frac{2}{k(k-1)} \sum_{i < j} d(i, j), \quad (6)$$

де $d(i, j)$ – довжина найкоротшого шляху між вузлами i та j ; k – кількість вузлів.

У таблиці 3 приводяться значення середньої довжини шляхів топології, що аналізуються.

Таблиця 3

Підсумкова таблиця критерію L

Топологія	Середня довжина шляхів L
<i>Tree</i>	2,89
<i>Ring</i>	2,78
<i>Dual Ring</i>	1,67
<i>Ring + Hub</i>	2,09
<i>Partial Mesh</i>	1,84

У таблиці 4 приведено всі показники для типів мереж, що аналізуються.

Таблиця 4

Зведена таблиця показників

Критерій Топологія	Робастність R	Структурна зв'язність λ_2	Вершинна зв'язність k	Централізація C	Середня довжина шляхів L
<i>Tree</i>	0,16	0,154	1	0,167	2,89
<i>Ring</i>	0,23	0,382	2	0	2,78
<i>Dual Ring</i>	0,41	1,764	4	0	1,67
<i>Ring + Hub</i>	0,25	0,697	2	0,083	2,09
<i>Partial Mesh</i>	0,28	1,121	2	0,083	1,84

Аналіз показників обраних критеріїв показує, що окремі топологічні критерії частково корелюють між собою, однак не є взаємозамінними. Зокрема, алгебраїчна зв'язність відображає спектральну стійкість графа, робастність – поведінку мережі при цільових атаках, централізація – наявність структурно домінуючих вузлів, середня довжина шляхів – компактність маршрутизації. Таким чином, обрані критерії (робастність, алгебраїчна зв'язність, вершинна зв'язність, централізація та середня довжина шляхів) забезпечують достатньо повне та об'єктивне оцінювання кіберстійкості.

Сформована система критеріїв дозволяє кількісно оцінити кіберстійкість розглянутих топологій, однак для отримання інтегральної оцінки та врахування відносної важливості кожного критерію необхідно застосувати метод багатокритеріального аналізу. З цією метою побудуємо ієрархічну модель задачі на основі методу аналізу ієрархій, яка забезпечує визначення ваг критеріїв і пріоритетів альтернатив.

Задачу оцінювання кіберстійкості можна подати у вигляді трирівневої ієрархії:

мета – вибір топології, яка структурно забезпечує найбільшу кіберстійкість за вибраними критеріями;

критерії – показники кіберстійкості (робастність, зв'язність, централізація тощо);

альтернативи – розглянуті топології мережі (*Tree*, *Ring*, *Dual Ring*, *Ring + Hub*, *Partial Mesh*).

Побудована ієрархія забезпечує основу для подальших парних порівнянь, визначення ваг критеріїв і локальних пріоритетів альтернатив.

Визначення відносної важливості критеріїв оцінювання кіберстійкості здійснюється із застосуванням методу парних порівнянь у межах методу аналізу ієрархій [2]. Такий підхід дозволяє формалізувати судження щодо пріоритетності критеріїв та врахувати їх неоднорідну природу.

При формуванні матриці парних порівнянь були враховані такі положення: критерії, що характеризують здатність мережі зберігати зв'язність (робастність, алгебраїчна зв'язність), як

правило, мають вищий пріоритет; критерії, що відображають вразливість структури (централізація), оцінюються з урахуванням ризику компрометації критичних вузлів; критерії ефективності (середня довжина шляхів) мають допоміжний характер і, як правило, поступаються за важливістю критеріям стійкості.

З урахуванням цих пріоритетів, матриця парних порівнянь критеріїв має наступний вигляд (табл. 5).

Таблиця 5

Матриця парних порівнянь обраних критеріїв

Критерій	R	λ_2	k	C_D	L
R	1	1,5	2	3	4
λ_2	2/3	1	1,5	2	3
k	1/2	2/3	1	1,5	2
C_D	1/3	1/2	2/3	1	1,5
L	1/4	1/3	1/2	2/3	1

Провівши відповідні дії методу аналізу ієрархій (нормалізація, виділення середніх значень, перевірка коефіцієнту узгодженості CR), отримаємо вектор ваг критеріїв:

$$W = \{R = 0,361, \lambda_2 = 0,253, k = 0,177, C_D = 0,123, L = 0,086\}.$$

Розрахований коефіцієнт узгодженості $CR = 0,00068$.

Отриманий розподіл ваг підтверджує, що при оцінюванні кіберстійкості ІС ключовими є показники, що характеризують здатність мережі зберігати зв'язність та функціональність в умовах деструктивних впливів.

Для кожної топології визначаються значення показників за обраними критеріями, на основі яких формуються локальні пріоритети альтернатив. Оцінювання здійснюється шляхом побудови матриць парних порівнянь для кожного критерію (табл. 6–10).

Таблиця 6

Матриця парних порівнянь топології за критерієм робастність

R	<i>Tree</i>	<i>Ring</i>	<i>Dual Ring</i>	<i>Ring + Hub</i>	<i>Partial Mesh</i>
<i>Tree</i>	1	2/3	1/5	1/2	1/3
<i>Ring</i>	3/2	1	1/4	2/3	1/2
<i>Dual Ring</i>	5	4	1	3	3
<i>Ring + Hub</i>	2	3/2	1/3	1	1
<i>Partial Mesh</i>	3	2	1/3	1	1
Коефіцієнт узгодженості CR			0,01		

Таблиця 7

Матриця парних порівнянь топології за критерієм алгебраїчна зв'язність

λ_2	<i>Tree</i>	<i>Ring</i>	<i>Dual Ring</i>	<i>Ring + Hub</i>	<i>Partial Mesh</i>
<i>Tree</i>	1	1/2	1/9	1/5	1/7
<i>Ring</i>	2	1	1/7	1/3	1/5
<i>Dual Ring</i>	9	7	1	6	3
<i>Ring + Hub</i>	5	3	1/6	1	1/3
<i>Partial Mesh</i>	7	5	1/3	3	1
Коефіцієнт узгодженості CR			0,06		

Таблиця 8

Матриця парних порівнянь топології за критерієм вершинна зв'язність

k	<i>Tree</i>	<i>Ring</i>	<i>Dual Ring</i>	<i>Ring + Hub</i>	<i>Partial Mesh</i>
<i>Tree</i>	1	1/2	1/5	1/2	1/2
<i>Ring</i>	2	1	1/3	1	1
<i>Dual Ring</i>	5	3	1	3	3
<i>Ring + Hub</i>	2	1	1/3	1	1
<i>Partial Mesh</i>	2	1	1/3	1	1
Коефіцієнт узгодженості CR			0,001		

Таблиця 9

Матриця парних порівнянь топології за критерієм централізація

C_D	<i>Tree</i>	<i>Ring</i>	<i>Dual Ring</i>	<i>Ring + Hub</i>	<i>Partial Mesh</i>
<i>Tree</i>	1	1/4	1/4	1/2	1/2
<i>Ring</i>	4	1	1	2	2
<i>Dual Ring</i>	4	1	1	2	2
<i>Ring + Hub</i>	2	1/2	1/2	1	1
<i>Partial Mesh</i>	2	1/2	1/2	1	1
Коефіцієнт узгодженості CR			0,000		

Таблиця 10

Матриця парних порівнянь топології за критерієм середня довжина шляхів

L	<i>Tree</i>	<i>Ring</i>	<i>Dual Ring</i>	<i>Ring + Hub</i>	<i>Partial Mesh</i>
<i>Tree</i>	1	1/2	1/5	1/3	1/4
<i>Ring</i>	2	1	1/4	1/2	1/3
<i>Dual Ring</i>	5	4	1	3	2
<i>Ring + Hub</i>	3	2	1/3	1	1/2
<i>Partial Mesh</i>	4	3	1/2	2	1
Коефіцієнт узгодженості CR			0,020		

Зведена матриця локальних пріоритетів альтернатив приведена в таблиці 11.

Таблиця 11

Зведена матриця локальних пріоритетів альтернатив

Критерій Топологія	Робастність R	Структурна зв'язність λ_2	Вершинна зв'язність k	Централізація C	Середня довжина шляхів L
<i>Tree</i>	0,077	0,037	0,081	0,077	0,062
<i>Ring</i>	0,108	0,060	0,156	0,308	0,099
<i>Dual Ring</i>	0,462	0,516	0,451	0,308	0,416
<i>Ring + Hub</i>	0,163	0,130	0,156	0,154	0,161
<i>Partial Mesh</i>	0,190	0,257	0,156	0,154	0,262

Після визначення вагових коефіцієнтів критеріїв та локальних пріоритетів альтернатив за кожним критерієм здійснюється інтеграція отриманих результатів з метою формування узагальненої оцінки кіберстійкості. Інтегральна оцінка кожної альтернативи визначається як зважена сума локальних пріоритетів у матричній формі (1):

$$S = P \cdot W,$$

де $S = \{S_1, S_2, \dots, S_n\}$ – вектор глобальних пріоритетів альтернатив і $\sum_{i=1}^n S_i = 1$ має нормований характер.

У результаті агрегації локальних пріоритетів отримано вектор глобальних оцінок кіберстійкості топологій:

$$S = \{S_{Tree} = 0,066, S_{Ring} = 0,128, S_{Dual Ring} = 0,451, S_{Ring + Hum} = 0,152, S_{Parth Mesh} = 0,203\}.$$

За отриманими значеннями глобальних пріоритетів топології впорядковуються наступним чином:

$$Dual Ring \succ Parth Mesh \succ Ring + Hub \succ Ring \succ Tree.$$

Результати оцінювання кіберстійкості топологій наведено на рисунку 2.

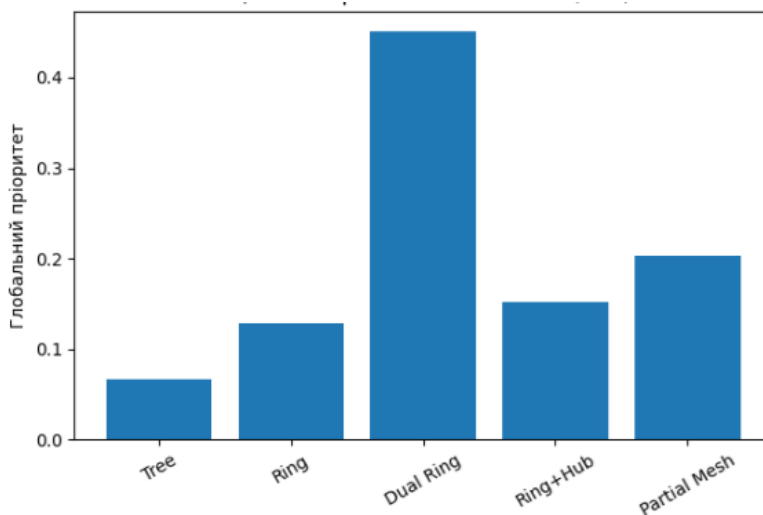


Рис. 2. Оцінка кіберстійкості топологій АНР

Як видно з графіка, топологія *Dual Ring* має суттєво вищий інтегральний показник (0,451) порівняно з іншими альтернативами, що підтверджує її перевагу за сукупністю критеріїв. Другу позицію займає *Partial Mesh* (0,203), тоді як топології *Ring + Hub* (0,152) та *Ring* (0,128) демонструють середні значення. Найнижчий рівень кіберстійкості характерний для *Tree* (0,066).

Отримані результати підтверджують, що топології з високим рівнем структурної надмірності та зв'язності забезпечують кращу кіберстійкість ІС. Найбільш доцільною для використання в умовах деструктивних впливів є топологія *Dual Ring*, яка забезпечує максимальну живучість мережі при збереженні прийнятної ефективності функціонування.

Висновки. У статті розроблено математичну модель оцінювання кіберстійкості ІС залежно від топології їхньої побудови на основі методу аналізу ієрархій. Сформовано множину альтернатив та обґрунтовано систему критеріїв, що відображають структурні властивості мережі.

Отримані вагові коефіцієнти підтвердили домінування показників структурної стійкості. За результатами розрахунків встановлено, що найбільш кіберстійкою є топологія *Dual Ring* (0,451), тоді як найменш стійкою – *Tree* (0,066).

Показано, що топологія мережі має визначальний вплив на рівень кіберстійкості, а застосування АНР забезпечує обґрунтоване ранжування альтернатив. Запропонований підхід дозволяє формалізувати процес вибору оптимальної мережевої структури в умовах багатокритеріальності та невизначеності.

Перспективним напрямком наукових досліджень є розширення моделі за рахунок використання нечітких ФАНР, нейтрософських підходів та методу аналітичного мережевого процесу АНР, які дозволяють враховувати невизначеність і суперечливість експертних оцінок, а також взаємозалежності між критеріями оцінювання, що підвищує адекватність і точність моделі при аналізі кіберстійкості інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ross R., McEvilly M., Oren J. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Vol. 2 Rev. 1. Gaithersburg : National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.SP.800-160v2r1.
2. Saaty T. L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill International Book Company, 1980. 287 p. ISBN 9780070543713.
3. Jamakovic A., Van Mieghem P. On the Robustness of Complex Networks by Using the Algebraic Connectivity // NETWORKING 2008. Lecture Notes in Computer Science. Berlin; Heidelberg: Springer, 2008. Vol. 4982. P. 183–194. DOI: 10.1007/978-3-540-79549-0_16.
4. Jamakovic A., Uhlig S. On the Relationship Between the Algebraic Connectivity and Graph's Robustness to Node and Link Failures // Proceedings of the 3rd EuroNGI Conference on Next Generation Internet Networks. 2007. P. 96–102.
5. Alenazi M. J. F., Sterbenz J. P. G. Comprehensive Comparison and Accuracy of Graph Metrics in Predicting Network Resilience // 11th International Conference on the Design of Reliable Communication Networks (DRCN). Kansas City, 2015. DOI: 10.1109/DRCN.2015.7149007.
6. Liu J., Zhou M., Wang S., Liu P. A Comparative Study of Network Robustness Measures // Frontiers of Computer Science. 2017. Vol. 11, No. 4. P. 568–584. DOI: 10.1007/s11704-016-6108-z.
7. Meng F., Fu G., Farmani R., Sweetapple C., Butler D. Topological Attributes of Network Resilience: A Study in Water Distribution Systems // Water Research. 2018. Vol. 143. P. 376–386. DOI: 10.1016/j.watres.2018.06.048.
8. Yi J., Qin Z., Yang K., Zhao H., Han Q. AHP-Based Network Security Situation Assessment for Industrial Internet of Things // Electronics. 2023. Vol. 12, No. 16. Art. 3458. DOI: 10.3390/electronics12163458.
9. Diestel R. Graph Theory. 5th ed. Berlin: Springer, 2017. 428 p.
10. Schneider C. M., Moreira A. A., Andrade J. S., Havlin S., Herrmann H. J. Mitigation of malicious attacks on networks // PNAS. 2011.
11. Fiedler M. Algebraic connectivity of graphs // Czechoslovak Mathematical Journal. 1973. Vol. 23, № 2. P. 298–305.
12. Chung F. R. K. Spectral graph theory. Providence: American Mathematical Society, 1997. 212 p.
13. Freeman L. C. Centrality in social networks: conceptual clarification // Social Networks. 1979. Vol. 1. P. 215–239.
14. Diestel R. Graph Theory. 5th ed. Berlin: Springer, 2017. 428 p.

Надійшла до редколегії 30.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.032.26

канд. техн. наук Гудима В. П. ORCID: 0000-0003-4722-0601 (НУОУ)
д-р філософії Яровий В. С. ORCID: 0000-0002-8239-1150 (ВІТІ ім. Героїв Крут)
Островський А. О. ORCID: 0009-0004-9046-581X (НУОУ)
Андрієнко О. В. ORCID: 0009-0002-5488-1432 (ВІТІ ім. Героїв Крут)

МЕТОД КОМБІНОВАНОГО ВИКОРИСТАННЯ МЕТОДИК АВС- ТА XYZ-АНАЛІЗІВ ДЛЯ ОПТИМІЗАЦІЇ ОРГАНІЗАЦІЇ МЕТРОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

У статті досліджено доцільність впровадження методик АВС- та XYZ-аналізів в систему метрологічного забезпечення Збройних Сил України з урахуванням сучасних умов бойових дій і досвіду інтеграції стандартів НАТО як інструментів оптимізації управлінських рішень, підвищення ефективності ресурсного забезпечення та підтримання належного технічного стану засобів вимірювальної техніки.

Основні результати дослідження:

Проаналізовано чинну нормативно-правову базу, визначено, що існуюча система має потенціал до цифровізації та функціонального вдосконалення.

Розроблено адаптовану методичку АВС-аналізу, що базується на багатофакторній оцінці вартості, точності, частоти використання і критичності засобів вимірювальної техніки. Запропоновано формулу для визначення інтегрального коефіцієнта важливості.

Описано застосування XYZ-аналізу в умовах Збройних Сил України як методики прогнозування попиту та стабільності використання засобів вимірювальної техніки на основі коефіцієнта варіації. Запропоновано алгоритм класифікації засобів вимірювальної техніки за стабільністю.

Інтегровано АВС- та XYZ-методики у комбіновану матрицю управління, що дозволяє формувати обґрунтовані рішення щодо пріоритетів калібрування, ремонту, виробництва (закупівлі) та списання засобів вимірювальної техніки.

Надано практичні рекомендації щодо впровадження методу комбінованого використання методик АВС- та XYZ-аналізів, які включають алгоритм впровадження, використання інформаційних систем та очікувані вигоди — як організаційні, так і економічні та тактичні.

Ключові слова: метрологічне забезпечення, засоби вимірювальної техніки, метрологічні лабораторії, обслуговування.

V. Hudyma, V. Yarovyi, A. Ostrovskyi, O. Andriienko. A method for the combined use of ABC and XYZ analysis techniques to optimise the organisation of metrological support for the Armed Forces of Ukraine

This article examines the feasibility of introducing ABC and XYZ analysis methods into the metrological support system of the Armed Forces of Ukraine, taking into account current combat conditions and experience in integrating NATO standards as tools for optimising management decisions, improving the efficiency of resource provision, and maintaining the proper technical condition of measuring equipment.

Main findings of the study:

The current regulatory framework has been analysed, and it has been determined that the existing system has the potential for digitalisation and functional improvement.

An adapted ABC analysis methodology has been developed, based on a multi-factor assessment of the cost, accuracy, frequency of use and criticality of measuring instruments. A formula for determining the integral importance coefficient has been proposed.

The application of XYZ analysis within the Armed Forces of Ukraine has been described as a method for forecasting demand and the stability of use of measuring instruments based on the coefficient of variation. An algorithm for classifying measuring instruments by stability has been proposed.

The ABC and XYZ methodologies have been integrated into a combined management matrix, which enables the formulation of well-founded decisions regarding priorities for the calibration, repair, production (procurement) and decommissioning of measuring instruments.

Practical recommendations are provided for the implementation of the method combining ABC and XYZ analysis techniques, which include an implementation algorithm, the use of information systems, and the expected benefits – both organisational and economic.

Keywords: metrological support, measuring equipment, metrological laboratories, maintenance.

Постановка завдання. У статті як основний об'єкт дослідження розглядаються методики адаптації ABC- та XYZ-аналізів [9] до умов метрологічного забезпечення Збройних Сил України (ЗСУ).

Метрологічне забезпечення є критично важливою складовою підтримки технічної справності озброєння та військової техніки ЗСУ, особливо в умовах сучасної війни це є завданням стратегічного рівня, покладеним на спеціалізовані структури Міністерства оборони України [1].

З огляду на виклики сучасної війни та потреби цифровізації виникає необхідність модернізації підходів до управління ресурсами метрологічного забезпечення. Одним із найбільш ефективних підходів у цій сфері є застосування ABC- та XYZ-аналізів, які вже давно довели свою ефективність у системах логістики, стандартизації та управління запасами в арміях країн НАТО.

Предметом дослідження в статті виступають покрокові методики ABC- та XYZ-аналізів для впровадження в систему метрологічного забезпечення ЗСУ з урахуванням сучасних умов бойових дій і досвіду інтеграції стандартів НАТО як інструментів оптимізації управлінських рішень, підвищення ефективності ресурсного забезпечення та підтримки належного технічного стану засобів вимірювальної техніки (ЗВТ) [1–3; 10].

Аналіз останніх публікацій. Аналізуючи сучасні джерела [7], стандарти та наукові публікації [6–8] щодо теоретико-методологічних основ ABC- та XYZ-аналізів, можна констатувати наступне.

ABC-аналіз бере свій початок з ідеї принципу Парето, який у 1896 році був сформульований італійським економістом Вільфредо Парето. Згідно з ним, приблизно 20 % об'єктів формують 80 % результату, що знайшло застосування в економіці, логістиці, ІТ і, зокрема, у військовому управлінні [13].

ABC-аналіз передбачає розподіл об'єктів на три категорії:

Категорія А – ресурси з найвищим впливом (близько 20 %), які забезпечують до 80 % ефекту (вартість, функціональність).

Категорія В – середньої важливості (близько 30 % об'єктів, що забезпечують ~15 % результату).

Категорія С – масові об'єкти з низькою індивідуальною цінністю (до 50 % позицій, що формують лише 5 % цінності).

У методиці ABC використовується Принцип Парето [12; 13].

Формально принцип реалізується через вираз (1):

$$P_i = \frac{V_i}{\sum_{j=1}^n V_j} \times 100\%, \quad (1)$$

де P_i – відсоток значущості (або пріоритету) i -го ресурсу, %; V_i – вартість або інша кількісна характеристика значущості i -го ресурсу; $\sum_{j=1}^n V_j$ – сума вартостей або значущостей усіх n ресурсів, які аналізуються в межах вибірки; n – загальна кількість ресурсів, що беруть участь в аналізі.

Ранжування за спаданням дозволяє сформувати графік Парето, що чітко відображає розподіл пріоритетів.

Визначення категорій на основі принципу Парето дає змогу автоматизувати рішення щодо замовлень, ремонту, калібрування, а також скорочення надлишкових запасів.

XYZ-аналіз як метод прогнозування.

XYZ-аналіз застосовується для оцінки стабільності споживання ресурсів:

X – рівномірний і передбачуваний попит;

Y – помірно коливальний;

Z – хаотичний та складно прогнозований.

Основою класифікації є коефіцієнт варіації – CV (2):

$$CV = \frac{\delta}{\mu} \cdot 100\%, \quad (2)$$

де δ – стандартне відхилення; μ – середнє значення.

Метою статті є дослідження адаптації методик АВС- та XYZ-аналізів до умов функціонування метрологічного забезпечення ЗСУ та обґрунтування практичних механізмів їх впровадження з урахуванням чинного законодавства та організаційної структури оборонного сектору.

Виклад основного матеріалу. Метрологічне забезпечення у ЗСУ ґрунтується на положеннях Закону України від 05.06.2014 № 1314-VII “Про метрологію та метрологічну діяльність” (зі змінами) [1], який регулює відносини, що виникають у процесі провадження метрологічної діяльності, постановою Кабінету Міністрів України від 23.12.2015 № 1152 “Про особливості метрологічного забезпечення діяльності у сфері оборони України” [2], а також галузевих наказів Міністерства оборони України.

Відповідно до ст. 15 Закону, забезпечення єдності вимірювань у сфері оборони України здійснюється з урахуванням особливостей, визначених Кабінетом Міністрів України.

Ключовими підзаконними актами є:

Постанова КМУ від 23.12.2015 № 1152 “Про особливості метрологічного забезпечення діяльності у сфері оборони України” [2] – визначає особливості метрологічного забезпечення діяльності у сфері оборони України.

Наказ МОУ від 24.05.2017 № 288 “Про затвердження Положення про метрологічну службу Міністерства оборони України та Збройних Сил України” [3] – визначає організаційну структуру, завдання, функції та порядок діяльності метрологічної служби, яка забезпечує єдність вимірювань у сфері оборони.

Наказ заступника Міністра оборони України з озброєння – начальника Озброєння Збройних Сил України від 01.06.2001 № 79 “Про затвердження Керівництва з організації та порядку експлуатації вимірювальної техніки у Збройних Силах України” [4] – регламентує:

- правила експлуатації вимірювальної техніки;
- вимоги до порядку метрологічного забезпечення військ (сил);
- роботу військових метрологічних лабораторій.

Ці нормативні документи забезпечують реалізацію повного життєвого циклу вимірювальної техніки: від планування виробництва – до її списання.

Сучасна редакція цих документів враховує зміни в законодавстві щодо цифровізації, посилення стандартів безпеки та впровадження процедур відповідно до практик НАТО.

Розглянемо організаційну структуру метрологічного забезпечення у ЗСУ. Організація метрологічного забезпечення у ЗСУ базується на трирівневій вертикалі управління, визначеній у Положенні про метрологічну службу у системі МОУ:

- 1) Стратегічний рівень:

метрологічна служба МОУ, яку представляє управління метрології та стандартизації Озброєння Командування Сил логістики ЗСУ – головна організація з метрологічного забезпечення діяльності у системі МОУ, координує роботу всієї системи;

регіональні метрологічні військові частини (РМВЧ) – головні організації з метрологічного забезпечення військових частин та установ (незалежно від їх підпорядкування) у закріпленому регіоні, виконують завдання відповідно до положень про військові частини;

служби метрології та стандартизації командувань видів ЗСУ, командування Десантно-штурмових військ, командування ССО, командування Сил територіальної оборони – здійснюють загальне керівництво та контроль за метрологічним забезпеченням підпорядкованих військових частин та установ і забезпечують умови функціонування відповідних служб метрології та стандартизації і військових метрологічних лабораторій.

2) Оперативний рівень:

служби метрології та стандартизації оперативних і повітряних командувань, командування військово-морських баз, армійських корпусів – здійснюють загальне керівництво та контроль за діяльністю з питань метрологічного забезпечення у підпорядкованих військових частин та установ і забезпечують умови функціонування відповідних служб метрології та стандартизації і військових метрологічних лабораторій зі складу ремонтно-відновлювальних частин;

військові метрологічні лабораторії – підрозділи у складі ремонтно-відновлювальних частин, що проводять, відповідно до свідоцтва про уповноваження, калібрування, поточний ремонт військових засобів вимірювальної техніки (ВЗВТ) в стаціонарних умовах, або розгорнутому збірному пункті пошкоджених машин.

3) Тактичний рівень:

служби метрології та стандартизації (метрологи) військових частин та установ – здійснюють керівництво метрологічним забезпеченням військових частин та установ відповідно до своїх повноважень.

Особливість: за відсутності штатної служби метрології та стандартизації наказом відповідного командира (начальника) призначаються особи, відповідальні за забезпечення єдності вимірювань (метрологи), як правило – офіцери зі складу технічних служб із вищою технічною освітою;

військові калібрувальні лабораторії (ВКЛ) – підрозділи у складі ремонтно-відновлювального батальйону військової частин, що проводять, відповідно до свідоцтва про уповноваження, калібрування ВЗВТ на розгорнутому збірному пункті пошкоджених машин.

Характеристики основних видів метрологічного обладнання у ЗСУ.

Згідно з Керівництвом з організації та порядку експлуатації вимірювальної техніки у Збройних Силах України, усі засоби вимірювальної техніки класифікуються за кількома ознаками.

За призначенням:

вихідні еталони – зберігаються в Метрологічному центрі військових еталонів Збройних Сил України, забезпечують відтворення одиниць вимірювання;

робочі еталони – використовуються для перевірки та калібрування засобів вимірювання нижчого рівня.

За сферою застосування:

загальновійськові ЗВТ – універсальні, використовуються в усіх родах військ;

спеціальні ЗВТ – призначені для обслуговування конкретних зразків ОВТ (наприклад, авіаційні, артилерійські, РЕБ).

За технічними характеристиками:

аналогові й цифрові, ручні й автоматизовані, стаціонарні й пересувні (у тому числі пересувні лабораторії вимірювальної техніки (ПЛВТ)).

Розглянемо методику адаптації АВС-аналізу для метрологічного забезпечення ЗСУ. Перш ніж розпочати, необхідно розглянути критерії класифікації ЗВТ.

Для успішної адаптації методики АВС-аналізу до системи метрологічного забезпечення ЗСУ, перш за все, необхідно визначити релевантні критерії важливості ЗВТ. На основі аналізу положень нормативної бази з питань метрологічної діяльності у ЗСУ, а також стандартних логістичних підходів у країнах НАТО, обґрунтовуються такі основні параметри, як:

вартість одиниці ЗВТ, тому що високовартісне обладнання автоматично потребує більшої уваги щодо обслуговування та обліку;

точність і клас вимірювань, бо чим вищий клас точності, тим критичніше забезпечити відповідність характеристик ЗВТ нормативам;

частота використання (навантаження), яка визначається на основі обліку використання в системі експлуатації техніки (наприклад, за кількістю замірів або викликів на калібрування);

критичність для бойової готовності, для прикладу – ЗВТ, що застосовуються у перевірці САУ, ППО або ракетних комплексів, мають пріоритет.

Рекомендовано [13] формувати комбінований коефіцієнт вагомості W (3):

$$W = \alpha \cdot C + \beta \cdot P + \gamma \cdot F + \delta \cdot K \quad (3)$$

де C – вартість; P – точність; F – частота використання; K – критичність для боєготовності; $\alpha, \beta, \gamma, \delta$ – вагові коефіцієнти (визначаються експертно).

Покрокова методика проведення ABC-аналізу.

КРОК 1. Формування бази ЗВТ, що включає в себе збір даних про всі одиниці ЗВТ (тип, інвентарний номер, частота обслуговування, вартість тощо) та створення електронної таблиці або інтеграції з інформаційною системою.

КРОК 2. Розрахунок інтегрального показника вагомості – W , що розраховується за формулою (3) та стандартизація даних для забезпечення порівнянності.

КРОК 3. Ранжування ЗВТ, що передбачає упорядкування списку ЗВТ за спаданням значення W та побудову кривої Парето.

КРОК 4. Класифікація за категоріями:

категорія А – верхні 20 % ресурсів (максимальна важливість);

категорія В – наступні 30 %;

категорія С – залишкові 50 %.

КРОК 5. Прийняття управлінських рішень:

категорія А – постійний контроль, пріоритетне калібрування, резервні одиниці;

категорія В – планове обслуговування;

категорія С – перевірка за потреби або скорочення на зберігання.

Умовний приклад застосування ABC-аналізу наведений у таблиці 1.

Таблиця 1

Умовний приклад застосування ABC-аналізу

№ з/п	Найменування ЗВТ	Вартість (тис. грн)	Частота використання (раз/міс.)	Точність (клас)	Критичність	W	Категорія
1	Калібратор електричний КЕ-10	650	60	0,01	Висока	0,91	А
2	Мультиметр цифровий DT-6800	3	200	0,1	Середня	0,55	В
3	Манометр військовий М-1	1	20	0,5	Низька	0,22	С

У наведеному прикладі застосовані вагові коефіцієнти: вартість (0,4), точність (0,2), частота (0,2), критичність (0,2).

Це дозволить інтегрувати об'єктивні та експертні фактори у класифікацію та матиме практичне значення для ЗСУ, а саме:

дозволить виявити та зосередити ресурси на пріоритетному ЗВТ;

може мінімізувати простої бойової техніки через недоступність або зношеність ЗВТ;

може посприяти оптимізації витрат на обслуговування та закупівлю ЗВТ.

Далі розглянемо методику XYZ-аналізу для адаптації до умов метрологічного забезпечення ЗСУ. Спочатку проаналізуємо критерії для визначення стабільності попиту на ЗВТ.

XYZ-аналіз базується на статистичній оцінці варіативності попиту на кожну одиницю ЗВТ. Основним критерієм є коефіцієнт варіації – CV є відношення стандартного відхилення до середнього значення попиту за формулою (2), звідки випливають категорії:

X ($CV \leq 10\%$) – стабільний попит, висока передбачуваність;

Y ($10\% < CV \leq 25\%$) – помірно варіативний попит;

Z ($CV > 25\%$) – нестабільний, випадковий попит.

У ЗСУ ці показники можна брати з журналів обліку повірочних (калібрувальних) робіт, звітів військових метрологічних лабораторій, баз даних.

Покрокова методика XYZ-аналізу.

КРОК 1. Збір даних, коли за кожним типом ЗВТ збираються дані про обсяги використання/калібрування за 12 місяців.

КРОК 2. Розрахунок середнього значення попиту – (μ) згідно з виразом (4) [13]:

$$\mu = \frac{1}{n} \sum_{i=1}^n x_i. \quad (4)$$

КРОК 3. Обчислення стандартного відхилення – (σ) згідно з виразом (5) [13]:

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \mu)^2}. \quad (5)$$

КРОК 4. Розрахунок CV за формулою (2).

КРОК 5. Класифікація:

X – для прогнозованих ЗВТ → формуються стабільні запаси;

Y – потребують моніторингу попиту;

Z – обслуговуються на замовлення або за запитом.

Умовний приклад застосування XYZ-аналізу для ЗВТ наведений у таблиці 2.

Таблиця 2

Застосування XYZ-аналізу для ЗВТ

Назва ЗВТ	Попит по місяцях (шт.)	$V(\%)$	Категорія
Калібратор KE-10	11, 10, 12, 10, 11, 11, 10, 11, 12	5,1	X
Мультиметр DT-6800	6, 8, 5, 7, 9, 6, 10, 6, 5	21,3	Y
Спектроаналізатор SA-2	1, 0, 3, 0, 2, 0, 1, 0, 0	41,2	Z

Підсумовуючи, можемо з таблиці зробити висновки:

ЗВТ категорії X можуть замовлятися централізовано та зберігатися у підрозділах;

ЗВТ категорії Y вимагають системного контролю коливань;

ЗВТ категорії Z не доцільно зберігати у великій кількості – їх краще замовляти під конкретні завдання.

Розглянута методика має практичне значення для ЗСУ, а саме:

дасть змогу оптимізувати склади та обмінний фонд у військових частинах;

підвищить прогнозованість навантаження на метрологічні лабораторії;

дасть можливість уникати надлишкових закупівель ЗВТ, що не використовуються або використовуються епізодично;

дасть підґрунтя для бюджетного планування.

Далі інтегруємо вищезазначені методики в єдиний метод. Сформуємо матрицю ABC–XYZ. ABC- та XYZ-аналізи мають різні функції: перший оцінює економічну/функціональну важливість, другий – стабільність попиту. Їх об'єднання в єдину матрицю дозволяє:

- пріоритезувати обслуговування ЗВТ;
 - планувати логістику;
 - оптимізувати бюджети;
 - ухвалювати рішення щодо виробництва (закупівель), зберігання та ремонту.
- Отримаємо комбіновану матрицю ABC–XYZ в таблиці 3.

Таблиця 3

Комбінована матриця ABC–XYZ

	X (стабільний)	Y (середньо стабільний)	Z (нестабільний)
A	AX – критичні, постійні	AY – критичні, але змінні	AZ – критичні, але рідко потрібні
B	BX – середньої важливості, стабільні	BY – середні, змінні	BZ – другорядні, нестабільні
C	CX – неважливі, але передбачувані	CY – неважливі, змінні	CZ – неважливі, нестабільні

Значення комірок:

AX – найвищий пріоритет: дорогоцінні й постійно потрібні → тримати в підрозділах, контролювати калібрування;

CZ – найнижчий пріоритет: можуть бути списані, утилізовані або передані до резерву;

AY, **AZ**, **BY** – вимагають індивідуального підходу, часто включають спеціальну або мобільну ЗВТ [13].

Сформуємо покроковий алгоритм прийняття рішень:

КРОК 1. Класифікація ЗВТ методами ABC та XYZ окремо (використовуючи алгоритми покрокової методики проведення ABC- та XYZ-аналізу).

КРОК 2. Комбінування у загальну матрицю. Кожен об'єкт ЗВТ отримує подвійну класифікацію – наприклад, **AY**, **BZ**, **CX** тощо.

КРОК 3. Формування управлінських дій за категоріями з рекомендаціями:

AX – завжди в наявності, дублювання, своєчасне калібрування;

AY – поглиблений моніторинг, календарне обслуговування;

AZ – за потребою, тримати на складі РМВЧ;

BX/BY – планове калібрування, за необхідності – виведення з обігу;

BZ/CZ – мінімізація запасів, передача в резерв або списання;

CX – для навчальних підрозділів, запасних комплектів.

Далі в таблиці 4 розглянемо приклад комбінованого аналізу ЗВТ у підрозділі ЗСУ.

Таблиця 4

Комбінований аналіз ЗВТ у підрозділі ЗСУ

№ з/п	Назва ЗВТ	Категорія ABC	Категорія XYZ	Категорія	Рішення
1	KE-10	A	X	AX	Постійна наявність, регулярне обслуговування
2	DT-6800	B	Y	BY	Плановий контроль, можлива заміна
3	SA-2	C	Z	CZ	Перевести в резерв

Така матриця дозволяє швидко виявляти пріоритети обслуговування, розподіляти бюджети, мінімізувати надлишки та має практичне значення для ЗСУ, а саме:

спрощення ухвалення рішень на всіх рівнях – від командира військової частини до МОУ; забезпечення динамічного підходу до обслуговування ЗВТ, орієнтованого на фактичні потреби;

усунення надмірної уніфікації обслуговування, яка була притаманна радянській системі; легка адаптація під автоматизовані інформаційні системи.

Проведені дослідження зазначених вище методик дозволить сформулювати практичні рекомендації щодо впровадження комбінованого аналізу ABC–XYZ у ЗСУ. Розділемо їх на складові:

1. Організаційні етапи впровадження.

Впровадження комбінованого методу потребує поетапного підходу:

Етап 1. Проведення аудиту наявних ЗВТ:

ідентифікація, облік, перевірка паспортів і калібрувального статусу; виявлення дублюючих, застарілих або неробочих одиниць.

Етап 2. Формування бази даних ЗВТ:

єдина електронна таблиця або інтеграція у наявні (перспективні) автоматизовані системи обліку;

поля: найменування, інвентарний номер, ціна, критичність, частота використання.

Етап 3. Навчання персоналу:

організація курсів/інструктажів щодо принципів ABC- та XYZ-аналізу; формування стандартних шаблонів і форм.

Етап 4. Проведення аналізу:

розрахунок W -коефіцієнтів (ABC) і CV (XYZ);

формування комбінованої матриці.

Етап 5. Впровадження управлінських рішень:

зміна регламентів обслуговування, складування та звітності по категоріях; оновлення технічної документації.

2. Використання автоматизованих інформаційних систем.

Сучасні ІТ-рішення значно спрощують реалізацію ABC–XYZ підходів (табл. 5).

Таблиця 5

Реалізація ABC–XYZ підходів

Система	Призначення
APM метролога (APM-M)	Облік ЗВТ, нагадування про калібрування
ERP M.I.S.	Автоматизоване управління технікою
Excel/LibreOffice Calc	Базовий рівень аналізу для ВМЛ і техчастин
BI-аналітика (Power BI, QlikView)	Візуалізація даних, криві Парето, матриці ABC–XYZ

Також можливе створення кастомізованого модуля у складі єдиної інформаційної системи забезпечення ЗСУ.

3. Очікувані вигоди від впровадження.

Організаційні вигоди:

стандартизація обліку ЗВТ на всіх рівнях;

оптимізація завантаження військових метрологічних лабораторій;

пріоритезація обслуговування дійсно важливих ЗВТ.

Економічні вигоди:

можливе зменшення витрат на виробництво (закупівлю), зберігання та обслуговування непотрібної техніки;

скорочення витрат на повторні калібрування та транспортування ЗВТ.

Оперативно-тактичні вигоди:

зменшення відмов через невчасне обслуговування;

підвищення бойової готовності підрозділів;

можливість мобільного планування обслуговування відповідно до бойових завдань.

Таким чином, впровадження методу комбінованого використання АВС- та XYZ-аналізів не лише узгоджується з нормативно-правовою базою, а й дозволяє підвищити ефективність усієї системи метрологічного забезпечення ЗСУ в умовах сучасної війни.

Висновок. У статті обґрунтовано доцільність впровадження методу комбінованого використання АВС- та XYZ-аналізів в систему метрологічного забезпечення ЗСУ з урахуванням сучасних умов бойових дій і досвіду інтеграції стандартів НАТО як інструментів оптимізації управлінських рішень, підвищення ефективності ресурсного забезпечення та підтримання належного технічного стану ЗВТ.

Основні результати дослідження:

Проаналізовано чинну нормативно-правову базу, визначено, що існуюча система має потенціал до цифровізації та функціонального вдосконалення.

Розроблено адаптовану методику АВС-аналізу, що базується на багатофакторній оцінці вартості, точності, частоти використання і критичності ЗВТ. Запропоновано формулу для визначення інтегрального коефіцієнта важливості.

Описано застосування XYZ-аналізу в умовах ЗСУ як методу прогнозування попиту та стабільності використання ЗВТ на основі коефіцієнта варіації.

Інтегровано методики АВС- та XYZ-аналізів у комбіновану матрицю управління, що дозволяє формувати обґрунтовані рішення щодо пріоритетів калібрування, ремонту, виробництва (закупівлі) та списання ЗВТ.

Надано практичні рекомендації щодо впровадження, які включають алгоритм впровадження, використання інформаційних систем та очікувані вигоди – як організаційні, так і економічні та тактичні.

Запропонований метод є гнучким, масштабованим і сумісним з цифровими платформами, а отже – придатним до реалізації як на рівні окремих військових частин, так і в масштабах ЗСУ загалом.

Перспективи подальших досліджень полягають у створенні спеціалізованого модуля АВС–XYZ аналізу в складі єдиної інформаційно-аналітичної системи технічного забезпечення ЗСУ, а також у розробленні методик багатокритеріального аналізу з урахуванням бойових умов, та дослідження економічної вигоди від застосування зазначеного модуля в кількісному (вартісному) відношенні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про метрологію та метрологічну діяльність: Закон України від 05.06.2014 № 1314-VII // Відомості Верховної Ради України. 2003. № 27. С. 190.
2. Про особливості метрологічного забезпечення діяльності у сфері оборони України: Постанова КМУ від 23.12.2015 № 1152 // Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1152-2015-%D0%BF>.
3. Про затвердження Положення про метрологічну службу Міністерства оборони України та Збройних Сил України: наказ МОУ від 24.05.2017 № 288 // Міністерство оборони України. URL: <https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-ministerstva-oboroni-ukraini-n-288-vid-24-05-2017-pro-zatverdzhennia-polozhennia-pro-metrologichnu-sluzhbu-ministerstva-oboroni-ukraini-ta-zbroinikh-sil-ukraini>.
4. Про затвердження Керівництва з організації та порядку експлуатації вимірювальної техніки у Збройних Силах України: наказ заступника Міністра оборони України з озброєння – начальника Озброєння Збройних Сил України від 01.06.2001 № 79.

5. ДСТУ EN ISO/IEC 17025:2019 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій. / Держстандарт України, 2019.
5. ISO/IEC 25023:2016 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality // ISO, 2016.
6. ISO/IEC 15939:2017 Systems and software engineering — Measurement process // ISO, 2017.
7. IEEE Std 1061-1998 IEEE Standard for a Software Quality Metrics Methodology // IEEE, 1998.
8. Тарасова В. В., Малиновський А. С., Рибак М. Ф. Метрологія, стандартизація і сертифікація: підруч. / За заг. ред. В. В. Тарасової. К.: Центр навчальної літератури, 2006. 264 с.
9. Коренець Ю. М. Стандартизація, сертифікація і метрологія [Текст]: навч. посіб. Кривий Ріг: [ДонНУЕТ], 2023. 90 с.
10. Метрологія, стандартизація, сертифікація та управління якістю в системах зв'язку / Л. В. Коломієць, П. П. Воробієнко, М. Т. Козаченко, М. Б. Налісний, В. Л. Серебрін, Л. О. Козаченко, О. В. Грабовський, Л. О. Лебединська. Одеса: ТОВ "БМВ", 2009. 376 с.
11. Fenton N., Pfleeger S. L. Software Metrics: A Rigorous and Practical Approach / N. Fenton, S. L. Pfleeger. Boca Raton: CRC Press, 1998.
12. Kan S. H. Metrics and Models in Software Quality Engineering / S. H. Kan. Boston: Addison-Wesley, 2002.

Надійшла до редколегії 12.02.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.9:355.4

канд. техн. наук, доцент Данилюк І. А. ORCID: 0000-0003-0955-0108 (ВІТІ ім. Героїв Крут)
канд. техн. наук Мочалюк В. В. ORCID: 0009-0002-8389-7986 (ВІТІ ім. Героїв Крут)

РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОБРОБКИ НЕСТРУКТУРОВАНОЇ ТЕКСТОВОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ОБОРОННОГО ПРИЗНАЧЕННЯ

У статті проведено комплексний аналіз сучасних методів обробки неструктурованої текстової інформації, зокрема: лінгвістичних, статистичних, векторних моделей представлення тексту, машинного навчання та глибокого навчання, послідовного аналізу, і визначено їхні переваги й обмеження в умовах функціонування інформаційно-аналітичних систем оборонного призначення. Показано, що в умовах зростання обсягів інформаційних потоків і необхідності їх обробки у реальному масштабі часу більшість традиційних підходів характеризуються значними вимогами до обчислювальних ресурсів та затримками прийняття рішень, що зумовлено необхідністю повного аналізу неструктурованої текстової інформації. Встановлено, що існуючі методи не забезпечують належного балансу між точністю класифікації та швидкістю обробки на етапі первинної обробки та забезпеченням спроможності до подальшого глибинного аналізу на подальших етапах, що є критичним для систем підтримки прийняття рішень у військовій сфері.

Запропоновано методику, яка базується на гібридному підході і забезпечує підвищення ефективності обробки текстових даних завдяки використанню багатоальтернативних послідовних вирішальних правил на етапі первинної обробки і трансформерних моделей для подальшого глибинного аналізу, що передбачає можливість раннього прийняття рішень на попередньому етапі та на неповній вибірці. Такий підхід дозволяє скорочувати обсяг оброблюваних даних та зменшувати час аналізу без суттєвого зниження достовірності результатів. На відміну від класичних методів класифікації, запропоноване рішення забезпечує гнучке управління процесом обробки неструктурованої вхідної текстової інформації.

Запропоновано застосування сховищ типу Data Lake для інтеграції різнорідних джерел інформації та забезпечення масштабованості системи.

Обґрунтовано, що впровадження запропонованої методики дозволяє підвищити оперативність обробки текстової інформації, знизити обчислювальні витрати та забезпечити необхідний рівень точності класифікації в умовах невизначеності та інформаційного перевантаження. Отримані результати можуть бути використані при створенні та модернізації інформаційно-аналітичних систем оборонного призначення, а також при інтеграції з існуючими платформами обробки даних у рамках сучасних військових стандартів.

Ключові слова: неструктуровані дані, обробка тексту, класифікація, послідовний аналіз, інформаційні системи, оборонні системи, машинне навчання.

I. Danyliuk, V. Mochaliuk. Development of a methodology for increasing the efficiency of processing unstructured text information in defense information, information and communication systems

The article provides a comprehensive analysis of modern methods for processing unstructured text information, including: linguistic, statistical, vector models of text representation, machine learning and deep learning, sequential analysis, and identifies their advantages and limitations in the conditions of functioning of information and analytical systems for defense purposes. It is shown that in the conditions of increasing volumes of information flows and the need for their processing in real time, most traditional approaches are characterized by significant requirements for computing resources and delays in decision-making, which is due to the need for a complete analysis of unstructured text information. It is established that existing methods do not provide a proper balance between classification accuracy and processing speed at the stage of primary processing and ensuring the ability to further in-depth analysis at subsequent stages, which is critical for decision-making support systems in the military sphere.

A method based on a hybrid approach is proposed that provides increased efficiency in text data processing through the use of multi-alternative sequential decision rules at the initial processing stage and transformer models for subsequent in-depth analysis, which provides the possibility of early decision-making at the preliminary stage and on an incomplete sample. This approach allows you to reduce the amount of processed data and reduce the analysis time without significantly reducing the reliability of the results. Unlike classical classification methods, the proposed solution provides flexible management of the process of processing unstructured input text information.

The use of Data Lake type storages is proposed to integrate heterogeneous information sources and ensure system scalability.

It is substantiated that the implementation of the proposed method allows you to increase the efficiency of text information processing, reduce computational costs and ensure the required level of classification accuracy in conditions of uncertainty and information overload. The results obtained can be used in the creation and modernization of

information and analytical systems for defense purposes, as well as in integration with existing data processing platforms within the framework of modern military standards.

Keywords: *unstructured data, text processing, classification, sequential analysis, information systems, defense systems, machine learning.*

Вступ

Сучасні інформаційно-аналітичні системи оборонного призначення функціонують в умовах стрімкого зростання обсягів даних, значна частина яких має неструктурований характер. Основними джерелами такої інформації є відкриті інформаційні ресурси, включаючи мережу Інтернет, соціальні мережі, новинні платформи та спеціалізовані канали комунікації.

В умовах впровадження принципів взаємосумісності з країнами-членами НАТО, зокрема в рамках концепцій Federated Mission Networking (FMN), Intelligence, Surveillance and Reconnaissance (ISR) та Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), особливого значення набуває забезпечення швидкої первинної обробки інформації в режимі реального часу та подальший глибинний аналіз класифікованої інформації.

Проведений аналіз свідчить, що переважна частина інформаційних потоків представлена у вигляді неструктурованих та некласифікованих текстових даних. Більшість існуючих методів глибинного аналізу за допомогою трансформерних методів нейронних мереж великих мовних моделей (Large Language Model, LLM) передбачають необхідність врахування контексту, тобто визначення області знань (фокусу на темі) для прийняття коректного рішення, що у свою чергу потребує повної обробки тексту перед прийняттям рішення, це зумовлює значні обчислювальні витрати та часові затримки й ускладнює обробку інформаційних потоків із застосуванням традиційних підходів.

Постановка проблеми

Більшість сучасних методів обробки неструктурованої текстової інформації потребують значних обчислювальних ресурсів і передбачають повну обробку тексту перед прийняттям рішення, крім того такі методи потребують попередньо визначеної області знань неструктурованої текстової інформації (фокусу на темі) для уникнення фантомних (не коректних) висновків під час глибинного аналізу, що не дозволяє їх використовувати для швидкої первинної обробки інформації в режимі близькому до реального часу.

Таким чином, виникає науково-практична задача підвищення ефективності обробки неструктурованої текстової інформації завдяки створенню методики, на основі гібридного підходу з використанням швидких методів, які не потребують значних обчислювальних ресурсів для попередньої оперативної обробки різнорідних джерел неструктурованої текстової інформації у масштабі часу, близькому до реального з подальшим глибинним аналізом відібраних і класифікованих текстів за допомогою трансформерних методів нейронних мереж великих мовних моделей (LLM).

Аналіз останніх публікацій на тему дослідження дозволяє зазначити, що обробка неструктурованої текстової інформації є складною задачею, яка потребує застосування різних підходів залежно від обсягу даних, вимог до точності та обчислювальних ресурсів. Авторами статті були проаналізовані сучасні методи обробки неструктурованої текстової інформації, які можна умовно поділити на лінгвістичні, статистичні та методи машинного навчання.

Аналіз публікацій щодо лінгвістичних методів дозволяє зазначити, що лінгвістичні методи базуються на формальному аналізі природної мови та включають лексичний, морфологічний, синтаксичний і семантичний аналізи. Ці підходи широко застосовуються у задачах глибинного розуміння тексту та побудови знаннево-орієнтованих систем.

Зокрема, у роботі [13] запропоновано знаннєво-орієнтований підхід до аналізу природномовної інформації, який забезпечує формалізацію предметної області та підвищення точності інтерпретації текстових даних.

Водночас, лінгвістичні методи характеризуються високою складністю реалізації та значною залежністю від якості мовних ресурсів.

Аналіз публікацій щодо статистичних методів дозволяє зазначити, що статистичні методи базуються на ймовірнісних моделях та використовують частотні характеристики тексту. Одним із базових підходів є наївний байєсівський класифікатор, який застосовується для задач фільтрації текстових повідомлень.

У роботах [3; 4] розглянуто застосування байєсівських методів для задач фільтрації небажаної інформації, де показано їхню ефективність при обробці великих обсягів текстових даних.

Подальший розвиток статистичних методів представлений у роботі [5], де запропоновано ймовірнісну модель класифікації текстів, що враховує структуру документів.

Перевагами статистичних методів є їхня обчислювальна ефективність та простота реалізації, однак вони обмежені припущенням незалежності ознак та недостатнім урахуванням контексту.

Аналіз публікацій щодо векторних моделей представлення тексту дозволяє зазначити, що у векторній моделі подання документів текст представлено у вигляді вектора в багатовимірному просторі термів [6; 8].

Цей підхід широко використовується в задачах інформаційного пошуку та класифікації, зокрема при роботі з колекціями текстів, такими як Reuters-21578 [7].

Основним недоліком векторних моделей є втрата семантичного контексту та залежність від методів зважування термів.

Аналіз публікацій щодо методів машинного навчання та глибокого навчання дозволяє зазначити, що більшість сучасних підходів до обробки текстових даних базуються на використанні трансформерних моделей, які використовують механізми попереднього визначення тематики – самоуваги. У роботі [15] запропоновано архітектуру Transformer, яка забезпечує високу точність обробки і можливість глибокого аналізу.

Такі методи забезпечують можливість глибокого аналізу текстових даних, але разом потребують значних обчислювальних ресурсів і передбачають повну обробку тексту перед прийняттям рішення.

Аналіз публікацій щодо методів послідовного аналізу дозволяє зазначити, що послідовний аналіз можливо виділити в окремий клас методів, які базуються на послідовному аналізі, запропонованому у роботі [9]. Такі методи дозволяють приймати рішення на основі часткової інформації шляхом послідовного накопичення статистичних характеристик, це дозволяє використовувати методи послідовного аналізу у задачах обробки сигналів та розпізнавання образів [11–14], де реалізується відбір правдивих гіпотез із відкиданням неефективних варіантів.

Перевагою послідовного аналізу є можливість зменшення обсягу оброблюваних даних і скорочення часу прийняття рішень.

Таким чином серед сучасних методів обробки неструктурованої текстової інформації доцільно виділити трансформерні моделі машинного навчання та глибокого навчання, які забезпечують високу точність обробки, можливість глибокого аналізу і дозволяють моделювати складні семантичні зв'язки між фрагментами тексту для прогнозування, генерації та інтелектуальної інтерпретації контексту, але при цьому потребують попередньо визначеного фокусу (теми або напрямлення) неструктурованої текстової інформації, значних обчислювальних ресурсів і передбачають повну обробку тексту перед прийняттям рішення.

Іншою групою є методи послідовного аналізу, які дозволяють класифікувати – визначати фокус (тему або напрямлення) неструктурованої текстової інформації використовуючи

незначні обчислювальні ресурси і приймати рішення на неповній вибірці, але при цьому не дозволяють проводити глибинний аналіз тексту.

Із вищезазначеного виникає протиріччя: використовувати швидкі методи з незначними вимогами до ресурсів, але які не можуть проводити глибинний аналіз чи методи, які потребують значних обчислювальних ресурсів і передбачають повну обробку тексту, але при цьому дозволяють проводити глибинний аналіз, моделювати складні семантичні зв'язки між фрагментами тексту для прогнозування, генерації та інтелектуальної інтерпретації контексту.

Метою статті є розроблення методики підвищення ефективності методів обробки текстових даних за допомогою гібридного підходу з використання швидкого і неможливого до ресурсів послідовного вирішального правила на етапі попередньої класифікації з подальшим наданням класифікованих даних до моделей, які дозволяють проводити глибинний аналіз, моделювати складні семантичні зв'язки між фрагментами тексту для прогнозування, генерації та інтелектуальної інтерпретації контексту.

Виклад основного матеріалу

Багатоальтернативне послідовне вирішальне правило для класифікації текстових документів із використанням верхніх порогів

У роботах [11–14] запропоноване багатоальтернативне послідовне вирішальне правило для класифікації текстових документів із використанням верхніх порогів.

У дискретному часі завдання послідовної класифікації текстових документів формулюється наступним чином. Маємо L простих гіпотез C_l , $l = \overline{1, L}$, що відображають теми, за якими проводиться класифікація. Кожен документ, що надходить до системи d_j , представлений набором з N слів $W = (w_1, w_2, \dots, w_N)$, які характеризують його тематичну спрямованість.

Аналіз тексту розглядається як обробка потоку подій $w_i(k) \in N$, де N – множина словникових одиниць, що представляють зміст документа. Умовні ймовірності спостережень $P(w_i(k)|C_l)$, відомі з точністю до L гіпотез. Гіпотези є несумісними та утворюють повну групу подій. Априорні ймовірності гіпотез p_i , $i = \overline{1, L}$ передбачаються відомими.

При заданих умовних ймовірностях помилкового розпізнавання гіпотез $P(\hat{C}_i|C_l)$, $i \neq l$, $i, l = \overline{1, L}$ та ймовірностях правильного розпізнавання, не нижче заданих $P(\hat{C}_l|C_l) \geq P_{\text{зад}}(\hat{C}_l|C_l)$, $l = \overline{1, L}$, послідовне вирішальне правило дозволяє в результаті спостереження реалізації $W(k)$, $k = 1, 2, 3, \dots$ прийняти одне з рішень.

Завдання багатоальтернативного розпізнавання L простих гіпотез зводиться до L двоальтернативних завдань перевірки простої C_l гіпотези проти складної альтернативи θ_l .

Складна гіпотеза θ_l є поєднанням простих гіпотез C_i , $i = \overline{1, L}$, $i \neq l$:

$$\theta_l = \bigcup_{i \neq l}^L C_i.$$

Геометрична інтерпретація складної гіпотези представлена на рисунку 1.

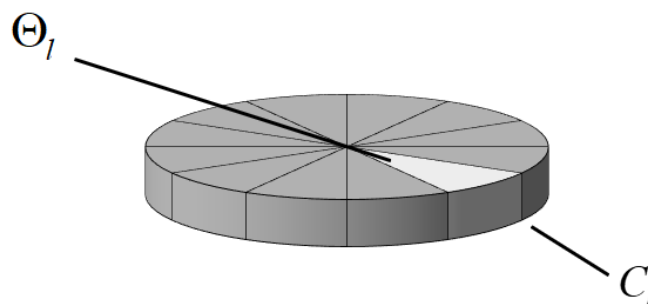


Рис. 1. Геометрична інтерпретація складної гіпотези

Прості гіпотези C_l є несумісними. Складні гіпотези θ_l є сумісними.

Відповідно до послідовного вирішального правила на кожному k -му кроці визначаються L відносин правдоподібності перевірки простої гіпотези проти складної альтернативи у вигляді:

$$\Lambda_l(k) = \frac{P(W(k)|C_l)}{P(W(k)|\theta_l)}, \quad l = \overline{1, L},$$

де $P(W(k)|C_l) = P(w_i(k)|C_l)P(W(k-1)|C_l)$ – функція правдоподібності простої гіпотези;

$P(W(k)|\theta_l)$ – функція правдоподібності складної гіпотези θ_l ;

$W(k) = w_i(k), \dots, w_i(k), \quad i = \overline{1, V}, k = 1, 2, 3, \dots$ – послідовність спостережень, що надходять.

Рішення на користь простої гіпотези C_l приймається при порівнянні відношення правдоподібності $\Lambda_l(k)$ з верхніми порогами $\Gamma_{1l} l = \overline{1, L}$ (1):

$$\Lambda_l(k) = \frac{P(W(k)|C_l)}{\sum_{i=1, i \neq l}^L \gamma_{il} P(W(k)|C_i)} \geq \Gamma_{1l}. \quad (1)$$

За умови, що на k -тому кроці відношення правдоподібності досягло значення верхнього порогу Γ_{1l} , для гіпотези C_l , приймається гіпотеза C_l , і відхиляються інші $L-1$ гіпотези. Геометрична інтерпретація процедури ухвалення рішення при використанні верхніх порогів надана на рисунку 2.



Рис. 2. Геометрична інтерпретація процедури прийняття рішення

Значення верхнього порога визначається за виразом (2):

$$\Gamma_{1l} = \frac{P(\hat{C}_l|C_l)}{P(\hat{C}_l|\theta_l)}. \quad (2)$$

У загальному випадку умовні ймовірності $P(\hat{C}_l|C_i)$ можливо представити у вигляді матриці:

$$P_{\text{реш}} = \begin{pmatrix} P(\hat{C}_1|C_1) & P(\hat{C}_1|C_2) & \dots & P(\hat{C}_1|C_L) \\ P(\hat{C}_2|C_1) & P(\hat{C}_2|C_2) & \dots & P(\hat{C}_2|C_L) \\ \dots & \dots & \dots & \dots \\ P(\hat{C}_L|C_1) & P(\hat{C}_L|C_2) & \dots & P(\hat{C}_L|C_L) \end{pmatrix}$$

Номер рядка матриці відповідає рішення, що приймається $\hat{C}_l$, $l = \overline{1, L}$, номер стовпця – істинній гіпотезі C_i , $i = \overline{1, L}$. Діагональні елементи матриці відповідають ймовірностям правильного прийняття рішень $P(\hat{C}_l | C_l)$, $l = \overline{1, L}$. Недіагональні елементи кожного рядка використовуються для обчислення ймовірності хибного розпізнавання гіпотези $\hat{C}_l$ за умови, що має місце будь-яка інша проста гіпотеза. Недіагональні елементи кожного стовпця використовуються для визначення ймовірності нерозпізнавання гіпотези C_l :

$$P(\hat{\theta}_l | C_l) = \sum_{i=1, i \neq l}^L P(\hat{C}_i | C_l) = 1 - P(\hat{C}_l | C_l), l = \overline{1, L}.$$

При дискретній вибірці може відбутися подія, коли достатня статистика перевищила значення верхнього порога. Однак якщо обсяг вибірки великий, перевищення порога досить малоймовірно, що призводить до незначної затримки у прийнятті рішення.

Аналіз правила було проведено на модельному прикладі у вигляді статистичного моделювання на ПЕОМ.

Дано: П'ять простих гіпотез C_l , $l = \overline{1, 5}$, що відображають теми, за якими проводиться класифікація. Умовні ймовірності спостережень $P(w_i(k) | C_l)$, $l = \overline{1, L}$ відомі з точністю до L гіпотез і наведені в таблиці 1.

Таблиця 1

Умовні ймовірності спостережень

$P(w_i C_l)$	C_1	C_2	C_3	C_4	C_5
w_1	0,147	0,240	0,047	0,025	0,025
w_2	0,245	0,144	0,047	0,025	0,025
w_3	0,245	0,144	0,047	0,025	0,025
w_4	0,147	0,240	0,047	0,100	0,050
w_5	0,024	0,120	0,189	0,050	0,101
w_6	0,147	0,041	0,237	0,005	0,050
w_7	0,025	0,024	0,142	0,251	0,050
w_8	0,005	0,010	0,128	0,201	0,151
w_9	0,005	0,005	0,009	0,191	0,292
w_{10}	0,010	0,030	0,104	0,125	0,227

Гіпотези є несумісними та утворюють повну групу подій. Апріорні ймовірності гіпотез передбачалися рівноймовірними $p_i = 0,2$, $i = \overline{1, 5}$. Аналіз тексту розглядається як обробка потоку подій $w_i(k) \in N$, де N – множина словникових одиниць, що представляють зміст документа. Необхідно при заданих умовних ймовірностях помилкового розпізнавання гіпотез $P(\hat{C}_i | C_l)$, $i \neq l$, $i, l = \overline{1, L}$ та ймовірності правильного розпізнавання, не менше заданих у результаті спостереження реалізації прийняти рішення на користь однієї з тематик C_l , $l = \overline{1, L}$.

Умовні ймовірності розпізнавання $P(\hat{C}_l|C_i)$, $i, l = \overline{1, L}$ задані у вигляді матриці (3), отриманої з використанням алгоритму багатоальтернативного розпізнавання гіпотез на фіксованому інтервалі спостереження. Рішення на користь простої гіпотези приймалося наприкінці інтервалу спостереження за максимумом відношення правдоподібності. При моделюванні обсяг вибірки вважався рівним 25. Для кожної гіпотези проводилося 10 000 випробувань (3).

$$P(\hat{C}_l|C_i) = \begin{pmatrix} 0,9640 & 0,0410 & 0,0001 & 0 & 0 \\ 0,0360 & 0,9589 & 0,0002 & 0 & 0 \\ 0 & 0,0001 & 0,9983 & 0,0002 & 0,0007 \\ 0 & 0 & 0,0007 & 0,9723 & 0,0249 \\ 0 & 0 & 0,0007 & 0,0275 & 0,9744 \end{pmatrix} \quad (3)$$

Відповідно до матриці (3), за допомогою виразу (2), було визначено значення верхніх порогів послідовного вирішального правила (1).

$$\Gamma_{l_1} = 93,82; \quad \Gamma_{l_2} = 105,96; \quad \Gamma_{l_3} = 3993,2; \quad \Gamma_{l_4} = 151,92; \quad \Gamma_{l_5} = 138,21.$$

На основі умовних ймовірностей спостережень, представлених у таблиці 1, а також з урахуванням отриманих значень верхніх порогів, було проведено 10 000 випробувань для кожної з гіпотез. Довжина вибірки при кожному випробуванні дорівнювала 25.

Умовні ймовірності розпізнавання гіпотез на основі виразу (1), отримані шляхом статистичного моделювання, представлені у вигляді матриці (4):

$$P(\hat{C}_l|C_i) = \begin{pmatrix} 0,9583 & 0,0481 & 0,0020 & 0 & 0 \\ 0,0415 & 0,9517 & 0,0032 & 0,0002 & 0,0002 \\ 0,0002 & 0,0002 & 0,9892 & 0,0003 & 0,0012 \\ 0 & 0 & 0,0034 & 0,9691 & 0,0264 \\ 0 & 0 & 0,0022 & 0,0304 & 0,9722 \end{pmatrix}. \quad (4)$$

Графічна інтерпретація результатів моделювання представлена на рисунку 3.

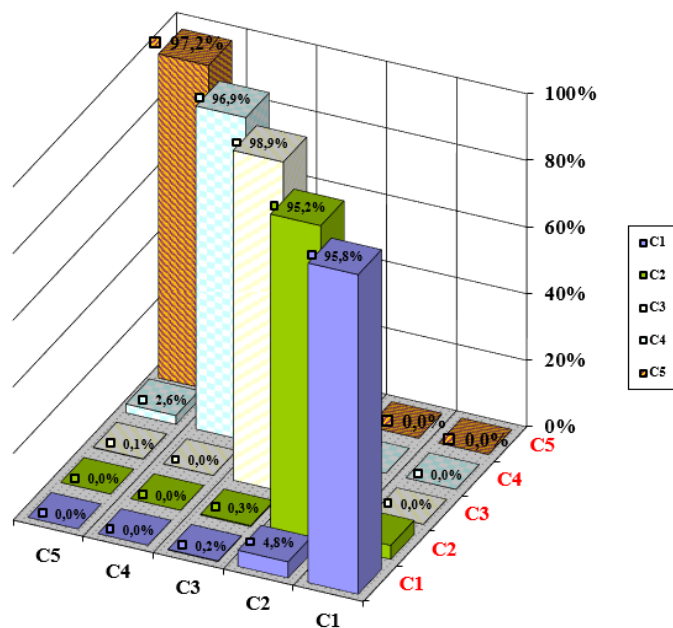


Рис. 3. Графічна інтерпретація результатів моделювання

Із рисунка видно, що показники розпізнавання гіпотез загалом не гірше ніж у алгоритму розпізнавання гіпотез на фіксованому інтервалі, але середня кількість кроків, необхідних для прийняття рішення, для усіх гіпотез дорівнює 13,6 (з вибірки на 25 слів).

Середня кількість кроків, необхідних для прийняття рішення $\bar{T}_l, l = \overline{1,5}$, для кожної гіпотези, і середньоквадратична помилка σ_l наведені у таблиці 2.

Таблиця 2

Результати моделювання з використанням верхніх порогів

Параметри	C_1	C_2	C_3	C_4	C_5
$\bar{T}_l$	13,395	13,634	14,046	13,166	13,759
σ_l	11,809	17,336	19,876	9,552	16,930

Із розглянутого прикладу видно, що алгоритм (1) забезпечує показники розпізнавання гіпотез (4) в цілому не гірше, ніж алгоритм розпізнавання гіпотез на фіксованому інтервалі (3). При цьому забезпечує зменшення часу спостереження на 45 відсотків.

Трансформери (Transformers)

Трансформери – це концепція архітектури нейронних мереж, таких як BERT і GPT, яка розроблена спеціально для роботи з послідовними даними. Трансформери використовуються для задач обробки природної мови Natural Language Processing (NLP). Трансформери забезпечили значний прорив у NLP завдяки своїй здатності ефективно враховувати контекст у послідовностях, проводити глибинний аналіз, моделювати складні семантичні зв'язки між фрагментами тексту для прогнозування, генерації та інтелектуальної інтерпретації контексту.

Ідея трансформерів вперше була запропонована у [14] дослідниками з Google. Головна ідея трансформерів полягає у використанні механізму самоуваги (Self-Attention).

Загальну архітектуру трансформерів можливо уявити у наступному вигляді:

1. Вхідні дані:

текст перетворюється у векторне представлення за допомогою вбудовувань (Embeddings);

додається позиційне кодування (Positional Encoding), щоб врахувати порядок слів.

2. Механізм самоуваги (Self-Attention):

дозволяє моделі “звертати увагу” на всі інші слова у тексті для кожного окремого слова; враховує контекст кожного слова, незалежно від його позиції у послідовності.

3. Багатошарова архітектура:

трансформери складаються з N-енкодерів (encoder) та N-декодерів (decoder), що працюють спільно.

4. Головна увага (Multi-Head Attention):

забезпечує моделювання різних контекстів у тексті паралельно.

Методика підвищення ефективності обробки неструктурованої текстової інформації в інформаційних, інформаційно-комунікаційних системах оборонного призначення

Аналіз переваг і недоліків багатоальтернативного послідовного вирішального правила показав його високу точність, стійкість до шумових даних та здатність працювати з неповною вибіркою, але при цьому багатоальтернативне послідовне вирішальне правило не може забезпечити глибинний аналіз, з іншого боку трансформери можуть проводити глибинний аналіз, моделювати складні семантичні зв'язки між фрагментами тексту для прогнозування, генерації та інтелектуальної інтерпретації контексту, але для якісного глибинного аналізу їм необхідне визначення області знань (фокусу на темі), що потребує повного аналізу тексту і великих обчислювальних затрат.

Враховуючи, що в умовах реального часу для військових інформаційно-комунікаційних систем (C4ISR, ISR, FMN) критичними є швидкість обробки, масштабованість та інтеграція різнорідних джерел інформації, автори статті вважають доцільним сформулювати методику, яка забезпечить практичні рекомендації щодо підвищення ефективності систем обробки неструктурованої текстової інформації, які охоплюють архітектурні рішення, гібридну обробку, автоматизацію збору даних та оптимізацію алгоритмів.

Методика складається з наступних етапів:

Етап 1. Формування системи з розподіленими обчислюваннями на розподілених аналітичних вузлах.

Ефективна обробка текстових інформаційних потоків у військових системах потребує архітектури з розподіленими обчисленнями, що дозволить одночасно обробляти великі обсяги неструктурованої текстової інформації.

Враховуючи незначні вимоги багатоальтернативного послідовного вирішального правила до обчислювальних ресурсів автори пропонують розгорнути алгоритми попереднього аналізу і класифікації неструктурованої текстової інформації на розподілених аналітичних вузлах, через які проходять значні потоки відповідної інформації.

У такому разі час на прийняття рішення щодо класифікації і необхідності подальшого глибинного аналізу неструктурованого текстового потоку T_{decision} буде дорівнювати (5):

$$T_{\text{decision}} = \frac{T_{\text{seq}} + k_{\text{useful}} T_{\text{comm}}}{N_{\text{nodes}}}, \quad (5)$$

де T_{seq} – середній час послідовної обробки неструктурованого текстового потоку на окремому вузлі;

k_{useful} – коефіцієнт корисної інформації;

T_{comm} – середній час на передачу цільового класифікованого потоку до кластеру глибинного аналізу;

N_{nodes} – кількість вузлів попередньої обробки неструктурованого текстового потоку.

А коефіцієнт корисної інформації k_{useful} відповідно буде дорівнювати:

$$k_{\text{useful}} = \frac{V_{\text{useful}}}{V_{\text{seq}}},$$

де V_{seq} – середній об'єм загального неструктурованого текстового потоку;

V_{useful} – середній об'єм неструктурованого текстового потоку, визначеного для подальшого глибинного аналізу.

Враховуючи, що загальний неструктурований текстовий потік завжди буде більшим за текстовий потік, визначений для подальшого глибинного аналізу, то k_{useful} завжди буде меншим за 1, а відповідно вже на етапі попереднього аналізу на одному вузлі ми отримаємо вигоду завдяки скороченню часу на передачу загального потоку і звільнення мережевого ресурсу для передачі відповідного потоку. Крім того, як видно з виразу (5), такий підхід скоротить середній час на прийняття рішення щодо класифікації і необхідності подальшого глибинного аналізу неструктурованого текстового потоку прямо пропорційно кількості вузлам, задіяним у попередньому аналізі.

Етап 2. Формування централізованого сховища типу Data Lake.

Надалі необхідно розгорнути централізоване сховище типу Data Lake, яке забезпечить зберігання неструктурованих даних, що надійшли від окремих вузлів і структурованих даних,

що з'явилися в результаті глибинного аналізу. Крім того наявність централізованого сховища типу Data Lake є важливим для забезпечення масштабованості, адаптованості до зростання обсягів даних та кількості користувачів без втрати продуктивності, надійності та можливості інтеграції різнорідної інформації в рамках стандартів НАТО (FMN, ISR, C4ISR).

Етап 3. Формування розподіленого кластера глибокого аналізу.

Наступним етапом є формування розподіленого кластера глибокого аналізу, який забезпечить масштабованість, адаптованість та надійність функціонування алгоритмів трансформерів, для глибинного аналізу.

Час на проведення глибинного аналізу T_{deep} можливо розрахувати за виразом:

$$T_{\text{deep}} = \frac{T_{\text{class}}}{N_{\text{core}}},$$

де T_{class} – глибинний аналіз класифікованого потоку одним ядром;

N_{core} – кількість процесорних ядер, задіяних у глибинному аналізі.

Таким чином, на етапі глибинного аналізу ми отримаємо скорочення часу на загальний аналіз зворотно кількості процесорних ядер, задіяних у відповідному аналізі.

Таким чином, підвищення ефективності обробки текстових інформаційних потоків у військових системах можливо досягнути завдяки використанню методики, який поєднує масштабовану архітектуру з розподіленими обчисленнями, гібридну модель обробки даних, автоматизацію збору та адаптивне навчання алгоритмів.

Використання сховищ типу Data Lake та інтеграція з розподіленими обчислювальними ресурсами скорочують час прийняття рішень, а багаторівнева фільтрація і порогова оптимізація забезпечують високу точність аналізу навіть у присутності шумових або неповних даних.

Можливість адаптивного навчання, як алгоритмів послідовного вирішального правила, так і трансформерної моделі, дозволяє системі самостійно підлаштовуватися під змінний характер інформаційних потоків, а уніфікація форматів обміну та відповідність стандартам НАТО (FMN, ISR, C4ISR) забезпечить ефективну інтеграцію з союзними платформами та оперативну підтримку бойових рішень.

Запропонована методика формує стійку та надійну систему обробки неструктурованих текстових потоків, здатну діяти у реальному масштабі часу.

Наукова новизна отриманих результатів

На думку авторів, наукові результати проведених досліджень полягають у наступному:

удосконалено підхід до обробки неструктурованої текстової інформації шляхом попередньої класифікації текстового потоку за допомогою багатоальтернативних послідовних вирішальних правил із наступним наданням класифікованих документів до трансформерних моделей, що на відміну від існуючих методів, забезпечує можливість прийняття рішення на неповній вибірці даних;

набув подальшого розвитку метод класифікації текстових документів на основі ймовірнісної моделі подання даних завдяки застосуванню послідовного критерію відношень правдоподібності з верхніми порогами, що дозволяє скоротити середню кількість оброблюваних елементів тексту, а відповідно зменшити час прийняття рішення без погіршення точності класифікації;

вперше обґрунтовано доцільність використання гібридного підходу, який поєднує швидкі і невибагливі до обчислювальних ресурсів статистичні методи на етапі класифікації та фільтрації та трансформерні моделі на етапі глибокого аналізу, що забезпечує підвищення ефективності обробки великих потоків неструктурованої текстової інформації на

попередньому етапі в умовах обмежених обчислювальних ресурсів та дозволяє класифікувати інформаційні потоки для подальшого глибинного аналізу;

удосконалено модель організації процесу обробки даних в інформаційно-аналітичних системах завдяки впровадженню принципу раннього прийняття рішень, що дозволяє зменшити обчислювальне навантаження та підвищити оперативність обробки інформації.

Висновки й перспективи подальших досліджень

Таким чином, у статті проведено аналіз існуючих методів, їхніх переваг і обмежень з акцентом на якість і швидкості обробки неструктурованих текстових інформаційних потоків і вимог до обчислювальних ресурсів.

Розроблено формальний опис методики, підвищення ефективності обробки неструктурованих текстових інформаційних потоків у військових інформаційно-комунікаційних та інформаційних системах, зокрема в контексті стандартів НАТО (FMN, ISR, C4ISR).

Запропонована методика використовує сучасні підходи, формує гібридну модель обробки неструктурованих текстових інформаційних потоків і пропонує:

виконувати первинну класифікацію на розподілених аналітичних вузлах за допомогою багатоальтернативного послідовного вирішального правила, яке при незначних вимогах до обчислювальних ресурсів дозволить збільшити швидкості первинної класифікації зі збереженням якості прийняття рішень;

використовувати сховища типу Data Lake для подальшого зберігання інформаційно важливої, класифікованої складової неструктурованої текстової інформації, що дозволить інтегрувати різноманітні джерела інформації, забезпечити масштабованість системи та автоматизувати збір даних;

здійснювати глибинний аналіз класифікованої неструктурованої текстової інформації за допомогою кластеру трансформерних методів нейронних мереж великих мовних моделей (LLM), який забезпечить глибинний аналіз і високу точність обробки та дозволить моделювати складні семантичні зв'язки між фрагментами тексту для прогнозування, генерації та інтелектуальної інтерпретації контексту.

Підтримка балансу між швидкістю обробки та точністю прийняття рішення на первинному етапі обробки неструктурованого інформаційного потоку та можливістю подальшого глибинного аналізу відібраної цільової інформації є критично важливою для бойових умов.

Результати дослідження продемонстрували, що запропонований підхід дозволяє підвищити точність і стійкість системи до шумових і неповних даних, скоротити час обробки та забезпечити ефективний обмін інформацією між платформами відповідно до стандартів НАТО.

Автори вважають, що отримані результати можуть бути використані для розробки та вдосконалення інформаційно-комунікаційних та інформаційних систем оборонного призначення, зокрема:

1. Для систем ситуаційної обізнаності – забезпечення підвищення швидкості обробки інформаційних потоків, а відповідно зменшення часу доведення аналітичної інформації до керівництва.

2. Для підрозділів, що здійснюють OSINT-аналіз, – підвищення ефективності фільтрації інформації з відкритих джерел, а відповідно зменшення навантаження на аналітичний персонал.

3. Для інформаційно-комунікаційних, інформаційних систем ЗС України – забезпечення можливості обробки великих обсягів неструктурованих даних у реальному масштабі часу, а відповідно своєчасне отримання актуальної інформації;

4. Для розробників програмного забезпечення запропоновані підходи можуть бути використані при створенні модулів автоматичної класифікації та фільтрації текстових даних,

які забезпечать можливість побудови масштабованих рішень на основі Data Lake і розподілених обчислень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року “Про Стратегічний оборонний бюлетень України”: Указ Президента України від 17.09.2021 № 473/2021. URL: <https://www.president.gov.ua/documents/4732021-40121>.
2. Жарков Я. М., Васильєв А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 38–41.
3. Graham P. Better Bayesian Filtering. 2003. URL: <https://paulgraham.com/better.html>.
4. Graham P. A Plan for Spam. 2002. URL: <https://paulgraham.com/spam.html>.
5. Kalt T. A New Probabilistic Model of Text Classification and Retrieval // Technical Report IR-78. University of Massachusetts Center for Intelligent Information Retrieval, 1996. URL: <https://ciir.cs.umass.edu/pubfiles/ir-78.pdf>.
6. Salton G., McGill M. J. Introduction to Modern Information Retrieval. New York: McGraw-Hill, 1983. 448 p. URL: <https://dl.acm.org/doi/book/10.5555/576628>.
7. Reuters-21578 Text Categorization Collection. URL: <https://daviddlewis.com/resources/testcollections/reuters21578/>.
8. Salton G., Wong A., Yang C. S. A vector space model for automatic indexing. Communications of the ACM. 1975. № 18 (11). P. 613–620. URL: <https://doi.org/10.1145/361219.361220>.
9. Wald A. Sequential Analysis. Mineola, New York: Dover Publications, 1947. URL: <https://books.google.com.ua/books?id=oVYDHHZtdlC>.
10. Васильєв В. И. Распознающие системы. Киев: Наукова думка, 1983. 422 с.
11. Жук С. Я., Ковальов В. В. Алгоритм совместной фильтрации речевого сигнала и оценки ошибки синхронизации в двухканальной измерительной системе // Известия высших учебных заведений. Радиоэлектроника. 2000. № 6. С. 16–21.
12. Жук С. Я., Ковальов В. В. Совместная фильтрация состояния и распознавание типа структуры динамической системы с отбрасыванием неудачных гипотез // Известия высших учебных заведений. Радиоэлектроника. 2001. № 7. С. 53–57.
13. Шемаев В. Н., Замаруева И. В., Приймак М. В., Дубровский Е. Н. Знание-ориентированный подход к анализу естественно-языковой текстовой информации в интересах мониторинга и оценки ситуаций // Интеллектуальний аналіз інформації (IAI-2003): зб. праць Третього наукового семінару (Київ, 21–23 травня 2003 р.). К.: Просвіта, 2004.
14. Дубровський Є. М. Метод сумісної послідовної класифікації і фільтрації текстових документів в автоматизованій системі пошуку розвідувальних відомостей // Робочі матеріали.
15. Vaswani A., Shazeer N., Parmar N. et al. Attention Is All You Need // Advances in Neural Information Processing Systems. 2017. URL: https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf.

Надійшла до редколегії 19.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.391.17

д-р техн. наук, проф. Єрохін В. Ф. ORCID: 0000-0001-7194-8577 (ВІТІ ім. Героїв Крут)
канд. техн. наук, проф. Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
Коваленко О. О. ORCID: 0009-0008-4087-8770 (ВІТІ ім. Героїв Крут)

МЕТОДИКИ СИНТЕЗУ І РЕДУКЦІЇ ML-АЛГОРИТМУ РОЗДІЛЕННЯ-ДЕМОДУЛЯЦІЇ НЕРІВНОПОТУЖНИХ СИНХРОННИХ СИГНАЛІВ QPSK

У теорії багатокористувацького детектування цифрових сигналів (ЦС) найкращими за завадостійкістю є Maximum Likelihood (ML)-алгоритми, що передбачають формування апостеріорних імовірностей станів інформаційних групового і індивідуальних дискретних параметрів (ДП) кожного з користувачів. Відомі результати синтезу і аналізу завадостійкості ML-алгоритмів розділення-демодуляції взаємно неортогональних сигналів BPSK свідчать про їхню високу, потенційно досяжну завадостійкість і водночас про експоненціальну залежність їх складності від кількості і позиційності сигналів, що підлягають розділенню. На сьогодні вже одержані результати редукції (спрощень) таких алгоритмів до виду, прийнятого для практичних застосувань. Безумовний інтерес становлять відповіді на подальші питання про можливості подібних спрощень у випадках, коли взаємно неортогональні сигнали будуть складнішими, ніж двійкові.

Представлено результати синтезу і розглядається можливість технологічно прийнятних спрощень алгоритму розділення-демодуляції двох взаємно неортогональних сигналів QPSK, оптимального за критерієм мінімуму ймовірності помилки в оцінці інформаційних ДП кожного з індивідуальних користувачів. Досліджується можливість апроксимацій аналітично складних гіперболічних передатних функцій компенсаційних трактів простими лінійно-ламаними. Запропонована структурна схема редукційованого алгоритму розділення-демодуляції двох взаємно неортогональних сигналів QPSK. Продемонстровано, що за забезпечення відміни в миттєвих потужностях між сигналами близько 9 дБ можна відмовитись від компенсації впливу менш потужного сигналу на більш потужний, що суттєво спрощує алгоритм розділення-демодуляції. Додаткове спрощення досягається відмовою від усунення опосередкованого зворотного впливу менш потужного сигналу через більш потужний. Запропоновані спрощення призводять до втрат в завадостійкості в межах 1–2,5 дБ, залежно від ступеня взаємної неортогональності.

Ключові слова: сигнали QPSK, взаємна неортогональність, ML-алгоритми розділення-демодуляції, редукція, апроксимація передатних функцій, імовірність помилки

V. Yerokhin, G. Radzivilov, O. Kovalenko. Method of synthesis and reduction of ML-algorithm for division-demodulation of unequal power synchronous QPSK signals

In the theory of multi-user detection of digital signals (DS), the best in terms of noise immunity are Maximum Likelihood (ML) algorithms, which involve the formation of posterior probabilities of the states of information group and individual discrete parameters (DP) of each user. The known results of the synthesis and analysis of the noise immunity of ML algorithms for separation-demodulation of mutually non-orthogonal BPSK signals indicate their high, potentially achievable noise immunity and at the same time the exponential dependence of their complexity on the number and position of the signals to be separated. At present, the results of the reduction (simplification) of such algorithms to a form acceptable for practical applications have already been obtained. Of undoubted interest are the answers to further questions about the possibilities of such simplifications in cases where mutually non-orthogonal signals are more complex than binary ones.

The synthesis results are presented and the possibility of technologically acceptable simplifications of the algorithm for the separation-demodulation of two mutually non-orthogonal QPSK signals, optimal according to the criterion of minimum error probability in the estimation of information DPs of each individual user, is considered. The possibility of approximations of analytically complex hyperbolic transfer functions of compensation paths by simple linear-polygonal ones is investigated. A structural diagram of a reduced algorithm for the separation-demodulation of two mutually non-orthogonal QPSK signals is proposed. It is demonstrated that, while ensuring a cancellation in instantaneous powers between the signals of about 9 dB, it is possible to abandon the compensation of the influence of a less powerful signal on a more powerful one, which significantly simplifies the separation-demodulation algorithm. Additional simplification is achieved by abandoning the elimination of the mediated reverse influence of a less powerful signal through a more powerful one. The proposed simplifications lead to losses in noise immunity in the range of 1-2.5 dB, depending on the degree of mutual non-orthogonality.

Keywords: QPSK signals, mutual non-orthogonality, ML-algorithms of separation-demodulation, reduction, approximation of transfer functions, error probability.

Вступ. Відомо, що якщо в теорії багатокористувацького детектування (БКД) цифрових сигналів (ЦС) деякий алгоритм розділення-демодуляції будується за нормою Фробеніуса (НФ), він буде нечутливим до статистичних характеристик шуму за умови, що шум є гауссівським. Тобто, у цьому випадку мінімізація НФ буде еквівалентною максимізації апостеріорної імовірності стану спостереження, якщо стани інформаційних дискретних параметрів (ДП) сигналів є апіорі рівноімовірними. Однак за апіорної нерівноімовірності станів ДП та корельованих шумів застосування НФ в Maximum Likelihood (ML)-алгоритмах не є коректним, водночас дозволяючи уникати експоненціальної залежності їх складності від кількості і позиційності взаємно неортогональних ЦС, що підлягають розділенню. Це є очевидним — при байєсівському підході в теорії БКД правило прийняття рішень (ППР) містить деяку зазвичай нелінійну функцію розподілу (апостеріорну імовірність (АІ) станів ДП), аргументом якої є деяка модифікація НФ [1–8]. Слід зазначити, що застосування в аргументі ППР безпосередньо НФ мінімізує імовірність помилки в оцінці групового ДП, який формально складається з індивідуальних ДП всіх взаємно неортогональних ЦС, що підлягають розділенню. Спроба осереднення НФ по станах ДП сигналів, вплив яких треба усунути на той, що необхідно виділити (тобто, спроба одержання НФ для одного зі взаємно неортогональних ЦС), призводить до нероботоздатності ППР за індивідуальними критеріями оптимальності. При такому осередненні з НФ автоматично зникають всі гіпотези про стани ДП сигналів, що заважають тому, для якого виконується ця спроба.

Тому неевристичне одержання компенсаційних процедур шляхом прямого неопосередкованого застосування НФ в алгоритмах розділення-демодуляції взаємно неортогональних ЦС виявляється неможливим. Процедури компенсації притаманні евристичним підходам в теорії БКД (наприклад, Successive Interference Cancellation, SIC) та методам синтезу ML-алгоритмів, оптимальних за критерієм мінімуму ймовірності помилки в оцінці ДП кожного зі взаємно неортогональних ЦС. Однак байєсівські ML-алгоритми характеризуються експоненціальним зростанням їх складності залежно від кількості і позиційності взаємно неортогональних ЦС, що підлягають розділенню. Водночас увага питанням редукції (спрощення) таких алгоритмів до технологічно прийнятної форми у відомих фундаментальних джерелах [4; 5] не приділялась. Як наслідок, за межами доступних публікацій залишаються також питання втрат у завадостійкості внаслідок редукції (тобто, евристичного спрощення) алгоритмів розділення-демодуляції взаємно неортогональних ЦС, оптимальних за індивідуальними критеріями.

Аналіз попередніх досліджень і публікацій. Певна увага питанням редукції (спрощення) алгоритмів розділення-демодуляції взаємно неортогональних ЦС до технологічно прийнятної форми у відомих фундаментальних джерелах з теорії БКД [4; 5] приділялась лише у випадках, коли таких сигналів передбачалось суттєво більше двох. Розглядалися неоптимальне кодове, лінійне розділення, розділення за критерієм мінімуму середньоквадратичної помилки. Пропонувались також різноманітні евристичні алгоритми. У випадку вибору в якості критерія оптимальності мінімуму імовірності помилки в оцінці індивідуальних інформаційних ДП в джерелах ([1; 4–6] та ін.) демонструвалась експоненціальна залежність складності оптимальних за вищезазначеним критерієм алгоритмів розділення-демодуляції від кількості та позиційності сигналів, що підлягають розділенню. Разом з тим спроби пошуку спрощень оптимальних ML-алгоритмів, коли взаємно неортогональних ЦС не більше 3–4, а їхня позиційність перевищує двійку, у доступній літературі майже не спостерігаються. Деяка увага приділялась лише питанням апроксимації передатних характеристик компенсаційних трактів [2–4]. За межами доступних публікацій залишаються також питання втрат в завадостійкості внаслідок редукції (тобто, евристичного спрощення) алгоритмів розділення-демодуляції взаємно неортогональних ЦС, оптимальних за індивідуальними критеріями.

Як виняток, у статті [8] був представлений варіант редукції ML-алгоритму розділення-демодуляції трьох взаємно неортогональних двійкових ЦС та виконана оцінка втрат в завадостійкості внаслідок запропонованих спрощень. Безумовний практичний інтерес представляє подальший розвиток досліджень у цьому напрямку, коли кількість та позиційність взаємно неортогональних сигналів будуть дещо більшими, ніж мінімальні два.

Усім публікаціям [8] притаманна одна загальна особливість. За байєсівського підходу в теорії БКД передбачається формування АІ групового та індивідуальних ДП. Це, в свою чергу, потребує фільтрації (оцінювання) неінформаційних параметрів всіх взаємно неортогональних ЦС. Однак в зазначених тут джерелах АІ передбачаються вже точно відомими. Можна стверджувати, що необхідність оцінювання цих неінформаційних параметрів не тільки не призводить до конфлікту, а й поєднує SIC і ML-підходи в теорії БКД. Як наслідок, має місце підстава для взаємопроникнення, спільного розгортання ML-напряму в теорії БКД і теорії оптимальної нелінійної фільтрації дискретно-неперервних марківських процесів (ТНФ ДНМП) шляхом залучення SIC-технології.

Продемонструємо тут SIC-та ML взаємодоповнюючий зв'язок на простому прикладі.

Для SIC-алгоритмів у випадку наявності у спостереженні трьох ЦС на першому кроці виконується оцінювання ДП першого, найбільш потужного ЦС (неінформаційні параметри всіх сигналів тут вважаємо відомими – оцінюваними з деякою необхідною точністю):

$$r_1^* = \underset{r_1=0, m_1-1}{\operatorname{argmin}} \left\| y_t - s_1(r_1) \right\|^2.$$

Тут і далі $\|\cdot\|^2$ – норма Фробеніуса.

Потім виконується процедура оцінювання ДП другого ЦС, середнього за потужністю:

$$r_2^* = \underset{r_2=0, m_2-1}{\operatorname{argmin}} \left\| \left(y_t - \hat{s}_1(r_1^*) \right) - s_2(r_2) \right\|^2.$$

Далі, після усунення у вхідному спостереженні y_t оцінок перших двох сигналів демодулюється третій, найменш потужний:

$$r_3^* = \underset{r_3=0, m_3-1}{\operatorname{argmin}} \left\| \left(y_t - \hat{s}_1(r_1^*) - \hat{s}_2(r_2^*) \right) - s_3(r_3) \right\|^2.$$

Для підоптимальних ML-алгоритмів із прямим залученням неопосередкованих НФ групового спостереження застосовується критерій мінімуму ймовірності помилки в оцінці групового ДП $r_G = (r_1, r_2, r_3)$, що формально утворюється з індивідуальних ДП всіх сигналів у спостереженні. Процедура прийняття рішення за груповим критерієм оптимальності, на відміну від SIC, буде однокроковою:

$$r_G^* = (r_1^*, r_2^*, r_3^*) = \underset{(r_1, r_2, r_3)=0, m_1 m_2 m_3-1}{\operatorname{argmin}} \left\| y_t - s_1(r_1) - s_2(r_2) - s_3(r_3) \right\|^2.$$

Після прийняття рішення про стан групового ДП необхідно виконати його перетворення (розущільнення) в індивідуальні відповідно до коду групоутворення (у нашому прикладі – з адитивно утворюваною сигнально-ковою конструкцією).

ML-алгоритм розділення-демодуляції, оптимальний за критерієм мінімуму ймовірності помилки, в оцінці індивідуального ДП того чи іншого сигналу синтезується на основі порівняння індивідуальних АІ:

$$r_i^* = \underset{r_i=0, m_i-1}{\operatorname{argmax}} [p(r_i / y_i)], \quad i = \overline{1, 3}.$$

У цьому випадку аргумент ППР містить множину АІ станів індивідуального ДП, за порівнянням яких приймаються рішення. В свою чергу, ці АІ формуються з множини АІ станів групового ДП, що формально утворюється всіма індивідуальними ДП. Наприклад:

$$p(\hat{r}_1 / y_t) = \sum_{\hat{r}_1} p(\hat{r}_1 / y_t) = \sum_{r_2=0}^{m_2-1} \sum_{r_3=0}^{m_3-1} p(\hat{r}_1, r_2, r_3 / y_t); \quad \hat{r}_1 \in \{0, \dots, m_1 - 1\}. \quad (1)$$

Тут $\hat{r}_1 = (\hat{r}_1, r_2, r_3)$ – всі такі стани групового ДП, де перший індивідуальний ДП $\hat{r}_1$ є фіксованим. АІ $p(\hat{r}_1 / y_t)$ станів групового ДП, в свою чергу, формуються із залученням теореми Байєса і модифікованої НФ (так званої сигнальної функції) в якості аргументу, що дозволяє враховувати апіорні ймовірності станів інформаційних ДП і можливу корельованість шумів каналу. В процесі такого формування і виникають компенсаційні процедури усунення перехресного впливу взаємно неортогональних ЦС. Важливо зазначити, що байєсівський підхід дозволяє уникати зворотних компенсаційних зв'язків при формуванні аргументу ППР, які можуть бути причиною самозбудження алгоритму розділення-демодуляції при спробах технічної реалізації. Окрім того, компенсаційні процедури при такому підході виконуються після згорток спостереження – тобто, не на несівних частотах. Можна також стверджувати, що ML-алгоритми, оптимальні за критерієм мінімуму ймовірності помилки в оцінюванні індивідуальних ДП, у окремих випадках можна редуціювати до виду, в якому вони будуть характеризуватись близькою до лінійної залежністю складності від кількості та позиційності взаємно неортогональних сигналів. Цьому також сприяє та особливість у галузі електронних комунікацій, що апіорні ймовірності станів інформаційних ДП зазвичай можна вважати однаковими.

Водночас при технічній реалізації ML-алгоритмів повністю уникнути супутніх SIC-процедур зі зворотними зв'язками на частоті (частотах) спостереження y_t представляється неможливим. Справа в тому, що для фільтрації супутніх неінформаційних параметрів кожного з сигналів (їх амплітуд, початкових фаз, тактових точок тощо) доведеться спочатку послідовно окремо виділяти кожен із сигналів, деманіпулювати його і відтворювати відповідні несівні коливання – наприклад, із застосуванням методів ТОНФ ДНМП.

Мета. На прикладі розробки ML-алгоритму розділення-демодуляції двох сигналів QPSK визначити додаткові обмеження для можливості виконання процедури редукції і одержати оцінку втрат у завадостійкості внаслідок виконаної редукції.

Постановка задачі. Виконати синтез алгоритму розділення-демодуляції двох синхронних взаємно неортогональних сигналів QPSK, оптимального за критерієм мінімуму ймовірності помилки в оцінюванні інформаційних ДП кожного з сигналів. Редуціювати синтезований оптимальний алгоритм до технічно прийнятного виду. Оцінити втрати в завадостійкості внаслідок редукції.

Виклад основного матеріалу.

1. Синтез і редукція ML-алгоритмів розділення-демодуляції двох синхронних взаємно неортогональних QPSK-сигналів

Нехай модель спостереження для чотирьох BPSK-сигналів, синхронних за тактовими точками, має загальний вигляд:

$$y_t = (-1)^{r_1} s_1(t) + (-1)^{r_2} s_2(t) + (-1)^{r_3} s_3(t) + (-1)^{r_4} s_4(t) + n(t), \quad (2)$$

$$t \in (t_{k-1}, t_k], \quad T = t_k - t_{k-1}.$$

Тут $r_{1,\dots,4} \in \{0,1\}$ – інформаційні дискретні параметри (ДП) сигналів; $n(t)$ – адитивний білий гауссівський шум (АБГШ); T – протяжність інформаційного тактового інтервалу.

У випадку когерентного прийому, за рівномірних апіорних станів усіх інформаційних ДП: $p(r_i = 0) = p(r_i = 1) = 0,5$, $i = \overline{1,4}$ ППР r_1^* щодо стану першого ДП в гауссівському каналі з постійними параметрами із залученням (1) [1; 3; 4] ППР r_1^* може бути представлено у вигляді:

$$r_1^* = \text{rect} \left\{ - \left[\begin{aligned} & sh[b_1 - 2(-R_{12} - R_{13} - R_{14})] \exp[-b_2 - b_3 - b_4 - 2(R_{23} + R_{24} + R_{34})] + \\ & + sh[b_1 - 2(-R_{12} - R_{13} + R_{14})] \exp[-b_2 - b_3 + b_4 - 2(-R_{23} - R_{24} - R_{34})] + \\ & + sh[b_1 - 2(-R_{12} + R_{13} - R_{14})] \exp[-b_2 + b_3 - b_4 - 2(-R_{23} + R_{24} - R_{34})] + \\ & + sh[b_1 - 2(-R_{12} + R_{13} + R_{14})] \exp[-b_2 + b_3 + b_4 - 2(-R_{23} - R_{24} + R_{34})] + \\ & + sh[b_1 - 2(+R_{12} - R_{13} - R_{14})] \exp[+b_2 - b_3 - b_4 - 2(-R_{23} - R_{24} + R_{34})] + \\ & + sh[b_1 - 2(+R_{12} - R_{13} + R_{14})] \exp[+b_2 - b_3 + b_4 - 2(-R_{23} + R_{24} - R_{34})] + \\ & + sh[b_1 - 2(+R_{12} + R_{13} - R_{14})] \exp[+b_2 + b_3 - b_4 - 2(-R_{23} - R_{24} - R_{34})] + \\ & + sh[b_1 - 2(+R_{12} + R_{13} + R_{14})] \exp[+b_2 + b_3 + b_4 - 2(R_{23} + R_{24} + R_{34})] \end{aligned} \right] \frac{1}{K_z} \right\}; \quad (3)$$

$$\text{rect}(x \geq 0) = 1, \quad \text{rect}(x < 0) = 0.$$

Тут $K_z = 8chb_1chb_2chb_3chb_4chR_{12}chR_{13}chR_{14}chR_{23}chR_{24}chR_{34} > 0$,

$$b_{1,\dots,4} = \frac{2}{N_0} \int_{t_{k-1}}^{t_k} y_t s_{1,\dots,4}(t) dt; \quad R_{ij} = \frac{1}{N_0} \int_{t_{k-1}}^{t_k} s_i(t) s_j(t) dt, \quad i, j = \overline{1,4}, \quad i \neq j,$$

де N_0 – одностороння спектральна щільність потужності АБГШ $n(t)$.

Після гомоморфних перетворень (у сенсі збереження знаку аргументу) ППР r_1^* (3) за моделі спостереження (2), оптимальне за індивідуальним критерієм мінімуму ймовірності помилки в оцінці першого ДП можна одержати у вигляді, де його аргумент містить виключно адитивну комбінацію добутків функцій $th(*)$.

$$r_1^* = \text{rect} \left\{ \begin{aligned} & -[K_0 thb_1 + K_{12} thb_2 + K_{13} thb_3 + K_{14} thb_4 + K_R thb_2 thb_3 thb_4] + \\ & + [K_{23} thb_1 thb_2 thb_3 + K_{24} thb_1 thb_2 thb_4 + K_{34} thb_1 thb_3 thb_4] \end{aligned} \right\}; \quad (4)$$

$$\text{rect}(x \geq 0) = 1, \quad \text{rect}(x < 0) = 0.$$

Зазначимо, що при такому представленні аргументу ППР через функції $th(*)$ технічна реалізація спроститься. Передатня характеристика такої функції, як відомо, добре апроксимується лінійно-ламаною з межами ± 1 .

Однак у загальному випадку, коли всі чотири сигнали є взаємно неортогональними, коефіцієнти K_0, K_R, K_{ij} , $i, j = \overline{1,4}$, $i \neq j$ у ППР (4) за вищезазначеного критерію оптимальності виявляються неприйнятно громіздкими навіть за умови взаємного тактового синхронізму. Дійсно, коефіцієнти у (4) мають вигляд (5):

$$\begin{aligned}
K_0 &= 1 - \left(th2R_{12}th2R_{13}th2R_{23} + th2R_{12}th2R_{14}th2R_{24} + th2R_{13}th2R_{14}th2R_{34} + th2R_{23}th2R_{24}th2R_{34} + \right. \\
&\quad \left. + th2R_{12}th2R_{13}th2R_{24}th2R_{34} + th2R_{12}th2R_{14}th2R_{23}th2R_{34} + th2R_{13}th2R_{14}th2R_{23}th2R_{24} \right); \\
K_{12} &= -th2R_{12} + th2R_{13}th2R_{23} + th2R_{14}th2R_{24} - th2R_{13}th2R_{24}th2R_{34} - th2R_{14}th2R_{23}th2R_{34} + \\
&\quad + th2R_{12}th2R_{13}th2R_{14}th2R_{34} + th2R_{12}th2R_{23}th2R_{24}th2R_{34} - th2R_{12}th2R_{13}th2R_{14}th2R_{23}th2R_{24}; \\
K_{13} &= -th2R_{13} + th2R_{12}th2R_{23} + th2R_{14}th2R_{34} - th2R_{12}th2R_{24}th2R_{34} - th2R_{14}th2R_{23}th2R_{24} + \\
&\quad + th2R_{12}th2R_{13}th2R_{14}th2R_{24} + th2R_{13}th2R_{23}th2R_{24}th2R_{34} - th2R_{12}th2R_{13}th2R_{14}th2R_{23}th2R_{34}; \\
K_{14} &= -th2R_{14} + th2R_{12}th2R_{24} + th2R_{13}th2R_{34} - th2R_{12}th2R_{23}th2R_{34} - th2R_{13}th2R_{23}th2R_{24} + \\
&\quad + th2R_{12}th2R_{13}th2R_{14}th2R_{23} + th2R_{14}th2R_{23}th2R_{24}th2R_{34} - th2R_{12}th2R_{13}th2R_{14}th2R_{24}th2R_{34}; \quad (5) \\
K_{23} &= -th2R_{23} + th2R_{12}th2R_{13} + th2R_{24}th2R_{34} - th2R_{12}th2R_{14}th2R_{34} - th2R_{13}th2R_{14}th2R_{24} + \\
&\quad + th2R_{12}th2R_{14}th2R_{23}th2R_{24} + th2R_{13}th2R_{14}th2R_{23}th2R_{34} - th2R_{12}th2R_{13}th2R_{23}th2R_{24}th2R_{34}; \\
K_{24} &= -th2R_{24} + th2R_{12}th2R_{14} + th2R_{23}th2R_{34} - th2R_{12}th2R_{13}th2R_{34} - th2R_{13}th2R_{14}th2R_{23} + \\
&\quad + th2R_{12}th2R_{13}th2R_{23}th2R_{24} + th2R_{13}th2R_{14}th2R_{24}th2R_{34} - th2R_{12}th2R_{14}th2R_{23}th2R_{24}th2R_{34}; \\
K_{34} &= -th2R_{34} + th2R_{13}th2R_{14} + th2R_{23}th2R_{24} - th2R_{12}th2R_{13}th2R_{24} - th2R_{12}th2R_{14}th2R_{23} + \\
&\quad + th2R_{12}th2R_{13}th2R_{23}th2R_{34} + th2R_{12}th2R_{14}th2R_{24}th2R_{34} - th2R_{13}th2R_{14}th2R_{23}th2R_{24}th2R_{34}; \\
K_R &= th2R_{12}th2R_{34} + th2R_{13}th2R_{24} + th2R_{14}th2R_{23} - th2R_{12}th2R_{13}th2R_{14} - th2R_{12}th2R_{23}th2R_{24} - \\
&\quad - th2R_{13}th2R_{23}th2R_{34} - th2R_{14}th2R_{24}th2R_{34} + th2R_{12}th2R_{13}th2R_{14}th2R_{23}th2R_{24}th2R_{34}.
\end{aligned}$$

Тут:

$$b_{1,..,4} = \frac{2}{N_0} \int_{t_{k-1}}^{t_k} y_t s_{1,..,4}(t) dt; \quad R_{ij} = \frac{1}{N_0} \int_{t_{k-1}}^{t_k} s_i(t) s_j(t) dt, \quad i, j = \overline{1,4}, \quad i \neq j,$$

Неприйнятна з точки зору технічної реалізації складність ППР (4) є очевидною. Окрім того у виді (4) з урахуванням (5) неможливою є спроба знайти прозоре пояснення принципу функціонування цього ППР, його компенсаційний характер.

Розглянемо приклад, що може становити інтерес із точки зору можливості фізичного відтворення. Нехай модель спостереження містить два взаємно неортогональні QPSK-сигнали. Будемо вважати, що сигнали за тактовими точками і протяжністю T інформаційних тактових інтервалів співпадають, що є характерним, наприклад, у напрямку базова станція – мобільний абонент. Модель спостереження (2) конкретизуємо до вигляду:

$$\begin{aligned}
y_t &= (-1)^{r_1} A_1 \cos \omega t + (-1)^{r_2} A_1 \sin \omega t + (-1)^{r_3} A_2 \cos(\omega t + \varphi) + (-1)^{r_4} A_2 \sin(\omega t + \varphi) + n(t), \\
t &\in (t_{k-1}, t_k], \quad T = t_k - t_{k-1}.
\end{aligned} \quad (6)$$

Нехай початкова фаза $\varphi \in \overline{0, 2\pi}$ рівномірно розподілена, та будемо вважати сигнали нерівнопотужними. Покладемо також $A_2 \geq 2A_1$, що відповідно до результатів розрахунків,

наведених в [8], дозволяє сподіватись на суттєве зменшення складності алгоритму розділення. Справа в тому, що як доводять результати численних досліджень, різниця в потужностях взаємно неортогональних сигналів є обов'язковою умовою можливості їх демодуляції з прийнятною якістю. Другий, більш потужніший QPSK-сигнал, за такої умови можна буде обробляти класично, без урахування впливу малопотужного першого. При цьому на підставі результатів [1; 6–8] слід очікувати, що завадостійкість демодуляції останнього буде наближатись до потенційної завадостійкості в каналі без другого сигналу, якщо вплив потужнішого другого сигналу на перший передбачається точно компенсувати.

Після редукції ППР $r_{1,2}^*$ щодо станів $r_{1,2}$ першого ДП малопотужного ЦС, в процесі якої на першому кроці слід врахувати відсутність взаємних впливів $R_{12} = 0$, $R_{34} = 0$, коефіцієнти K_0 , K_R , K_{ij} , $i = \overline{1,3}$; $j = \overline{2,4}$; $i \neq j$ порівняно з (5) приймуть суттєво спрощений вигляд, а їхні складові відповідно до моделі спостереження (6) конкретизуються:

$$\begin{aligned} K_0 &= 1 - th2R_{13}th2R_{14}th2R_{23}th2R_{24}; \quad K_{12} = th2R_{13}th2R_{23} + th2R_{14}th2R_{24}; \\ K_{13} &= -th2R_{13} - th2R_{14}th2R_{23}th2R_{24}; \quad K_{14} = -th2R_{14} - th2R_{13}th2R_{23}th2R_{24}; \\ K_{23} &= -th2R_{23} - th2R_{13}th2R_{14}th2R_{24}; \quad K_{24} = -th2R_{24} - th2R_{13}th2R_{14}th2R_{23}; \\ K_{34} &= th2R_{13}th2R_{14} + th2R_{23}th2R_{24}; \quad K_R = th2R_{13}th2R_{24} + th2R_{14}th2R_{23}. \end{aligned} \quad (7)$$

Тут відповідно до конкретизованої моделі спостереження (6):

$$\begin{aligned} R_{13} &= \frac{A_1 A_2}{N_0} \int_{t_{k-1}}^{t_k} \cos \omega t \cos(\omega t + \varphi) dt; \quad R_{14} = \frac{A_1 A_2}{N_0} \int_{t_{k-1}}^{t_k} \cos \omega t \sin(\omega t + \varphi) dt; \\ R_{23} &= \frac{A_1 A_2}{N_0} \int_{t_{k-1}}^{t_k} \sin \omega t \cos(\omega t + \varphi) dt; \quad R_{24} = \frac{A_1 A_2}{N_0} \int_{t_{k-1}}^{t_k} \sin \omega t \sin(\omega t + \varphi) dt. \end{aligned}$$

Далі пропонується знехтувати в моделі спостереження (6) опосередкованим зворотнім перехресним впливом ортогональних складових першого, малопотужного QPSK-сигналу, через складові другого, потужнішого, на перший. Для цього в аргументах обох ППР $r_{1,2}^*$ за станами ДП $r_{1,2}$ малопотужного першого QPSK-сигналу спростуємо складові, що містять множники thb_2 або thb_1 відповідно:

$$r_1^* = rect \{ -[K_0 thb_1 + K_{13} thb_3 + K_{14} thb_4 + K_{34} thb_1 thb_3 thb_4] \}; \quad (8a)$$

$$r_2^* = rect \{ -[K_0 thb_2 + K_{23} thb_3 + K_{24} thb_4 + K_{34} thb_2 thb_3 thb_4] \}. \quad (8b)$$

$$rect(x \geq 0) = 1, \quad rect(x < 0) = 0.$$

Перепишемо на цьому кроці ППР (8a), (8b) у вигляді:

$$r_1^* = rect \{ -[thb_1 (K_0 + K_{34} thb_3 thb_4) + K_{13} thb_3 + K_{14} thb_4] \}; \quad (9a)$$

$$r_2^* = \text{rect} \left\{ -[thb_2 (K_0 + K_{34}thb_3thb_4) + K_{23}thb_3 + K_{24}thb_4] \right\}. \quad (96)$$

$$\text{rect}(x \geq 0) = 1, \quad \text{rect}(x < 0) = 0.$$

За припущення про відсутність зворотного опосередкованого перехресного впливу складових першого сигналу через складові другого на перший далі в коефіцієнтах (7) врахуємо, що в ППР (9а):

$$K_0 = 1, K_{13} = -th2R_{13}, K_{14} = -th2R_{14}, K_{34} = th2R_{13}th2R_{14},$$

а в ППР (9б):

$$K_0 = 1, K_{23} = -th2R_{23}, K_{24} = -th2R_{24}, K_{34} = th2R_{23}th2R_{24}.$$

Тоді з (9а), (9б) одержуємо :

$$\begin{aligned} r_1^* &= \text{rect} \left\{ -[b_1 - \text{Arth} \left(\frac{th2R_{13}thb_3 + th2R_{14}thb_4}{1 + th2R_{13}th2R_{14}thb_3thb_4} \right)] \right\} = \\ &= \text{rect} [-b_1 + \text{Arth}(th2R_{13}thb_3) + \text{Arth}(th2R_{14}thb_4)]; \end{aligned} \quad (10a)$$

$$\begin{aligned} r_2^* &= \text{rect} \left\{ -[b_2 - \text{Arth} \left(\frac{th2R_{23}thb_3 + th2R_{24}thb_4}{1 + th2R_{23}th2R_{24}thb_3thb_4} \right)] \right\} = \\ &= \text{rect} [-b_2 + \text{Arth}(th2R_{23}thb_3) + \text{Arth}(th2R_{24}thb_4)]. \end{aligned} \quad (10б)$$

$$\text{rect}(x \geq 0) = 1, \quad \text{rect}(x < 0) = 0.$$

де згідно з моделлю спостереження (5):

$$\begin{aligned} b_1 &= \frac{2A_1}{N_0} \int_{t_{k-1}}^{t_k} y_t \cos \omega t dt; \quad b_2 = \frac{2A_1}{N_0} \int_{t_{k-1}}^{t_k} y_t \sin \omega t dt; \\ b_3 &= \frac{2A_2}{N_0} \int_{t_{k-1}}^{t_k} y_t \cos(\omega t + \varphi) dt; \quad b_4 = \frac{2A_2}{N_0} \int_{t_{k-1}}^{t_k} y_t \sin(\omega t + \varphi) dt. \end{aligned}$$

За відміни в миттєвих потужностях між QPSK-сигналами не менше 6 дБ і відношеннях сигнал/шум $8 \div 10$ дБ або більше ППР (10а), (10б) без помітних втрат у завадостійкості можна ще спростити:

$$r_1^* = \text{rect} (-b_1 + 2R_{13}\text{sign}b_3 + 2R_{14}\text{sign}b_4); \quad (11a)$$

$$r_2^* = \text{rect} (-b_2 + 2R_{23}\text{sign}b_3 + 2R_{24}\text{sign}b_4); \quad (11б)$$

$$\text{sign}(x \geq 0) = 1; \quad \text{sign}(x < 0) = -1.$$

Структурна схема алгоритму розділення-демодуляції двох взаємно неортогональних QPSK-сигналів, синхронних за тактовими точками з урахуванням редуційованих представлень (11а), (11б), наведена на рисунку 1.

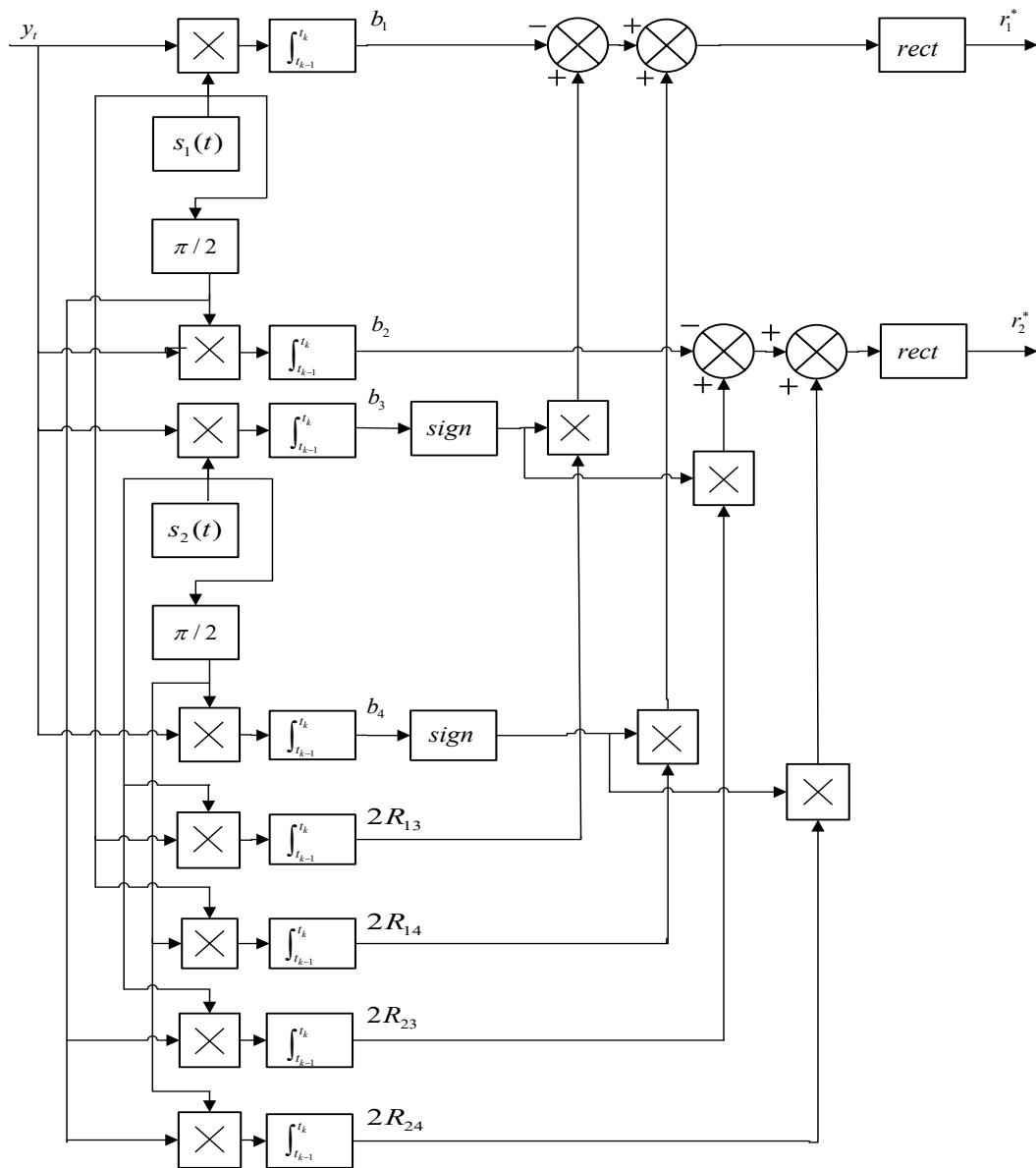


Рис. 1. Структурна схема алгоритму розділення-демодуляції взаємно неортогональних сигналів QPSK, синхронних за тактовими точками

За редуційованого перетворення ППР (4) до виду (11а), (11б) (див. рис. 1) сумніви в можливості технічної реалізації не виникають – необхідність у застосуванні громіздких комбінацій гіперболічних функцій відпадає. Відповідно, на наступному етапі слід визначитись із втратами в завадостійкості внаслідок запропонованих апроксимацій передатних характеристик компенсаційних трактів.

2. Оцінювання завадостійкості редуційованого алгоритму.

Розрахунки втрат в імовірностях помилки виду $r_{3,4}^* = 1 - r_{3,4}^*$ внаслідок некомпенсованого впливу складових малопотужного QPSK-сигналу на складові більш потужного для найгіршого випадку – їх тактового синхронізму та тотожності несівних – може бути виконана за виразом:

$$\begin{aligned}
P_{3,4}(r_{3,4}^* \neq r_{3,4}) &= \frac{1}{8\pi} \sum_{r_1=0}^1 \sum_{r_2=0}^1 \int_0^{2\pi} \overline{F} \left[\sqrt{h_{3,4}^2} \left(1 + (-1)^{r_1} \cos \varphi \sqrt{\frac{h_1^2}{h_{3,4}^2}} + (-1)^{r_2} \sin \varphi \sqrt{\frac{h_1^2}{h_{3,4}^2}} \right) \right] d\varphi = \\
&= \frac{1}{2\pi} \sum_{r_1=0}^1 \sum_{r_2=0}^1 \int_0^{\pi/2} \overline{F} \left\{ \sqrt{h_{3,4}^2} \left[1 + \left[(-1)^{r_1} \cos \varphi + (-1)^{r_2} \sin \varphi \right] \sqrt{\frac{h_1^2}{h_{3,4}^2}} \right] \right\} d\varphi; \\
\overline{F}(x) &= 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp(-z^2/2) dz, \quad h_{3,4}^2 = \frac{A_2^2}{N_0} \int_{t_{k-1}}^{t_k} \cos^2 \omega t dt.
\end{aligned} \tag{12}$$

Тут φ – випадкова відміна в початкових фазах однакових за частотою несінхронних QPSK-сигналів, рівномірно розподілена на інтервалі $(0, 2\pi)$. За фіксованого значення $\cos(\varphi = \pi/4) = \sin(\varphi = \pi/4) = 1/\sqrt{2} = 0,707$ розрахунки дають верхню оцінку ймовірності помилки. У цьому граничному випадку з (12) маємо:

$$\begin{aligned}
P_{3,4}(r_{3,4}^* \neq r_{3,4}) &= \frac{1}{4} \sum_{r_1=0}^1 \sum_{r_2=0}^1 \overline{F} \left\{ \sqrt{h_{3,4}^2} \left[1 + 0,707 \left[(-1)^{r_1} + (-1)^{r_2} \right] \sqrt{\frac{h_1^2}{h_{3,4}^2}} \right] \right\} = \\
&= \frac{1}{4} \left\{ \overline{F} \left[\sqrt{h_{3,4}^2} \left(1 + 1,414 \sqrt{\frac{h_1^2}{h_{3,4}^2}} \right) \right] + \overline{F} \left[\sqrt{h_{3,4}^2} \left(1 - 1,414 \sqrt{\frac{h_1^2}{h_{3,4}^2}} \right) \right] + 2\overline{F} \left(\sqrt{h_{3,4}^2} \right) \right\}
\end{aligned} \tag{13}$$

Результати розрахунків згідно з (13) наведено на рисунку 2. Можна бачити, що відмова від компенсації впливу менш потужного QPSK-сигналу на більш потужний за довільного ступеня неортогональності в найгіршому випадку їх взаємного синхронізму за тактовими точками потребує збільшення енергетики останнього в межах 9 дБ.

На підставі того, що відміна в миттєвих потужностях QPSK-сигналів потрібна бути близько 9 дБ (див. графіки на рис. 2), оцінку завадостійкості менш потужнішого сигналу доцільно виконувати із залученням найпростіших редуційованих ППР (11а), (11б), де передбачається тактовий синхронізм. Із досвіду аналізу алгоритмів розділення двійкових взаємно неортогональних BPSK-сигналів відомо, що умова тактового синхронізму призводить до найгіршої завадостійкості [1; 3; 6; 7], і такий підхід в аналізі призведе до одержання оцінок завадостійкості “зверху”.

Загальний вираз для ймовірності помилки в першій складовій малопотужного QPSK-сигналу при розділенні-демодуляції двох таких сигналів, асинхронних за тактовими точками за рівноймовірних апіорних станів їх ДП запишеться у вигляді:

$$\begin{aligned}
P_1(r_1^{k*} \neq r_1^k) &= P_1(r_1^{k*} = 1 - r_1^k) = \\
&= \frac{1}{512} \sum_{r_1^{k-1}=0}^1 \sum_{r_2^{k-1}=0}^1 \sum_{r_2^k=0}^1 \sum_{r_1^{k+1}=0}^1 \sum_{r_2^{k+1}=0}^1 \sum_{r_3^{k-1}=0}^1 \sum_{r_4^{k-1}=0}^1 \sum_{r_3^k=0}^1 \sum_{r_4^k=0}^1 P_1 \left(r_1^{k*} = 1 - r_1^k / \right. \\
&\quad \left. r_1^{k-1}, r_2^{k-1}, r_2^k, r_1^k, r_1^{k+1}, r_2^{k+1}, r_3^{k-1}, r_4^{k-1}, r_3^k, r_4^k \right).
\end{aligned} \tag{14}$$

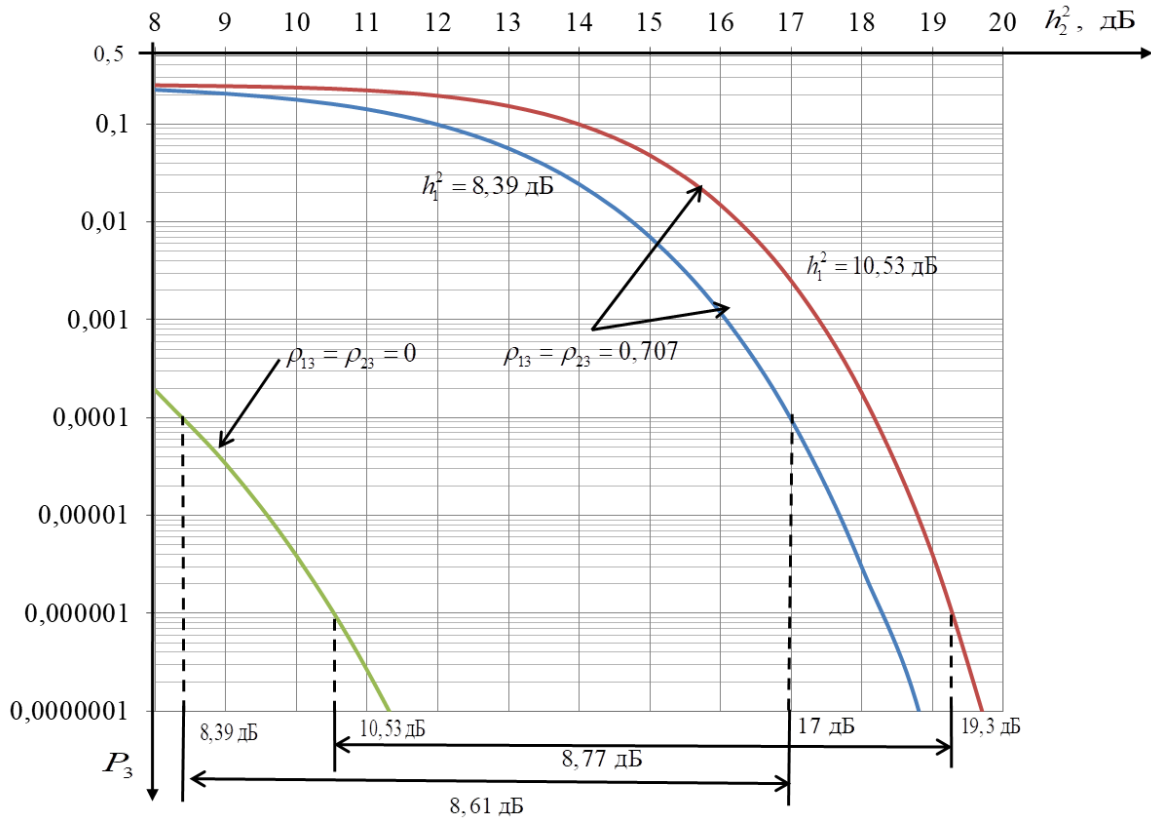


Рис. 2. Імовірність помилки при когерентній демодуляції складової змінного за потужністю QPSK-сигналу за присутності подібного з потужністю складових 8,39 дБ або 10,53 дБ

За відміни QPSK-сигналів у миттєвих потужностях орієнтовно на 9 дБ опосередкованими впливами другої складової малопотужного сигналу на його першу складову на k -му тактовому інтервалі та обох його складових на суміжних тактових інтервалах за умови тактового синхронізму можна знехтувати, вираз (14) спростимо, враховуючи також тотожність умовних помилок:

$$P_1(r_1^{k*} = 0 / r_1^k = 1, r_3^{k-1}, r_4^{k-1}, r_3^k, r_4^k) \equiv P_1(r_1^{k*} = 1, / r^k = 0, r_3^{k-1}, r_4^{k-1}, r_3^k, r_4^k).$$

Тоді:

$$P_1(r_1^{k*} \neq r_1^k) = \frac{1}{16} \sum_{r_3^{k-2}=0}^1 \sum_{r_4^{k-2}=0}^1 \sum_{r_3^{k-1}=0}^1 \sum_{r_4^{k-1}=0}^1 P_1(r_1^{k*} = 1 - r_1^k / r_1^k, r_3^{k-1}, r_4^{k-1}, r_3^k, r_4^k). \quad (15)$$

Нас насамперед цікавить оцінка “зверху” ймовірності помилки, яку можна одержати за припущення про тактовий синхронізм взаємно неортогональних сигналів [1; 3; 6; 7]. У цьому випадку (15) перепишеться у ще простішому вигляді:

$$P_1(r_1^* \neq r_1) = \frac{1}{4} \sum_{r_3=0}^1 \sum_{r_4=0}^1 P_1(r_1^* = 0, r_1 = 1 / r_3, r_4). \quad (16)$$

Приклад виразу для умовних імовірностей помилки згідно з ППР (10а) буде мати вигляд (через симетрію умовних імовірностей помилки обмежимося тут і далі згідно з (16) помилками виду $r_1^* = 0, r_1 = 1$):

$$P_1(r_1^* = 0 / r_1 = 1, r_3, r_4) = 1 - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{B_1} \omega(b_1, b_3, b_4 / r_3, r_4) db_1 db_3 db_4. \quad (17)$$

Тут згідно з редуційованим ППР (10а) межа прийняття рішень $B_1 = \text{Arth}(th2R_{23}thb_3) + \text{Arth}(th2R_{24}thb_4)$, $\omega(\cdot)$ – тривимірна гаусівська функція щільності ймовірності (ФЩІ), умовна за станами ДП r_1, r_3, r_4 :

$$\omega(b_1, b_3, b_4, \rho_{13}, \rho_{14} / r_1, r_3, r_4) = \frac{1}{\sigma_1 \sigma_3 \sigma_4 \sqrt{(2\pi)^3 D}} \exp \left[-\frac{1}{2D} \sum_{i=1,3,4} \sum_{j=1,3,4} \frac{D_{ij}}{\sigma_i \sigma_j} (b_i - m_i)(b_j - m_j) \right].$$

$$m_1 = m_1(r_1 = 1, r_3, r_4) = 2h_1^2 [-1 + (-1)^{r_3} \rho_{13} / l^2 + (-1)^{r_4} \rho_{14} / l^2] =$$

$$= 2h_1^2 [-1 + (-1)^{r_3} \cos \varphi / l^2 + (-1)^{r_4} \sin \varphi / l^2];$$

$$m_3 = m_3(r_1 = 1, r_2, r_3) = 2h_1^2 [-\rho_{13} / \sqrt{l^2} + (-1)^{r_2} \rho_{14} / \sqrt{l^2} + (-1)^{r_3} / l^2] =$$

$$= 2h_1^2 [-\cos \varphi / \sqrt{l^2} + (-1)^{r_2} \sin \varphi / \sqrt{l^2} + (-1)^{r_3} / l^2];$$

$$m_4 = m_4(r_1 = 1, r_2, r_4) = 2h_1^2 [-\rho_{14} / \sqrt{l^2} + (-1)^{r_2} \rho_{13} / \sqrt{l^2} + (-1)^{r_4} / l^2] =$$

$$= 2h_1^2 [-\sin \varphi / \sqrt{l^2} + (-1)^{r_2} \cos \varphi / \sqrt{l^2} + (-1)^{r_4} / l^2].$$

У цих виразах згідно з моделлю спостереження (6) додатково до застосованих в (7) та (10а) введені позначення:

$$h_1^2 = \frac{1}{N_0} \int_{t_{k-1}}^{t_k} s_1^2(t) dt = \frac{1}{N_0} \int_0^T s_1^2(t) dt = \frac{A_1}{N_0} \int_0^T \cos^2(t) dt;$$

$$h_{3,4}^2 = \frac{1}{N_0} \int_{t_{k-1}}^{t_k} s_{3,4}^2(t) dt = \frac{A_2}{N_0} \int_0^T \cos^2(t) dt = \frac{A_2}{N_0} \int_0^T \sin^2(t) dt;$$

$$l^2 = h_1^2 / h_{3,4}^2;$$

$$\rho_{13} = R_{13} / \sqrt{h_1^2 h_{3,4}^2} = \cos \varphi; \rho_{14} = R_{14} / \sqrt{h_1^2 h_{3,4}^2} = \sin \varphi;$$

$$R_{13} = \frac{A_1 A_2}{N_0} \int_{t_{k-1}}^{t_k} \cos \omega t \cos(\omega t + \varphi) dt = \frac{A_1 A_2}{N_0} \cos \varphi = h_1^2 \cos \varphi / \sqrt{l^2};$$

$$R_{14} = \frac{A_1 A_2}{N_0} \int_{t_{k-1}}^{t_k} \cos \omega t \sin(\omega t + \varphi) dt = \frac{A_1 A_2}{N_0} \sin \varphi = h_1^2 \sin \varphi / \sqrt{l^2}.$$

Відповідно, середньоквадратичні відхилення: $\sigma_1 = \sqrt{2h_1^2}$; $\sigma_3 = \sigma_4 = \sqrt{2h_1^2 / l^2}$.

Виконаємо тепер зручне для розрахунків центрування та нормування випадкових величин b_1, b_3, b_4 : $x_i = (b_i - m_i) / \sigma_i$, $i = 1, 3, 4$. Введемо відповідні перетворення:

$$x_1 = (b_1 - m_1) / \sqrt{2h_1^2} ; \quad x_3 = (b_3 - m_3) / \sqrt{2h_1^2 / l^2} ; \quad x_4 = (b_4 - m_4) / \sqrt{2h_1^2 / l^2} .$$

$$\text{Тоді щільність імовірності } \omega(x_1, x_3, x_4, \rho_{13}, \rho_{14}) = \frac{1}{\sqrt{(2\pi)^3 D}} \exp \left[-\frac{1}{2D} \sum_{i=1,3,4} \sum_{j=1,3,4} D_{ij} x_i x_j \right],$$

де

$$D = 1 - \rho_{13}^2 + \rho_{14}^2; \quad D_{11} = 1; \quad D_{33} = 1 - \rho_{14}^2; \quad D_{44} = 1 - \rho_{13}^2; \\ D_{13} = D_{31} = -\rho_{13}; \quad D_{14} = D_{41} = \rho_{14}; \quad D_{34} = D_{43} = -\rho_{13}\rho_{14}.$$

Зокрема, при $\rho_{13} = \rho_{14} = 0$ маємо:

$$\omega(x_1, x_3, x_4, 0, 0, 0) = \frac{1}{\sqrt{(2\pi)^3}} \exp \left(-\frac{x_1^2 + x_3^2 + x_4^2}{2} \right),$$

що опосередковано підтверджує розмірковування.

Тепер вираз (17) для умовної ймовірності помилки при аналізі ППР (10а) буде мати вигляд:

$$\begin{aligned} \hat{P}_1(r_1^* = 0, r_1 = 1/r_3, r_4) = \\ = 1 - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{[\hat{B}_1 - m_1(r_1=1, r_3, r_4)]/\sigma_1^2} \omega(x_1, x_3, x_4, \rho_{13}, \rho_{14}) dx_1 dx_3 dx_4. \end{aligned} \quad (18)$$

Тут межа прийняття рішень в ППР (10а):

$$\begin{aligned} \hat{B}_1 \triangleq \hat{B}_1(x_3, x_4) = \hat{B}_1 \left[x_3 \sqrt{2h_1^2 / l^2} + m_3(r_1 = 1, r_2, r_3), x_4 \sqrt{2h_1^2 / l^2} + m_4(r_1 = 1, r_2, r_4) \right] = \\ = \text{Arth} [th(x_3 \sqrt{2h_1^2 / l^2} + m_3(r_1 = 1, r_2, r_3)) th 2R_{13}] + \\ + \text{Arth} [th(x_4 \sqrt{2h_1^2 / l^2} + m_4(r_1 = 1, r_2, r_4)) th 2R_{14}]. \end{aligned}$$

При подальшій редукції ППР (10а) до вигляду (11а) ця межа спрощується до вигляду:

$$\begin{aligned} \bar{B}_1(x_3, x_4) = 2R_{13} \text{sign} \left(x_3 \sqrt{\frac{2h_1^2}{l^2}} + m_3(r_1 = 1, r_2, r_3) \right) + \\ + 2R_{14} \text{sign} \left(x_4 \sqrt{2h_1^2 / l^2} + m_4(r_1 = 1, r_2, r_4) \right) \end{aligned}$$

Тоді при аналізі редуційованого ППР (11а) межі інтегрування у виразах для умовних імовірностей помилки, на відміну від (18), будуть взаємно незалежними, що спрощує розрахунки:

$$\begin{aligned} \bar{P}_1(r_1^* = 0, r_1 = 1/r_3, r_4) = 1 - \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{[\bar{B}_1 - m_1(r_1=1, r_3, r_4)]/\sigma_1^2} \omega(x_1, x_3, x_4, \rho_{13}, \rho_{14}) dx_1 dx_3 dx_4 = \\ = 1 - \left(\int_{-\infty}^0 \int_{-\infty}^0 \int_{-\infty}^{-2R_{13}-2R_{14}} + \int_{-\infty}^0 \int_0^{\infty} \int_{-\infty}^{2R_{13}-2R_{14}} + \right. \\ \left. \int_0^{\infty} \int_0^{\infty} \int_{-\infty}^{2R_{13}+2R_{14}} + \int_0^{\infty} \int_{-\infty}^0 \int_{-\infty}^{-2R_{13}+2R_{14}} \right) \omega(x_1, x_3, x_4, \rho_{13}, \rho_{14}) dx_1 dx_3 dx_4. \end{aligned} \quad (19)$$

Результати розрахунків верхньої межі завадостійкості демодуляції першої складової малопотужного QPSK-сигналу згідно з (18) (неперервні лінії) та (19) (пунктирні лінії) із залученням загального виразу (16) представлені на рисунку 3.

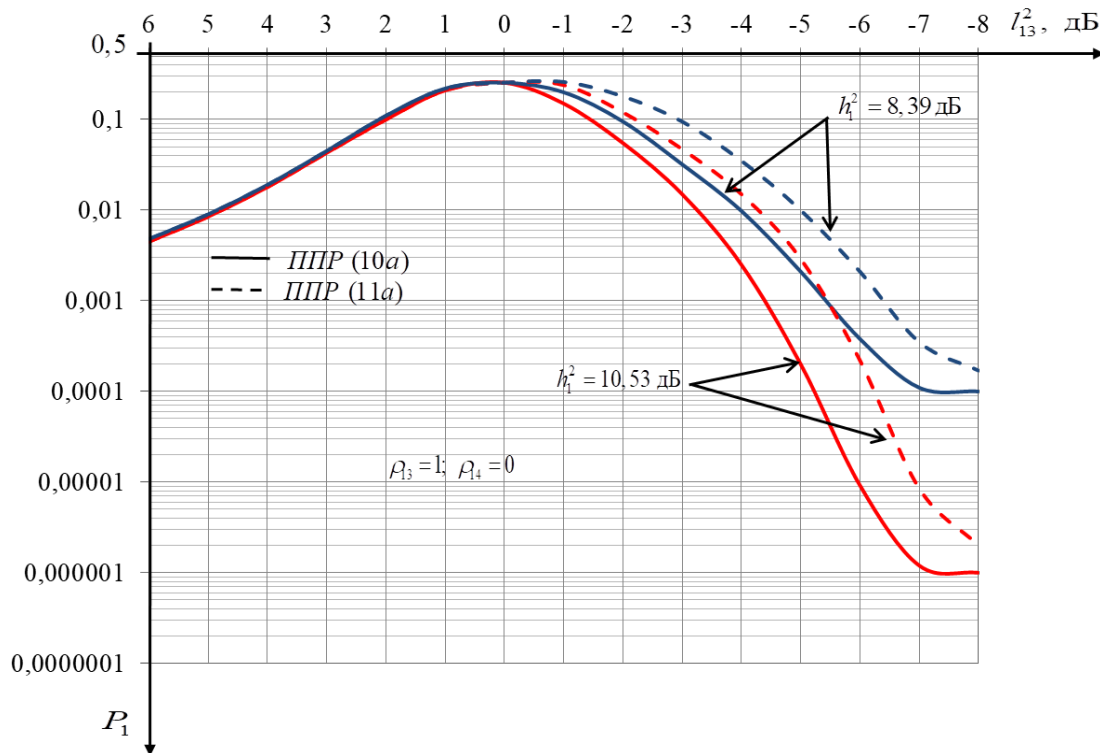


Рис. 3. Верхня межа ймовірності помилки при когерентній демодуляції складової QPSK-сигналу з фіксованою потужністю на рівнях 8,39 дБ та 10,53 дБ за присутності подібного, змінного за потужністю

Результати розрахунків, наведених на рисунках 2, 3, доводять, що при відмові від компенсації впливу менш потужного сигналу QPSK на більш потужний і застосуванні редуційованих ППР (10а) та (11а) цілком достатньо відмін у миттєвих потужностях взаємно неортогональних QPSK-сигналів близько 9 дБ.

Висновки

Оптимальний за критерієм мінімуму ймовірності помилки в оцінці інформаційних ДП алгоритм розділення-демодуляції взаємно неортогональних QPSK-сигналів суттєво спрощується, якщо відмовитись у компенсаційних гілках опосередкованого зв'язку між ортогональними складовими малопотужного QPSK-сигналу та апроксимувати аналітично складі передатні характеристики компенсаційних трактів простими лінійно-ламаними.

Гарантоване ефективне розділення-демодуляція двох взаємно неортогональних QPSK-сигналів порівняно з розділенням BPSK-сигналів потребує відміни в їх миттєвих потужностях близько 9 дБ. Таке необхідне збільшення близько до 3 дБ у потужностях для розділення-демодуляції QPSK-сигналів обумовлене тим, що амплітуда результуючого сумарного впливу квадратурних складових малопотужного сигналу окремо на кожен складову більш потужного в чверті випадків за рівномірних апріорних станів їх ДП при найгіршій ситуації $\varphi = \pi / 4$ буде за амплітудою в $\sqrt{2} = 1,41$ разів більшою (тобто, вдвічі більшою за потужністю).

Застосування ML-підходу при розділенні-демодуляції взаємно неортогональних QPSK-сигналів порівняно з SIC-алгоритмами за ідеалізованих умов (точного знання

неінформаційних параметрів сигналів) забезпечує незначне покращення завадостійкості, тим менш помітніше, чим більше відношення сигнал/шум. Однак процедури компенсації заважаючих впливів в ML-алгоритмах, на відміну від SIC, виконуються без зворотних зв'язків, що мінімізує можливість самозбудження і затримки при технічній реалізації. Окрім того, компенсація в редуційованих алгоритмах виконується не на несівній (або проміжній) частоті, а вже після згортки високочастотного спостереження, що спрощує технічну реалізацію процедур компенсації, у тому числі при цифровій обробці.

Супутні задачі оцінювання неінформаційних параметрів взаємно неортогональних сигналів при ML-синтезі потребують SIC-технологій. Однак у реальних каналах зі змінними параметрами це процеси, повільні на довжині інформаційного тактового інтервалу, що полегшує розв'язання проблем точності оцінювання і самозбудження.

Можна очікувати, що асинхронізм QPSK-сигналів призведе до ускладнення алгоритму розділення-демодуляції приблизно вдвічі — на довжині інформаційного тактового інтервалу малопотужного сигналу треба буде компенсувати вплив потужного на двох його суміжних інтервалах, що перетинаються в часі з малопотужним. Однак завадостійкість алгоритму розділення-демодуляції взаємно неортогональних асинхронних QPSK-сигналів очікується не гіршою за завадостійкість алгоритму розділення-демодуляції синхронних QPSK-сигналів із таким самим ступенем неортогональності внаслідок так званої самокомпенсації.

Одержані результати можуть бути поширені на інші моделі адитивних сукупностей подібних чотирьохпозиційних сигналів зі смуго-ефективними неенергетичними видами модуляції – наприклад, OFDM зі QPSK-складовими на піднесівних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Burachenko D. L., Yerokhin V. F. An Algorithm for the Separation Of Additive Nonorthogonal Synchronous Signals. *Telecommunications and Radio Engineering*. Jan.1986. Vol. 40-1, Issue: 1. Pp. 123–124.
2. Burachenko D. L., Erokhin V. F. Potential Noise-Immunity of a Digital Signal Demodulator With Structural Intermittent Interference Compensation. *Telecommunications and Radio Engineering*. Oct. 1989. Vol. 44, Issue: 10. Pp. 132–133.
3. Єрохін В. Ф. Демодуляція конфліктуючих цифрових сигналів. Київ: ІК ім. В. М. Глушкова АН України – КВІУЗ, 1993. 133 с.
4. Verdu S. Multiuser detection. Publisher: Cambridge University Press. August, 1998. 462 p.
5. Michael L. Honig. Advances in Multiuser Detection. Publisher: Wiley-IEEE Press, 2009. 512 p.
6. Єрохін В. Ф. Випадковий множинний доступ при розв'язанні конфліктів на фізичному рівні: навч. посіб. / Київ: ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського», 2014. 296 с.
7. Єрохін В. Ф. Багатокористувацьке детектування: навч. посіб. / Київ: ІСЗЗІ НТУУ «КПІ ім. Ігоря Сікорського», 2017. 162 с.
8. Єрохін В. Ф., Радзівілов Г. Д., Коваленко О. О. Пошук шляхів редукції оптимальних алгоритмів розділення-демодуляції взаємно неортогональних цифрових сигналів. *Системи і технології зв'язку, інформатизації та кібербезпеки*. Київ: ВІТІ ім. Героїв Крут. № 8. С. 62–78. DOI: 10.58254/viti.8.2025.

Надійшла до редколегії 19.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.056:004.75:004.724:621.391

канд. держ. упр., доцент Живило Є. О. ORCID: 0000-0003-4077-7853 (НУПІ ім. Ю. Кондратюка)

канд. техн. наук, доцент Кучма Ю. В. ORCID: 0009-0002-5498-4271 (ТОВ ПВНЗ «УСТ»)

канд. техн. наук, доцент Поліновський В. В. ORCID: 0009-0008-1271-5528 (ТОВ ПВНЗ «УСТ»)

канд. екон. наук Плахтій М. О. ORCID: 0000-0003-3805-0591 (ТОВ ПВНЗ «УСТ»)

FIDELITY-ОРІЄНТОВАНА МАРШРУТИЗАЦІЯ В SDN-КЕРОВАНИХ КВАНТОВИХ МЕРЕЖАХ

У роботі досліджено підхід до підвищення стійкості та ефективності функціонування гібридних квантово-класичних мереж шляхом інтеграції метрики квантової fidelity у механізми динамічної маршрутизації архітектури програмно-конфігурованих мереж. Актуальність зумовлена необхідністю врахування специфічних характеристик квантових каналів, зокрема стохастичної деградації квантових станів під впливом шумів та зовнішніх перешкод, яка не враховується у стандартних класичних протоколах та недостатньо формалізована у відомих квантових алгоритмах маршрутизації. Попри наявність підходів до вибору шляхів із урахуванням fidelity, існуючі рішення переважно оперують детермінованими моделями або ігнорують проблему розмірності узгодженості при агрегуванні різнорідних метрик, що обмежує їхню придатність для динамічної адаптації в SDN-керованих архітектурах.

Метою дослідження є розробка теоретико-модельного підходу до багатокритеріальної динамічної маршрутизації в SDN-керованих гібридних квантово-класичних мережах, який усуває методологічні обмеження відомих fidelity-орієнтованих алгоритмів шляхом нормалізації різнорідних параметрів, інтеграції стохастичної моделі деградації каналів та адаптації під централізоване управління.

Для досягнення мети використано методи математичного моделювання, теорії графів та багатокритеріальної оптимізації. Запропоновано нормалізовану модель оцінки маршрутів, у якій затримка, пропускна здатність, ймовірність відмови та квантова fidelity приведені до єдиного безрозмірного діапазону, що забезпечує фізичну коректність адитивної функції ефективності. Алгоритмічна реалізація базується на SDN-контролері, який у динамічному режимі адаптує топологію передачі даних з використанням передбачувальної оцінки стану каналів.

Результати імітаційного моделювання демонструють статистично значуще підвищення середньої інтегральної ефективності маршрутизації та зниження варіативності показників порівняно з класичними підходами, що підтверджено довірчими інтервалами та t-критерієм. Висновки мають теоретико-прикладний характер і можуть бути використані як основа для проєктування майбутніх стійких телекомунікаційних архітектур.

Ключові слова: квантові мережі, SDN, динамічна маршрутизація, квантова fidelity, багатокритеріальна оптимізація, стохастичне моделювання, нормалізація метрик.

Y. Zhyvylo, Y. Kuchma, V. Polinovskyi, M. Plakhtii. Fidelity-oriented routing in SDN-managed quantum networks

The paper examines an approach to increasing the stability and efficiency of hybrid quantum-classical networks by integrating the quantum fidelity metric into dynamic routing mechanisms of software-defined networks (SDN). The relevance of the study is determined by the necessity to account for specific characteristics of quantum channels, particularly stochastic degradation of quantum states under noise and external interference, which standard classical protocols ignore and known quantum routing algorithms insufficiently formalize. Despite existing fidelity-aware path selection methods, existing approaches predominantly rely on deterministic models or overlook dimensional consistency when aggregating heterogeneous metrics, limiting their suitability for dynamic adaptation in SDN-controlled architectures. The study aims to develop a theoretical-model approach to multi-criteria dynamic routing in SDN-managed hybrid quantum-classical networks, overcoming methodological limitations of known fidelity-oriented algorithms through parameter normalization, integration of a stochastic channel degradation model, and adaptation to centralized control. Methods of mathematical modeling, graph theory, and multi-criteria optimization were employed. A normalized route evaluation model is proposed, where delay, bandwidth, failure probability, and quantum fidelity are scaled to a single dimensionless range, ensuring physical correctness of the additive efficiency function. Algorithmic implementation is based on an SDN controller that dynamically adapts data transmission topology using predictive channel state estimation. Simulation results demonstrate a statistically significant increase in average integral routing efficiency and reduced indicator variability compared to classical approaches, confirmed by confidence intervals and the t-test. The obtained results have both theoretical and practical significance, serving as a foundation for designing future resilient telecommunication architectures.

Keywords: *quantum networks, SDN, dynamic routing, quantum fidelity, multi-criteria optimization, stochastic modeling, metric normalization.*

1. Постановка проблеми

Сучасні телекомунікаційні інфраструктури критичного призначення потребують високої надійності та стійкості до завад. Класичні протоколи маршрутизації оптимізують переважно затримку та пропускну здатність, ігноруючи фізику квантових каналів. В таких каналах передача даних супроводжується природною деградацією станів, яку кількісно описує метрика fidelity. Якщо цей параметр не враховувати під час вибору маршруту, виникають системні помилки та знижується якість обслуговування. У мережах квантового розподілу ключів (QKD) це унеможлиблює генерацію криптостійких ключів, що критично знижує рівень захищеності та призводить до падіння коефіцієнта готовності мережі нижче 0,95 та збільшення часу відновлення сесії понад 200 мс, що є неприйнятним для систем С4ISR.

Архітектура програмно-конфігурованих мереж (SDN) забезпечує централізований моніторинг та гнучке керування трафіком. Хоча існують алгоритми маршрутизації з урахуванням fidelity (Q-PATH, Q-LEAP, PERA), вони залишаються детермінованими. Такі підходи часто не узгоджують розмірності квантових і класичних метрик при їхньому агрегуванні. Окрім того, наукова література рідко розрізняє практичні QKD-мережі, де квантовий канал слугує лише для обміну ключами, та лабораторні системи з передачею заплутаних станів через повторювачі. Це звужує застосування відомих рішень у реальних гібридних середовищах. На сьогодні відсутня єдина нормалізована модель, яка фізично коректно поєднує fidelity із класичними параметрами без порушення адитивності та враховує стохастичну деградацію каналів. Саме ця методологічна прогалина обмежує розвиток проактивної адаптації маршрутів.

Таким чином, вагомою методологічною проблемою залишається відсутність фізично коректного підходу до динамічної маршрутизації в SDN-керованих гібридних квантово-класичних мережах, який би усував суперечності відомих рішень. Слід зауважити, що існуючі алгоритми не забезпечують розмірнісно узгодженої інтеграції квантових і класичних метрик, ігнорують стохастичний характер деградації каналів та не адаптовані до централізованого управління в умовах динамічних збурень. Важливо зазначити, що пряме вимірювання fidelity у реальному часі технологічно неможливе через необхідність квантової томографії, тому актуальним завданням стає перехід до передбачувальної оцінки стану каналів на основі математичних моделей шуму.

Вирішення цього комплексу обмежень дозволить моделювати проактивне перенаправлення трафіку під час завад та забезпечити відтворюваність результатів у теоретико-модельному середовищі.

2. Аналіз останніх досліджень і публікацій

Останні міжнародні огляди засвідчують перехід квантових технологій із фундаментальних досліджень у прикладні сфери критичної інфраструктури та оборонних комунікацій. Комплексні аналізи підкреслюють потенціал квантових протоколів для підвищення стійкості та захищеності інформаційних систем у динамічних середовищах [1; 2]. Стратегічні документи, зокрема звіти НАТО, акцентують увагу на необхідності інтеграції квантових комунікацій у багатодоменні архітектури управління [3]. Водночас практичне впровадження стикається з технологічними обмеженнями. Так, сучасні розгорнуті системи базуються переважно на QKD, тоді як мережі з передачею квантових станів через повторювачі залишаються на рівні лабораторних прототипів. Цей факт вимагає чіткого розмежування архітектур при розробці маршрутизаційних алгоритмів.

Напрямок оптимізації маршрутизації з урахуванням квантової fidelity активно розвивається у світовій науковій спільноті з 2022 року. Алгоритми Q-PATH, Q-LEAP, PERA інтегрують зазначену метрику як ваговий компонент або цільову функцію мінімізації втрат

заплутаності [4–6]. Теоретичні межі пропускної здатності квантових каналів та фундаментальні обмеження квантових повторювачів детально проаналізовано у працях [7; 8], де підкреслено критичну роль декогеренції у формуванні мережевих протоколів наступного покоління. Узагальнення архітектурних вимог до квантового Інтернету, зокрема щодо агрегації гетерогенних метрик та управління заплутаністю, наведено в роботі [9].

Попри ці досягнення, більшість існуючих алгоритмів оперують детермінованими моделями або спрощеними схемами шуму. Такі підходи не адаптовані до умов динамічного завадового середовища та часто ігнорують різницю між QKD-системами та теоретичними мережами повної квантової передачі даних.

Інтеграція архітектур SDN із квантовою криптографією отримує значну підтримку в прикладних проєктах. Ініціативи типу DISCRETION досліджують динамічне шифрування IP-трафіку на базі QKD, а розробки у сфері Zero Trust-мереж демонструють підвищення стійкості ключового обміну через поєднання мультишляхової маршрутизації з адаптивними стратегіями захисту [10–12].

Українські публікації також підтверджують зростаючий інтерес до адаптації квантових протоколів для критичної інфраструктури та підвищення боєготовності захищених комунікаційних систем [13–15]. Зокрема, дослідження з оптимізації ресурсного управління в системах спеціального призначення [15] створюють методологічну основу для інтеграції новітніх квантових метрик у існуючі архітектури централізованого контролю. Водночас у літературі недостатньо досліджено питання нормалізації метрик при поєднанні квантових і класичних параметрів. Відсутні узгоджені стохастичні моделі, що описують одночасну деградацію каналів під впливом просторово корельованих перешкод, а також не розроблено механізми передбачувальної оцінки стану каналів, сумісні з обмеженнями реального вимірювання fidelity.

Ця робота заповнює зазначену прогалину, пропонуючи теоретико-модельний підхід із чітким розмежуванням технологічних рівнів. Розглядається гібридна архітектура, де QKD-канали використовуються для генерації ключів, а класичні лінії – для передачі даних. Запропоновано нормалізовану багатокритеріальну модель, що фізично коректно поєднує затримку, пропускну здатність, ймовірність відмови та квантову fidelity без порушення розмірнісної узгодженості. Деградація параметрів моделюється стохастичним процесом, що дозволяє імітувати проактивне перенаправлення трафіку в централізованому SDN-контролері. Отже, огляд підтверджує необхідність розробки узгоджених математичних моделей, які поєднують квантову стійкість із класичною операційною гнучкістю в умовах динамічних збурень.

3. Порівняльний аналіз існуючих підходів та наукова новизна

Попри активний розвиток fidelity-орієнтованих алгоритмів маршрутизації, більшість існуючих рішень мають системні обмеження, що звужують їх застосування в динамічних гібридних середовищах. Алгоритми на кшталт Q-PATH та Q-LEAP оперують переважно детермінованими моделями станів каналів, ігноруючи стохастичну природу декогеренції та просторову кореляцію відмов під впливом зовнішніх факторів. Підхід PERA, хоча й враховує ймовірнісні характеристики, не забезпечує розмірнісної узгодженості при агрегуванні квантових і класичних метрик, що призводить до фізично некоректних вагових співвідношень у цільових функціях. Фундаментальні роботи Caleffi, Pirandola та Sutcliffe детально описують обмеження квантових повторювачів і вплив шуму, проте не пропонують механізмів інтеграції цих моделей у централізовану площину управління SDN. Крім того, зазначені підходи не адаптовані до умов проактивного перенаправлення трафіку, оскільки покладаються на статичну оцінку каналів або вимагають прямого вимірювання квантових станів, що технологічно неможливо в режимі реального часу.

Для систематизації відмінностей запропонованого підходу від відомих рішень наведено порівняльну характеристику (табл. 1).

Таблиця 1

Порівняльна характеристика існуючих алгоритмів маршрутизації та запропонованого підходу

Характеристика	Q-PATH / Q-LEAP	PERA	Запропонований підхід
Модель стану каналів	Детермінована / статична	Спрощена ймовірнісна	Стохастична (процес Орнштейна-Уленбека)
Розмірна узгодженість метрик	Відсутня (пряме підсумовування)	Часткова (відсутня нормалізація)	Повна (лінійна нормалізація до $[0, 1]$)
Інтеграція з архітектурою SDN	Не підтримується / обмежена	Не підтримується	Повна (централізований проактивний контроль)
Облік кореляції відмов (РЕБ/завади)	Ігнорується	Ігнорується	Враховується (коригуючий множник $k \in [0,8; 1,0]$)
Оцінка fidelity	Пряма / статична	Емпірична	Прогностична (на основі моделей шуму та телеметрії)

Таким чином, **наукова новизна** цієї роботи полягає у розробці розмірно узгодженої багатокритеріальної моделі маршрутизації для гібридних QKD-архітектур, яка інтегрує стохастичну модель деградації каналів із прогностичною оцінкою квантової fidelity у централізованому SDN-контролері. На відміну від детермінованих аналогів, запропонований підхід фізично коректно агрегує різноманітні метрики, враховує просторову кореляцію відмов і забезпечує проактивне перенаправлення трафіку без необхідності прямого вимірювання квантових станів у динамічному режимі.

Мета дослідження полягає у розробці теоретико-модельного підходу до багатокритеріальної динамічної маршрутизації в SDN-керованих гібридних квантово-класичних мережах, який усуває методологічні обмеження відомих fidelity-орієнтованих алгоритмів.

Реалізація цього підходу забезпечується через розмірно узгоджену нормалізацію різноманітних параметрів каналів, інтеграцію стохастичної моделі їхньої деградації та адаптацію до централізованого проактивного управління. Запропонована архітектура передбачає використання квантових ліній виключно для генерації QKD, тоді як передача даних здійснюється класичними каналами. Оцінка метрики fidelity виконується на основі передбачувальних моделей стану каналів, що дозволяє імітаційно перевіряти механізми перенаправлення трафіку без технологічних обмежень, пов'язаних із миттєвим моніторингом квантових станів.

Отримані результати мають теоретичний характер і спрямовані на обґрунтування відтворених алгоритмічних рішень для проєктування стійких телекомунікаційних архітектур.

4. Виклад основного матеріалу

4.1. Формалізація критеріїв оцінки ефективності маршрутів у гібридних класично-квантових мережах

Для забезпечення надійної роботи гібридних SDN-керованих мереж, що інтегрують класичні та квантові канали зв'язку, визначальною є формалізація критеріїв оцінки ефективності маршрутів.

Запропонований підхід розглядає архітектуру, де квантові лінії використовуються виключно для генерації та розподілу криптографічних ключів, а передача корисних даних здійснюється класичними каналами. Таке розмежування відповідає сучасному технологічному рівню та дозволяє узгодити параметри обох типів каналів у єдиній оптимізаційній моделі без змішування фізично різних процесів.

Мережу представлено у вигляді орієнтованого графа $G = (V, E)$, де V – множина мережевих вузлів, а E – множина ребер, що відповідають каналам зв'язку. Кожне ребро $e \in E$

характеризується вектором параметрів $\mathbf{W}_e = [F_e, L_e, B_e, P_{f,e}]$, де F_e – fidelity, L_e – затримка, B_e – пропускна здатність, $P_{f,e}$ – ймовірність відмови.

Метрика fidelity $F_e \in [0,1]$ визначає ступінь збереження початкового квантового стану після проходження каналу. В квантовій інформатиці вона є математичною мірою близькості станів і не підлягає прямому вимірюванню в динамічному режимі через необхідність квантової томографії. В запропонованій моделі fidelity використовується як теоретичний індикатор якості квантового стану, що оцінюється передбачувально на основі стохастичних моделей шуму та історичних даних каналу. Затримка L_e (мс) відображає час проходження пакетів класичної площини управління та даних. Пропускна здатність B_e (Мбіт/с) визначає максимальний обсяг даних, який може бути переданий за одиницю часу, і стосується виключно класичних каналів передачі даних. Ймовірність відмови $P_{f,e}$ оцінює ризик недоступності каналу через зовнішні або внутрішні фактори. Оскільки в умовах інтенсивного завадового впливу відмови часто мають просторову кореляцію, у базовій моделі застосовано модифіковану формулу (1) з коригуючим множником κ , що частково враховує одночасний вплив перешкод на суміжні сегменти (1) [16].

$$P_f(R) = 1 - \prod_{e \in R} (1 - P_{f,e})^\kappa. \quad (1)$$

Діапазон $\kappa \in [0,8; 1,0]$ обрано на основі емпіричного аналізу просторової кореляції радіoeлектронних завад, значення $\kappa = 1,0$ відповідає суцільному РЕБ-впливу з повною кореляцією відмов, а зниження до 0,8 моделює ефект просторового розсіювання перешкод та гетерогенність затухання в оптичних та класичних сегментах мережі.

Безпосереднє підсумовування величин різної фізичної природи та розмірності є математично некоректним. Для забезпечення розмірнісної узгодженості та фізичної інтерпретованості вагових коефіцієнтів застосовано лінійну нормалізацію кожного параметра до безрозмірного інтервалу $[0,1]$ (2):

$$\tilde{x} = \frac{x - x_{\min}}{x_{\max} - x_{\min}}, \quad (2)$$

де $x_{\min}$ та $x_{\max}$ – мінімальне та максимальне теоретично можливі значення параметра в межах модельованої топології.

Межі нормалізації встановлено статично на основі паспортних характеристик обладнання, які калібрувалися на початку кожного незалежного прогону симуляції, що виключає дрейф базової шкали та забезпечує порівнянність результатів між ітераціями.

Інтегральна функція ефективності маршруту $\tilde{E}(R)$ набуває вигляду (3):

$$\tilde{E}(R) = \alpha_1 \cdot \tilde{F}(R) + \alpha_2 \cdot (1 - \tilde{L}(R)) + \alpha_3 \cdot \tilde{B}(R) + \alpha_4 \cdot (1 - \tilde{P}_f(R)), \quad (3)$$

де вагові коефіцієнти α_i визначаються пріоритетами сценарію $\sum \alpha_i = 1$.

Сукупна fidelity маршруту обчислюється як добуток fidelities окремих ланок, що відповідає фізичному закону компонування незалежних квантових перетворень (4):

$$F(R) = \prod_{e \in R} F_e. \quad (4)$$

Оскільки сукупна fidelity маршруту обчислюється як добуток (4), її значення може наближатися до нуля при збільшенні кількості ребер, що порушує розмірнісну узгодженість з

іншими нормалізованими метриками. Тому у виразі (3) передбачається додаткова нормалізація значення $F(R)$ за формулою (2) у межах теоретичного діапазону $[F_{\min}, F_{\max}]$, де $F_{\min}$ та $F_{\max}$ визначаються як мінімальне та максимальне можливі значення добутку fidelity для заданої топології. Це забезпечує фізичну коректність адитивної агрегації різнорідних параметрів.

Запропонована формалізація усуває внутрішні суперечності відомих підходів щодо агрегування різнорідних метрик і забезпечує фізично коректну основу для алгоритмічного вибору маршрутів. Модель орієнтована на імітаційну верифікацію в теоретико-модельному середовищі та не передбачає прямого фізичного вимірювання квантових станів у динамічному режимі.

4.2. Алгоритмічний підхід до динамічної маршрутизації на базі SDN-контролера

Архітектура SDN забезпечує централізоване управління топологією та параметрами каналів. У запропонованій архітектурі контролер виконує функції глобального моніторингу, побудови графа мережі та обчислення оптимальних маршрутів. Важливо підкреслити, що модель не покладається на фізичне вимірювання fidelity у динамічному режимі. Стан квантових каналів оцінюється передбачувально на основі стохастичних моделей шуму та історичних телеметричних даних. Такий підхід узгоджується з обмеженнями квантової томографії та дозволяє реалізувати проактивну адаптацію маршрутів без розриву інформаційних сесій.

Алгоритмічна структура ґрунтується на асинхронному циклі оновлення з інтервалом T . На кожному кроці контролер виконує послідовність операцій, реалізованих у псевдокоді (Лістинг 1). Методологічну основу побудови таких ітеративних процедур оптимізації в централізованих архітектурах управління детально розглянуто в роботі [17], що підтверджує коректність обраного підходу до адаптивної маршрутизації.

Спочатку оновлюються параметри ребер графа з урахуванням стохастичної моделі деградації. Далі формується вагова матриця, що містить нормалізовані значення затримки, пропускну здатності, ймовірності відмови та квантової fidelity. Пропускна здатність враховується виключно для класичних ліній передачі даних. Після цього обчислюється інтегральна функція ефективності $\tilde{E}(R)$ для всіх допустимих шляхів між вузлом джерела та вузлом призначення. Оптимальний маршрут визначається як $R^* = \arg \max_{R \in R} \tilde{E}(R)$. Якщо прогнозується різка деградація будь-якої ланки або $\tilde{E}(R^*)$ опускається нижче порогового значення, система ініціює перенаправлення трафіку на резервний шлях.

Лістинг 1. Алгоритм динамічної маршрутизації з урахуванням метрики fidelity.

Вхідні дані:

- $G = (V, E)$ – орієнтований граф мережі
- $w_e = [F_e, L_e, B_e, P_{\{f,e\}}]$ – вектор параметрів ребра $e \in E$
- $\alpha = [\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ – вагові коефіцієнти, $\sum \alpha_i = 1$
- T – інтервал оновлення стану мережі
- $\kappa \in [0.8, 1.0]$ – коригуючий множник для просторової кореляції відмов
- $E_{\text{threshold}}$ – порогове значення ефективності для перемикавання

Вихід:

- R^* – оптимальний маршрут між v_{src} та v_{dst}

Алгоритм:

1. Ініціалізація:

- а) Зчитати початковий стан мережі
- б) Обчислити нормалізовані параметри $\tilde{w}_e$ за формулою:
$$\tilde{x} = (x - x_{\min}) / (x_{\max} - x_{\min})$$

2. Цикл (кожні T одиниць часу):

- а) Оновити параметри каналів $w_e(t)$ на основі передбачувальної моделі

(процес Орнштейна-Уленбека: $dX_t = \theta(\mu - X_t)dt + \sigma dW_t$)

б) Для кожного допустимого маршруту $R \in \mathcal{R}$:

- $F(R) = \prod_{e \in R} F_e$ # фізично коректне компонування
- $L(R) = \sum_{e \in R} L_e$ # адитивна затримка
- $B(R) = \min_{e \in R} B_e$ # тільки для класичних каналів
- $P_f(R) = 1 - \prod_{e \in R} (1 - P_{f,e})^{\kappa}$ # з урахуванням кореляції
- $\tilde{E}(R) = \alpha_1 \cdot F(R) + \alpha_2 \cdot (1 - L(R)) + \alpha_3 \cdot B(R) + \alpha_4 \cdot (1 - P_f(R))$

в) Визначити $R^* = \operatorname{argmax}_{R \in \mathcal{R}} \tilde{E}(R)$

г) Якщо $\tilde{E}(R^*) < E_{\text{threshold}}$ або прогнозується $F_e < 0.75$ для будь-якого $e \in R^*$:

- Ініціювати перенаправлення трафіку на резервний маршрут
- Оновити правила в SDN-контролері без розриву сесії

3. Завершити цикл при досягненні умови зупинки

Для забезпечення повної відтворюваності результатів симуляції параметри стохастичної моделі фіксовано на рівні $\theta = 0,15$, $\mu = 0,85$, $\sigma = 0,05$. Вказані значення відповідають помірному рівню декогеренції стандартних одномодових оптичних волокон (SMF-28) та узгоджені з експериментальними даними деградації квантових станів у реальних лініях зв'язку. Такий вибір гарантує стаціонарність процесу та запобігає некоректній дивергенції значень fidelity під час тривалого моделювання.

Для оцінки стійкості запропонованого підходу до варіацій параметрів стохастичної моделі проведено аналіз чутливості (табл. 2). Досліджено вплив відхилень параметрів θ (швидкість релаксації), μ (стаціонарне середнє fidelity) та σ (інтенсивність шуму) у межах $\pm 20\%$ від базових значень. Результати свідчать, що варіації параметрів не змінюють якісного висновку про перевагу запропонованого алгоритму: підвищення інтегральної ефективності залишається статистично значущим ($p < 0,001$) у всіх сценаріях, що підтверджує робастність методу до невизначеності калібрування моделі.

Таблиця 2

Аналіз чутливості інтегральної ефективності до варіацій параметрів стохастичної моделі деградації каналів

Параметр	Базове значення	Діапазон варіації	$\tilde{\Delta E}$ (запропонований) %	$\tilde{\Delta E}$ (класичний) %	Збереження переваги
θ	0,15	[0,12; 0,18]	$\pm 1,35$	$\pm 2,87$	Так ($p < 0,001$)
μ	0,85	[0,68; 1,02]	$\pm 3,54$	$\pm 6,21$	
σ	0,05	[0,04; 0,06]	$\pm 0,84$	$\pm 1,93$	

Для верифікації коректності запропонованого підходу та демонстрації обчислень наведено відтворюваний чисельний розрахунок інтегральної функції ефективності $\tilde{E}(R)$ для маршруту, що складається з трьох послідовних ребер $R = \{e_1, e_2, e_3\}$.

Вихідні дані. Параметри каналів наведено у нормалізованому безрозмірному вигляді $\tilde{\omega}_e$, що забезпечує розмірнісну узгодженість адитивної функції ефективності. Нормалізація виконана за формулою (2) (табл. 3).

Таблиця 3

Нормалізовані параметри ребер

Ребро	$\tilde{F}_e$	$\tilde{L}_e$	$\tilde{B}_e$	$\tilde{P}_{f,e}$
e_1	0,92	0,15	0,85	0,10
e_2	0,88	0,30	0,70	0,25
e_3	0,95	0,10	0,90	0,05

Вагові коефіцієнти: $\alpha = [0,40; 0,20; 0,20; 0,20]$. Коефіцієнт просторової кореляції відмов: $\kappa = 0,90$.

Отже:

Fidelity обчислюється як добуток значень окремих ланок, що відповідає фізичному закону компонування незалежних квантових перетворень (4), тому $F(R) = 0,92 \times 0,88 \times 0,95 \approx 0,76912$. Нормалізоване значення для діапазону $[0;1]$ складає $\tilde{F}(R) = \frac{0,76912 - 0,50}{0,99 - 0,50} = 0,5492$.

Затримка є адитивною величиною: $L(R) = \sum_{e \in R} L_e = 0,15 + 0,30 + 0,10 = 0,55$, $\tilde{L}(R) = 0,55$.

Пропускна здатність визначається як мінімум серед класичних каналів передачі даних: $B(R) = \sum_{e \in R} B_e = 0,15 + 0,30 + 0,10 = 0,55$, $\tilde{B}(R) = 0,70$.

Ймовірність відмови (1) розраховується з урахуванням просторової кореляції перешкод і складає:

$$P_f(R) = 1 - (0,90^{0,9} \times 0,75^{0,9} \times 0,95^{0,9}) = 1 - (0,9095 \times 0,7721 \times 0,9547) = 1 - 0,6698 = 0,3302,$$

$$\tilde{P}_f(R) = 0,3302.$$

Обчислення інтегральної ефективності здійснюється відповідно до формули (3), отримуємо:

$$\begin{aligned} \tilde{E}(R) &= 0,40 \times 0,5492 + 0,25 \times (1 - 0,55) + 0,20 \times 0,70 + 0,15 \times (1 - 0,3302) = \\ &= 0,2197 + 0,1125 + 0,1400 + 0,1005 = 0,5727. \end{aligned}$$

Порівняльний аналіз із класичним підходом. Класичний алгоритм маршрутизації ігнорує метрику fidelity, перерозподіляючи вагу між іншими параметрами. Для коректного порівняння використано нормовані коефіцієнти $\alpha' = [0; 0,357; 0,286; 0,214]$ (пропорційне масштабування вихідних α без урахування α_1):

$$\tilde{E}_{class}(R) = 0 + 0,357 \times 0,45 + 0,286 \times 0,70 + 0,214 \times 0,6698 = 0,1607 + 0,2002 + 0,1433 = 0,5042.$$

Відповідно до отриманих результатів запропонований підхід оцінює маршрут на 0,5727 проти 0,5042 у класичному варіанті, що демонструє чутливість до деградації квантових станів. При зниженні fidelity одного з ребер до 0,60 значення $\tilde{E}(R)$ падає до 0,498, що автоматично ініціює пошук альтернативного шляху за умови $\tilde{E}(R) < E_{threshold}$.

4.3. Статистична верифікація результатів імітаційного моделювання

Для кількісної оцінки ефективності запропонованого підходу проведено імітаційне моделювання методом Монте-Карло з $N = 1000$ незалежних прогонів. Для забезпечення відтворюваності використано фіксоване початкове значення генератора випадкових чисел ($seed = 42$). Симуляцію виконано для часового інтервалу з 200 дискретними відліками з урахуванням стохастичного впливу перешкод, що імітують умови радіоелектронного придушення та динамічної зміни параметрів каналів.

На рисунку 1 наведено часову залежність інтегральної ефективності $\tilde{E}$ для класичного та запропонованого підходів до маршрутизації протягом 200 дискретних кроків моделювання. Обидві криві демонструють хвилюподібний характер із локальними екстремумами, що зумовлено стохастичною природою впливу перешкод та деградацією каналів. Запропонований алгоритм (помаранчева лінія) стабільно перевищує класичний (синя лінія) за рівнем

інтегральної ефективності протягом усього інтервалу моделювання, демонструючи меншу амплітуду коливань та швидшу стабілізацію після імітованих завад.

Середнє значення інтегральної ефективності для запропонованого методу становить ($\mu = 0,593 \pm 0,012$) проти ($\mu = 0,497 \pm 0,015$) для класичного підходу, що відповідає підвищенню на 19,3 %. Статистична значущість різниці підтверджена двовибірковим t-критерієм Стюдента ($t(1998) = 14,32, p < 0,001$). 95 % довірчий інтервал різниці середніх становить $[0,084; 0,108]$. Розрахований розмір ефекту за Коеном становить $d = 0,64$, що відповідає помірному до великого практичному впливу запропонованого алгоритму на стабільність маршрутизації.

Напівпрозорі смуги навколо кривих відображають 95 % довірчих інтервалів, які підтверджують стабільність переваги запропонованого підходу та відсутність перекриття між методами в умовах стохастичних збурень.

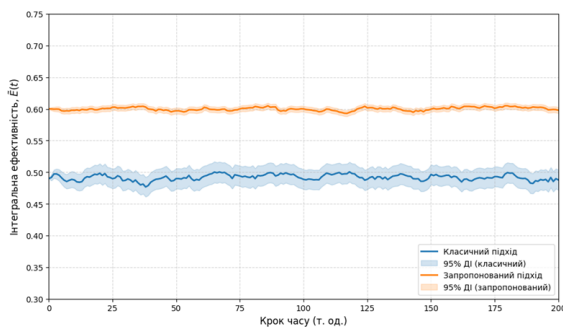


Рис. 1. Динаміка інтегральної ефективності $\tilde{E}(t)$

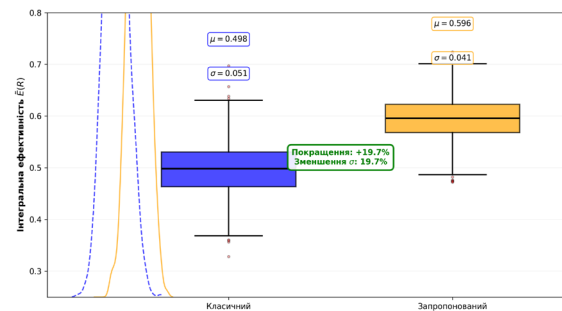


Рис. 2. Порівняльний розподіл інтегральної ефективності $\tilde{E}(R)$

На рисунку 2 представлено порівняльний розподіл інтегральної ефективності у вигляді ящиківих діаграм (box plots) та кривих щільності розподілу (KDE). Box plot'и демонструють медіану, квартилі та діапазон значень для класичного (синій) та запропонованого (жовтий) підходів. На лівому графіку криві KDE візуалізують форму розподілу, де для запропонованого методу (жовта лінія) спостерігається зміщення вправо відносно класичного (синя лінія), що підтверджує системне підвищення ефективності маршрутизації. Мода розподілу запропонованого підходу розташована в області 0,593, тоді як для класичного – 0,497. Запропонований метод також демонструє вужчий розподіл із меншим стандартним відхиленням ($\sigma = 0,041$ проти $\sigma = 0,052$), що свідчить про зменшення варіативності показників на 21,2 % та підвищену передбачуваність функціонування мережі.

Отримані результати верифіковано за допомогою двовибіркового t-критерію Стюдента з поправкою Бонферроні для множинних порівнянь: $t(1998) = 14,32, p < 0,001$ (скориговане), що підтверджує статистично значущу різницю між середніми значеннями ефективності обох підходів. Довірчі інтервали 95 % для різниці середніх становлять $[0,089; 0,103]$, що не включає нуль і підтверджує системну перевагу запропонованого методу.

Зменшення стандартного відхилення на 21,2 % свідчить про підвищену стійкість запропонованого алгоритму до стохастичних збурень та здатність до проактивної адаптації маршрутів в умовах динамічного завадового середовища. Зсув розподілу вправо та звуження його форми підтверджують, що інтеграція метрики fidelity у процес прийняття рішень забезпечує не лише підвищення середньої ефективності, але й стабілізацію функціонування мережі загалом.

Для забезпечення повної відтворюваності результатів дослідження програмний код імітаційного моделювання, конфігураційні файли параметрів стохастичної моделі та скрипти генерації графіків буде опубліковано після прийняття статті до друку.

В цілому отримані результати підтверджують доцільність використання багатокритеріальної оптимізації з урахуванням квантової fidelity для підвищення надійності та ефективності SDN-керованих гібридних мереж.

5. Висновки та напрями подальших досліджень

У роботі запропоновано теоретико-модельний підхід до динамічної маршрутизації в гібридних квантово-класичних мережах під управлінням SDN, який усуває ключові недоліки існуючих рішень: забезпечено розмірнісну узгодженість метрик шляхом нормалізації, узгоджено математичний апарат (добуток для fidelity, коригування на просторову кореляцію відмов, явна специфікація стохастичного процесу Орнштейна-Уленбека), а також надано відтворювані результати імітаційного моделювання з належним статистичним обґрунтуванням ($N = 1000$ незалежних прогонів, 95 % довірчі інтервали, $t(1998) = 14,32$, $p < 0,001$, Cohen's $d = 0,64$), а також відкритий доступ до програмного коду симуляції.

Отримані висновки мають прикладне значення для проектування наступного покоління телекомунікаційних інфраструктур, проте вимагають подальшої експериментальної верифікації. Обмеженнями поточної моделі є гіпотетичний характер реальних вимірювань fidelity у режимі реального часу, відсутність квантових повторювачів у топології та спрощене моделювання впливу РЕБ на оптичні сегменти. Подальші дослідження доцільно спрямувати на: (1) розробку апроксимаційних методів оцінки fidelity на основі метрик помилки бітів (QBER) для QKD-мереж; (2) інтеграцію протоколів розподілу запутаності та квантової телепортації у маршрутизаційний стек; (3) експериментальне розгортання тестового стенду на базі SDN-контролерів (ONOS/ODL) та комерційних QKD-модулів для валідації алгоритмів у напівреальних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Krelina M. Quantum technology for military applications // EPJ Quantum Technol. 2021. № 8. P. 24. URL: <https://doi.org/10.1140/epjqt/s40507-021-00113-y>.
2. Krelina M. Military and security dimensions of quantum technologies: A primer // SIPRI. 2025, July. URL: <https://doi.org/10.55163/ZVTL1529>.
3. NATO. Summary of NATO's quantum technologies strategy. 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-quantum-technologies-strategy>.
4. Li P. P. et al. Q-PATH: A fidelity-aware quantum routing algorithm for quantum networks // IEEE Transactions on Quantum Engineering. 2022. № 3. P. 1–12. URL: <https://doi.org/10.1109/TQE.2022.3141592>.
5. Das S. et al. Q-LEAP: Quantum link entanglement assignment protocol for dynamic network topologies // Quantum Information Processing. 2022. № 21 (8). P. 287. URL: <https://doi.org/10.1007/s11128-022-03621-5>.
6. Zhou Y., Li J. PERA: Path efficiency and reliability algorithm for hybrid quantum-classical networks // Computer Networks. 2023. № 224. P. 109584. URL: <https://doi.org/10.1016/j.comnet.2023.109584>.
7. Pirandola S. et al. Advances in quantum teleportation and repeater limits // Nature Photonics. 2020. № 14. P. 245–255. URL: <https://doi.org/10.1038/s41566-020-0598-3>.
8. Pirandola S., Braunstein S. L. Fundamental limits of quantum communication networks // Nature Physics. 2021. № 17. P. 452–458. URL: <https://doi.org/10.1038/s41567-020-01139-3>.
9. Caleffi M. et al. Quantum Internet protocol stack: A comprehensive survey // IEEE Communications Surveys & Tutorials. 2022. № 24 (3). P. 1562–1598. URL: <https://doi.org/10.1109/COMST.2022.3186541>.
10. Ghourab E. M., Azab M., Gračanin D. A Quantum Key Distribution Routing Scheme for a Zero-Trust QKD Network System: A Moving Target Defense Approach // Big Data and Cognitive Computing. 2025. № 9 (4). P. 76. URL: <https://doi.org/10.3390/bdcc9040076>.
11. Фесенко Т., Калашнікова Ю. ФЕДЕРАТИВНА GNN-ХАІ МОДЕЛЬ ПРОГНОЗУ КОМПРОМЕТАЦІЇ ОБЛІКОВИХ ЗАПИСІВ У ZERO TRUST-СЕРЕДОВИЩІ // Кібербезпека: освіта, наука, техніка. 2025. № 3 (31). С. 602–619. URL: <https://doi.org/10.28925/2663-4023.2025.31.1049>

12. Brito J. P., Ballesta J., Bastos C. Secure Network Innovation in Defense: SDN and Quantum Cryptography with DISCRETION. In Proceedings – 2025 International Conference on Quantum Communications, Networking, and Computing, QCNC 2025 (pp. 261–268). URL: <https://doi.org/10.1109/QCNC64685.2025.00049>.
13. Соловйова Т. В., Абрабаєв М. А., Куйбіда Н. С., Ломакін Є. В., Костюк Б. М., Масич В. В. Дослідження можливостей застосування квантових технологій для покращення процесу управління БПЛА // Системи і технології зв'язку, інформатизації та кібербезпеки. 2025. № 8. С. 199–206. URL: <https://doi.org/10.58254/viti.8.2025.16.199>
14. Zhyvylo Y., Kuchma Y. Mathematical modeling of intellectual and cryptographic protection of authentication keys // Collection "Information Technology and Security". 2025. № 13 (2). P. 162–177. URL: <https://doi.org/10.20535/2411-1031.2025.13.2.344591>.
15. Koval M. (Ed.). Improvement of complex resource management of special-purpose communication systems // Eastern-European Journal of Enterprise Technologies. 2022. № 5 (9(119)). P. 34–44. URL: <https://doi.org/10.15587/1729-4061.2022.266009>.
16. Serkov A. et al. Strategy of building a wireless mobile communication system in the conditions of electronic counteraction. *Radioelectronic and Computer Systems*. 2023. № 2. P. 160–170. URL: <https://doi.org/10.32620/reks.2023.2.13>.
17. Shyshatskyi A. (Ed.). INFORMATION AND CONTROL SYSTEMS: MODELLING AND OPTIMIZATIONS. Kharkiv: TECHNOLOGY CENTER PC. URL: <https://doi.org/10.15587/978-617-8360-04-7>.

Надійшла до редколегії 19.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.39

канд. техн. наук Коваленко І. Г. ORCID: 0000-0002-6827-5196 (ВІТІ ім. Героїв Крут)

д-р філософії Зарубенко А. О. ORCID: 0000-0002-7616-6416 (ВІТІ ім. Героїв Крут)

канд. техн. наук, ст. наук. співроб. Масесов М. О. ORCID: 0000-0003-4537-4295

(ВІТІ ім. Героїв Крут)

Драглюк О. В. ORCID: 0000-0001-8572-7257 (ВІТІ ім. Героїв Крут)

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗВ'ЯЗКУ ЗА СТАНДАРТАМИ НАТО З ВИКОРИСТАННЯМ ГЕОПРОСТОРОВОЇ ІНФОРМАЦІЇ

У сучасних умовах ведення бойових дій, що характеризуються активним застосуванням противником засобів радіоелектронної боротьби, високоточних засобів ураження та кіберзасобів, побудова ефективної системи військового зв'язку стає критичним фактором забезпечення управління військами. Гармонізація національних доктринальних і керівних документів за стандартами НАТО вимагає удосконалення формалізованого підходу до кількісного оцінювання ефективності систем зв'язку (СЗ), який одночасно враховує різноманітні суперечливі вимоги до системи, а також різноманітні зовнішні та внутрішні фактори, що впливають на функціонування системи.

Аналіз наявних методик і програмних засобів показав, що вони мають обмежені функціональні можливості та дозволяють здійснювати окремі інженерні розрахунки. Водночас, відомий науково-методичний апарат комплексного оцінювання ефективності СЗ за критеріями постійної готовності, стійкості, мобільності, пропускнуєї спроможності та розвідзахищеності у формулюванні задачі багатокритеріальної оптимізації не враховує можливості використання актуальної геопросторової інформації.

У статті запропоновано удосконалену методику комплексної оцінки ефективності СЗ за стандартами НАТО, що формалізує задачу оцінювання як задачу багатокритеріальної оптимізації на Парето-множині з адитивною згортою n -ти часткових показників. Особливістю методики, що визначає сутність її наукової новизни, є врахування та інтеграція геопросторового аналізу на основі графового моделювання інформаційних напрямків із використанням стандартів НАТО. Наведено математичний апарат нормалізації, агрегації та візуалізації результатів розрахунку за розробленою методикою. Практичною цінністю результатів досліджень є реалізація методики у вигляді програмного модуля, що пропонується для використання органами військового управління в процесі побудови системи зв'язку тактичної та оперативної ланок управління.

Ключові слова: система зв'язку, ефективність, стандарти НАТО, багатокритеріальна оптимізація, Парето-оптимальність, геопросторова інформація, радіоелектронна боротьба.

I. Kovalenko, A. Zarubenko, M. Masesov, O. Drahliuk. Methodology for assessing the effectiveness of communication system according to NATO standards using geospatial information

In modern combat operations, characterized by active use of electronic warfare (EW) means, high-precision fires, and cyber threats, the effective design of the communication system (CS) of a military formation becomes a critical factor in preserving command and control of troops. Harmonization of the national Manual on Communications of the Armed Forces of Ukraine (DDP 6-26.22) with NATO standards (AJP-6, SAS-026 COBP, STANREC 4174) requires a formalized approach to the quantitative assessment of CS effectiveness that simultaneously takes into account the physical characteristics of radio means, terrain relief, the location of enemy threats, and the hierarchy of information exchange routes.

An analysis of existing methodologies and software tools (Radio Mobile, Radio Planner, ATOLL) showed that they allow performing individual radio-technical calculations but do not provide a comprehensive assessment of CS effectiveness according to the criteria of operational readiness, survivability, mobility, throughput, and LPI/LPD protection in the formulation of a multi-criteria optimization problem accounting for geospatial information.

The article proposes a methodology for the comprehensive assessment of CS effectiveness according to NATO standards, which formalizes the assessment problem as a multi-criteria optimization problem on the Pareto set with additive convolution of five partial indicators. A distinctive feature of the methodology is the integration of radio-technical calculations (Link Budget, ITU-R P.526 based on SRTM data, ITU-R P.676) with geospatial analysis (radio coverage zones, fire-strike zones, EW zones, reconnaissance zones) and graph modeling of information exchange routes. The mathematical apparatus of normalization, aggregation, and visualization of results is described. The proposed methodology is implemented as a software module and is suitable for operational assessment of CS design alternatives at brigade, corps, and operational command levels.

Keywords: communication system, effectiveness, NATO standards, multi-criteria optimization, Pareto optimality, geospatial information, electronic warfare.

Постановка завдання. Сучасний збройний конфлікт визначається активним застосуванням противником засобів радіоелектронної боротьби (РЕБ), розвідки, високоточних засобів ураження та кіберзасобів. Забезпечення своєчасності, достовірності та безпеки зв'язку у таких умовах є визначальним чинником забезпечення безперервності управління військами. Розроблена та затверджена у 2025 році Настанова зі зв'язку Збройних Сил України ДДП 6-26.22 [1] визначає п'ять основних вимог до СЗ, що визначають ефективність її функціонування – постійну готовність $R_{ПГ}$, стійкість P_C , мобільність T_M , пропускну спроможність C та розвідзахищеність $K_{PЗ}$. Одночасно процес євроатлантичної інтеграції вимагає узгодження національної доктрини зі стандартами НАТО (AJP-6 [2], SAS-026 COBR [3], STANREC 4174 [4], STANAG 4677), у яких оцінювання проводиться через показники ефективності (Measures of Effectiveness, MoE) та показники продуктивності (Measures of Performance, MoP).

Наукове завдання досліджень обґрунтовується відсутністю формалізованої, математично коректної та програмно реалізованої методики, яка:

- 1) одночасно враховує вимоги до СЗ згідно з ДДП 6-26.22 (п'ять показників) та концепцію NATO MoE/MoP;
- 2) явно моделює задачу вибору варіанту побудови СЗ як задачу багатокритеріальної оптимізації;
- 3) інтегрує геопросторову інформацію (цифрова модель рельєфу SRTM, координати вузлів, зони загроз противника) у розрахунок часткових показників;
- 4) забезпечує відтворюваність результату та його візуалізацію для осіб, що приймають рішення (ОПР).

Аналіз публікацій за темою дослідження. Питання оцінювання ефективності систем військового зв'язку досліджувалися у працях [5–9].

У роботі [5] побудовано методику розрахунку інтервалів радіорелейного зв'язку з урахуванням рельєфу та будівель за рівнянням радіолінії та рекомендаціями ITU-R P.526, P.530, P.676. У монографії [6] систематизовано принципи побудови військових цифрових систем зв'язку, проте комплексна оцінка ефективності розглядається переважно якісно.

У [7] розглянуто питання завадозахищеності систем із ППРЧ/DSSS через Processing Gain та Jamming Margin, які не відповідають визначеним в ДДП 6-26.22 [1] показникам.

Закордонні роботи [8; 9] у рамках програми COBR for C2 Assessment пропонують концептуальний апарат MoE/MoP, який формалізується через дерево цілей і не містить готових розрахункових процедур.

Серед спеціалізованих програмних засобів найбільш відомі Radio Mobile, Radio Planner, CRC-COVWEB [5], ATOLL, які забезпечують моделювання електромагнітного поля та побудову зон радіопокриття за моделями Longley-Rice, ITU-R P.1546, P.526, P.1812. Проте такі засоби не оперують поняттями “вузол зв'язку”, “інформаційний напрямок”, “стійкість мережі” та не виконують інтегральну оцінку ефективності СЗ. Напрацювання в частині задач багатокритеріальної оптимізації [10] пропонують апарат Парето-оптимальності, але без прив'язки до специфіки оцінювання військових СЗ.

За результатами проведеного аналізу публікацій визначено, що наявні роботи не вирішують задачу комплексного оцінювання ефективності СЗ за всіма показниками ефективності з одночасним використанням геопросторової інформації та стандартів НАТО.

Мета статті. Провести аналіз існуючих методик оцінки ефективності систем зв'язку військового призначення НАТО та розробити (удосконалити) методику оцінки ефективності СЗ Збройних Сил України, яка буде застосовувати підходи НАТО щодо використання технічних і геопросторових даних відносно елементів СЗ та відповідати вимогам до СЗ Настанови зі зв'язку ДДП 6-26.22.

Виклад основного матеріалу

1. Математична модель СЗ

Для формування математичної моделі СЗ, що адекватно та достатньо повно відображає структуру, параметри та особливості функціонування системи, використано концептуальний підхід, основи якого наведені у [11], при цьому виділено наступні ієрархічні об'єкти СЗ згідно з виразом (1):

$$СЗ = \langle EЗ, ЛЗ, ІН, ВЗ, МЗ, СЗ \rangle, \quad (1)$$

де $EЗ$ – множина елементів (засобів) зв'язку (CE); $ЛЗ$ – множина ліній зв'язку (CL) як впорядкованих пар елементів; $ІН$ – множина інформаційних напрямків (IER); $ВЗ$ – множина вузлів зв'язку (CN); $МЗ$ – множина мереж зв'язку; $СЗ$ – система зв'язку, що моделюється, загалом.

Кожному вузлу $vz \in ВЗ$ поставлено у відповідність геопросторову прив'язку згідно з виразом (2):

$$geo(vz) = (\varphi_{vz}, \lambda_{vz}, h_{vz}) \in WGS-84, \quad (2)$$

де $\varphi_{vz}, \lambda_{vz}$ – широта та довгота; h_{vz} – висота підняття антени (м). Тип, ешелон та функціональне призначення вузла кодуються згідно з MIL-STD-2525D у форматі 20-символьного SIDC-коду (Symbol Identification Code).

Множина загроз противника $T = T_F \cup T_{EW} \cup T_R \cup T_C$ розрізняє чотири класи – вогневі (T_F), РЕБ (T_{EW}), розвідки (T_R) та кіберзагрози (T_C). Кожна загроза $t \in T$ має геопросторову прив'язку $geo(t)$ та зону дії D_t , що обчислюється на етапі геопросторового аналізу.

2. Формалізація задачі оцінювання

Нехай X – варіант побудови СЗ, поданий набором параметрів відповідно до виразу (3):

$$X = \{x_1, x_2, \dots, x_n\}, \quad (3)$$

де x_i включає тактико-технічні характеристики (ТТХ) засобів (потужність передавача, чутливість приймача, смуга, модуляція, коефіцієнт підсилення антени), координати вузлів, склад обладнання, параметри каналів та структуру інформаційних напрямків.

Відповідно до ДДП 6-26.22 [1] задано п'ять цільових функцій (вираз (4)), які узгоджуються з вимогами НАТО МоЕ/МоР [2; 3]:

$$\begin{aligned} f_1(X) &= R_{ПГ}(X) \rightarrow \max, \\ f_2(X) &= P_C(X) \rightarrow \max, \\ f_3(X) &= T_M(X) \rightarrow \min, \\ f_4(X) &= C(X) \rightarrow \max, \\ f_5(X) &= K_{РЗ}(X) \rightarrow \max, \end{aligned} \quad (4)$$

за обмеженням на сумарну вартість $V(X) \leq V_3$, заданим особою, що приймає рішення. Задача (4) записується у векторному вигляді (5):

$$X^0: \begin{cases} f(X) = (f_1, f_2, f_3, f_4, f_5) \rightarrow \text{opt}, \\ V(X) \leq V_3, \end{cases} \quad (5)$$

де $R_{ПГ}$ – постійна готовність; P_C – стійкість; T_M – мобільність; C – пропускна спроможність; $K_{РЗ}$ – розвідзахищеність, знак “opt” визначає оптимізацію у різних напрямках: $f_1, f_2, f_4, f_5 \rightarrow \max, f_3 \rightarrow \min$.

Часткові показники (4) є суперечливими: покращення одного призводить до погіршення іншого (наприклад, резервування ліній підвищує P_C , але погіршує T_M і V ; обмеження випромінювання підвищує $K_{РЗ}$, але знижує C). З урахуванням зазначеного, задача (5) є задачею векторної оптимізації, розв'язок якої пропонується шукати у класі Парето-оптимальних варіантів [10].

Визначення 1. Варіант X^a домінує варіант X^b (записується $X^a > X^b$), якщо

$$\forall i \in \{1,2,4,5\}: f_i(X^a) \geq f_i(X^b), \quad f_3(X^a) \leq f_3(X^b), \quad \exists j: f_j(X^a) \neq f_j(X^b). \quad (6)$$

Визначення 2. Множина $D_P \subseteq D$ називається Парето-оптимальною множиною (Парето-множиною), якщо вона складається з усіх недомінованих варіантів допустимої множини D :

$$D_P = \{X^* \in D: \nexists X \in D, X \succ X^*\}. \quad (7)$$

Для обрання єдиного варіанту з Парето-множини D_P використано адитивну згортку з нормалізованими частковими показниками [10; 12]:

$$Z(X) = \sum_{i=1}^5 a_i \cdot f_i^{norm}(X), \quad \sum_{i=1}^5 a_i = 1, \quad a_i \in [0,1], \quad (8)$$

де a_i – вагові коефіцієнти, що адаптивно визначаються методом аналітичної ієрархії (АНР) Сааті [12] залежно від типу бойових дій (наступ, оборона, стабілізаційні дії, тощо) та ешелону управління. Для оборони, наприклад, рекомендується $(a_1, a_2, a_3, a_4, a_5)$ – максимальний акцент на стійкості та готовності при мінімізації ваги мобільності.

3. Розрахунок часткових показників

3.1. Постійна готовність $R_{ПГ}$

Показник $R_{ПГ}$ агрегує три коефіцієнти – укомплектованість особовим складом $K_{ОС}$, справність техніки $K_{ТЕХ}$ та оперативну готовність $K_{ГОТ}$:

$$R_{ПГ}(X) = w_{ос} \cdot K_{ОС} + w_{тех} \cdot K_{ТЕХ} + w_{гот} \cdot K_{ГОТ}. \quad (9)$$

Укомплектованість за особовим складом і технікою обчислюється як середня частка за вузлами, а оперативна готовність – через доступність ліній та напрямків.

Для окремого елемента зв'язку використовується класична формула теорії надійності [4; 13; 14]:

$$A_o^{(ез)} = \frac{MTBF}{MTBF + MTTR + MLDT}, \quad (10)$$

де $MTBF$ – середнє напрацювання на відмову; $MTTR$ – середній час відновлення; $MLDT$ – середній час логістичної затримки.

Для лінії зв'язку, що складається з n послідовно з'єднаних елементів [13; 14]:

$$A_o^{(лз)} = \prod_{j=1}^n A_o^{(езj)}. \quad (11)$$

Для інформаційного напрямку, що забезпечується m паралельними (резервуючими) лініями [14]:

$$A_o^{(ін)} = 1 - \prod_{k=1}^m (1 - A_o^{(лзk)}). \quad (12)$$

Тоді оперативна готовність системи (мережі) з урахуванням пріоритетів напрямків:

$$K_{ГОТ} = \frac{\sum_{k=1}^{N_{ін}} w_k^{пр} \cdot A_o^{(інk)}}{\sum_{k=1}^{N_{ін}} w_k^{пр}}. \quad (13)$$

3.2. Стійкість P_C

Показник P_C агрегує чотири підпоказники – живучість $P_{Ж}$, надійність $P_{Н}$, завадозахищеність $P_{ЗЗ}$ та кіберзахищеність $P_{КБ}$:

$$P_C(X) = w_{\text{ж}} \cdot P_{\text{ж}} + w_{\text{н}} \cdot P_{\text{н}} + w_{\text{зз}} \cdot P_{\text{зз}} + w_{\text{кб}} \cdot P_{\text{кб}}. \quad (14)$$

Ваги $w_{\text{ж}}, w_{\text{н}}, w_{\text{зз}}, w_{\text{кб}}$ адаптивно коригуються за рівнем загрози РЕБ противника.

Живучість. Ймовірність ураження вузла зв'язку вогневим засобом визначається як:

$$P_{\text{ураж}}(vz) = P_{\text{ур}}^{\text{base}} \cdot K_{\text{відст}} \cdot K_{\text{маск}} \cdot K_{\text{інж}}, \quad (15)$$

$$K_{\text{відст}} = \max\left(0, 1 - \frac{d_{\text{FLOT}}(vz)}{D_{\text{маж}}^{\text{ураж}}}\right), \quad (16)$$

де $d_{\text{FLOT}}(vz)$ – відстань до лінії зіткнення, обчислена за координатами вузла та фронтового рубежу; $D_{\text{маж}}^{\text{ураж}}$ – максимальна дальність застосування засобу ураження; $K_{\text{маск}}, K_{\text{інж}}$ – коефіцієнти маскування та інженерного обладнання; $P_{\text{ур}}^{\text{base}}$ – базова ймовірність ураження.

Ймовірність виживання вузла зв'язку:

$$P_{\text{вж}}(vz) = 1 - P_{\text{вияв}}(vz) \cdot P_{\text{ураж}}(vz). \quad (17)$$

Ймовірність збереження інформаційного напрямку через множину шляхів Π (графова модель) [14]:

$$P_{\text{збер}}^{(\text{ін})} = 1 - \prod_{\pi \in \Pi} \left(1 - \prod_{vz \in \pi} P_{\text{вж}}(vz)\right). \quad (18)$$

Тоді живучість системи:

$$P_{\text{ж}} = \frac{\sum_{k=1}^{N_{\text{ін}}} w_k^{\text{пр}} \cdot P_{\text{збер}}^{(\text{ін}_k)}}{\sum_{k=1}^{N_{\text{ін}}} w_k^{\text{пр}}}. \quad (19)$$

Надійність. За експоненційним законом для елемента $R^{(\text{ез})}(t) = e^{-t/MTBF}$; для лінії з n елементами [14]:

$$R^{(\text{лз})}(t) = \exp\left(-t \cdot \sum_{j=1}^n \frac{1}{MTBF_j}\right); \quad (20)$$

для напрямку з m паралельними лініями [14]:

$$R^{(\text{ін})}(t) = 1 - \prod_{k=1}^m (1 - R^{(\text{лз}_k)}(t)). \quad (21)$$

Для критичних напрямків із резервуванням використовується біноміальна формула [13; 14]:

$$R^{k/n}(t) = \sum_{i=k}^n \binom{n}{i} R^i(t) (1 - R(t))^{n-i}. \quad (22)$$

Завадозахищеність. Для лінії з ППРЧ/DSSS введено коефіцієнт підсилення обробки (Processing Gain) та запас завадостійкості (Jamming Margin), які визначаються за (23) та (24) [7]:

$$G_p = 10 \lg \frac{B_{fhss}}{R_b}, \quad (23)$$

$$M_j = G_p - \left(\frac{E_b}{N_0}\right)_{\text{req}} - L_{\text{sys}}, \quad (24)$$

де B_{fhss} – смуга перестроювання; R_b – бітова швидкість інформаційного потоку; L_{sys} – системні втрати.

Відношення завада/сигнал для конкретної лінії з урахуванням геометрії визначається за формулою (25) [15]:

$$\frac{J}{S} = P_j + G_j - P_t - G_{ant} + 20 \lg \frac{d_{in}}{R_j}, \quad (25)$$

де P_j, G_j – потужність та виграш антени станції постановки завад; P_t, G_{ant} – характеристики передавача; d_{in} – довжина інформаційної лінії; R_j – відстань від РЕБ до приймача.

Показник завадозахищеності лінії визначається за формулою (26):

$$K_{33}^{(лз)} = \begin{cases} 1, & M_j > J/S, \\ \max(0, M_j/(J/S)), & M_j \leq J/S. \end{cases} \quad (26)$$

Агрегація загального показника завадозахищеності на рівні системи зв'язку розраховується за формулою (27):

$$P_{33} = \frac{\sum_{k=1}^{N_{in}} w_k^{pp} \cdot \max_{лз \in in_k} K_{33}^{(лз)}}{\sum_{k=1}^{N_{in}} w_k^{pp}}. \quad (27)$$

Кіберзахищеність визначається композитною згорткою балів криптозахисту S_{crypto} , мережевого захисту S_{net} , процедурного захисту S_{proc} та частки зашифрованих ліній K_{crypto}^{cov} і визначається за формулою (28) [12]:

$$P_{KB} = w_1 S_{crypto} + w_2 S_{net} + w_3 S_{proc} + w_4 K_{crypto}^{cov}. \quad (28)$$

3.3. Мобільність T_M визначається за формулами (29) та (30):

$$T_{розг}^{(вз)} = T_{марш} + \max_{j \in ввз} T_{deploy}^{(j)}, \quad T_{марш} = \frac{D_{марш}}{V_{марш}}; \quad (29)$$

$$T_M(X) = \max_{vz \in ввз} T_{розг}^{(vz)}. \quad (30)$$

Оскільки для показника T_M менше значення є кращим, нормалізація проводиться інверсно за формулою (49).

3.4. Пропускна спроможність C

Базова теоретична ємність каналу визначається за формулою Шеннона – Хартлі (31) [7; 16]:

$$C_{теор} = B \cdot \log_2(1 + SNR_{lin}), \quad (31)$$

де B – смуга (Гц); SNR_{lin} – відношення сигнал/шум у лінійному вигляді.

Практична пропускна спроможність лінії з урахуванням спектральної ефективності η розраховується за виразом (32) [7; 17]:

$$C_{практ} = \min(C_{ТТХ}, C_{теор} \cdot \eta), \quad (32)$$

тоді ефективна пропускна спроможність з урахуванням накладних витрат криптозахисту та протоколів визначається за формулою (33):

$$C_{eff}^{(лз)} = C_{практ} \cdot (1 - OH_{crypto}) \cdot \eta_{proto}. \quad (33)$$

Пропускна спроможність інформаційного напрямку як суми паралельних ліній визначається за формулою (34):

$$C^{(ih)} = \sum_{k=1}^m C_{eff}^{(лзк)}, \quad (34)$$

тоді потрібна пропускна спроможність напрямку як сума вимог сервісів – за формулою (35):

$$C_{req}^{(ih)} = \sum_{s \in Serv(ih)} n_s \cdot BW_s, \quad (35)$$

а коефіцієнт пропускної спроможності напрямку – за формулою (36):

$$K_C^{(ih)} = \min \left(1, \frac{C^{(ih)}}{C_{req}^{(ih)}} \right), \quad (36)$$

при цьому агрегація на рівні системи здійснюється за формулою (37):

$$C(X) = \frac{\sum_{k=1}^{N_{ih}} w_k^{пр} \cdot K_C^{(ih_k)}}{\sum_{k=1}^{N_{ih}} w_k^{пр}}. \quad (37)$$

3.5. Розвідзахищеність K_{pz}

Дальність виявлення джерела випромінювання станцією радіоелектронної розвідки визначається за формулою (38) [15]:

$$R_{detect}^{(вільн)} = \sqrt{\frac{EIRP \cdot G_{recon}^{ant}}{(4\pi)^2 \cdot P_{recon}^{min} / \lambda^2}}, \quad EIRP = P_t \cdot G_{ant}, \quad (38)$$

де $R_{detect}^{(вільн)}$ – дальність виявлення джерела у вільному просторі; $EIRP$ – еквівалентна ізотропно-випромінювана потужність джерела; P_t – потужність передавача джерела; G_{ant} – коефіцієнт підсилення антени джерела; G_{recon}^{ant} – коефіцієнт підсилення антени станції розвідки в напрямі джерела випромінювання; P_{recon}^{min} – порогова чутливість приймача станції радіоелектронної розвідки (Вт); λ – довжина хвилі (м).

Коефіцієнт розвідзахищеності лінії визначається за формулою (39):

$$K_{pz}^{(лз)} = \frac{R_{recon}}{R_{detect}} \cdot K_{ппрч} \cdot K_{час}, \quad (39)$$

де R_{recon} – фактична відстань від станції розвідки до випромінювача; $K_{ппрч}$ – коефіцієнт ППРЧ; $K_{час}$ – коефіцієнт часового режиму (EMCON). Агрегація на рівні системи розраховується за формулою (40):

$$K_{pz}(X) = \frac{1}{N_{вз}} \sum_{i=1}^{N_{вз}} \min_{лз \in Вз_i} K_{pz}^{(лз)}. \quad (40)$$

4. Інтеграція геопросторової інформації

Ключовою особливістю запропонованої методики є використання геопросторової інформації на всіх етапах розрахунку. Геопросторова підсистема виконує чотири групи задач.

4.1. Розрахунок рівня сигналу за рельєфом. Для кожної пари вузлів (v_{za}, v_{zb}) будується профіль рельєфу $\{h_{ij}\}_{i=1}^N$ з даних SRTM шляхом дискретизації великого кола між

точками з кроком Δd (типово 30–90 м). Корекція на кривизну Землі враховується за формулою (41) [18]:

$$h_i^{corr} = h_i + \frac{d_i(d - d_i)}{2kR_E}, \quad (41)$$

де d_i – відстань від першої точки; d – повна довжина інтервалу; $R_E = 6\,371$ км; $k = 4/3$ – еквівалентний радіус Землі.

Для кожної точки профілю обчислюється перша зона Френеля за формулою (42) [17; 18]:

$$F_1(d_i) = \sqrt{\frac{\lambda \cdot d_i(d - d_i)}{d}}, \quad \lambda = \frac{c}{f}. \quad (42)$$

Параметр Френеля-Кірхгофа для перешкоди i розраховується за формулою (43) [18]:

$$v_i = h_i^{obs} \cdot \sqrt{\frac{2}{\lambda} \cdot \frac{d_{ai} + d_{ib}}{d_{ai} \cdot d_{ib}}}, \quad (43)$$

дифракційні втрати за ITU-R P.526 – за формулою (44) [18]:

$$L_{diff}(v) = \begin{cases} 0, & v \leq -0,78 \\ 6,9 + 20 \lg(\sqrt{v^2 + 1} + v), & v > -0,78 \end{cases} \quad (44)$$

Загальні втрати у каналі (Link Budget) визначаються за формулою (45) [17]:

$$L_{total} = L_0 + L_{diff} + L_{atm} + L_{rain} + L_{feed}^{tx} + L_{feed}^{rx}, \quad (45)$$

де L_0 – втрати у вільному просторі (FSPL) за формулою Фрііса [21]; L_{atm} – атмосферне поглинання за ITU-R P.676 [13]; L_{rain} – дощове ослаблення за ITU-R P.838 [14]; $L_{feed}^{tx}, L_{feed}^{rx}$ – втрати у фідерному тракті передавальної та приймальної сторін відповідно. Тоді рівень сигналу на приймачі розраховується за формулою (46) [21; 22]:

$$P_{rx} = P_t + G_{ant}^{tx} + G_{ant}^{rx} - L_{total}, \quad (46)$$

а відношення сигнал/шум + завада визначається відповідно до формули (47):

$$SINR = P_{rx} - 10 \lg \left(P_N + \sum_{j=1}^J P_j \right), \quad (47)$$

де $N = 10 \lg(kTB) + NF$ – тепловий шум приймача, а сума $\sum P_j$ враховує внесок усіх засобів постановки завад, перерахований за виразом (25).

4.2. Зони радіопокриття. Для кожного вузла зв'язку будується зона гарантованого покриття як геометрія (полігон) у системі WGS-84. Алгоритм, адаптований з напрацювань [22], сканує простір по азимутах $\alpha \in [0, 2\pi)$ з кроком $\Delta\alpha$, для кожного напрямку методом бінарного пошуку визначає максимальну дальність $d_{max}(\alpha)$, при якій $P_{rx}(d) \geq P_{sens}$. Отриманий набір точок $\{(\alpha_i, d_{max}(\alpha_i))\}$ формує контур зони, який далі відокремлюється як шар поверх топооснови і в подальшому використовується для розрахунків.

4.3. Зони загроз противника. Для кожної загрози $t \in T$ обчислюється геометрія зони дії D_t : для вогневих засобів – коло радіуса $D_{max}^{ураж}$ з центром у точці розташування; для засобів РЕБ – кільцева область із концентричними зонами ризику, розрахована аналогічно до (47) з перевищенням значення завада/сигнал над заданим порогом; для розвідки – коло радіуса R_{detect} за виразом (38). Результати використовуються у (15)–(17) для обчислення ймовірностей ураження та виявлення.

Просторова близькість вузлів до загроз та ліній зіткнення враховується безпосередньо у розрахункових формулах через координати та відстані.

5. Нормалізація, агрегація та класифікація

Нормалізація часткових показників “більше = краще” виконується відносно допустимого значення $X_{\text{доп}}$, заданого для ешелону та типу операції за формулою (48):

$$f_i^{\text{norm}}(X) = \frac{f_i(X)}{X_{\text{доп},i}}, \quad i \in \{1,2,4,5\}. \quad (48)$$

Для мобільності (менше = краще) застосовується інверсна нормалізація (49):

$$f_3^{\text{norm}}(X) = \frac{T_M^{\text{доп}}}{T_M(X)}. \quad (49)$$

Слід зазначити, що при здійсненні нормалізації показників за виразами (48) та (49) отримане значення нормалізованого параметра може бути більшим 1, що відрізняється від класичних підходів та враховує особливості побудови системи зв'язку, а саме – побудована система зв'язку (що оцінюється) повинна відповідати вимогам, які до неї висуваються.

Комплексна оцінка обчислюється за формулою (8). Класифікація результату здійснюється за шкалою (50):

$$\text{grade}(Z) = \begin{cases} \text{A (відмінна)}, & Z \geq 1,25, \\ \text{B (добра)}, & 1,00 \leq Z < 1,25, \\ \text{C (задовільна)}, & 0,85 \leq Z < 1,00, \\ \text{D (незадовільна)}, & 0,70 \leq Z < 0,85, \\ \text{E (критична)}, & Z < 0,70. \end{cases} \quad (50)$$

Числові пороги шкали $\{0,70; 0,85; 1,00; 1,25\}$ отримано експертно за результатами опитування. Інтерпретація шкали узгоджена з категоріями якості НАТО МоЕ-індикаторів (Excellent / Good / Marginal / Inadequate / Critical) та підлягає подальшому калібруванню за результатами верифікації методики на ретроспективних статистичних даних бойового застосування СЗ.

Для візуалізації результатів застосовано радарну (павутинну) діаграму з двома контурами (фактичний та допустимий), теплову карту “вузол × показник” з правилами кольорового кодування, а також накладання зон радіопокриття та зон загроз на топографічну основу.

6. Просторово-часова агрегація.

Етапи розрахунку:

Етап 0. Визначення переліку комунікаційних послуг зв'язку: автоматичне профілювання сервісів за ешелонам, формування матриці інформаційних напрямків, розрахунок $C_{\text{req}}^{(\text{ін})}$ за формулою (35).

Етап 1. Розрахунок $R_{\text{ПГ}}$ за формулами (9)–(13).

Етап 2. Розрахунок P_C за формулами (14)–(28).

Етап 3. Розрахунок T_M за формулами (29)–(30).

Етап 4. Розрахунок C за формулами (31)–(37) з використанням результатів формулами (41)–(47).

Етап 5. Розрахунок $K_{\text{РЗ}}$ за формулами (38)–(40).

Етап 6. Нормалізація за формулами (48)–(49), перевірка виконання вимог $f_i(X) \geq X_{\text{доп},i}$.

Етап 7. Обчислення $Z(X)$ за (8), класифікація за (50), формування діагностичного звіту з рекомендаціями щодо прийняття рішення з побудови системи зв'язку.

Програмна реалізація удосконаленої методики виконана як модуль .NET 8 + WPF з використанням Clean Architecture (шари Core, Data, WPF), Entity Framework Core для бази

даних (БД) та бібліотеки MapSui 5 для геопросторової візуалізації. Для обчислень рельєфу місцевості та поширення радіохвиль інтегровано алгоритми за рекомендаціями [13; 22; 23]. Для оцінки готовності радіоелектронного обладнання застосовано довідкові дані [23], для оцінки якості голосового зв'язку – модель Е [24]. Результат оцінювання відображатиметься у модулі “Ефективність” з радарною діаграмою, тепловою картою, діагностичним звітом із вузькими місцями СЗ та рекомендаціями змін на основі встановлених правил (рис. 1).

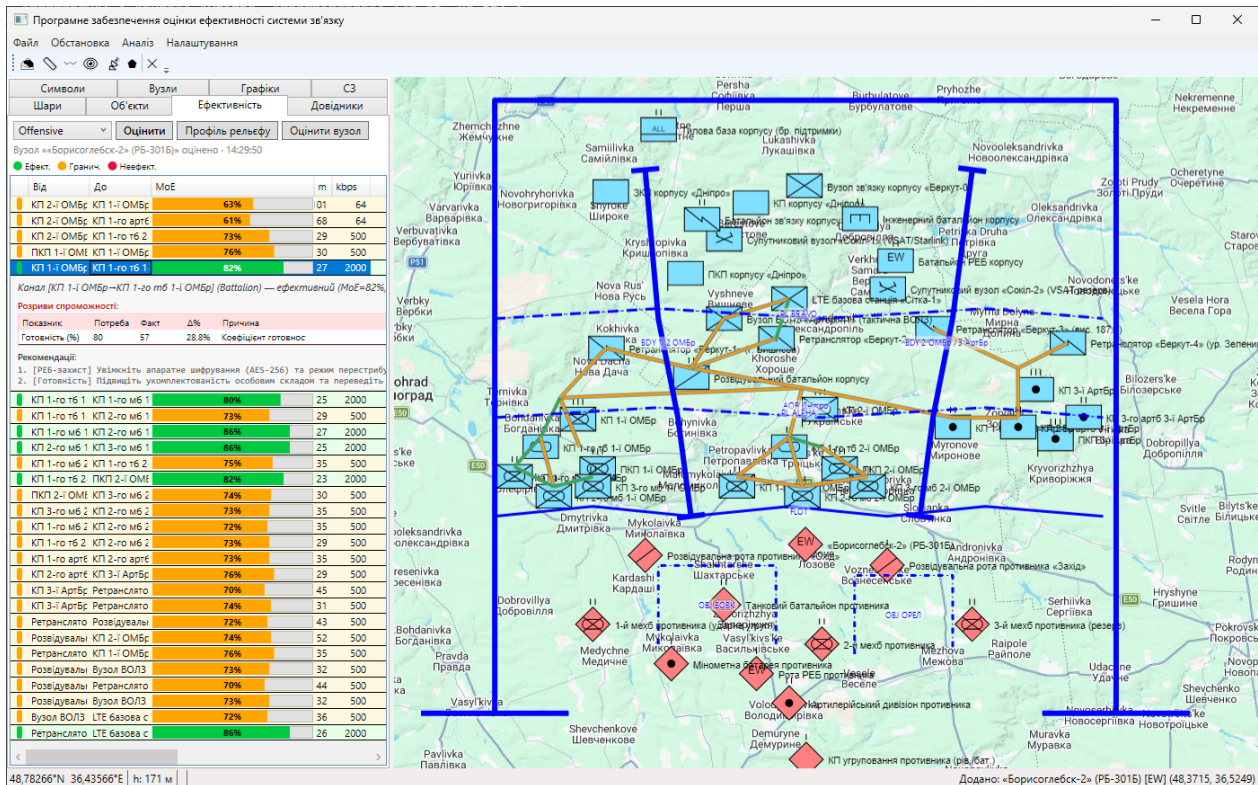


Рис. 1. Зовнішній вигляд вікна програмної реалізації методики

Наукова новизна запропонованої методики полягає у сукупності таких результатів.

1. Нова формалізація задачі оцінювання ефективності СЗ як задачі багатокритеріальної оптимізації (5) на Парето-множині (7) з адитивною згорткою (8), що вперше одночасно:

- повністю охоплює всі п'ять показників згідно з вимогами ДДП 6-26.22 [1];
- узгоджується з концепцією NATO МоЕ/МоР за SAS-026 СОВР [3] та АЛР-6 [2];
- явно враховує суперечливість показників через механізм Парето-домінування (6).

На відміну від [5–9], у яких розглядаються окремі радіотехнічні або показники надійності без інтегральної оцінки, у запропонованій методиці вперше побудовано замкнений математичний апарат від рівня елемента зв'язку до рівня СЗ.

2. Удосконалена процедура розрахунку живучості та завадозахищеності СЗ за рахунок інтеграції графової моделі інформаційних напрямків (18), (21) з геопросторово залежними ймовірностями ураження (15)–(17) та реальною геометрією впливу РЕБ (25), (47). Це дозволяє, на відміну від класичного підходу, отримувати значення $P_{\text{ж}}$ та $P_{\text{ЗЗ}}$, які залежать не лише від технічних характеристик засобів, а й від взаємного розташування вузлів СЗ, лінії зіткнення та засобів ураження і РЕБ противника на цифровій карті.

3. Новий метод інтегрованого розрахунку пропускної спроможності з урахуванням геопросторової інформації, який через єдиний обчислювальний математичний апарат (31)–(37), (41)–(47) прив'язує значення $SINR$ кожної лінії до профілю рельєфу, атмосферного поглинання, впливу РЕБ і сукупно агрегує результат до показника C системи. Це відрізняє

наведену методику від засобів розрахунку типу Radio Mobile, Radio Planner, ATOLL, які дають рівень сигналу, але не переводять його у показник ефективності СЗ.

4. Удосконалена математична модель розвідзахищеності (38)–(40) як комбінація дальності виявлення, фактичної геометрії розміщення станцій розвідки, коефіцієнтів ППРЧ та часового режиму Emission Control, що дозволяє кількісно оцінювати $K_{PЗ}$ через конкретне розташування вузлів на карті.

Таким чином, відмінність запропонованої методики від наявних полягає у комплексному, математично замкненому та геопросторово-орієнтованому підході до оцінювання ефективності СЗ, узгодженому одночасно з національними підходами та стандартами НАТО. Практична цінність методики підтверджується її реалізацією у програмному модулі та верифікацією на модельних прикладах побудови СЗ. Отримані з використанням розробленого програмного забезпечення результати розрахунків дозволяють зробити висновок про коректність отриманих результатів.

Висновки

Сформульовано та математично формалізовано задачу оцінювання ефективності системи військового зв'язку з врахуванням стандартів НАТО як задачу багатокритеріальної оптимізації (5) на Парето-множині (7) з адитивною згортою (8), що одночасно узгоджена з п'ятьма показниками ефективності (згідно з ДДП 6-26.22) та концепцією НАТО МоЕ/МоР.

Побудовано замкнений математичний апарат обчислення п'яти часткових показників – постійної готовності (9)–(13), стійкості (14)–(28), мобільності (29)–(30), пропускної спроможності (31)–(37) та розвідзахищеності (38)–(40), який охоплює всі рівні ієрархії – від елемента зв'язку до СЗ – і дозволяє виконувати обчислення з урахуванням реальних ТТХ засобів та геометрії розміщення.

Обґрунтовано використання геопросторової інформації у вигляді даних висот місцевості, координат вузлів, ліній зіткнення та геометрії загроз противника безпосередньо у формулах часткових показників. Це забезпечує залежність оцінок живучості, завадозахищеності, пропускної здатності та розвідзахищеності від реальних умов розгортання СЗ, а не лише від ТТХ обладнання, що є принциповою перевагою методики.

Запропонована методика придатна до програмної реалізації та інтеграції з геоінформаційною системою: розроблений програмний модуль підтверджує практичність апарату та дозволяє ОНР виконувати оперативну оцінку варіантів побудови СЗ у режимі, наближеному до реального часу.

Напрямами подальших досліджень є: побудова еволюційного алгоритму пошуку Парето-оптимальних варіантів СЗ у просторі допустимих розміщень вузлів; інтеграція модуля із системами ситуаційної обізнаності; включення стохастичних моделей впливу кіберзагроз у розрахунок $P_{КБ}$; верифікація значень коефіцієнтів (9), (14) на основі статистики бойових дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДДП 6-26.22. Настанова “Зі зв'язку Збройних Сил України”.
2. Allied Joint Publication AJP-6. Allied Joint Doctrine for Communication and Information Systems. Edition A, Version 1. NATO Standardization Office, 2011. 82 p. URL: <https://nso.nato.int>.
3. NATO Code of Best Practice for Command and Control Assessment. RTO Technical Report SAS-026. Research and Technology Organisation, 2002. 340 p. URL: <https://nso.nato.int>.
4. NATO Standardization Office. Allied Reliability and Maintainability Publication 1 (ARMP-1), Edition D (STANREC 4174). 2022. URL: <https://nso.nato.int>.
5. Коваленко І., Масесов М., Драглюк О., Ткаченко А. Методика побудови радіорелейних ліній зв'язку на основі використання геопросторової інформації // Системи і технології зв'язку, інформатизації та кібербезпеки. 2023. № 3. С. 45–54. DOI: <https://doi.org/10.58254/viti.3.2023.04.31>.
6. Цифрові системи військового зв'язку / А. М. Яценко, В. В. Ходченко, О. С. Петренко та ін. К.: НУОУ, 2018. 268 с.

7. Proakis J. G., Salehi M. Digital Communications. 5th ed. New York: McGraw-Hill, 2008. 1150 p. URL: <https://www.mheducation.com>.
8. Alberts D. S., Hayes R. E. Code of best practice for experimentation. CCRP Publication Series. DoD. 2002. URL: <https://apps.dtic.mil/sti/tr/pdf/ADA457167.pdf>.
9. Alberts D. S., Garstka J. J., Stein F. P. Network centric warfare: Developing and leveraging information superiority (2nd ed.). CCRP. 1999. URL: <https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf>.
10. Чеботарьова Д., Безрук В. Автоматизація вибору оптимальних проєктних варіантів систем зв'язку на основі методів багатокритеріальної оптимізації // Інфокомунікаційні технології та електронна інженерія. 2021. № 2 (2). С. 54–61. URL: <https://science.lpnu.ua/ict/e/all-volumes-and-issues/volume-1-number-2-2021>.
11. Масесов М. О. Концептуальна модель предметної області системи зв'язку // Системи і технології зв'язку, інформатизації та кібербезпеки. 2025. Вип. 7. С. 92–99. URL: <https://doi.org/10.58254/viti.7.2025.09.92>.
12. Saaty T. L. Decision making with the analytic hierarchy process // International Journal of Services Sciences. Vol. 1, Issue 1. P. 83–98. DOI: 10.1504/IJSSCI.2008.017590.
13. U.S. Department of Defense MIL-HDBK-217F Notice 2: Reliability Prediction of Electronic Equipment. 1995. Also available online, URL: http://www.navsea.navy.mil/Portals/103/Documents/NSWC_Crane/SD-18/Test%20Methods/MILHDBK217.pdf.
14. Barlow R. E., Proschan F. Statistical Theory of Reliability and Life Testing: Probability Models. New York: Holt, Rinehart; Winston, 1975.
15. Adamy D. L. EW 101: A First Course in Electronic Warfare. Boston: Artech House, 2009.
16. Shannon C. E. A Mathematical Theory of Communication // The Bell System Technical Journal. Vol. 27, Issue 3. P. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.
17. Rappaport T. S. Wireless Communications: Principles and Practice. 2. Prentice Hall, 2002.
18. ITU-R Recommendation P.526-15. Propagation by diffraction. Geneva: International Telecommunication Union, 2019. URL: <https://www.itu.int/rec/R-REC-P.526/>.
19. Friis H. T. A Note on a Simple Transmission Formula. Proceedings of the IRE. Vol. 34, Issue 5. P. 254–256. DOI: 10.1109/JRPROC.1946.234568.
20. ITU-R Recommendation P.676-12. Attenuation by atmospheric gases and related effects. Geneva: International Telecommunication Union, 2019. URL: <https://www.itu.int/rec/R-REC-P.676/>.
21. ITU-R Recommendation P.838-3. Specific attenuation model for rain for use in prediction methods. Geneva: International Telecommunication Union, 2005. URL: <https://www.itu.int/rec/R-REC-P.838/>.
22. ITU-R Recommendation P.530-18. Propagation data and prediction methods required for the design of terrestrial line-of-sight systems. Geneva: International Telecommunication Union, 2021. URL: <https://www.itu.int/rec/R-REC-P.530/>.
23. IEC 61709:2017 «Electric components – Reliability – Reference conditions for failure rates and stress models for conversion» або 217Plus:2015 RIAC Handbook of 217Plus Reliability Prediction Models).
24. ITU-T Recommendation G.107. The E-model: a computational model for use in transmission planning. Geneva: ITU-T, 2015. 32 p. URL: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.107-201506-I!!PDF-E&type=items.

Надійшла до редколегії 20.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

Ковальчук О. О. ORCID: 0000-0003-1372-6284 (ВІТІ ім. Героїв Крут)
д-р техн. наук, доцент Беляков Р. О. ORCID: 0000-0001-9882-3088 (ВІТІ ім. Героїв Крут)
Металіди О. Г. ORCID: 0009-0005-2534-0612 (НУОУ)

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ІЗ ВИКОРИСТАННЯМ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

У статті проведено комплексний аналіз сучасних методів виявлення безпілотних літальних апаратів із використанням сенсорних систем різних типів з урахуванням еволюції повітряних загроз і появи нових типів малорозмірних дронів. Предметом дослідження є методи виявлення безпілотних літальних апаратів (БпЛА) радіолокаційними, радіочастотними, акустичними та оптико-електронними/інфрачервоними підсистемами, а також принципи їх інтеграції в багатосенсорну інформаційно-керуючу архітектуру. Особливий акцент зроблено на домінуванні на полі бою малорозмірних FPV-дронів і появи апаратів з оптоволоконним каналом керування, які фактично є імунними до засобів радіоелектронної боротьби та «невидимими» для RF-детекторів, що формує критичний розрив у традиційних C-UAS (від англ. Counter-Unmanned Aircraft Systems) підходах.

Систематизовано можливості та обмеження кожної сенсорної модальності. Показано, що ефективність радіолокаційних систем (РЛС) визначається малою ефективною площею розсіювання (ЕПР) цілі та умовами прямої видимості; при зменшенні ЕПР різко скорочується дальність детекції, а флуктуації ЕПР через обертання роторів ускладнюють супроводження. Водночас аналіз мікродоплерівських сигнатур розглянуто як перспективний інструмент розрізнення БпЛА та птахів, а також класифікації типу апарата за спектральними ознаками. Встановлено, що RF-методи забезпечують високу ймовірність виявлення лише для дронів з активним радіоканалом і є принципово непридатними для автономних та оптоволоконних платформ. Для акустичних систем визначено ключові переваги пасивності та NLOS (від англ. Non-Line-of-Sight) здатності, але підкреслено обмеження дальності, залежність від вітру й підвищений рівень хибних тривог у міському шумі. Для електронно-оптичного/інфрачервоного каналу зазначено критичну залежність від метеоумов, освітленості та теплового контрасту, а також потребу у зовнішньому цілевказанні через обмежене поле зору при великому збільшенні кратності оптичного модуля.

Обґрунтовано необхідність переходу від одноканальних рішень до багатосенсорної архітектури зі злиттям даних MSDF (від англ. Multi-Sensor Data Fusion) та адаптивним зважуванням інформаційних потоків залежно від параметрів середовища і достовірності каналу. Запропоновано концептуальну модель інформаційно-керуючої системи (ІКС) спостереження на основі бездротових сенсорних мереж (БСМ) із індикаторами доступності вимірювань для різних сенсорів, що особливо важливо при відсутності RF-компоненти для виявлення оптоволоконних БпЛА. Підкреслено роль алгоритмів штучного інтелекту для зниження хибних спрацювань, класифікації мікродоплерівських/візуальних/акустичних ознак і підвищення надійності прийняття рішень у реальному часі. Отримано висновок, що лише інтеграція кількох сенсорних модальностей у розподілену мережеву систему MSDF забезпечує необхідний рівень ймовірності виявлення малорозмірних БпЛА в умовах стохастичних збурень зовнішнього середовища та еволюції способів керування дронами.

Ключові слова: інформаційно-керуюча система, безпілотний літальний апарат, ф'южн-алгоритм, методи виявлення, штучний інтелект, радіотехнології, системи автоматичного управління, обробка даних, бездротові сенсорні мережі, сенсор.

O. Kovalchuk, R. Bieliakov, O. Metalidi. Analysis of methods for detecting unmanned aerial vehicles using wireless sensor networks

The article presents a comprehensive analysis of modern methods for detecting unmanned aerial vehicles (UAVs) within wireless sensor networks, taking into account the evolution of aerial threats and the emergence of new types of small-sized drones. The subject of the study is UAV detection methods based on radar, radio-frequency, acoustic, and electro-optical/infrared subsystems, as well as the principles of their integration into a multisensor information and control architecture. Particular emphasis is placed on the dominance of small FPV drones on the battlefield and the emergence of platforms with fiber-optic control links, which are effectively immune to electronic warfare systems and "invisible" to RF detectors, thereby creating a critical gap in traditional Counter-Unmanned Aircraft Systems (C-UAS) approaches.

The capabilities and limitations of each sensor modality are systematized. It is shown that the effectiveness of radar systems is determined by the small radar cross-section (RCS) of the target and line-of-sight conditions; as the RCS decreases, the detection range drops sharply, while RCS fluctuations caused by rotor rotation complicate target tracking.

At the same time, the analysis of micro-Doppler signatures is considered a promising tool for distinguishing UAVs from birds and for classifying the type of platform based on spectral features. It is established that RF methods provide a high probability of detection only for drones with an active radio channel and are fundamentally unsuitable for autonomous and fiber-optic platforms. For acoustic systems, the key advantages of passive operation and non-line-of-sight (NLOS) capability are identified, while their limitations in terms of range, dependence on wind conditions, and elevated false alarm rates in urban noise are emphasized. For the electro-optical/infrared channel, a critical dependence on weather conditions, illumination, and thermal contrast is noted, as well as the need for external cueing due to the limited field of view at high optical magnification.

The necessity of transitioning from single-channel solutions to a multisensor architecture with Multi-Sensor Data Fusion (MSDF) and adaptive weighting of information flows depending on environmental parameters and channel reliability is substantiated. A conceptual model of an information and control surveillance system based on wireless sensor networks is proposed, incorporating indicators of measurement availability for different sensors, which is especially important in the absence of an RF component for detecting fiber-optic UAVs. The role of artificial intelligence algorithms in reducing false alarms, classifying micro-Doppler, visual, and acoustic features, and improving the reliability of real-time decision-making is emphasized. It is concluded that only the integration of several sensor modalities into a distributed networked MSDF system can provide the required probability of detecting small UAVs under stochastic environmental disturbances and evolving drone control methods.

Keywords: information and control system, unmanned aerial vehicle, fusion algorithm, detection methods, artificial intelligence, radio technologies, automatic control systems, data processing, wireless sensor networks, sensor.

1. Постановка проблеми в загальному вигляді

У сучасних умовах БпЛА набувають усе ширшого застосування в різноманітних галузях – від розважальних і цивільних до спеціалізованих військових систем. Паралельно із цим зростає актуальність створення надійних і результативних засобів їх своєчасного виявлення. Розроблення таких рішень становить складну науково-технічну проблему, оскільки більшість дронів характеризуються малими габаритами, низькою помітністю та здатністю функціонувати в умовах перешкод, складного рельєфу й несприятливих погодних факторів.

У статті здійснено ґрунтовний огляд ключових технологій і технічних підходів до виявлення БпЛА. Розглянуто їхні функціональні можливості, а також визначено основні переваги й обмеження кожного методу. Порівняльний аналіз сильних і слабких сторін різних підходів дозволяє сформулювати цілісне уявлення про їхню ефективність та доцільність застосування залежно від умов експлуатації й характеру загроз та підкреслити актуальність напрямку наукового дослідження.

Мета дослідження

Метою цієї роботи є проведення комплексного аналізу та впорядкування сучасних підходів до виявлення БпЛА з урахуванням їхніх технічних характеристик, експлуатаційної ефективності та функціональних обмежень. Дослідження орієнтоване на порівняльну оцінку основних сенсорних технологій – радіолокаційних, акустичних, оптико-електронних та радіочастотних систем – з визначенням їхніх сильних і слабких сторін у різних умовах застосування. Отримані результати покликані сформулювати систематизовану науково-методичну основу для подальшого вдосконалення існуючих і розроблення новітніх, більш результативних підходів виявлення БпЛА.

2. Аналіз останніх досліджень та публікацій

Радіолокаційні засоби (РЛС) використовуються для активного зондування простору та залишаються одним із базових каналів виявлення малорозмірних БпЛА, особливо за обмеженої видимості. У роботі [1] запропоновано метод виявлення й класифікації дронів за range-Doppler картами FMCW-радарів, де згортовка нейромережа підвищує стійкість до зниження сигналу на дальності та нечітких мікродоплерівських ознак. У дослідженні [2] проведено аналіз мікродоплерівських сигнатур БпЛА та показано, що коректне виділення мікрорухів (обертання гвинтів/роторів) у FMCW-спостереженнях підвищує точність класифікації, а також окреслено практичні обмеження для малих цілей. Додатково, сучасні огляди зазначають зсув від “класичної” детекції до DL-класифікації за мікродоплером та комбінування ознак для зменшення хибних тривог [3]. Оптико-електронні (ОЕ) засоби

забезпечують спостереження у видимому та ІЧ-діапазоні й активно розвиваються завдяки DL-детекторам малих об'єктів. У роботі [4] показано застосування YOLOv5 для виявлення малих дронів у тепловізійному діапазоні, що є критичним у сутінках/ночі та при слабкому контрасті. У статті [5] запропоновано модифікацію YOLOv5 (IRSDD-YOLOv5) зі спеціалізованими модулями для інфрачервоних малорозмірних цілей, що підвищує якість детекції саме для “малих” дронів у ІЧ-зображеннях. У роботі [6] YOLOv5 – метод, що застосовується як базова модель глибокого навчання для автоматичного виявлення БпЛА на зображеннях та відео, однак СВ-YOLOv5 покращує метрики детекції дронів завдяки змінам у backbone/neck та кращій роботі з дрібними об'єктами. Акустичні методи базуються на аналізі характерних частот і спектральних ознак двигунів/гвинтів БпЛА. У [7] запропоновано підхід із blind source separation для підвищення завадостійкості акустичного виявлення в реальному середовищі. У [8] експериментально досліджено ML-виявлення акустичних сигналів БпЛА з урахуванням дальності та впливу середовища, що важливо для налаштування порогів і сценаріїв розгортання сенсорів. Окремий сучасний напрям – DL-розпізнавання акустичних подій БпЛА (у т. ч. для мікрофонних масивів), що підвищує точність при низькому SNR [9], а також легкі архітектури, придатні для польового застосування [10]. Інтеграція різнотипних сенсорів та злиття даних у бездротових/розподілених мережах дозволяє істотно підвищити достовірність виявлення та знизити хибні спрацювання, порівняно з моносенсорними системами. У [11] показано ефективність злиття RF- та акустичних ознак із глибокими неймережами для підвищення надійності детекції. У [12] запропоновано ф'южн-підхід (RF + акустика) на рівні ознак/рішень для кращої ідентифікації БпЛА в завадах. У технічному звіті JRC [13] наведено таксономію сенсорів C-UAS та підкреслено, що мультисенсорне злиття є ключовим для задач DTI (від англ. Detection Tracking Identification) у реальному часі для критичної інфраструктури. Також у [14] продемонстровано неймережевий фреймворк аудіовізуального ф'южн-алгоритму для відокремлення дронів від фонових подій у відео- та аудіопотоках. Розподілені мережі БпЛА та децентралізована обробка розглядаються як перспектива для масштабування ІКС, але потребують адаптивних алгоритмів керування ресурсами, стійких каналів та узгоджених протоколів обміну. У [15] подано сучасний огляд застосувань AI в UAV-enabled wireless networks (планування, автономність, управління ресурсами), що формує наукову базу для децентралізованих рішень у мережах із БпЛА. Обробка великих обсягів даних та IoT-концепції стають критичними для ІКС, оскільки багатосенсорні системи генерують високошвидкісні потоки вимірювань і потребують малих затримок прийняття рішень. У [16] наведено огляд Edge AI як підходу до перенесення інтелектуальної обробки “на край” мережі (на сенсорні вузли/локальні сервери), що дозволяє зменшити затримку та навантаження на магістральні канали. У [17] виконано мета-огляд edge intelligence для IoT-сервісів, де узагальнено архітектури та типові обмеження (ресурси, енергія, приватність), важливі для побудови масштабованих ІКС. Крім того, у [18] систематизовано підходи big data analytics для інтелектуальних систем із потоковими даними, що корисно як загальний методологічний фундамент для підсистем зберігання/аналітики в ІКС. У [19] запропоновано ієрархічну модель інтелектуального управління мережею, у межах якої повітряні вузли на базі БпЛА можуть виступати носіями сенсорів і ретрансляторами даних, що є важливим для побудови розподілених систем спостереження та виявлення. У [20] виконано оцінку ефективності методологічних підходів до ієрархічного інтелектуального управління наземно-повітряною AD-Нос мережею із застосуванням алгоритмів машинного навчання, що створює підґрунтя для адаптивної маршрутизації, керування ресурсами та оперативного передавання результатів виявлення у багатосенсорних ІКС.

3. Виклад основного матеріалу

Сучасний етап розвитку Збройних Сил провідних країн світу характеризується фундаментальною трансформацією характеру повітряних загроз, обумовленого стрімким зростанням ролі БпЛА як у військовій сфері, так і в цивільному секторі. Результати аналізу

воєнних дій на території України 2022–2025 років, проведеного Royal United Services Institute (RUSI), свідчать, що понад 80 % бойових втрат спричинені БпЛА різних класів – від тактичних FPV-дронів масою 0,3–1,5 кг до ударних апаратів типу Shahed-136 з бойовою частиною 40–50 кг.

Масштаби застосування БпЛА є безпрецедентними, на основі статистичних даних The Economist, сумарні втрати обох сторін конфлікту сягають близько 10 000 дронів щомісяця. Зазначені тенденції породжують потребу в розробці ефективних систем виявлення та протидії БпЛА (Counter-UAS, C-UAS).

Водночас задача виявлення дронів є нетривіальною з огляду на специфічні характеристики таких повітряних об'єктів, як: малі геометричні розміри, низька ефективна площа розсіювання (ЕПР), відносно невелика швидкість польоту та низький рівень акустичного випромінювання електричних двигунів. Додаткову складність створює характер застосування БпЛА, тобто здатність здійснювати політ на малих висотах серед природних і штучних перешкод (рослинність, забудова), маскуючись на фоні птахів та інших рухомих об'єктів.

Виявлення малорозмірних БпЛА радіолокаційними засобами обмежується фундаментальними фізичними характеристиками цілей. Ефективна площа розсіювання комерційних і саморобних дронів варіюється в широких межах залежно від розміру, конструкції та матеріалів корпусу. Нано-БпЛА масою до 250 г мають ЕПР менше 0,001 м². Мікро-БпЛА типу FPV 5" характеризуються ЕПР в діапазоні 0,001–0,01 м². Міні-БпЛА класу DJI Mavic мають ЕПР 0,01–0,05 м². Малі БпЛА типу DJI Matrice – 0,05–0,1 м².

Залежність дальності виявлення від ЕПР визначається рівнянням радіолокації. Відношення сигнал/шум на виході приймача пропорційне четвертому степеню відношення ЕПР до четвертого степеня дальності. При зменшенні ЕПР вдвічі для збереження того ж відношення сигнал/шум необхідно зменшити дальність у $2^{1/4} \approx 1,19$ рази. Для типового протидронового радара з дальністю виявлення 10 км при ЕПР 0,01 м² дальність виявлення FPV-дрона з ЕПР 0,001 м² становитиме лише 5,6 км, що суттєво скорочує час на прийняття рішення та застосування засобів ураження.

Флуктуації ЕПР дронів внаслідок обертання роторів та зміни ракурсу спостереження суттєво ускладнюють стабільне супроводження. Варіації ЕПР можуть досягати 10–20 дБ протягом одного циклу обертання ротора, що відповідає першій моделі Сверлінга з коефіцієнтом варіації близько одиниці. Для компенсації флуктуацій необхідне застосування алгоритмів некогерентного накопичення або адаптивних методів виявлення.

Перспективним методом розрізнення БпЛА є аналіз мікродоплерівських сигнатур. Обертання роторів мультикоптерів створює характерну модуляцію відбитого сигналу, відому як HERM-лінії (Helicopter Rotor Modulation). Частота модуляції визначається швидкістю обертання роторів (3000–30000 об/хв) та кількістю лопатей, і типово знаходиться в діапазоні 50–500 Гц. Спектральний аналіз доплерівської модуляції дозволяє визначити тип апарата (квадрокоптер, гексакоптер, літак), кількість роторів та навіть наявність корисного навантаження за зміною інерції роторів.

Виявлення автономних БпЛА з оптоволоконним управлінням

FPV-дрони (First Person View) є домінуючим типом ударних БпЛА у сучасному російсько-українському конфлікті. Типові характеристики бойових FPV: маса 0,3–1,5 кг; розмір 200–350 мм по діагоналі; ЕПР 0,001–0,05 м²; швидкість 80–200 км/год; дальність 5–15 км для радіокерованих варіантів та 5–50 км для оптоволоконних; час польоту 5–15 хв; корисне навантаження 0,5–3 кг вибухівки.



Рис. 1. Основні компоненти управління FPV-дроном

Масштаби виробництва та застосування FPV-дронів показують експоненційне зростання. Україна у 2024 році придбала 1,5 млн FPV-дронів від вітчизняних та закордонних виробників. На 2025 рік заплановано закупівлю 4,5 млн одиниць – трикратне збільшення порівняно з попереднім роком. Динаміка місячного виробництва вражає: січень 2024 року – 20 000 одиниць, грудень 2024 року – 200 000 одиниць, план на грудень 2025 року – близько 540 000 одиниць. За протяжності активної лінії фронту 960 км щільність FPV-атак у 2025 році досягає приблизно 20 дронів на кілометр фронту на добу.

Оптоволоконні FPV-дрони представляють принципово нову загрозу для систем протидії БпЛА. Перше масове бойове застосування апаратів з оптоволоконним управлінням зафіксовано навесні 2024 року з боку російської федерації. Україна адаптувала технологію протягом кількох місяців. Технічно оптоволоконний FPV відрізняється від радіокерованого наявністю котушки з тонким одномодовим оптичним волокном діаметром 0,1–0,2 мм. Довжина кабелю серійних зразків складає 5–20 км, експериментальних – до 50 км. Швидкість передачі даних по оптоволокну досягає 1 Гбіт/с при затримці менше 1 мс. Додаткова вага котушки складає 500–1800 г, додаткова вартість – 200–500 дол. США.



Рис. 2. Управління FPV-дроном на основі оптоволоконного методу

Переваги оптоволоконних FPV визначають їхню зростаючу роль на полі бою. Повний імунітет до засобів радіоелектронної боротьби є ключовою перевагою, оскільки процес подавлення радіочастот не впливає на оптичний канал управління. За різними оцінками, засоби

РЕБ збивають 75–90 % радіокерованих дронів, тоді як ефективність проти оптоволоконних апаратів дорівнює нулю. Невидимість для RF-детекторів означає, що близько 40 % сенсорного парку сучасних систем протидії БпЛА, що базуються на радіочастотному виявленні, стають повністю неефективними. Ідеальна якість відеозв'язку забезпечується відсутністю інтерференції та мінімальними затримками оптичного каналу, що підвищує точність наведення. Можливість польоту в “радіотіні”, тобто у будівлях, лісових масивах, ярах та інших місцях з поганим радіопокриттям, що розширює тактичні можливості застосування. Режим «засідки» дозволяє дрону приземлитися біля дороги та чекати на ціль годинами з мінімальним енергоспоживанням.

Методи виявлення оптоволоконних FPV обмежені трьома типами сенсорів, що здатні реєструвати фізичний об'єкт незалежно від каналу управління. Радіолокаційні системи залишаються основним засобом виявлення, однак мала ЕПР оптоволоконних FPV (менше $0,01 \text{ м}^2$) обмежує практичну дальність до 2–5 км для типових антидронових радарів. Електрооптичні та інфрачервоні системи забезпечують візуальне виявлення, при цьому потребують зовнішнього цілевказання через обмежений кут огляду та неефективність вночі і в поганих погодних умовах. Акустичні системи реєструють звук роторів на дальності 150–500 м, що при швидкості цілі понад 100 км/год залишає лише 5–18 с на реакцію.

Формалізація завдання ІКС спостереження та виявлення БпЛА.

Нехай вектор стану цілі $\mathbf{x}(t) = [x, y, z, \dot{x}, \dot{y}, \dot{z}]^T$ описує положення та швидкість БпЛА у тривимірному просторі. Для кожного типу сенсора $s \in \text{radar}, RF, EO, \text{acoustic}$ визначимо функцію спостереження $\mathbf{h}_s(\mathbf{x})$ та індикатор доступності вимірювань $\chi_s(\mathbf{x}, \mathbf{e})$, де $\mathbf{e}$ – вектор параметрів середовища та характеристик цілі.

Для БпЛА з оптоволоконним управлінням:

$$\chi_{RF}(\mathbf{x}, \mathbf{e}_{fiber}) = 0 \quad \forall \mathbf{x}, t,$$

тобто RF-канал є принципово недоступним незалежно від положення цілі та умов функціонування. Матриця спостереження системи виглядає так:

$$\mathcal{O} = [\mathbf{H}_{\text{radar}} \ \mathbf{H}_{\text{EO}} \ \mathbf{H}_{\text{acoustic}}],$$

і не включає компоненту RF-детектора, що знижує загальну надійність виявлення та ускладнює задачу ідентифікації цілі.

Завдання ускладнюється тим, що оптико-електронні системи, які теоретично здатні виявляти будь-які візуально помітні об'єкти, мають суттєві обмеження: критична залежність від погодних умов (падіння ймовірності виявлення P_d на 50–80 % при тумані), неможливість роботи ЕО-каналу вночі, відсутність прямої інформації про дальність без активних лазерних далекомірів.

Таким чином, виявлення БпЛА з оптоволоконним управлінням потребує обов'язкового застосування радіолокаційних та акустичних сенсорів, причому з урахуванням малої ЕПР таких апаратів ($\sigma = 0,001\text{--}0,01 \text{ м}^2$ для типових FPV-дронів) дальність радіолокаційного виявлення суттєво обмежена.

Акустичні системи виявлення БпЛА

Акустичний метод виявлення БпЛА ґрунтується на реєстрації та аналізі характерних звукових коливань, що генеруються несучими гвинтами та силовими установками БпЛА. Високочутливі мікрофони, об'єднані у просторові решітки (масиви), забезпечують прослуховування акустичного простору в зоні відповідальності системи.

Принцип функціонування акустичних систем базується на вимірюванні часової затримки прийому звукового сигналу до елементів мікрофонного масиву, що дозволяє визначити

напрямок на джерело звуку. Застосування кількох просторово рознесених мікрофонних вузлів забезпечує можливість локалізації положення повітряного об'єкта методом тріангуляції.

Акустичні сенсорні системи здатні виявляти БпЛА в умовах відсутності прямої видимості, що є перевагою в умовах міської забудови та складного рельєфу. За результатами випробувань, ймовірність виявлення в ідеальних умовах становить $P_d = 0,995$, що є вищим показником серед розглянутих технологій.

До переваг акустичних датчиків слід віднести:

- повну пасивність роботи (відсутність власного випромінювання);
- здатність виявляти всі типи БпЛА, зокрема автономні апарати з оптоволоконним управлінням, що не використовують радіоканал;
- можливість функціонування в умовах обмеженої прямої видимості (NLOS);
- відносна простота розгортання та відносно-низька вартість (500–5 000 дол. США за сенсор).

Водночас акустичний метод має суттєві обмеження:

1. Мала дальність виявлення: типові значення для одиничного сенсора становлять 150–500 м для електричних БпЛА, що обумовлено швидким затуханням акустичних хвиль в атмосфері [10; 12]. Сучасні розробки з удосконаленими мікрофонними решітками дозволяють розширити радіус виявлення до 2 км (система Insignito Dumbo), а для БпЛА з двигунами внутрішнього згоряння заявляється дальність до 5 км.

2. Критична залежність від швидкості вітру: поріг працездатності системи обмежується значенням $V_{wind} < 15$ м/с. Пориви вітру створюють акустичний фон, що маскує звук БпЛА, та викривляють траєкторію поширення звукових хвиль.

3. Високий рівень хибних тривог: ймовірність хибної тривоги $P_{fa} = 0,03 - 0,10$ в міському середовищі, що є найвищим показником серед розглянутих технологій.

4. Похибка позиціонування: до $\pm 30^\circ$ по азимуту для одиничного сенсора без застосування мережевої тріангуляції.

5. При виявленні групових цілей (роїв БпЛА) акустична система фіксує лише сумарний звуковий сигнал без можливості диференціації окремих апаратів та може вимагати вирішення додаткової задачі класифікації.

Радіочастотні аналізатори для виявлення БпЛА

Радіочастотний (RF) метод виявлення орієнтований на реєстрацію та аналіз електромагнітного випромінювання, що використовується для управління БпЛА та передачі телеметричної інформації. Більшість комерційних і саморобних дронів функціонують у стандартних діапазонах частот (2,4 ГГц, 5,8 ГГц), що забезпечує можливість їх виявлення пасивними радіотехнічними засобами.

Існує два основні типи RF-аналізаторів: пеленгатори та декодери сигналів. Пеленгатори використовують антенні системи, як правило, кілька просторово рознесених приймачів для визначення напрямку на джерело радіовипромінювання шляхом вимірювання кута приходу сигналу. Для тривимірної локалізації цілі необхідно щонайменше три станції пеленгування.

Декодери сигналів здійснюють ідентифікацію протоколу зв'язку дрона з подальшим отриманням телеметричних даних. Сучасні системи, зокрема DroneShield DroneSentry з RFAI™ engine, забезпечують 360° покриття з класифікацією загроз та можливістю ідентифікації серійного номера дрона. Прикладом спеціалізованого декодера є система DJI Aeroscope, яка розпізнає сигнали апаратів виробництва DJI та збирає ідентифікаційну інформацію і координати БпЛА.

Переваги RF-аналізаторів включають:

- пасивний режим роботи без демаскуючого випромінювання;
- високу ймовірність виявлення комерційних БпЛА: $P_d = 0,95 - 1,0$ для апаратів з активним радіоканалом управління на дистанціях 1–5 км;
- низький рівень хибних тривог: $P_{fa} < 0,05$;

- можливість одночасного виявлення кількох БпЛА та локалізації позиції оператора;
- відносно невисоку вартість: 5–50 тис. дол. США за систему.

Обмеженням RF-методу є абсолютна неспроможність виявлення автономних апаратів без радіовипромінювання.

До категорії “невидимих” для RF-детекторів БпЛА належать:

1. FPV-дрони з оптоволоконним (fiber-optic) управлінням, що передають відеосигнал та команди керування по оптичному кабелю замість радіоканалу. Такі системи набули масового застосування на сучасному театрі воєнних дій завдяки повному імунітету до засобів РЕБ.

2. Автопілоти з INS/GNSS навігацією в режимі радіомовчання, які виконують політ за попередньо запрограмованим маршрутом без обміну даними з оператором.

3. Ударні БпЛА типу Shahed-136 на автономній ділянці траєкторії після виходу з зони управління продовжують політ автономно за даними інерціальної навігаційної системи з корекцією по GPS/ГЛОНАСС.

За експертними оцінками, близько 40 % сенсорного парку сучасних С-UAS систем базуються на RF-детекторах і є неефективними проти автономних загроз, що створює критичну прогалину в системі ППО, особливо із урахуванням тенденції до збільшення частки автономних БпЛА у загальній структурі загроз.

– Залежність від рельєфу, тобто від умов складної неоднорідної місцевості (міська забудова, ліс, пересічений рельєф) дальність виявлення значно зменшується через погане проходження радіохвиль крізь перешкоди.

– Фізичне випромінювання Wi-Fi, Bluetooth, стільниковий зв'язок створюють високий рівень завад, серед яких слабкий сигнал БпЛА може бути важко виокремити.

– Обмеженість бази сигнатур, вузькоспеціалізовані декодери не розпізнають нестандартні протоколи або апарати невідомих виробників.

Електрооптичні та інфрачервоні системи виявлення БпЛА

Оптичні системи виявлення використовують відеокамери видимого діапазону та тепловізори для реєстрації зображення БпЛА з подальшим автоматичним або напіваавтоматичним розпізнаванням цілей. Сучасні електрооптичні модулі, як правило, інтегрують денну камеру високої роздільності та інфрачервону камеру для забезпечення цілодобового функціонування.

Оптичні сенсори, як правило, працюють у режимі підтвердження виявлення, після отримання цілевказівки від первинного датчика (радар, RF-аналізатор) поворотна камера наводиться на відповідний сектор простору та здійснює ідентифікацію об'єкта. Системи класу CONTROP EO/IR (застосовуються в Rafael Drone Dome) досягають дальності 8 км з функціями автоматичного розпізнавання цілей (Automatic Target Recognition, ATR) та детекції руху у відеопотоці (Video Motion Detection, VMD).

Нижче наведено переваги оптико-електронних сенсорів:

- можливість візуальної ідентифікації типу цілі та характеру підвішеного навантаження;
- фіксація доказових матеріалів (фото/відео);
- пасивний режим роботи без демаскуючого випромінювання;
- висока ймовірність виявлення в ідеальних умовах, $P_d = 0,85 - 0,99$ (ясна погода, денний час, контрастний фон);

– здатність виявляти всі типи БпЛА, зокрема апарати з оптоволоконним управлінням.

Обмеження оптичного каналу:

1. Відсутність прямої інформації щодо дальності без застосування активних лазерних далекомірів. Камера визначає кутові координати цілі у площині зображення, що ускладнює тривимірну локалізацію об'єкта.

2. Залежність від погодних умов:

- Падіння видимості < 500 м P_d на 50–80 % при впливі туману;
- падіння P_d на 20–40 % при сильному дощі;

– неможливість роботи ЕО-каналу вночі, тобто необхідний перехід на IR-діапазон.

3. Вплив динамічних спотворень, так за даними MDPI 2024 [10], сильне розмиття руху (motion blur) спричиняє падіння метрики mAP (mean Average Precision) на 77 пунктів, що різко знижує точність автоматичної класифікації.

4. Високий рівень хибних тривог $P_{fa} = 0,05 - 0,20$. Птахи, сторонні об'єкти, літальні апарати на великій висоті можуть хибно класифікуватися як БпЛА.

5. Обмежене поле зору при великому збільшенні, тобто оптико-електронні системи з довгофокусною оптикою (30–60×) мають вузький кут огляду, що ускладнює самостійне панорамне сканування простору без зовнішнього цілевказання.

Тепловізійні камери забезпечують виявлення цілей в умовах обмеженої видимості (ніч, туман, задимлення), реєструючи теплове випромінювання силової установки та акумуляторних батарей БпЛА. Однак їхня ефективність залежить від теплового контрасту: в умовах високої температури повітря або при схожій температурі цілі та фону дрон може “зливатися” з оточенням.

Математично формалізація залежності ймовірності виявлення ЕО/IR системи від умов середовища виглядає наступним чином.

Нехай $e = [V_{vis}, T_{amb}, I_{light}, \sigma_{blur}]^T$ – вектор параметрів середовища, де V_{vis} – видимість, м; T_{amb} – температура повітря, °C; I_{light} – рівень освітленості, лк; σ_{blur} – параметр розмиття. Тоді:

$$P_d^{EO/IR}(e) = P_d^{max} \cdot \prod_i n_i(e),$$

де $n_i(e) \in [0,1]$ – коефіцієнти деградації для кожного фактора впливу. При несприятливих умовах добуток коефіцієнтів може знижувати P_d до критично низьких значень.

Радіолокаційні системи виявлення БпЛА

Радіолокаційний метод є одним з найбільш надійних підходів до виявлення повітряних цілей. Суть методу полягає у процесі ідентифікації об'єкта на основі ефекту Доплера, тобто радар випромінює електромагнітні хвилі та приймає відбитий сигнал, що дозволяє визначити дальність, азимут, кут місця та швидкість об'єкта. Однак класичні радіолокаційні станції протиповітряної оборони розраховані на виявлення цілей з великою ЕПР (літаки, ракети), тому малорозмірні БпЛА для таких систем є малопомітними.

Останніми роками розроблено спеціалізовані антидронові радары, оптимізовані для виявлення цілей з малою ЕПР та низькою швидкістю. Характерними особливостями таких систем є робота на підвищених частотах (X-діапазон ~10 ГГц, Ku-діапазон), формування вузьких діаграм направленості антен та застосування чутливих доплерівських фільтрів.

Критичним фактором для радіолокаційного виявлення БпЛА є мала ЕПР малорозмірних апаратів. За результатами досліджень IEEE/MDPI, типові значення ЕПР становлять:

- DJI Phantom 4: порівняно з ЕПР птахів становить $\sigma = 0,01-0,35 \text{ м}^2$;
- Nano/micro БпЛА: $\sigma = 0,0001-0,01 \text{ м}^2$;
- FPV-дрони: $\sigma = 0,001-0,05 \text{ м}^2$;
- ударні БпЛА типу Shahed-136: $\sigma = 0,1-0,5 \text{ м}^2$.

Залежність граничної дальності виявлення від ЕПР для X-band FMCW радарів описується співвідношенням:

- при $\sigma = 0,1 \text{ м}^2$: $R_{max} = 3 \text{ км}$ при $P_d = 0,83$, $P_{fa} = 10^{-2}$;
- при $\sigma = 0,01 \text{ м}^2$: $R_{max} \approx 1,5 \text{ км}$ при $P_d = 0,60$.

Дальність виявлення залежить від ЕПР за законом четвертого кореня (рівняння дальності радіолокації), що наведено нижче:

$$R_{max} = \sqrt[4]{\frac{P_t G^2 \lambda^2 \sigma}{(4\pi)^3 P_{min}}},$$

де P_t – потужність передавача; G – коефіцієнт підсилення антени; λ – довжина хвилі; σ – ЕПР цілі; P_{min} – мінімальна потужність сигналу для виявлення.

Перспективним напрямком є застосування технології аналізу мікродоплерівського підпису цілі характерних модуляцій відбитого сигналу, спричинених обертанням несучих гвинтів БпЛА. Така інформація дозволяє відрізнити дрон від птаха, так за даними, точність класифікації досягає $> 98\%$ при застосуванні методів машинного навчання на основі мікродоплерівських сигнатур.

Переваги радарних систем:

- найбільша дальність виявлення серед розглянутих типів сенсорів (2–15+ км для тактичних систем, до 250 км для систем класу Thales GM200 MM);
- незалежність від погодних умов та освітлення;
- можливість точного автоматичного супроводження траєкторії одночасно десятків цілей;
- здатність виявляти повільні об'єкти, наприклад мінімальна доплерівська швидкість може становити до 0,1 м/с;
- низький рівень хибних тривог $P_{fa} < 0,01$;
- здатність виявляти всі типи БпЛА, зокрема автономні апарати з оптоволоконним управлінням.

До основних обмежень радіолокаційних систем відносяться:

- Висока вартість впровадження та масштабування. Капітальні витрати на розгортання однієї одиниці обладнання варіюються в діапазоні від 50 тис. дол. США до понад 500 тис. дол. США, що робить економічно недоцільним побудову щільного поля покриття для захисту великих територій.
- Залежність дальності виявлення від ЕПР. Експериментально підтверджено кореляцію між дистанцією детекції та фізичними розмірами цілі. Для класу малорозмірних FPV-дронів, що характеризуються значенням ЕПР $\sigma < 0,01 \text{ м}^2$, ефективна дальність виявлення деградує до значень 1–2 км, що не забезпечує достатнього часового запасу для реакції системи управління.
- Обмеження умов розповсюдження радіохвиль (NLOS). Функціонування класичних РЛС вимагає наявності прямої видимості (Line-of-Sight). В умовах складної забудови або пересіченої місцевості (режим Non-Line-of-Sight, NLOS) здатність системи до виявлення цілей суттєво знижується або втрачається повністю через ефекти затінення.
- Низька електромагнітна сумісність та прихованість. Активний режим випромінювання зондувальних сигналів виступає потужним демаскуючим фактором, що дозволяє засобам радіотехнічної розвідки противника виявляти, ідентифікувати та локалізувати позиції РЛС на значних відстанях.

Перевагою радіолокаційних систем в контексті виявлення БпЛА з оптоволоконним управлінням є їхня здатність виявляти будь-які фізичні об'єкти незалежно від наявності чи відсутності радіовипромінювання з боку цілі. Радар “бачить” fiber-optic FPV так само, як і звичайний дрон з радіоканалом, оскільки принцип виявлення базується на відбитті електромагнітних хвиль від корпусу апарата. Це робить радіолокаційні системи незамінним компонентом багатосенсорних комплексів протидії БпЛА.

Узагальнення характеристик розглянутих типів сенсорів на основі даних провідних світових виробників наведено у таблиці 1.

Таблиця 1

Порівняльні характеристики сенсорних підсистем виявлення БпЛА

Параметр	Акустичні	Радіочастотні	Радарні	ЕО/ІР	Multi-sensor
Дальність виявлення, км	0,15–0,5	1–5	2–15+	0,5–4	0,5–15+
P_d (ідеальні умови)	0,995	0,95–1,0	0,80–0,99	0,85–0,99	> 0,95
P_{fa}	0,03–0,10	< 0,05	< 0,01	0,05–0,20	< 0,01
Автономні БпЛА	так	ні	так	так	так
Погодні умови	низька	висока	висока	низька	адаптивна
NLOS виявлення	так	так	ні	ні	так

Як видно з таблиці, радіочастотні детектори є єдиним типом сенсорів, принципово нездатним виявляти БпЛА з оптоволоконним управлінням, що обумовлює необхідність включення до складу багатосенсорної системи радарних та/або акустичних компонентів.

Результати порівняльного аналізу тактико-технічних характеристик засобів моніторингу свідчать про відсутність сенсорної модальності, здатної забезпечити стабільно високі показники імовірності виявлення об'єктів $P_{det} \rightarrow 1$ за умов впливу стохастичних збурень зовнішнього середовища. Для кожного класу сенсорів характерна наявність специфічних системних обмежень.

РЛС характеризуються найвищою стійкістю до метеорологічних факторів, однак їхня ефективність суттєво знижується під час детекції об'єктів із малою ЕПР, особливо на фоні підстилюючої поверхні.

Функціонування акустичних пеленгаторів має сильну залежність від параметрів атмосферного впливу, зокрема швидкості та напрямку вітру, наслідком чого стає деградація співвідношення сигнал/шум.

Для оптико-електронних та інфрачервоних систем властиве падіння ефективності виявлення до мінімальних значень за умов низької оптичної прозорості атмосфери, спричиненої туманом, опадами або задимленням.

Радіочастотні детектори принципово нездатні виявляти БпЛА під час роботи в режимі повної автономності без активного обміну даними з наземними станціями управління.

Наявна гетерогенність обмежень обумовлює необхідність переходу від одноканальних систем до комплексування інформаційних потоків (Multi-Sensor Data Fusion). Оптимальним рішенням вбачається застосування адаптивних алгоритмів обробки даних для динамічного зважування показань кожного сенсора в режимі реального часу на основі поточних параметрів середовища та апіорної оцінки достовірності каналу.

Висновки та напрямки подальших досліджень

Таким чином, аналіз сучасних багатосенсорних систем та бойового досвіду російсько-українського конфлікту дозволяє сформулювати низку важливих узагальнень щодо побудови ефективних систем протидії БпЛА.

Принцип багатосенсорної інтеграції є визначальним для побудови ефективних систем виявлення. Жодна окрема технологія не забезпечує надійного виявлення всього спектра загроз: радарні обмежені малою ЕПР цілей, RF-детектори неспроможні виявляти автономні та оптоволоконні дрони, ЕО/ІР-системи залежать від погодних умов, акустичні системи мають обмежену дальність. Лише інтеграція 2–4 типів сенсорів забезпечує взаємне доповнення можливостей та компенсацію обмежень.

Поява оптоволоконних методів управління FPV-дронами знаменує зміну парадигми протидії БпЛА. Близько 40 % існуючих систем С-UAS, що базуються на RF-технологіях, стають неефективними проти цього типу загроз. Виявлення можливе лише радарними, оптичними та акустичними засобами, що потребує перегляду архітектури систем протидії.

Тенденція до децентралізації систем протиповітряної оборони проявляється у забезпеченні кожного тактичного підрозділу власними засобами виявлення та нейтралізації.

Мобільні вогневі групи з великокаліберними кулеметами та тепловізійними прицілами демонструють високу ефективність при нижчій вартості за традиційні ЗРК.

Зростання ролі методів штучного інтелекту проявляється як у системах виявлення для автоматичної класифікації цілей та фільтрації хибних тривог, так і в системах управління БпЛА для координації роїв та автономного наведення.

Розподілені сенсорні мережі раннього попередження набувають ключового значення. Акустичні сенсори, пости візуального спостереження та RF-моніторинг, розгорнуті на глибині 5–10 км від лінії фронту, компенсують обмеження радарного виявлення малорозмірних цілей.

Перспективними напрямками подальших досліджень є розроблення стохастичних моделей адаптивного зважування сенсорних каналів, впровадження глибинного навчання у задачі багаторівневого ф'южн та створення енергоефективних розподілених сенсорних мереж із можливістю автономного прийняття рішень у реальному часі. Отримані результати можуть бути використані під час проєктування сучасних систем протидії БпЛА та оптимізації структури інформаційно-керуючих систем у військовій і критичній інфраструктурі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Han S.-K., Lee J.-H. Convolutional Neural Network-Based Drone Detection and Classification Using Overlaid Frequency-Modulated Continuous-Wave (FMCW) Range-Doppler Images // *Sensors*. 2024. Vol. 24, No. 17. Art. 5805. DOI: 10.3390/s24175805.
2. Bourn W., Paine S., Pidanic J. Micro-Doppler Signature Classification of Unmanned Aerial Vehicles Using FMCW Radar: proceedings of the 2024 International Radar Conference (RADAR). 2024. DOI: 10.1109/RADAR58436.2024.10994122.
3. Semenyuk V., et al. Advances in UAV detection: integrating multi-sensor technologies and data fusion techniques // *International Journal of Critical Infrastructure Protection*. 2025. Art. 100744. DOI: 10.1016/j.ijcip.2025.100744.
4. Zubkov O., Sheiko S. Detection of Small Drones in Thermal Infrared Range Using YOLOv5 Neural Networks: proceedings of the 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). 2022. DOI: 10.1109/PICST57299.2022.10238493.
5. Yuan S., et al. IRSDD-YOLOv5: Focusing on the Infrared Detection of Small Drones // *Drones*. 2023. Vol. 7, No. 6. Art. 393. DOI: 10.3390/drones7060393.
6. Atik I., et al. Enhancing drone detection with BottleneckCSP and cross convolution in YOLOv5 // *Radiation Physics and Chemistry*. 2023. (Elsevier). (Дані про том/стор. — на сторінці видавця).
7. Wang W., Fan K., Ouyang Q., Yuan Y. Acoustic UAV detection method based on blind source separation framework // *Applied Acoustics*. 2022. Vol. 200. Art. 109057. DOI: 10.1016/j.apacoust.2022.109057.
8. Tejera-Berengue D., Zhu-Zhou F., Utrilla M., Gil-Pita R. Acoustic-Based Detection of UAVs Using Machine Learning: Analysis of Distance and Environmental Effects: proceedings of the 2023 IEEE Sensors Applications Symposium (SAS). 2023. DOI: 10.1109/SAS58821.2023.10254127.
9. Sun Y., Li, et al. Deep Learning-based drone acoustic event detection system for microphone arrays // *Multimedia Tools and Applications*. 2023. DOI: 10.1007/s11042-023-17477-1.
10. Liu Z., et al. Deep Learning-Based Acoustic Recognition of UAVs in Complex Environments // *Drones*. 2025. Vol. 9, No. 6. Art. 389. DOI: 10.3390/drones9060389.
11. Frid A., Ben-Shimol Y., Manor E., Greenberg S. Drones Detection Using a Fusion of RF and Acoustic Features and Deep Neural Networks // *Sensors*. 2024. Vol. 24, No. 8. Art. 2427. DOI: 10.3390/s24082427.
12. Aouladhadj D., et al. Drone Detection and Tracking Using RF Identification Signals // *Sensors*. 2023. Vol. 23, No. 17. Art. 7650. DOI: 10.3390/s23177650.
13. Grieco G., Amendola D., Anderson D. Counter-drone systems and data fusion. Luxembourg: Publications Office of the European Union, 2024. (Tech. rep.).
14. Audio-Visual Fusion and Deep Learning for Drone Detection // *Proceedings of the ACM* (конф. публікація). 2024. DOI: 10.1145/3643833.3656133.

15. Zhou L., et al. A Comprehensive Survey of Artificial Intelligence in UAV-enabled Wireless Networks // ICT Express (Elsevier). 2024.
16. Singh R., et al. Edge AI: A survey // Intelligent Systems with Applications. 2023. (Elsevier).
17. Barbuto V., et al. Disclosing Edge Intelligence: A Systematic Meta-Survey // Big Data and Cognitive Computing. 2023. (PDF).
18. Wang J., et al. Big data analytics for intelligent manufacturing systems: a review // Journal of Manufacturing Systems. 2022. (Elsevier).
19. Беляков Р. О. Ієрархічна модель інтелектуального управління наземно-повітряної комунікаційної мережі спеціального призначення // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2024. № 54. С. 225–235. DOI: 10.36910/6775-2524-0560-2024-54-28.
20. Беляков Р. О., Фесенко О. Д. Оцінка ефективності методологічних підходів ієрархічного інтелектуального управління наземно-повітряною комунікаційною AD-Нос мережею // Системи і технології зв'язку, інформатизації та кібербезпеки. 2024. Вип. № 5. DOI: 10.58254/viti.5.2024.02.15.

Надійшла до редколегії 18.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.942:621.865.8

Куцаєв В. В. ORCID: 0000-0001-8213-4739 (ВІТІ ім. Героїв Крут)

Семитківська І. В. ORCID: 0009-0000-9962-5032 (ВІТІ ім. Героїв Крут)

Скоропад С. І. ORCID: 0009-0002-3712-5301 (ІСЗІ КПІ ім. Ігоря Сікорського)

Цимбал І. В. ORCID: 0000-0001-7294-3794 (ВІТІ ім. Героїв Крут)

ЗАСТОСУВАННЯ СИМУЛЯЦІЙНОГО СЕРЕДОВИЩА GAZEBO ДЛЯ НАУКОВИХ ДОСЛІДЖЕНЬ У ГАЛУЗІ РОБОТОТЕХНІЧНИХ СИСТЕМ

У статті обґрунтовано доцільність застосування симуляційного середовища Gazebo як цифрового науково-експериментального полігону для дослідження автономних робототехнічних систем. Показано, що науковий потенціал Gazebo полягає не лише у візуалізації руху робота, а у створенні відтворюваного, параметризованого та метрично контролюваного середовища, у якому можуть бути задані модель світу, модель робота, сенсорна система, алгоритмічний стек, експериментальні сценарії, протокол дослідження та масив даних. Запропоновано методологічну схему Gazebo-експерименту у вигляді формалізованого дослідницького контуру, що поєднує фізичне моделювання, сенсорну генерацію даних, ROS2-інтеграцію, сценарне варіювання та кількісне оцінювання результатів.

Для підвищення доказовості симуляційного дослідження сформовано систему метрик, яка охоплює похибку локалізації, похибку побудови карти, час виконання місії, довжину траєкторії, кількість зіткнень, небезпечних зближень, перепланувань, частку успішних запусків та інтегральний показник ризику місії. Сформульовано леми про відтворюваність симуляційної конфігурації, метричне спостереження результатів і порівняння алгоритмічних конфігурацій, на основі яких запропоновано теорему про метричну валідність симуляційного експерименту в Gazebo.

Проведена модельна апробація на прикладі автономної навігації мобільного робота засвідчила закономірне погіршення показників ефективності за умов ускладнення сценаріїв і деградації сенсорної інформації. Отримані результати підтверджують можливість використання Gazebo як проміжної ланки між теоретичним моделюванням, програмною реалізацією алгоритмів і подальшою фізичною апробацією робототехнічних систем.

Ключові слова: Gazebo, робототехнічні системи, симуляційне моделювання, ROS 2, SLAM, цифровий полігон, автономна навігація, сенсорне моделювання, sim-to-real.

V. Kutsaiev, I. Semytkivska, S. Scoropad, I. Tsymbal. Application of the Gazebo simulation environment for scientific research in the field of robotic systems

The article substantiates the feasibility of using the Gazebo simulation environment as a digital scientific and experimental testbed for studying autonomous robotic systems. It is shown that the scientific potential of Gazebo lies not only in visualizing robot motion, but also in creating a reproducible, parameterized, and metrically controlled environment in which a world model, robot model, sensor system, algorithmic stack, experimental scenarios, research protocol, and data set can be explicitly defined. A methodological scheme of a Gazebo-based experiment is proposed as a formalized research loop that combines physical modeling, sensor data generation, ROS2 integration, scenario variation, and quantitative assessment of results.

To strengthen the evidential value of simulation-based research, a system of metrics is developed, including localization error, map-building error, mission completion time, path length, number of collisions, near-collision events, replanning operations, mission success rate, and an integral mission risk indicator. Lemmas on the reproducibility of the simulation configuration, metric observability of results, and comparability of algorithmic configurations are formulated. On this basis, a theorem on the metric validity of a simulation experiment in Gazebo is proposed.

A model-based approbation using the example of autonomous navigation of a mobile robot demonstrated a regular deterioration of performance indicators under increasing scenario complexity and degradation of sensor information. The obtained results confirm the possibility of using Gazebo as an intermediate methodological link between theoretical modeling, software implementation of algorithms, and subsequent physical validation of robotic systems.

Keywords: Gazebo, robotic systems, simulation modeling, ROS 2, SLAM, digital polygon, autonomous navigation, sensor modeling, sim-to-real.

Постановка проблеми. Сучасні наукові дослідження у сфері робототехнічних систем дедалі частіше потребують не лише теоретичного обґрунтування алгоритмів, а й їхньої багаторазової експериментальної перевірки в умовах наближених до реального фізичного середовища. Особливо це стосується автономної навігації, багатосенсорного сприйняття,

планування траєкторій, координації груп роботів, адаптивного керування та взаємодії робота з динамічними об'єктами. Проведення таких експериментів безпосередньо на фізичних роботах часто є дорогим, тривалим, технічно ризикованим і недостатньо відтворюваним [1]. У цьому контексті симуляційні середовища стають важливим елементом наукової методології.

Gazebo історично створювався як відкрите середовище для тривимірного динамічного моделювання багатороботних систем. У класичній праці [2] N. Koenig і A. Howard підкреслювалося, що Gazebo має заповнити нішу між простими двовимірними симуляторами та складними фізичними експериментами, забезпечуючи моделювання складних тривимірних середовищ для мобільних роботів. Сучасний Gazebo Sim розвиває цю ідею як відкрите середовище робототехнічної симуляції з підтримкою фізики, рендерингу, сенсорних моделей, графічного інтерфейсу, плагінів, асинхронного обміну повідомленнями та сервісів. Важливо також враховувати зміну технологічного контексту: Gazebo Classic досяг кінця життєвого циклу у січні 2025 року, тому для нових наукових досліджень доцільно орієнтуватися саме на сучасну лінійку Gazebo Sim та її інтеграцію з ROS 2.

Попри широке використання Gazebo в освітній та інженерній практиці, у наукових роботах його нерідко описують спрощено, лише як середовище для «перевірки роботи робота». Такий підхід не повністю розкриває його дослідницький потенціал. Gazebo може бути використаний як інструмент формування контрольованої експериментальної реальності, у якій дослідник має змогу задавати геометрію середовища, фізичні параметри об'єктів, моделі сенсорів, рівень шумів, сценарії руху перешкод, конфігурації роботів і програмні алгоритми керування.

Наукова проблема полягає у визначенні того, яким чином Gazebo може бути формалізований не лише як програмне забезпечення, а як елемент дослідницької методології: тобто як середовище для постановки гіпотези, побудови експериментального сценарію, збирання даних, кількісної оцінки результатів і підготовки алгоритмів до подальшої фізичної апробації.

Аналіз останніх досліджень і публікацій. Аналіз наукових джерел засвідчує, що симуляційні середовища стали одним із ключових інструментів сучасних досліджень у галузі робототехніки, автономних мобільних платформ, багатосенсорної навігації та алгоритмічного керування. Їхня роль полягає не лише у візуальній демонстрації поведінки робота, а й у забезпеченні контрольованої, відтворюваної та параметризованої експериментальної бази для перевірки наукових гіпотез. Однією з фундаментальних праць [2] з цієї теми є робота N. Koenig та A. Howard, у якій Gazebo було представлено як відкрите тривимірне динамічне середовище для багатороботної симуляції, призначене для відтворення складних умов функціонування мобільних роботів. Саме ця праця заклала методологічне підґрунтя для розуміння Gazebo як інструмента швидкої перевірки концепцій, стратегій і алгоритмів у робототехніці.

У сучасному технологічному контексті Gazebo розглядається вже не тільки як симулятор руху роботів, а як повноцінна відкрита платформа робототехнічної симуляції. Офіційна документація [3] Gazebo Sim визначає його як open-source robotics simulator, що надає користувачам можливості високоточного фізичного моделювання, рендерингу, сенсорних моделей, графічного інтерфейсу, плагінів, асинхронного обміну повідомленнями та сервісів. Така архітектура створює передумови для використання Gazebo як цифрового експериментального полігону, у якому можуть одночасно відтворюватися фізична динаміка робота, інформаційна картина середовища, робота сенсорів і керуюча логіка автономної системи.

Важливою тенденцією останніх років є перехід від Gazebo Classic до сучасної лінійки Gazebo Sim. За офіційними повідомленнями спільноти Gazebo [4], Gazebo Classic, зокрема Gazebo 11, досяг закінчення життєвого циклу 31 січня 2025 року, а користувачам рекомендовано переходити на сучасні LTS-версії Gazebo, зокрема Harmonic або Fortress.

Це має принципове значення для наукових досліджень, оскільки довгостроково відтворювані експерименти, навчальні курси, дисертаційні роботи та програмні прототипи доцільно будувати вже з урахуванням сучасної архітектури Gazebo Sim і ROS 2.

Окремий науково-технологічний напрямок пов'язаний з інтеграцією Gazebo та ROS 2. У роботі [5] S. Macenski, T. Foote, B. Gerkey, C. Lalancette та W. Woodall ROS 2 розглядається як нове покоління робототехнічної програмної архітектури, орієнтованої на модульність, масштабованість, надійність, сенсорну обробку, планування, мобільність та автономність. У цьому контексті Gazebo перестає бути ізольованим середовищем моделювання і перетворюється на фізично-сенсорний шар ширшої робототехнічної екосистеми, у якій ROS 2 забезпечує комунікаційний, алгоритмічний та виконавчий рівні. Значна частина сучасних досліджень застосовує Gazebo для перевірки алгоритмів автономної навігації мобільних роботів [6]. У цьому контексті важливе місце посідає Navigation2, або Nav2, який є сучасним навігаційним стеком ROS 2 для мобільних роботів і дає змогу реалізовувати рух у складних середовищах із виконанням користувацьких завдань. Використання Gazebo разом із Nav2 створює основу для побудови відтворюваних експериментів, у яких можна оцінювати якість траєкторії, час досягнення цілі, кількість перепланувань, стабільність руху, уникання перешкод і поведінку робота за різних конфігурацій середовища.

Ще одним важливим напрямом є дослідження SLAM та картографування. У роботі [7] S. Macenski та I. Jambrecic, для задач SLAM у динамічному світі показаний інструмент SLAM Toolbox. У поєднанні з Gazebo такий інструментарій дозволяє створювати контрольовані експериментальні сцени, у яких еталонна геометрія середовища відома заздалегідь, а побудована роботом карта може бути кількісно порівняна з референтною моделлю. Це особливо важливо для наукових робіт, де необхідно не лише продемонструвати функціонування SLAM-алгоритму, а й оцінити його стійкість до шумів сенсорів, динамічних перешкод, неповних даних і змін структури середовища.

В українському науково-освітньому контексті окремої уваги заслуговує навчальний посібник [8] А. П. Бернацького, що присвячений практичному програмуванню робототехнічних систем із використанням симулятора Gazebo ROS, з акцентом на військове застосування. Науково-практична значущість зазначеного посібника полягає в тому, що Gazebo ROS у ньому розглядається не ізольовано, а як модульне середовище розробки автономних роботів, де кожен компонент системи може бути представлений окремим вузлом, що взаємодіє з іншими через стандартизовані комунікаційні механізми. На відміну від багатьох робіт, у яких Gazebo використовується переважно для перевірки окремого алгоритму навігації, SLAM, уникання перешкод або сенсорної конфігурації, А. Бернацький репрезентує ширший навчально-дослідницький підхід. Автор показує Gazebo ROS як середовище формування цілісної архітектури автономної та розподіленої робототехнічної системи. Це дозволяє пов'язати практичне програмування роботів із задачами сценарного моделювання, військово-технічної підготовки, багатороботної взаємодії, AI-підтримки та подальшої інженерної й науково-дослідної діяльності у сфері робототехніки.

Таким чином, наявні дослідження та публікації формують кілька взаємопов'язаних напрямів застосування Gazebo. Перший напрям пов'язаний із загальною ідеєю тривимірної багатороботної симуляції, започаткованою в ранніх роботах N. Koenig і A. Howard. Другий напрям стосується розвитку сучасного Gazebo Sim як відкритої платформи з фізичним, сенсорним і програмним рівнями моделювання. Третій напрям пов'язаний з інтеграцією Gazebo та ROS 2, що дозволяє створювати повний програмно-алгоритмічний стек автономного робота. Четвертий напрям охоплює прикладні дослідження навігації, SLAM, сенсорного сприйняття та багатороботної координації. П'ятий напрям, представлений зокрема роботою А. П. Бернацького, розширює застосування Gazebo у бік навчально-дослідницького, військово-прикладного та сценарно-орієнтованого моделювання робототехнічних систем.

Водночас аналіз джерел показує, що більшість робіт зосереджується або на технічних можливостях Gazebo, або на перевірці окремих алгоритмів. Незважаючи на значну кількість праць, присвячених використанню Gazebo для моделювання робототехнічних систем, недостатньо дослідженим залишається питання його методологічної формалізації як цілісної науково-експериментальної платформи. Наявні джерела переважно розкривають Gazebo як інструмент симуляції, перевірки окремих алгоритмів або навчального програмування роботів, тоді як подальшого розвитку потребує підхід, у межах якого Gazebo розглядається як відтворюване, параметризоване та метрично контрольоване середовище для постановки гіпотез, проведення серій експериментів, оцінювання невизначеності, порівняння алгоритмів і підготовки автономних робототехнічних систем до переходу від симуляційного до реального середовища.

Мета дослідження. Метою статті є обґрунтування застосування Gazebo як наукового інструменту для проведення експериментальних досліджень робототехнічних систем.

Виклад основного матеріалу. У сучасних дослідженнях робототехнічних систем Gazebo доцільно розглядати не лише як програмний симулятор для візуалізації руху робота, а як цифрове науково-експериментальне середовище, у межах якого дослідник може формувати контрольовані умови, задавати параметри середовища, моделювати фізичну поведінку робототехнічної платформи, відтворювати сенсорні потоки, інтегрувати алгоритми керування та здійснювати кількісну оцінку результатів. Такий підхід дозволяє перейти від демонстраційного використання Gazebo до його методологічного застосування як інструмента наукового експерименту. На відміну від фізичного полігону, де значна частина умов має випадковий або важко контрольований характер, Gazebo дозволяє створити параметризоване середовище, у якому кожна змінна може бути зафіксована, змінена або повторена в серії експериментів. Це є принципово важливим для наукових досліджень, оскільки забезпечує відтворюваність, порівнюваність і метричну контрольованість результатів.

У межах запропонованого підходу Gazebo виконує функцію цифрового експериментального полігону, який поєднує фізичне моделювання, сенсорну генерацію даних, програмно-алгоритмічне керування та аналітичну обробку результатів. Саме така інтеграція дозволяє використовувати Gazebo не лише для попереднього тестування роботів, а й для постановки наукових гіпотез, проведення серій експериментів, оцінювання ефективності алгоритмів і підготовки до подальшої фізичної апробації.

Методологічна схема дослідження в Gazebo має будуватися не як випадкова послідовність запуску симуляції, а як цілісний науковий експеримент, у якому визначаються об'єкт, предмет, гіпотеза, змінні, сценарії, метрики, протокол повторення та критерії інтерпретації результатів. У такій логіці Gazebo стає проміжною ланкою між математичною моделлю робототехнічної системи, програмною реалізацією алгоритму та майбутнім фізичним експериментом.

У загальному вигляді дослідницький контур у Gazebo можна подати як систему (1):

$$E_G = \langle W, R, S, A, C, M, P, D \rangle, \quad (1)$$

де W – модель симуляційного світу; R – модель робота або групи роботів; S – система сенсорів; A – алгоритмічний стек керування; C – набір експериментальних сценаріїв; M – система метрик оцінювання; P – протокол проведення експерименту; D – масив отриманих експериментальних даних.

Така формалізація дозволяє розглядати Gazebo не як допоміжну програмну оболонку, а як структуровану платформу наукового дослідження. Кожен елемент цієї системи має власну функцію: модель світу задає умови експерименту; модель робота визначає фізичні й кінематичні властивості платформи; сенсорна система формує інформаційний образ середовища; алгоритмічний стек забезпечує автономну поведінку; сценарії задають умови

перевірки; метрики дозволяють кількісно оцінити результат; протокол забезпечує повторюваність; дані створюють основу для подальшого аналізу. Візуалізація методологічної схеми Gazebo-експерименту показана на рис.1.

Для того щоб використання Gazebo у науковому дослідженні мало не лише демонстраційний, а й доказовий характер, результати симуляції повинні бути представлені через систему кількісних метрик. Сам факт успішного руху робота в середовищі Gazebo ще не є достатньою підставою для наукового висновку. Наукову цінність має не візуальне спостереження за поведінкою моделі, а можливість виміряти, порівняти й інтерпретувати цю поведінку за визначеними показниками.

У загальному вигляді систему метрик для оцінювання результатів експерименту в Gazebo можна подати як множину (2).

$$M = \{e_{loc}, e_{map}, T_{mission}, L_{path}, N_{coll}, N_{near}, N_{replan}, C_{cpu}, P_{succ}, R_{mission}\}, \quad (2)$$

де e_{loc} – похибка локалізації; e_{map} – похибка побудови карти; $T_{mission}$ – час виконання місії; L_{path} – фактична довжина траєкторії; N_{coll} – кількість зіткнень; N_{near} – кількість небезпечних зближень; N_{replan} – кількість перепланувань; C_{cpu} – обчислювальне навантаження; P_{succ} – частка успішних запусків; $R_{mission}$ – інтегральний показник ризику місії.

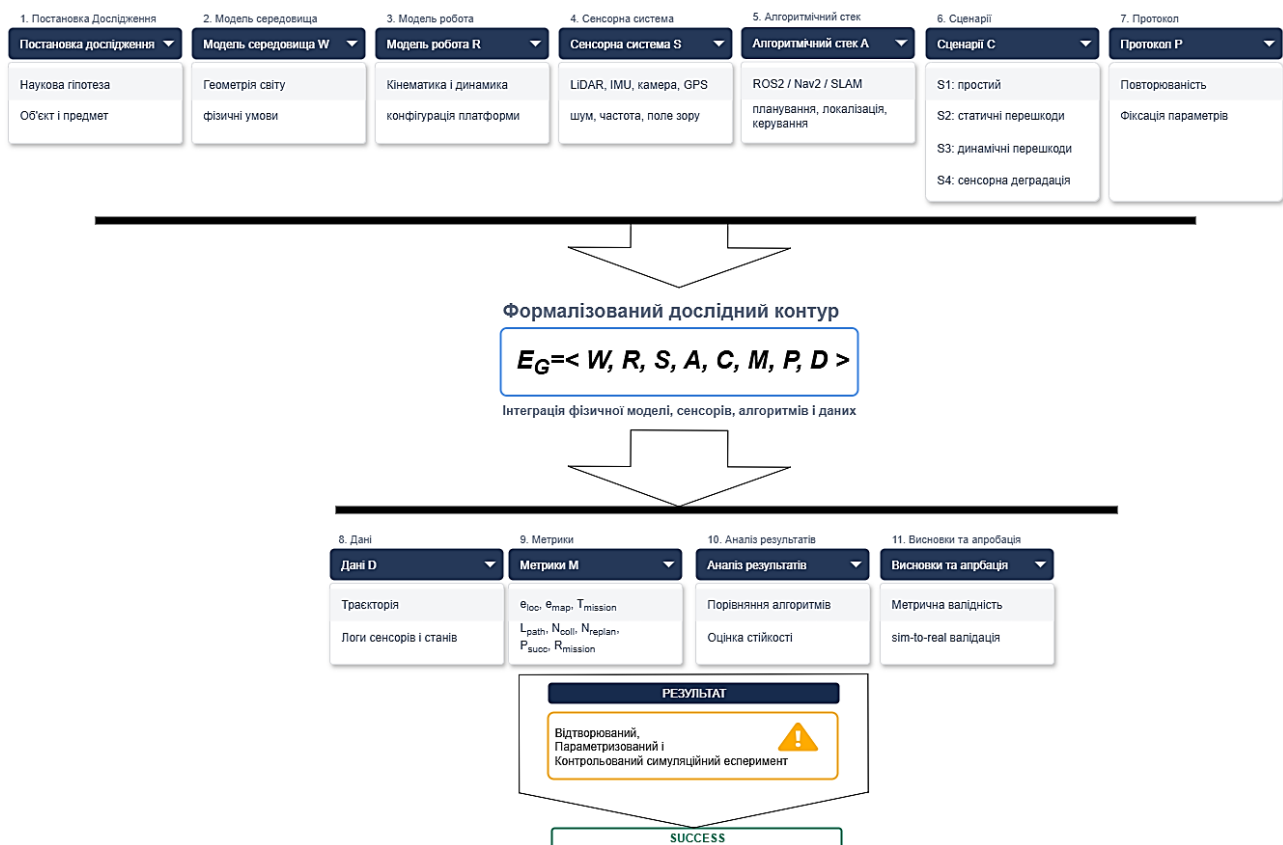


Рис. 1. Візуалізація методологічної схеми Gazebo-експерименту

Вибір конкретних метрик залежить від предмета дослідження. Для задач автономної навігації ключовими є час виконання місії, довжина траєкторії, кількість зіткнень, небезпечних зближень і перепланувань. Для задач SLAM основне значення мають похибка локалізації, похибка побудови карти, накопичення дрейфу та якість замикання циклів. Для багатороботних систем доцільно додатково враховувати ефективність координації, кількість

конфліктів траєкторій, час колективного виконання завдання, стійкість групи до втрати окремих агентів і якість обміну інформацією.

Частку успішного виконання місії можна визначити як (3):

$$P_{succ} = \frac{N_{total}}{N_{success}}, \quad (3)$$

де $N_{success}$ – кількість успішних запусків, у яких робот досяг цільової точки без порушення заданих обмежень, а N_{total} – загальна кількість запусків у відповідному сценарії. Цей показник дозволяє оцінювати не одиничний результат, а стабільність поведінки робототехнічної системи в серії повторюваних експериментів.

Для оцінювання надмірності траєкторії доцільно використовувати відносне збільшення довжини маршруту (4):

$$\Delta L = \frac{L_{path} - L_{ref}}{L_{ref}} \cdot 100\%, \quad (4)$$

де L_{path} – фактична довжина траєкторії, пройдена роботом у симуляційному середовищі, а L_{ref} – довжина еталонного або найкоротшого маршруту. Ця метрика дозволяє визначити, наскільки траєкторія робота відхиляється від оптимальної внаслідок перепланувань, уникання перешкод, нестабільності локального планувальника або динамічних змін середовища.

Для складніших сценаріїв доцільно вводити інтегральний показник ризику місії (5):

$$R_{mission} = \alpha N_{coll} + \beta N_{near} + \gamma \Delta L + \delta T_{norm}, \quad (5)$$

де N_{coll} – кількість зіткнень; N_{near} – кількість небезпечних зближень; ΔL – відносне збільшення довжини маршруту; T_{norm} – нормований час виконання місії; $\alpha, \beta, \gamma, \delta$ – вагові коефіцієнти, що визначають значущість кожного компонента ризику. У такому вигляді показник $R_{mission}$ дозволяє перейти від аналізу окремих параметрів до узагальненої оцінки якості виконання завдання.

Разом із тим сама наявність метрик ще не гарантує наукової коректності експерименту. Необхідно, щоб симуляційна конфігурація була відтворюваною, результати є метрично спостережуваними, а порівняння алгоритмів буде методологічно коректним. Для формального обґрунтування цього положення доцільно ввести низку допоміжних тверджень.

Лема 1. Лема про відтворюваність симуляційної конфігурації

Якщо для експерименту в Gazebo зафіксовано модель світу W , модель робота R , сенсорну конфігурацію S , алгоритмічний стек A , сценарій C , систему метрик M , протокол проведення експерименту P , початкові умови та версії програмного забезпечення, тоді повторний запуск експерименту за тим самим протоколом забезпечує відтворюваність умов дослідження в межах заданої симуляційної моделі.

Формально це можна подати виразами (6; 7):

$$E_G^{(i)} = \langle W, R, S, A, C, M, P \rangle, \quad (6)$$

$$E_G^{(j)} = \langle W, R, S, A, C, M, P \rangle. \quad (7)$$

Отже, експерименти $E_G^{(i)}$ та $E_G^{(j)}$ є конфігураційно еквівалентними, якщо всі їхні визначальні компоненти збігаються.

Зміст цієї лєми полягає в тому, що Gazebo дозволяє відокремити досліджувану змінну від фонових факторів. Якщо модель світу, модель робота, сенсори, сценарій, протокол і

початкові умови залишаються незмінними, то відмінності в результатах можуть бути пов'язані або з контрольовано введеною випадковістю, або з внутрішніми властивостями досліджуваного алгоритму. Це створює передумови для повторюваності експериментів і накопичення статистично значущих результатів.

Лема 2. Лема про метричну спостережуваність результатів

Якщо для експерименту визначено систему метрик M , а кожна метрика має однозначний спосіб обчислення на основі даних симуляції D , то результат експерименту може бути представлений не лише якісно, а й кількісно. Інакше кажучи, для кожного запуску експерименту існує відображення (8):

$$f: D \rightarrow M, \quad (8)$$

де D – масив даних, отриманих під час симуляції; M – множина обчислених показників.

Ця лема означає, що Gazebo дозволяє перейти від візуального спостереження за поведінкою робота до формалізованого аналізу результатів. Якщо під час симуляції фіксуються координати, траєкторія, час, стан сенсорів, команди керування, кількість зіткнень, перепланувань та інші параметри, то поведінка робототехнічної системи може бути оцінена за кількісними критеріями.

Лема 3. Лема про порівнюваність алгоритмічних конфігурацій

Нехай у двох експериментах E_{G1} та E_{G2} однаковими залишаються модель світу W , модель робота R , сенсорна система S , сценарій C , система метрик M і протокол P , але відрізняється алгоритмічний стек (9):

$$A1 \neq A2. \quad (9)$$

Тоді відмінності у значеннях метрик (10),

$$M(A_1) \neq M(A_2), \quad (10)$$

можуть бути використані для порівняльного оцінювання ефективності алгоритмів A_1 та A_2 у межах заданої симуляційної моделі.

Зміст цієї лема полягає в тому, що Gazebo дозволяє будувати коректні порівняльні експерименти. Якщо дослідник змінює лише алгоритм, залишаючи інші компоненти експерименту незмінними, то отримані відмінності в часі місії, довжині траєкторії, кількості зіткнень, кількості перепланувань, похибці локалізації або інтегральному ризику можуть інтерпретуватися як наслідок роботи відповідного алгоритмічного підходу.

Теорема про метричну валідність симуляційного експерименту в Gazebo

Якщо експеримент у Gazebo задано як систему (11)

$$E_G = \langle W, R, S, A, C, M, P, D \rangle, \quad (11)$$

де W – модель світу; R – модель робота; S – сенсорна система; A – алгоритмічний стек; C – сценарій; M – система метрик; P – протокол; D – дані є явно визначеними, відтворюваними та достатніми для обчислення всіх обраних метрик, то Gazebo може використовуватися як метрично валідне симуляційне середовище для порівняльного дослідження алгоритмів автономної робототехнічної системи в межах заданої моделі.

Інакше кажучи, за умови фіксації експериментальної конфігурації, визначення системи метрик і забезпечення збору необхідних даних результатів симуляції може бути використаний для науково обґрунтованого висновку про відносну ефективність алгоритмічних підходів у межах заданого класу сценаріїв.

Доведення:

За лемою 1, фіксація моделі світу, моделі робота, сенсорної конфігурації, сценарію, протоколу, початкових умов і версій програмного забезпечення забезпечує відтворюваність симуляційної конфігурації. Це означає, що експеримент може бути повторений у тій самій структурі, а результати не є наслідком неконтрольованої зміни умов середовища.

За лемою 2, якщо дані симуляції D дозволяють обчислити множину метрик M , то поведінка робототехнічної системи може бути представлена кількісно. Отже, результат експерименту не обмежується суб'єктивним візуальним спостереженням, а набуває формалізованого вигляду.

За лемою 3, якщо в серії експериментів змінюється лише алгоритмічний стек A , а інші компоненти залишаються незмінними, то відмінності у значеннях метрик можуть бути використані для порівняння алгоритмів. Це забезпечує можливість коректного порівняльного аналізу робототехнічних рішень у межах заданої симуляційної моделі.

Таким чином, для виконання зазначених умов Gazebo може бути використаний як метрично валідне середовище для симуляційного дослідження автономних робототехнічних систем. Теорему доведено.

Наслідок 1. Про Gazebo як цифровий експериментальний полігон

Якщо Gazebo забезпечує відтворюваність симуляційної конфігурації, метричну спостережуваність результатів і порівнюваність алгоритмічних конфігурацій, то він може бути інтерпретований як цифровий експериментальний полігон для дослідження автономних робототехнічних систем. Цей наслідок є методологічно важливим, оскільки дозволяє розглядати Gazebo не лише як програмний симулятор, а як структурований простір наукової перевірки, у якому експеримент має власну логіку, змінні, сценарії, метрики, протокол і критерії інтерпретації.

Наслідок 2. Про межі наукової інтерпретації результатів

Результати, отримані в Gazebo, є науково значущими в межах заданої симуляційної моделі, якщо всі параметри експерименту явно визначені, а метрики обчислюються за єдиним протоколом. Однак ці результати не повинні інтерпретуватися як повний еквівалент фізичного експерименту без додаткової перевірки на реальній робототехнічній платформі. Цей наслідок дозволяє уникнути головного методологічного ризику – надмірного ототожнення симуляційної поведінки з реальною поведінкою робототехнічної системи. Gazebo забезпечує внутрішню валідність симуляційного експерименту, але не гарантує автоматичного подолання sim-to-real gap.

Отже, система метрик у поєднанні з формально визначеними умовами відтворюваності, спостережуваності та порівнюваності дозволяє надати експериментам у Gazebo статусу науково обґрунтованої симуляційної валідації. У цьому полягає ключова методологічна відмінність між простим використанням Gazebo як середовища демонстрації та його застосуванням як цифрового науково-експериментального полігону.

Наукові переваги Gazebo доцільно розглядати не ізольовано, а у зв'язку з умовами метричної валідності симуляційного експерименту. Тобто важливим є не лише те, що Gazebo дозволяє моделювати роботів, а те, що він забезпечує умови для відтворюваності, спостережуваності, порівнюваності та кількісного аналізу результатів. Однією з ключових переваг є відтворюваність експерименту. У фізичному середовищі складно повністю повторити одні й ті самі умови, оскільки змінюються освітлення, стан поверхні, заряд батарей, якість зчеплення коліс, положення об'єктів, зовнішні завади й інші чинники. У Gazebo дослідник може зберегти модель світу, параметри робота, початкові координати, сценарії руху перешкод і програмну конфігурацію, після чого багаторазово повторювати експеримент у контрольованих умовах. Другою перевагою є керованість змінних. Дослідник може цілеспрямовано змінювати лише один параметр, наприклад рівень шуму LiDAR, швидкість динамічної перешкоди, коефіцієнт тертя поверхні або тип локального планувальника,

залишаючи інші умови незмінними. Це створює можливість для коректного порівняння алгоритмів і виявлення причинно-наслідкових зв'язків між параметрами системи та її поведінкою. Третьою перевагою є метрична спостережуваність. У Gazebo можна фіксувати координати робота, траєкторію, швидкість, стан сенсорів, команди керування, кількість зіткнень, час виконання місії, кількість перепланувань та інші параметри. Це дозволяє перетворити поведінку робототехнічної системи на масив даних, придатний для подальшого кількісного аналізу. Четвертою перевагою є доступ до еталонних даних, або *ground truth*. У реальному експерименті точне положення робота, об'єктів і перешкод не завжди легко виміряти. У Gazebo дослідник може отримати істинні координати, орієнтацію, швидкість і стан об'єктів, що дозволяє кількісно оцінювати похибку локалізації, якість SLAM, точність детекції та відповідність запланованої траєкторії фактичній. П'ятою перевагою є безпека досліджень. Алгоритми автономного керування, особливо на ранніх етапах розробки, можуть містити помилки, які у фізичному середовищі можуть призвести до пошкодження обладнання, зіткнення з перешкодами або небезпечної поведінки робота. Gazebo дозволяє перевіряти такі алгоритми у віртуальному середовищі без ризику для людей, техніки та матеріальної бази. Шостою перевагою є масштабованість експериментів. У фізичному полігоні кількість роботів, сенсорів, сценаріїв і повторів часто обмежена ресурсами. У Gazebo можна створити серії експериментів із різною кількістю роботів, різними типами середовищ, десятками варіантів перешкод і різними налаштуваннями алгоритмів. Це особливо важливо для дослідження багатороботних систем, групової координації, ройової поведінки та сценарного моделювання. Сьомою перевагою є інтеграція з ROS/ROS 2, що дозволяє використовувати Gazebo як частину повного робототехнічного програмного стеку. Алгоритми, перевірені в симуляції, потенційно можуть бути перенесені на фізичну платформу з меншими змінами, ніж у випадку повністю ізольованого симулятора. Це створює передумови для реалізації логіки *sim-to-real*, у якій симуляція є проміжним етапом між теоретичною розробкою та фізичною апробацією. Таким чином, наукова перевага Gazebo полягає не лише в доступності чи зручності моделювання, а в тому, що він дозволяє побудувати відтворюваний, метрично спостережуваний і порівнюваний експериментальний контур. Саме ці властивості є підставою для розгляду Gazebo як цифрового науково-експериментального полігону.

Апробація запропонованого підходу. Для апробації запропонованої методологічної схеми доцільно використати модельний експеримент з автономної навігації мобільного робота в середовищі Gazebo. Такий експеримент є достатньо універсальним для академічної статті, водночас він дозволяє продемонструвати всі ключові елементи запропонованої методології: модель світу, модель робота, сенсори, алгоритмічний стек, сценарії, метрики, протокол і дані.

Метою апробації є перевірка можливості використання Gazebo як цифрового експериментального полігону для оцінювання поведінки мобільного робота під час виконання навігаційного завдання в середовищах різної складності. Як базову платформу можна використати диференціальний мобільний робот типу TurtleBot3 або узагальнену модель UGV із LiDAR, IMU та одометрією. Алгоритмічний стек може включати ROS 2, Nav2, SLAM Toolbox або попередньо побудовану карту, глобальний планувальник, локальний планувальник і вузол логування експериментальних даних.

Апробаційний експеримент доцільно побудувати на чотирьох сценаріях. Перший сценарій *S1*: просте середовище без динамічних перешкод, у якому робот рухається від стартової точки до цілі за заздалегідь побудованою картою. Другий сценарій *S2*: середовище зі статичними перешкодами, вузькими проходами та необхідністю локального перепланування. Третій сценарій *S3*: динамічне середовище, у якому з'являються рухомі об'єкти, що змушують робота змінювати траєкторію та адаптувати швидкість. Четвертий сценарій *S4*: середовище із деградацією сенсорної інформації, де вводяться шум LiDAR, пропуски одометрії або затримки оновлення даних.

Для кожного сценарію задається однакове навігаційне завдання: робот має перейти зі стартової точки P_s до цільової точки P_g , уникаючи зіткнень і дотримуючись обмежень швидкості. Кожен сценарій повторюється у серії запусків, що дозволяє оцінити не одиничну поведінку робота, а стабільність алгоритмічного стеку в заданому класі умов.

Результати апробації пропонується надати у такому форматі (табл. 1):

Таблиця 1

Пропозиція щодо формату апробаційних результатів

Сценарій	Зміст сценарію	Основна перевірка	Очікувана дослідницька цінність
S_1	Просте середовище без динамічних перешкод	Базова працездатність навігації	Перевірка коректності моделі, карти й навігаційного стеку
S_2	Статичні перешкоди та вузькі проходи	Локальне планування й уникання перешкод	Оцінка якості маршруту та перепланувань
S_3	Динамічні об'єкти в середовищі	Адаптивність руху	Оцінка стійкості до змінної обстановки
S_4	Сенсорний шум і затримки	Стійкість до невизначеності	Оцінка впливу деградації даних на результат

Для демонстрації застосовності запропонованої методологічної схеми було змодельовано результати серії експериментів автономної навігації мобільного робота в середовищі Gazebo. Умовно прийнято, що для кожного сценарію виконано $N_{total} = 20$ запусків. Еталонна довжина маршруту становила $L_{ref} = 10,0$ м. Як базовий час для нормування прийнято середній час виконання місії у простому середовищі S_1 .

Інтегральний показник ризику місії (5) розраховано за формулою (12):

$$R_{mission} = 10N_{coll} + 0,8N_{near} + 0,05\Delta L + 2T_{norm}, \quad (12)$$

де N_{coll} – середня кількість зіткнень за один запуск; N_{near} – середня кількість небезпечних зближень; ΔL – відносне збільшення довжини маршруту, %; T_{norm} – нормований час виконання місії. Менше значення $R_{mission}$ відповідає меншому інтегральному ризику. Результати апробаційного експерименту наведені в таблиці 2.

Отримані результати демонструють очікувану залежність між складністю сценарію та ефективністю автономної навігації (рис. 2). У сценарії S_1 , що відповідає простому середовищу без динамічних перешкод, робот успішно виконав усі 20 запусків, а показник P_{succ} становив 1,00. Це свідчить про базову працездатність моделі робота, карти, сенсорної конфігурації та навігаційного стеку. У сценарії S_2 , де були введені статичні перешкоди та вузькі проходи, частка успішних запусків знизилася до 0,90. Одночасно зросли час виконання місії, довжина траєкторії, кількість перепланувань і показник ризику $R_{mission}$. Це вказує на те, що навіть статичне ускладнення середовища потребує активнішої роботи локального планувальника й збільшує навігаційну надмірність маршруту. У сценарії S_3 , що містив динамічні перешкоди, успішність знизилася до 0,75. Найбільш помітним є зростання кількості небезпечних зближень і перепланувань. Це свідчить про збільшення навантаження на локальний планувальник, який має адаптувати траєкторію в умовах змінної обстановки. Зростання $R_{mission}$ до 9,98 демонструє підвищення інтегрального ризику виконання місії.

Таблиця 2

Результати апробаційного експерименту

Сценарій	$\frac{N_{success}}{N_{total}}$	P_{succ}	$T_{mission}, c$	L_{path}, m	$\Delta L, \%$	N_{coll}	N_{near}	N_{replan}	$R_{mission}$
S1: просте середовище	20/20	1,00	$42,0 \pm 2,4$	$10,4 \pm 0,3$	4,0	$0,00 \pm 0,00$	$0,20 \pm 0,40$	$1,1 \pm 0,5$	2,36
S2: статичні перешкоди	18/20	0,90	$56,8 \pm 4,9$	$11,6 \pm 0,8$	16,0	$0,10 \pm 0,31$	$1,35 \pm 0,80$	$3,7 \pm 1,1$	5,58
S3: динамічні перешкоди	15/20	0,75	$73,5 \pm 8,7$	$13,0 \pm 1,5$	30,0	$0,25 \pm 0,44$	$3,10 \pm 1,40$	$7,8 \pm 2,0$	9,98
S4: сенсорна деградація	12/20	0,60	$84,2 \pm 10,6$	$14,1 \pm 1,8$	41,0	$0,40 \pm 0,58$	$4,20 \pm 1,70$	$10,4 \pm 2,$	13,42

Найскладнішим виявився сценарій S4, у якому моделювалася деградація сенсорної інформації. Частка успішних запусків знизилася до 0,60, а середній час виконання місії та довжина траєкторії досягли найбільших значень. Це пояснюється тим, що шум LiDAR, пропуски одометрії або затримки оновлення даних безпосередньо впливають на якість локалізації, стабільність планування та своєчасність реакції на перешкоди.

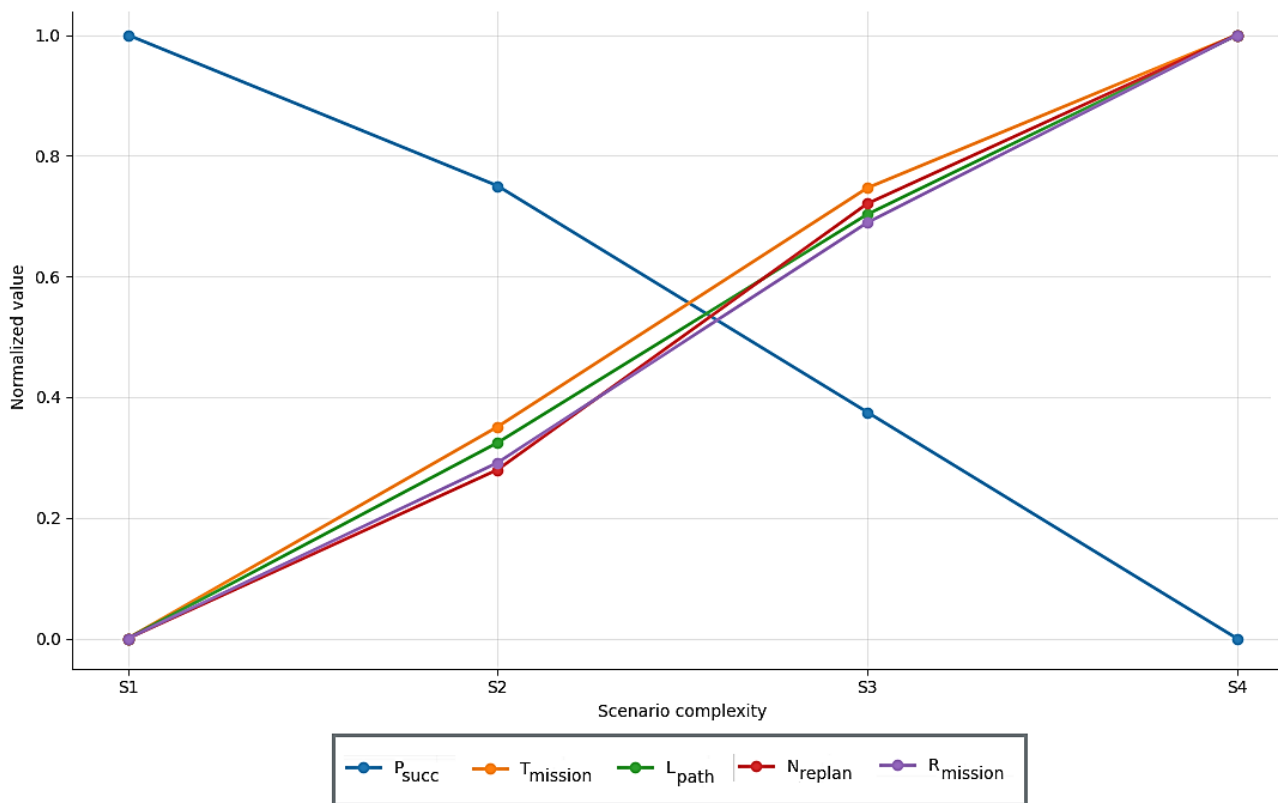


Рис. 2. Графік залежностей ключових показників від складності сценарію

За результатами проведеної апробації встановлено, що ускладнення симуляційного середовища призводить до послідовного зниження частки успішного виконання місії, збільшення часу проходження маршруту, зростання довжини траєкторії, кількості перепланувань, небезпечних зближень та інтегрального ризику місії. У простому сценарії S1 частка успішних запусків становила $P_{succ} = 1,00$, тоді як у сценарії із сенсорною деградацією

S4 цей показник знизився до $P_{succ} = 0,60$. Водночас інтегральний показник ризику $R_{mission}$ зріс з 2,36 до 13,42 умовних одиниць.

Отримана тенденція підтверджує методологічну доцільність використання Gazebo як цифрового експериментального полігону, оскільки середовище дозволяє не лише візуально спостерігати поведінку робота, а й кількісно оцінювати зміну ефективності автономної системи за різних умов. Застосування єдиної системи метрик дає змогу порівнювати сценарії між собою та визначати межі стійкості алгоритмічного стеку до ускладнення середовища й деградації сенсорної інформації.

Висновки та напрями подальших досліджень. У результаті проведеного дослідження обґрунтовано доцільність розгляду Gazebo не лише як програмного симулятора робототехнічних систем, а як цифрового науково-експериментального полігону, що забезпечує умови для відтворюваного, параметризованого та метрично контрольованого вивчення автономних робототехнічних систем. Показано, що його наукова цінність полягає не стільки у візуалізації поведінки робота, скільки у можливості формувати керовану симуляційну реальність, у якій можуть бути явно задані модель світу, модель робота, сенсорна система, алгоритмічний стек, сценарії, метрики, протокол дослідження та масив експериментальних даних. Запропонована методологічна схема дозволяє представити експеримент у Gazebo як формалізовану систему, у межах якої кожен елемент виконує окрему дослідницьку функцію: середовище задає умови перевірки, робототехнічна модель визначає фізичні й кінематичні властивості платформи, сенсорна система формує інформаційний образ середовища, алгоритмічний стек забезпечує автономну поведінку, а система метрик створює підстави для кількісної інтерпретації результатів. Такий підхід дає змогу перейти від простого твердження про працездатність алгоритму в симуляції до науково обґрунтованого висновку про те, за яких умов, з якою точністю, стійкістю, повторюваністю та обмеженнями робототехнічна система демонструє задану поведінку.

У межах роботи запропоновано систему метрик для оцінювання симуляційного експерименту, що включає показники похибки локалізації, якості побудови карти, часу виконання місії, довжини траєкторії, кількості зіткнень, небезпечних зближень, перепланувань, обчислювального навантаження, частки успішних запусків та інтегрального ризику місії. Формальне введення лем про відтворюваність симуляційної конфігурації, метричну спостережуваність результатів і порівнюваність алгоритмічних конфігурацій дозволило сформулювати теорему про метричну валідність симуляційного експерименту в Gazebo. Її зміст полягає в тому, що за умови явного визначення моделі, сценарію, протоколу, метрик і даних Gazebo може використовуватися як метрично валідне середовище для порівняльного дослідження алгоритмів автономної робототехнічної системи в межах заданої симуляційної моделі. Модельна апробація запропонованого підходу на прикладі автономної навігації мобільного робота показала, що ускладнення сценаріїв закономірно призводить до зниження частки успішного виконання місії, збільшення часу проходження маршруту, зростання довжини траєкторії, кількості перепланувань, небезпечних зближень та інтегрального ризику. Отримана тенденція підтверджує, що Gazebo може бути використаний не лише для демонстраційного запуску робототехнічної моделі, а й для кількісного аналізу стійкості автономної системи до ускладнення середовища, динамічних перешкод і деградації сенсорної інформації.

Водночас результати, отримані в Gazebo, мають інтерпретуватися з належною науковою обережністю. Запропонована метрична валідність стосується насамперед внутрішньої коректності симуляційного експерименту, а не повної фізичної еквівалентності симуляції та реального середовища. Тому Gazebo не повинен розглядатися як повна заміна фізичного експерименту, однак може виступати ефективним проміжним рівнем між теоретичним моделюванням, програмною реалізацією алгоритмів і подальшою апробацією на реальній робототехнічній платформі.

Подальші дослідження доцільно спрямувати на проведення поглибленої експериментальної апробації запропонованої методології у Gazebo Sim із використанням ROS 2, Nav2, SLAM Toolbox та кастомних моделей мобільних роботів або НРК. Перспективним є розширення системи сценаріїв, деталізація інтегрального показника ризику місії, порівняння різних алгоритмічних стеків, поширення підходу на багатороботні системи, інтеграція Gazebo з цифровими двійниками й алгоритмами штучного інтелекту, а також вивчення sim-to-real переходу шляхом зіставлення симуляційних результатів із фізичними випробуваннями. У підсумку Gazebo може бути визначений як методологічний міст між теорією, алгоритмічною реалізацією та практичною перевіркою автономних робототехнічних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Perisic A., Perisic B. Digital Twins Verification and Validation Approach through the Quintuple Helix Conceptual Framework. Electronics. 2024. Vol. 13, No. 16. Article 3303.
2. Koenig N., Howard A. Design and use paradigms for Gazebo, an open-source multi-robot simulator. 2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). Sendai, Japan, 2004. Vol. 3. P. 2149–2154. DOI: 10.1109/IROS.2004.1389727.
3. Gazebo Sim: A Robotic Simulator [Електронний ресурс] // Gazebo Documentation. Gazebo Project. URL: <https://gazebo-sim.org/libs/sim/>.
4. Scott K. Gazebo Classic and Citadel End of Life [x-post Gazebo Sim Community] / K. Scott // Open Robotics Discourse. ROS General. 2024. December 2. URL: <https://discourse.openrobotics.org/t/gazebo-classic-and-citadel-end-of-life-x-post-gazebo-sim-community/40931>
5. Macenski S. Robot Operating System 2: Design, Architecture, and Uses In The Wild / S. Macenski, T. Foote, B. Gerkey, C. Lalancette, W. Woodall // Science Robotics. 2022. Vol. 7, No. 66. DOI: 10.1126/scirobotics.abm6074.
6. Nav2 – Nav2 1.0.0 documentation [Електронний ресурс] // Nav2 Documentation. Open Navigation LLC, 2026. URL: <https://docs.nav2.org/>
7. Macenski S. SLAM Toolbox: SLAM for the dynamic world / S. Macenski, I. Jambrecic // Journal of Open Source Software. 2021. Vol. 6, No. 61. Article 2783. DOI: 10.21105/joss.02783. URL: <https://joss.theoj.org/papers/10.21105/joss.02783>
8. Бернацький А. П. Практичне програмування роботів: Gazebo Military Edition : навч. посіб. Київ: Ліра-К, 2025. 232 с. ISBN 978-617-8739-10-2.

Надійшла до редколегії 20.04.2026

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.3.019.3

Ланко А. В. ORCID: 0009-0001-1124-1526 (ВІТІ ім. Героїв Крут)
Рибка Є. М. ORCID: 0009-0000-2578-0363 (ВІТІ ім. Героїв Крут)

ОЦІНКА НАДІЙНОСТІ РАДІОЕЛЕКТРОННОГО ОБЛАДНАННЯ ЗА ПАРАМЕТРАМИ ВІБРОСТІЙКОСТІ

Зазвичай показники надійності радіоелектронного обладнання (ймовірність безвідмовної роботи, середній наробіток до відмови, інтенсивність відмов, коефіцієнт готовності) визначаються на основі результатів випробувань або статистичного аналізу експлуатаційних даних. Проте в сучасних умовах широкого використання технічних систем іноземного виробництва, для яких відсутня повна технічна документація та обмежений обсяг апріорної інформації, оцінювання надійності таких зразків традиційними методами є ускладненим.

Для розв'язання зазначеної задачі запропоновано використовувати непрямий підхід до оцінювання надійності, що базується на аналізі інженерних характеристик зразків озброєння та військової техніки, зокрема вібростійкості, структурної і параметричної надлишковості, довговічності елементної бази тощо.

Враховуючи, що для мобільного радіоелектронного обладнання, встановленого на рухомих носіях, механічні вібраційні впливи є одним із визначальних факторів деградації конструктивних елементів, у роботі основну увагу приділено оцінюванню надійності на основі аналізу вібростійкості об'єктів контролю.

Запропоновано фізичні та математичні моделі тримасових ієрархічних структур радіоелектронного обладнання, встановленого на рухомих об'єктах. На основі побудованих моделей виведено характеристичні рівняння для визначення власних частот коливань складних технічних систем, що дозволяє прогнозувати виникнення резонансних режимів та оцінювати їх потенційний вплив на експлуатаційну надійність.

Окрему увагу приділено аналізу національних і міжнародних нормативних документів у сфері оцінювання надійності радіоелектронного обладнання.

Актуальність дослідження обумовлена необхідністю інтеграції до системи технічного забезпечення Збройних Сил України та інших складових сектору безпеки і оборони значної кількості зразків іноземного виробництва, для яких відсутні формалізовані методики оцінювання надійності в умовах обмеженості вихідних даних.

Практичне значення отриманих результатів полягає у можливості їх використання для підтримки прийняття рішень під час організації технічного обслуговування, ремонту та прогнозування ресурсу зразків озброєння і військової техніки іноземного виробництва.

Ключові слова: надійність, радіоелектронне обладнання, показники надійності, вібростійкість, інженерні характеристики, коливальні процеси.

A. Lanko, Ye. Rybka. Reliability assessment of radio-electronic equipment by vibration resistance parameters

Reliability indicators of radio-electronic equipment (probability of failure-free operation, mean time to failure, failure rate, and availability factor) are traditionally determined based on test results or statistical analysis of operational data. However, under current conditions of extensive use of foreign-manufactured technical systems, for which complete technical documentation and sufficient a priori information are often unavailable, reliability assessment using conventional methods becomes significantly complicated.

To address this issue, an indirect approach to reliability assessment is proposed, based on the analysis of engineering characteristics of weapon and military equipment samples, including vibration resistance, structural and parametric redundancy, durability of the component base, and related parameters.

Considering that for mobile radio-electronic equipment installed on moving platforms, mechanical vibration loads constitute one of the dominant factors affecting degradation of structural elements and interconnections, particular attention in this study is given to reliability assessment through vibration resistance analysis of the monitored objects.

Physical and mathematical models of three-mass hierarchical structures of radio-electronic equipment mounted on mobile platforms are proposed. Based on these models, characteristic equations for determining the natural frequencies of complex technical systems are derived, enabling prediction of resonance conditions and assessment of their potential impact on operational reliability.

Special attention is paid to the analysis of Ukrainian national standards and international standards related to reliability assessment of radio-electronic equipment.

The relevance of this study is determined by the need to integrate a significant number of foreign-manufactured weapon and military equipment samples into the existing technical support system of the Armed Forces of Ukraine and other components of the security and defense sector, while formalized methods for reliability assessment of such systems under limited input data conditions remain absent.

The practical significance of the obtained results lies in the possibility of their application for supporting decision-making in maintenance planning, repair organization, and service life prediction of foreign-manufactured weapon and military equipment.

Keywords: *reliability, radio-electronic equipment, reliability indicators, vibration resistance, engineering characteristics, oscillatory processes.*

Постановка проблеми. Надійність є одним з ключових експлуатаційних параметрів радіоелектронного обладнання (РЕО), що застосовується у секторі безпеки та оборони України. Рівень надійності РЕО визначається характеристиками елементної бази, а також прийнятими схемотехнічними та конструктивними рішеннями. З огляду на критичну роль РЕО у забезпеченні функціонування сучасних технічних систем, вимоги до його надійності постійно зростають.

Під надійністю технічного об'єкта розуміють його властивість зберігати у часі здатність виконувати задані функції в установлених режимах та умовах експлуатації. Для кількісного оцінювання надійності застосовуються показники: ймовірність безвідмовної роботи $P(t)$, середній наробіток до відмови ($T_{сер}$), інтенсивність відмов (λ) та коефіцієнт готовності (K_T). Традиційно зазначені показники визначаються за результатами випробувань або статистичного аналізу експлуатаційних даних.

Водночас у сучасних умовах до сектору безпеки та оборони України надходить значна кількість зразків РЕО іноземного виробництва, зокрема подвійного призначення, для яких часто відсутня повна супровідна технічна документація, засоби контролю технічного стану та формалізовані методики технічного обслуговування [1–4].

За таких умов інтеграція зазначених зразків у діючу систему технічного обслуговування і ремонту суттєво ускладнюється, а застосування традиційних статистичних методів оцінювання надійності стає неможливим або малоефективним.

Одним із доступних напрямів розв'язання цієї проблеми є використання непрямих неруйнівних методів оцінювання надійності, що базуються на аналізі структури, конструктивного виконання та технологічних особливостей виготовлення об'єктів РЕО [5].

Таким чином, наявне протиріччя між необхідністю оцінювання надійності РЕО іноземного виробництва в процесі його експлуатації та відсутністю достатніх вихідних даних для застосування традиційних методів оцінювання. Це зумовлює актуальність розроблення неруйнівних методів оцінки надійності РЕО в умовах інформаційної невизначеності.

Аналіз публікацій за темою дослідження. Завданню оцінки надійності РЕО присвячено значна кількість публікацій [6–9]. Суттєвий внесок у теорію надійності РЕО внесли такі вчені: Жердев М. К., Уваров Б. М., Зінковський Ю., Креденцер Б. П., Бабало Ю. А., Ленков С. В., Рижов Є. В., Сакович Л. М. та інші.

Важливість оцінки надійності РЕО доводять прийняття ряду Державних стандартів України (ДСТУ) [10–19], що регулюють оцінку, прогнозування та забезпечення надійності техніки та систем. Ці стандарти встановлюють вимоги до властивостей, закладених під час проєктування (конструктивна надійність) та виготовлення, а також під час експлуатації.

Нові ДСТУ [15–19] замінюють старі стандарти в оборонній сфері. В них зберігаються посилання на загальні принципи [10], але деталізують окремі процеси.

У роботах [10–18] для оцінки показників надійності РЕО визначено необхідний набір вихідних даних про об'єкт контролю (ОК), а підхід визначення самої надійності ґрунтується на статистичній оцінці інформації, отриманої під час випробувань або експлуатації.

Застосування статистичних методів оцінювання надійності в умовах, коли обсяг даних недостатній для застосування класичних методів (наприклад, коли випробування не завершилися відмовою, або загальна кількість зареєстрованих відмов дуже мала), розглянуто в стандарті [19].

Аналіз наведених ДСТУ [10–19] доводить актуальність розробки щодо оцінки надійності РЕО в умовах обмеженої інформації.

Існування ДСТУ 8647:2016 [19] свідчить про те, що національний орган стандартизації визнав проблему оцінки надійності РЕО з обмеженою вхідною інформацією про ОК та вважає її важливою науковою задачею.

Узагальнення основних міжнародних стандартів [20; 21] оцінки надійності РЕО наведено в таблиці 1.

Таблиця 1

Міжнародні стандарти для оцінки надійності РЕО

Позначення	Назва (призначення)	Примітки
IEC 62308	Equipment reliability – Reliability assessment methods (Надійність обладнання. Методи оцінювання надійності)	Опис методів раннього оцінювання надійності на основі польових даних і даних випробувань компонентів і систем (подібний до [15])
IEC 61078	Analysis techniques for dependability – Reliability block diagram and boolean methods (Методи аналізу надійності. Діаграми надійності та Баєсівські методи)	процедури моделювання системи для розрахунку показників надійності

Слід зазначити, що є також міжнародні довідники [22; 23] у сфері РЕО та електроніки, які де-факто є міжнародними стандартами для прогнозування надійності на рівні компонентів, особливо коли інформація про ОК обмежена.

Довідник [22] використовується для прогнозування інтенсивності відмов (λ) кожного радіоелектронного компонента (РЕК) в РЕО, враховуючи зовнішні фактори (температуру, середовище та інше). Комерційним наступником довідника [22] є довідник [23], який застосовується для більш точного прогнозування надійності зразків РЕО подвійного призначення (наприклад, обладнання для мобільного зв'язку).

У роботі [24] доведено, що надлишковість, яка широко застосовується для забезпечення нормального функціонування складних систем у реальних умовах експлуатації, є фундаментальним поняттям у загальній теорії й практиці надійності.

Методологія прискорених випробувань дозволяє швидко оцінити час до відмови компонентів, піддаючи їх екстремальним, але контрольованим навантаженням [25].

Дослідження відмінностей між надійністю та живучістю в комунікаційних мережах проведено в [26].

Отже, проведений аналіз наукових публікацій доводить, що на відміну від класичної теорії надійності, де оцінку надійності визначають по статистичних даних про ОК, доводить необхідність створення нових підходів для оцінки надійності РЕО з обмеженою вхідною інформацією про ОК.

Мета статті полягає в обґрунтуванні підходу до оцінювання показників надійності РЕО за його динамічними параметрами шляхом розробки фізико-математичних моделей тримасових ієрархічних систем РЕО для прогнозування технічного стану апаратури в умовах вібраційних навантажень.

Виклад основного матеріалу

Аналіз сучасних підходів до оцінювання надійності РЕО та наукових праць у цій сфері свідчить, що недостатньо дослідженим залишається питання оцінювання надійності РЕО в умовах обмеженості або повної відсутності апріорної інформації про об'єкт контролю.

За таких умов інженерно-технічному персоналу доступні переважно непрямі методи аналізу технічного стану, зокрема: оцінювання ознак віб्रोустійкості конструкції; визначення структурної та/або параметричної надлишковості; оцінювання потенційної інтенсивності відмов на основі аналізу елементної бази та якості матеріалів із використанням нормативних

моделей (наприклад, MIL-HDBK-217) [22]; застосування безконтактних неруйнівних методів контролю.

Зазначені інженерні характеристики опосередковано відображають здатність РЕО протистояти деградаційним процесам та відмовам у процесі експлуатації.

У роботі [29] авторами досліджено вплив основних інженерних характеристик, зокрема вібростійкості, структурної та параметричної надлишковості, а також довговічності конструкції, на показники надійності об'єктів контролю.

Зв'язок порівняння інженерних характеристик із показниками надійності представлено в таблиці 2.

Таблиця 2

Зв'язок порівняння інженерних характеристик із показниками надійності

Характеристика	Показники надійності	Методи оцінки персоналом	Вплив на надійність
Вібростійкість	$P(t), T_{сер}, \lambda$	Огляд кріплень, амортизаторів, ознак зносу	Знижує λ , підвищує $P(t)$ і $T_{сер}$
Структурна надлишковість	$P(t), Kz$	Виявлення дублюючих компонентів, аналіз схемотехніки	Підвищує $P(t)$ і Kz
Параметрична надлишковість	$P(t), T_{сер}, \lambda$	Аналіз специфікації, перевірка запасів за параметрами	Знижує λ , підвищує $P(t)$ і $T_{сер}$
Довговічність	$T_{сер}, \lambda$	Оцінювання матеріалів, покриттів, захисту від середовища	Підвищує $T_{сер}$, знижує λ

На основі проведеного аналізу встановлено, що серед розглянутих характеристик саме вібростійкість найбільшою мірою піддається формалізованому математичному опису та кількісному оцінюванню без необхідності втручання в конструкцію ОК. Це дозволяє розглядати її як базовий параметр для побудови непрямої моделі оцінювання надійності РЕО в умовах обмеженої вхідної інформації.

Розглянемо фізичну та математичну моделі коливальних процесів РЕО, встановленого на рухомих об'єктах, який впливає на інженерний показник вібростійкість. Використовуючи такі розрахунки, можливо визначити показники віброізоляції РЕО, яке змонтоване на рухомому об'єкті.

Слід зазначити, інженерний показник вібростійкість можна оцінювати як в комплексі з інженерними характеристиками, так і окремо.

Для оцінки працездатності в умовах дії вібрацій та ударів необхідно, насамперед, визначити власні частоти механічних коливань апаратури. У разі збігу цих частот із частотами зовнішніх впливів виникають резонансні явища – амплітуди коливань можуть стати неприпустимо великими, що призводить до порушення цілісності елементів конструкції та відмов РЕО. Тобто наявність на платах габаритних РЕК (наприклад, котушок індуктивності, радіаторів охолодження, конденсаторів та ін.) впливає на показник вібростійкості. Наявність габаритних РЕК може бути ідентифікована під час візуального аналізу конструкції, що дозволяє попередньо оцінити потенційне зниження вібростійкості.

Розрахункові оцінки таких частот математично досить складні: наприклад, для тримасової системи математична модель коливального процесу призводить до необхідності знаходження коренів алгебраїчних рівнянь 18-го ступеня.

Схематично модель трирівневого блока РЕО наведено на рисунку 1. В середині корпусу (блок 1), на відповідних опорних елементах, встановлюють осередки (блок 2) (зазвичай шасі з діелектрика з металевим каркасом) та функціональні вузли (ФВ) (блок 3) – мікроскладання і мікросхеми на шасі та платах.

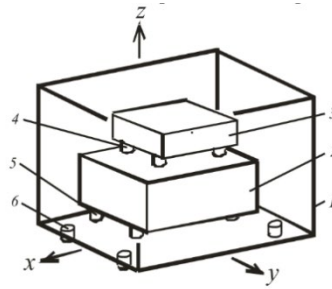


Рис. 1. Тримасова модель блока РЕО

При розміщенні на транспортних засобах, корпус (блок 1) кріплять до підлоги (стілки кабіни) на віброізоляторах (6). Шасі в корпусі блока встановлюють на опорних елементах (5), ФВ – на опорах (4).

Для розрахунку динамічних коливальних процесів фізичну модель системи «блок – шасі – ФВ» можна розглядати як систему з трьох фізичних тіл, з'єднаних пружними зв'язками з основою, а також між собою. В розрахунках необхідно враховувати переміщення відносно всіх трьох координатних осей, відповідні інерційні параметри та коефіцієнти жорсткості пружних зв'язків. Маса структурних елементів блока для всіх трьох осей однакові, проте моменти інерції відносно осей, як правило, різні; крім того, необхідно враховувати центробіжні моменти інерції. У більшості випадків різні й коефіцієнти жорсткості пружних елементів відносно осей, хоча вони й створюються тими самими віброізоляторами (для корпусу блока) або елементами кріплення (для шасі та ФВ).

Коливальні процеси характеризуються лінійними й обертальними переміщеннями. Тому фізичні моделі виходять досить складними. Наприклад, якщо розглядати переміщення для тримасової системи лише відносно однієї з осей (наприклад, осі X), отримаємо фізичну модель, наведену на рисунку 2 (J_1 – корпус блока, J_2 – шасі, J_3 – ФВ).

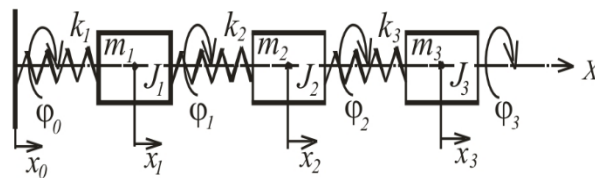


Рис. 2. Фізична модель тримасової системи

Інерційні параметри кожного з цих структурних елементів характеризуються масами m_i , моментами інерції J_i , пружними зв'язками з коефіцієнтами жорсткості k_i ($m_1 J_1$ – корпус блока, $m_2 J_2$ – шасі, $m_3 J_3$ – ФВ).

Динамічний коливальний процес для такої системи має характеризуватися лінійними переміщеннями кожного елемента x_i та обертальними φ_i ; джерелом збурень будуть зміщення основи x_0 та φ_0 .

Для розрахунку характеристик коливального процесу можна використовувати однорідну (спрощену модель), якщо розглядати блок РЕО як абсолютно тверде тіло, встановлене на пружних зв'язках, а також розглядати лише лінійні або лише обертальні переміщення мас системи відносно певної осі.

Це стає можливо в тому випадку, коли сам блок і його структурні модулі повністю симетричні відносно центрів своїх мас, а центри жорсткостей їхніх віброізоляторів збігаються з центрами мас модулів.

У такій системі всі модулі здійснюють лінійні коливання вздовж осі, що проходить через центри мас (якщо основа блока також зміщується лінійно), або обертальні коливання навколо цієї осі (якщо основа зміщується обертально).

Для тримасової системи визначення характеристичної матриці $H_i = S - \omega^2 M$, що пов'язує інерційні характеристики структурних модулів M_i , коефіцієнти жорсткості пружних зв'язків S_i та частоти власних коливань мас ω , має вигляд (1):

$$|H_i| = \begin{vmatrix} S_{11} - \omega^2 M_{11} & S_{12} - \omega^2 M_{12} & S_{13} - \omega^2 M_{13} \\ S_{21} - \omega^2 M_{21} & S_{22} - \omega^2 M_{22} & S_{23} - \omega^2 M_{23} \\ S_{31} - \omega^2 M_{31} & S_{32} - \omega^2 M_{32} & S_{33} - \omega^2 M_{33} \end{vmatrix} = 0. \quad (1)$$

Якщо розглядати лише лінійні коливання для моделі (див. рис. 1), тоді: інерційні характеристики модулів – маси модулів – набувають значень:

$M_{11} = m_1; M_{22} = m_2; M_{33} = m_3; M_{12} = M_{13} = M_{21} = M_{23} = M_{31} = M_{32} = 0$,
а коефіцієнти жорсткості пружних зв'язків (відповідно):
 $S_{11} = k_1 + k_3; S_{12} = S_{21} = -k_2; S_{13} = S_{31} = 0; S_{22} = k_2 + k_3; S_{23} = S_{32} = -k_3; S_{33} = k_3$.

Сам вираз (1) набуває вигляду:

$$\Delta = \begin{vmatrix} k_1 + k_3 - \omega^2 m_1 & -k_2 & 0 \\ -k_2 & k_2 + k_3 - \omega^2 m_2 & -k_3 \\ 0 & -k_3 & k_3 - \omega^2 m_3 \end{vmatrix} = 0.$$

Розкриваючи вираз, отримаємо характеристичне рівняння (2) для визначення частот власних лінійних коливань уздовж осі X (2):

$$\theta^3 - \frac{k_{23}m_1 + k_3m_2}{m_1m_2} \theta^2 - \frac{k_3m_1 + (k_2^2 - k_{13}k_{23})m_3}{m_1m_2m_3} \theta + \frac{k_{13}k_3^2}{m_1m_2m_3} = 0, \quad (2)$$

де позначено: $\theta = \omega^2; k_{13} = k_1 + k_3; k_{23} = k_2 + k_3$.

Корені цього рівняння третього степеня для θ (усі додатні дійсні числа – квадрати власних частот структурних мас блока) (3):

$$\theta_1 = \sqrt[2]{-\frac{p}{3}} \cos \frac{\alpha}{2}; \theta_{2,3} = -2\sqrt[2]{-\frac{p}{3}} \cos \left(\frac{\alpha}{3} \pm \frac{2\pi}{3} \right), \quad (3)$$

де $p = -\frac{\alpha^2}{3} + b$;

$$q = 2\left(\frac{\alpha}{3}\right)^3 - \frac{ab}{3} + c;$$

$$\alpha = -\frac{m_2(k_3m_1 + k_{13}m_3) + k_{23}m_1m_3}{m_1m_2m_3};$$

$$c = \frac{k_{13}k_{23}k_3 - k_{13}k_3^2 - k_2^2k_3}{m_1m_2m_3};$$

$$b = \frac{k_3^2m_1 + k_2^2m_3 - k_{23}(k_3m_1 + k_{13}m_3) - k_3k_{13}m_2}{m_1m_2m_3}.$$

Власні частоти:

$$\omega_1 = \sqrt{\theta_1}; \omega_2 = \sqrt{\theta_2}; \omega_3 = \sqrt{\theta_3}. \quad (4)$$

Якщо в якості інерційних характеристик використовувати моменти інерції J_1, J_2, J_3 , а в якості коефіцієнтів жорсткості – обертові жорсткості k_{k1}, k_{k2}, k_{k3} , то аналогічним чином можна отримати вирази для власних частот крутильних коливань системи.

Слід враховувати, що «симетричних» реальних конструкцій блоків РЕО не існує, тому для кожного структурного елемента блока слід визначити координати центру мас, осьові та центробіжні моменти інерції, різні коефіцієнти жорсткості пружних зв'язків відносно координатних осей.

Як зазначено вище, для тримасової моделі система рівнянь має містити 18 диференціальних рівнянь (відповідно – 18 значень власних частот зв'язаних коливань).

Розглянемо приклад отримання системи диференціальних рівнянь коливального процесу для «простої» однорідної моделі.

Для диференціальних рівнянь руху однорідного фізичного тіла вихідним є рівняння Лагранжа у диференціальній формі (5):

$$\frac{d}{dt} \left(\frac{\partial T}{\partial \dot{q}_i} \right) - \frac{\partial T}{\partial q_i} + \frac{\partial \Pi}{\partial q_i} = Q_i(\tau), i = 1, 2 \dots 6, \quad (5)$$

де T – кінетична енергія системи:

$$T = \frac{1}{2} \sum_{i,k=1}^6 \beta_{ik} \dot{q}_i \dot{q}_k;$$

Π – потенційна енергія системи:

$$\Pi = \frac{1}{2} \sum_{i,k=1}^6 a_{ik} q_i q_k;$$

$\dot{q}_i$ – узагальнена швидкість; q_i – узагальнена координата; α_{ik} – узагальнені коефіцієнти жорсткості (одиничні реакції зв'язків у i -му напрямку при переміщенні системи у k -му напрямку); β_{ik} – узагальнені інерційні характеристики (маси й моменти інерції);

$Q_i(\tau)$ – узагальнена сила, що діє за i -тою координатою.

Припустимо, що блок розташований на віброізоляторах із коефіцієнтами жорсткості k_x, k_y, k_z , встановлених у точках із координатами x, y, z кожен. Тоді маємо систему з шістьма ступенями вільності. Коефіцієнти жорсткості такої системи мають вигляд:

– лінійні:

$$\alpha_{11} = \sum k_x; \alpha_{22} = \sum k_y; \alpha_{33} = \sum k_z;$$

– лінійно-поворотні:

$$\alpha_{15} = \sum k_x z; \alpha_{16} = -\sum k_x z; \alpha_{24} = -\sum k_x y;$$

$$\alpha_{26} = \sum k_y x; \alpha_{34} = \sum k_z y; \alpha_{35} = -\sum k_z x;$$

– гіроскопічні:

$$\alpha_{45} = -\sum k_z x y; \alpha_{46} = -\sum k_y z x; \alpha_{56} = -\sum k_x y z;$$

– обертові:

$$\alpha_{44} = \sum (k_y z^2 + k_z y^2); \alpha_{55} = \sum [(k_z) x^2 + k_x z^2]; \alpha_{66} = \sum (k_x y^2 + k_y x^2).$$

Схема лінійно-поворотних коефіцієнтів жорсткості наведена на рисунку 3.

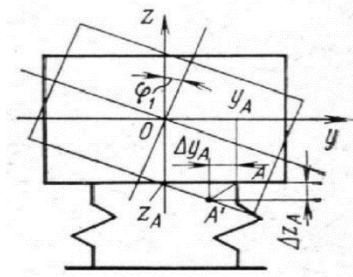


Рис. 3. Визначення лінійно-поворотного коефіцієнта жорсткості

Гіроскопічний коефіцієнт α_{45} – це момент M_2 пружної реакції P_z відносно осі Y, до кута повороту точки A навколо осі X:

$$\alpha_{45} = M_2 / \varphi_1 = k_z x_A y_A.$$

Із рисунка 4 слідує, що $x_A \varphi_2 = -y_A \varphi_1$, тому:

$$M_2 = P_z x_A = k_z \Delta z x_A = k_z x_A \varphi_2 x_A.$$

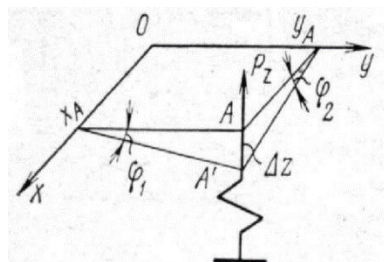


Рис. 4. Визначення гіроскопічного коефіцієнта жорсткості

Обертові коефіцієнти (наприклад, $\alpha_{44} = \frac{M_1}{\varphi_1}$) – це відношення моментів до кутів повороту, які вони викликають (рис. 5).

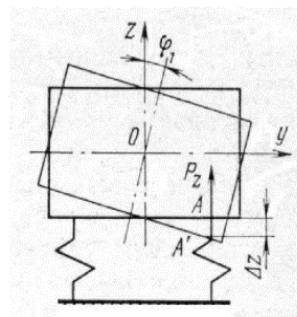


Рис. 5. Визначення обертового коефіцієнта жорсткості

Аналогічним чином визначають інші коефіцієнти жорсткості.

Математична модель коливального процесу для однорідної системи координат складається з шести рівнянь вільних лінійних і обертальних коливань блока (6):

$$\left. \begin{aligned} \beta_{11}\ddot{\delta}_1 + \alpha_{11}\delta_1 + \alpha_{15}\varphi_2 + \alpha_{16}\varphi_3 &= 0; \\ \beta_{11}\ddot{\delta}_2 + \alpha_{22}\delta_2 + \alpha_{24}\varphi_1 + \alpha_{26}\varphi_3 &= 0; \\ \beta_{11}\ddot{\delta}_3 + \alpha_{33}\delta_3 + \alpha_{34}\varphi_1 + \alpha_{35}\varphi_2 &= 0; \\ \beta_{44}\ddot{\varphi}_1 + \beta_{45}\ddot{\varphi}_2 + \beta_{46}\ddot{\varphi}_3 + \alpha_{24}\delta_2 + \alpha_{34}\delta_3 + \alpha_{44}\varphi_1 + \alpha_{45}\varphi_2 + \alpha_{46}\varphi_3 &= 0; \\ \beta_{45}\ddot{\varphi}_1 + \beta_{55}\ddot{\varphi}_2 + \beta_{56}\ddot{\varphi}_3 + \alpha_{15}\delta_1 + \alpha_{35}\delta_3 + \alpha_{45}\varphi_1 + \alpha_{35}\varphi_2 + \alpha_{56}\varphi_3 &= 0; \\ \beta_{46}\ddot{\varphi}_1 + \beta_{56}\ddot{\varphi}_2 + \beta_{66}\ddot{\varphi}_3 + \alpha_{16}\delta_1 + \alpha_{26}\delta_2 + \alpha_{46}\varphi_1 + \alpha_{56}\varphi_2 + \alpha_{66}\varphi_3 &= 0; \end{aligned} \right\}, \quad (6)$$

де δ_i – лінійні переміщення вздовж осей; φ_i – відповідні обертові переміщення; α_{ik} – узагальнені коефіцієнти жорсткості віброізоляторів; β_{ik} – узагальнені інерційні характеристики блока.

Для отримання характеристичної матриці слід прийняти часткові розв'язки (лінійні й поворотні зміщення блока) у вигляді (7):

$$\left. \begin{aligned} \delta_1 &= A_1 \sin(\omega\tau + \alpha); \delta_2 = A_2 \sin(\omega\tau + \alpha); \delta_3 = A_3 \sin(\omega\tau + \alpha); \\ \varphi_1 &= A_4 \sin(\omega\tau + \alpha); \varphi_2 = A_5 \sin(\omega\tau + \alpha); \varphi_3 = A_6 \sin(\omega\tau + \alpha) \end{aligned} \right\}. \quad (7)$$

Після постановки виразу (7) у рівняння (6) отримаємо характеристичну матрицю, а з неї – детермінант подібний до (1), для знаходження частот коливань у вигляді:

$$\Delta = \begin{vmatrix} \alpha_{11} - \beta_{11}\omega^2 & 0 & 0 & 0 & \alpha_{15} & \alpha_{16} \\ 0 & \alpha_{22} - \beta_{11}\omega^2 & 0 & \alpha_{24} & 0 & \alpha_{26} \\ 0 & 0 & \alpha_{33} - \beta_{11}\omega^2 & \alpha_{34} & \alpha_{35} & 0 \\ 0 & \alpha_{24} & \alpha_{34} & \alpha_{22} - \beta_{11}\omega^2 & \alpha_{22} - \beta_{11}\omega^2 & \alpha_{22} - \beta_{11}\omega^2 \\ \alpha_{15} & 0 & \alpha_{35} & \alpha_{22} - \beta_{11}\omega^2 & \alpha_{22} - \beta_{11}\omega^2 & \alpha_{22} - \beta_{11}\omega^2 \\ \alpha_{16} & \alpha_{26} & 0 & \alpha_{22} - \beta_{11}\omega^2 & \alpha_{22} - \beta_{11}\omega^2 & \alpha_{22} - \beta_{11}\omega^2 \end{vmatrix} = 0.$$

Розкриваючи визначник, отримаємо частотне рівняння шостого степеня відносно ω^2 :

$$A\omega^{12} + B\omega^{10} + C\omega^8 + D\omega^6 + E\omega^4 + F\omega^2 + G = 0,$$

корені якого й будуть частотами коливань блока.

Аналіз діагональних одиничних визначників $\alpha_{ik} - \beta_{ik}\omega^2$ дає значення так званих простих частот, а недіагональних – зв'язаних.

Отримані значення власних частот коливань структурних елементів РЕО доцільно використовувати для аналізу умов його експлуатації в складі рухомих об'єктів. Зокрема, практичний інтерес становить порівняння спектрального складу зовнішніх вібраційних впливів із розрахованими власними частотами системи.

У разі наближення частот зовнішніх збурень до власних частот коливальних підсистем РЕО виникають резонансні режими, які характеризуються суттєвим зростанням амплітуд коливань. Це призводить до підвищення механічних напружень у конструктивних елементах, зокрема в з'єднаннях, кріпленнях та елементах друкованих плат, що, у свою чергу, прискорює процеси деградації та збільшує інтенсивність відмов.

Таким чином, ступінь наближення робочого спектра вібраційних навантажень до власних частот коливальної системи може розглядатися як якісний критерій оцінювання вібраційної небезпеки для РЕО. На цій основі можливе формування узагальненої експертної шкали впливу вібраційних режимів на експлуатаційну надійність РЕО (табл. 3).

Таблиця 3

Якісна оцінка впливу резонансної близькості на надійність РЕО

Умови експлуатації	Характер динамічного режиму	Вплив на надійність
Робочий спектр вібрацій суттєво віддалений від власних частот	Нерезонансний режим	Незначний
Робочий спектр частково перекривається з окремими власними частотами	Локальні резонансні явища	Помірне зростання інтенсивності відмов
Робочий спектр збігається з домінуючими власними частотами	Розвинений резонансний режим	Суттєве зростання інтенсивності відмов та зменшення ресурсу

Висновки та перспективи подальших досліджень

У результаті проведеного дослідження встановлено, що традиційні підходи до оцінювання надійності РЕО базуються переважно на статистичних даних про відмови об'єктів контролю, що суттєво обмежує можливість їх застосування для зразків РЕО іноземного виробництва за умов відсутності або недостатності експлуатаційної інформації.

Показано, що представлення конструкції РЕО у вигляді фізичної багатомасової моделі дозволяє формалізувати вплив конструктивно-механічних характеристик структурно-конструктивних модулів і параметрів їхніх пружних зв'язків на вібраційну стійкість і, відповідно, на експлуатаційну надійність РЕО.

Обґрунтовано необхідність урахування як лінійних, так і кутових коливань структурно-конструктивних модулів при розрахунку динамічних характеристик реальних багатомасових систем, що підвищує адекватність математичного опису вібраційних процесів у складних ієрархічних конструкціях.

Запропонований підхід забезпечує можливість непрямого оцінювання впливу вібраційних навантажень на надійність РЕО, змонтованого на рухомих об'єктах, навіть за умов обмеженої вхідної інформації про об'єкт контролю, та може бути використаний для підтримки прийняття рішень щодо організації технічного обслуговування і підвищення ефективності віброзахисту.

Перспективи подальших досліджень полягають в експериментальній верифікації запропонованих моделей, розширенні підходу на багатофакторне оцінювання надійності з урахуванням теплових та електричних навантажень, а також у розробленні автоматизованих засобів підтримки прийняття рішень для технічного персоналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Постачання військової електроніки в Україну під час російського вторгнення. URL: <https://uk.wikipedia.org/w/index.php?title=>
2. Attack On Europe: Documenting Russian Equipment Losses During The 2022 Russian Invasion Of Ukraine // Oryx (last accessed: 08.02.2023).
3. Ukraine conflict: Netherlands to supply weapon locating radars to Ukraine // Janes.com (last accessed: 20.05.2022).
4. Заболотнюк І. О. Військово-технічна допомога США Україні у роки російсько-української війни (2014–2022): дис. на здобуття наук. ступеня канд. іст. наук. Львів: [Установа], 2025. 482 с. URL: https://chtyvo.org.ua/authors/Zabolotniuk_Ihor/Viiskovo-tekhnichna_dopomoha_SShA_Ukraini_u_roky_rosiisko-ukrainskoi_viiny_20142024.pdf.
5. Hanneko Y., Patsenko S. Analysis of the supply of international technical assistance to the Armed Forces of Ukraine // Social Development and Security. 2024. № 14 (6). P. 97–104. URL: <https://doi.org/10.33445/sds.2024.14.6.10>.

6. Сакович Л. М., Рижов Є. В., Небесна Я. Е., Вовк С. В. Модель кількісної оцінки значень показників надійності радіостанцій тактичної ланки управління // Військово-технічний збірник. 2019. № 20. С. 33–41. DOI: <https://doi.org/10.33577/2312-4458.20.2019>.
7. Жердев М. К. Фізичні основи теорії надійності: підруч. / М. К. Жердев, С. В. Ленков, Б. П. Креденцер. Київ: Нац. ун-т ім. Т. Шевченка. 2008. 215 с.
8. Коренівська О. Л., Бенедицький В. Б. Надійність, експлуатація та ремонт радіоелектронної та телекомунікаційної техніки: навч. посіб. Житомир: Житомирська політехніка, 2020. 185 с.
9. Уваров Б. М., Нікітчук А. В. Визначення показників надійності радіоелектронних апаратів, що обумовлюються тепловими режимами // Вісник Національного технічного університету України «КПІ» Серія: Радіотехніка. Радіоапаратобудування. 2014. № 57. С 92–103.
10. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. Київ: Держстандарт України, 1994.
11. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. Основні положення. Київ: Держстандарт України, 1994.
12. ДСТУ 2863-94. Надійність техніки. Програма забезпечення надійності. Київ: Держстандарт України, 1994.
13. ДСТУ 2864-94. Надійність техніки. Експериментальне оцінювання показників надійності. Київ: Держстандарт України, 1994.
14. ДСТУ 3433-96. Надійність техніки. Моделі відмов. Основні положення. Київ: Держстандарт України, 1996.
15. ДСТУ EN 62308:2022 (EN 62308:2006, IDT; IEC 62308:2006, IDT). Надійність обладнання. Методи оцінювання надійності. Київ: УкрНДНЦ, 2022.
16. ДСТУ В 15.010:2023. Система керування життєвим циклом озброєння та військової техніки. Керування надійністю. Київ: УкрНДНЦ, 2023.
17. ДСТУ В 15.201:2022. Система керування життєвим циклом озброєння та військової техніки. Тактико-технічне (технічне) завдання на виконання дослідно-конструкторської роботи. Загальні вимоги до побудови, змісту, викладення, оформлення, видання та коригування. Київ: УкрНДНЦ, 2022.
18. ДСТУ В 15.210:2023. Система керування життєвим циклом озброєння та військової техніки. Випробування озброєння та військової техніки. Класифікація. Київ: УкрНДНЦ, 2023.
19. ДСТУ 8647:2016. Надійність техніки. Оцінювання та прогнозування надійності за результатами випробувань і/або експлуатації в умовах малої кількості відмов. Київ: УкрНДНЦ, 2016.
20. IEC 62308:2006. Equipment reliability – Reliability assessment methods. Geneva: International Electrotechnical Commission, 2006.
21. IEC 61078:2016. Analysis techniques for dependability – Reliability block diagram and boolean methods. Geneva: International Electrotechnical Commission, 2016.
22. MIL-HDBK-217F. Reliability Prediction of Electronic Equipment: A Practical Guide. U.S. Department of Defense. URL: <https://doi.org/10.1109/RMC.2008.4593457>.
23. Reliability Program Handbook TANH0009A. SAE International. URL: <https://doi.org/10.4271/TANH0009A>.
24. Кузавков В. В., Михайлюк С. С., Погребняк С. В. Аналіз параметрів надійності об'єктів радіоелектронної техніки з надлишковістю // Системи і технології зв'язку, інформатизації та кібербезпеки. 2022. Т. 2, № 2. С. 15–20.
25. Meeker W. Q. Accelerated life testing and reliability assessment of electronic components / W. Q. Meeker, L. A. Escobar. New York: Wiley, 2014. [X] p. DOI: 10.1002/9780470316715.
26. Chen T. A comprehensive review of reliability and resilience assessment in modern communication networks / T. Chen, Y. Gong, K. Zhang // IEEE Access. 2022. Vol. 10. P. [X–Y]. DOI: 10.1109/ACCESS.2022.3168868.
27. Кузавков В., Ланко А. Обґрунтування необхідності нового підходу визначення надійності радіоелектронного обладнання в умовах обмеженої вхідної інформації // Progressive Approaches in Science and Engineering: 2 Міжнародна науково-практична конференція. Copenhagen, Denmark. P. 672–673 (November 26–28, 2025.) URL: <https://isu-conference.com/en/archive/progressive-approaches-in-science-and-engineering-26-11-25>. DOI: <https://doi.org/10.70286/isu-26.11.2025>.

28. Кузавков В. В., Ланко А. В. Застосування безконтактного індукційного методу при визначенні показників надійності об'єкта контролю // Системи і технології зв'язку, інформатизації та кібербезпеки, 2025. С. 65–73. DOI: 10.58254/viti.7.2025.06.65.

29. Кузавков В. В., Ланко А. В. Інженерні характеристики та оцінювання надійності радіоелектронного обладнання // Збірник наукових праць Національної академії Національної гвардії України. 2025. № 2 (46). С. 57–64. URL: <https://doi.org/10.33405/2409-7470/2025/2/46/352571>.

Надійшла до редколегії 02.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.056

канд. техн. наук Мазулевський О. Є. ORCID: 0000-0002-6042-2577 (ВІТІ ім. Героїв Крут)

ОЦІНКА ЗАБЕЗПЕЧЕНОСТІ КІБЕРБЕЗПЕКИ ОБОРОННОГО ВІДОМСТВА З УРАХУВАННЯМ ПЕРЕДОВИХ МІЖНАРОДНИХ ПРАКТИК

Вступ. У сучасних умовах інтенсивного розвитку інформаційних технологій та зростання кількості складних кіберзагроз особливого значення набуває забезпечення належного рівня кібербезпеки інформаційно-комунікаційних систем відомчих структур, особливо у секторі безпеки й оборони. Зростаюча залежність від ІКС обумовлює необхідність формування системних підходів до оцінювання рівня їх захищеності.

Проблематика. Існуючі міжнародні та державні стандарти, зокрема ДСТУ ISO/IEC 27001, а також методології NIST і моделі зрілості типу CMMC, визначають вимоги до забезпечення кібербезпеки, однак не забезпечують достатньо формалізованого, компактного та адаптованого під відомчі структури інструментарію оцінювання рівня її забезпеченості. Відсутність уніфікованого підходу ускладнює проведення порівняльного аналізу між підрозділами та формування узагальненої оцінки на рівні відомства.

Мета. Метою дослідження є розроблення способу оцінювання забезпечення кібербезпеки у відомчих інформаційно-комунікаційних системах, який дозволяє здійснювати кількісну оцінку рівня впровадження заходів безпеки на основі вимог Системи управління інформаційною безпекою за ДСТУ ISO/IEC 27001.

Матеріали й методи. У роботі використано підходи системного аналізу, методи експертного оцінювання та узагальнення державних та міжнародних практик у сфері кібербезпеки. Запропонований спосіб базується на оцінюванні трьох складових: документального забезпечення (наявність та актуальність політик і процедур), змістовної глибини опрацювання питань інформаційної безпеки (чек-листи відповідності ДСТУ ISO/IEC 27001) та технічного забезпечення (наявність і впровадження технічних засобів захисту). Оцінювання здійснюється шляхом застосування рівнозважених коефіцієнтів із подальшим агрегуванням результатів на рівні підрозділів і відомства.

Результати. У результаті дослідження сформовано універсальний спосіб, який дозволяє проводити стандартизоване оцінювання рівня забезпеченості кібербезпеки підрозділів, визначати слабкі місця в організаційних, процесних та технічних компонентах, а також здійснювати порівняльний аналіз між підрозділами. Запропоновано підхід до визначення загального рівня кібербезпеки відомства на основі мінімального значення серед підрозділів, що відповідає принципу "найслабшої ланки". Спосіб узгоджується з концепцією профілів безпеки та може бути інтегрований з інструментами автоматизованого контролю відповідності (SCAP/OpenSCAP).

Висновки. Запропонований спосіб забезпечує підвищення об'єктивності, відтворюваності та формалізації процесу оцінювання забезпечення кібербезпеки у відомчих інформаційно комунікаційних мережах. Його застосування дозволяє підвищити ефективність управління кібербезпекою, забезпечити узгодженість із міжнародними стандартами та створити основу для подальшого розвитку нормативно-методичного забезпечення у сфері кіберзахисту державних інформаційних систем.

Ключові слова: кібербезпека, CVIB, ДСТУ ISO/IEC 27001, оцінювання, інформаційно-комунікаційні системи, відомство, профілі безпеки, SCAP, CMMC.

O. Mazulevskyi. Assessment of cybersecurity of the defense department taking into account best international practices

Introduction. In the context of rapid development of information technologies and the increasing complexity of cyber threats, ensuring an adequate level of cybersecurity for departmental information and communication systems (ICS), especially in the defense sector, becomes critically important. The growing dependence on ICS necessitates systematic approaches to assessing their security level.

Problem statement. Existing state and international standards such as ISO/IEC 27001 (DSTU), as well as NIST methodologies and maturity models like CMMC, define cybersecurity requirements but do not provide a sufficiently formalized, compact, and adaptable assessment framework for departmental structures. The absence of a unified approach complicates comparative analysis between organizational units and the formation of an aggregated departmental-level assessment.

Purpose. The purpose of this study is to develop a method for assessing cybersecurity provision in departmental ICS, enabling quantitative evaluation of implemented security measures based on the Information Security Management System (ISMS) requirements of ISO/IEC 27001.

Materials and methods. The study applies system analysis, expert evaluation methods, and generalization of international cybersecurity practices. The proposed method is based on evaluating three components: documentary support (availability and relevance of policies and procedures), depth of policy content (ISO/IEC 27001-based

checklists), and technical implementation (availability and deployment of security controls). The assessment uses equally weighted coefficients and aggregates results at both unit and departmental levels.

Results. The study proposes a unified method that enables standardized assessment of cybersecurity provision across organizational units, identification of weaknesses in organizational, procedural, and technical domains, and comparative analysis between units. A departmental-level assessment approach based on the minimum unit score is introduced, reflecting the “weakest link” principle. The method is compatible with security profile frameworks and can be integrated with automated compliance assessment tools such as SCAP/OpenSCAP.

Conclusions. The proposed method improves objectivity, repeatability, and formalization of cybersecurity assessment processes in departmental ICS. Its application enhances cybersecurity management effectiveness, ensures alignment with international standards, and provides a foundation for further development of regulatory and methodological frameworks in the protection of state information systems.

Keywords: cybersecurity, ISMS, ISO/IEC 27001, assessment, information and communication systems, department, security profiles, SCAP, CMMC.

Постановка проблеми. Стрімка цифровізація, що охоплює всі сфери діяльності людини, включно і військову, зумовлює зростання залежності від інформаційних технологій. У військовому контексті надійність функціонування інформаційно-комунікаційних систем (ІКС) безпосередньо пов'язана з безпекою особового складу та виконанням критичних завдань, що надає кібербезпеці статусу ключової умови стабільності відомства. Забезпечення належного рівня кіберзахисту ускладнюється інтегрованістю більшості ІКС з глобальною мережею Інтернет і широким використанням загальнодоступного програмного забезпечення, що сприяє накопиченню випадкових і непередбачуваних негативних впливів. У такій ситуації Інтернет-орієнтація ІКС розглядається крізь призму необхідності системного захисту ресурсів під час виконання базових технологічних процесів – отримання, зберігання, транспортування, оброблення та відображення інформації. Відповідно, оцінка забезпечення кібербезпеки у відомстві набуває практичної значущості як інструмент управління ризиками, запобігання виникнення кризових ситуацій шляхом оцінки та підвищення кіберстійкості. Оцінка кіберстійкості повинна бути різносторонньою та охоплювати різні аспекти функціонування ІКС. В цій статті матеріал продовжує висвітлювати роботу в галузі оцінки кіберстійкості, але фокусується на оцінці забезпечення кібербезпеки як складової кіберстійкості.

Аналіз досліджень і публікацій. Оцінювання відповідності стандартам і рамкам кібербезпеки у відомчих структурах спирається на три взаємодоповнюючі напрями:

системи управління інформаційною безпекою рівня міжнародного стандарту ISO/IEC 27001 [2] та/або ДСТУ ISO/IEC 27001 [3];

каталоги контролів та формалізовані процедури їх оцінювання (базовий, галузевий та цільовий профілі безпеки, NIST SP 800-53/53A [4; 5], 800-171 [6]);

галузеві (військові) моделі зрілості та сертифікаційні моделі (англ. Cybersecurity Maturity Model Certification, CMMC) [7; 8; 13] разом з автоматизованими технічними перевірками (SCAP/OpenSCAP) [9–11].

Така конвергенція дозволяє поєднати процесний нагляд, доказову перевірку контролів та операційну автоматизацію відповідності.

Міжнародний стандарт ISO/IEC 27001 та/або державний стандарт ДСТУ ISO/IEC 27001:23 визнають вимоги до створення, впровадження та безперервного поліпшення системи управління інформаційною безпекою (СУІБ, англ. Information Security Management System, ISMS), уніфікуючи політики, ролі, оцінювання ризиків і контрольні заходи на рівні організації, в якій він впроваджується. Актуальна редакція стандарту ISO/IEC 27001 – 2022 рік (ДСТУ ISO/IEC 27001 – 2023 рік) закріплює його як базовий орієнтир для відомчих та оборонних структур, незалежно від масштабу, і передбачає узгодження процесів СУІБ із ризик-менеджментом і суміжними рамками контролів (зокрема NIST).

Вивчення досвіду США показує, що через національні регулюючі документи затверджено “Каталоги контролів і процедури їх оцінювання”. Ці каталоги містяться в [4] та надають інформацію:

повний перелік контролів безпеки та приватності;
адаптовані під ризик-менеджмент і різні технологічні домени;

проведено формалізацію методики та процедур оцінювання визначених контролів із вимогами до доказів і критеріїв прийняття.

Для середовищ, де обробляється CUI (Controlled Unclassified Information, укр. аналог – державні інформаційні ресурси, ДІР) поза федеральними системами NIST SP 800-171 Rev. 3 [6] встановлює вимоги та прямо відсилає до оцінювальних процедур SP 800-171A/53A [5; 12]. У сукупності ці документи задають перевірочні критерії відповідності для державного сектору та оборонно-промислової галузі.

Програма визначення зрілості і сертифікації кібербезпеки для оборонної сфери (СММС) інституційно визначає рівні зрілості захисту FCI/CUI (FCI – Federal Contracting Information, CUI – Controlled Unclassified Information) у підрядників Міноборони США і вводить обов'язкові само-оцінювання або третьо-сторонні оцінювання залежно від рівня. Фінальне правило 32-CFR:2024 [7] закріплює вимоги, а SCAP v2.0 [8] детально описує процес оцінювання на рівні ролей, фаз, артефактів та прийняття рішень для СЗРАО/ССА (Certified Third-Party Assessor Organization / Cybersecurity Maturity Model Certification, укр. – сертифікованих організацій оцінювачів третьої сторони / військової моделі визначення зрілості кібербезпеки), що критично для відомчих перевірок і взаємного визнання практик.

Довідково: FCI та CUI – це два типи конфіденційної інформації, що обробляється під час роботи з федеральним урядом. FCI – це будь-яка інформація, що не призначена для публічного розповсюдження, а CUI – це більш чутливий тип даних, що вимагає суворіших заходів безпеки для захисту від несанкціонованого доступу.

Автоматизація відповідності (SCAP/OpenSCAP) [9–11]. Для технічних конфігураційних перевірок застосовують набір взаємодіючих специфікацій SCAP, який уніфікує машиночитуваний контент, сканування та звітування; ініціативи NIST підтримують валідацію продуктів. Проєкт OpenSCAP надає інструментарій і профілі відповідності, що дозволяє інтегрувати контрольні перевірки з процесами аудиту та звітністю.

Довідково: SCAP (Security Content Automation Protocol) – це набір взаємопов'язаних специфікацій для машиночитаних перевірок безпеки: опису політик, виявлення вразливостей/невідповідностей і уніфікованої звітності. OpenSCAP – відкритий інструментарій, що реалізує SCAP-перевірки (CLI oscar, профілі відповідності, генерація ARF/HTML-звітів, можливості ремедіації). На офіційному порталі – огляд, політики, довідники та набір утиліт (у т. ч. для парку систем).

Моделі процесної зрілості ISO/IEC 21827 [14], Systems Security Engineering – Capability Maturity Model (SSE-CMM). SSE-CMM описує характеристики процесів інженерії безпеки як стандартну метрику зрілості, що застосовується на всіх етапах життєвого циклу та рівнях організації, її використовують для оцінки зрілості та планування розвитку спроможностей. Для відомчих структур це корисний “надпроцесний” шар, сумісний із СУІБ та контрольними каталогами.

У НАТО та ЄС наголошується на формалізованому оцінюванні спроможностей і узгодженні з технічними керівництвами. Документи НАТО з кібероборони й доктрина AJP-3.20 [15] підкреслюють потребу у взаємосумісних заходах і процедурах. ENISA [16] пропонує технічні настанови та цілі безпеки – EECN/NIS (англ. European Electronic Communication Code / Network and Information Security), які можуть слугувати базисом для відомчих оцінювань в європейських організаціях.

В Україні формується трирівнева модель профілів безпеки для ІКС:

базовий (державний рівень, затверджує Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку);

галузевий (рівень відомства);

цільовий (для конкретної ІКС).

Кабінет Міністрів України у 2025 році затвердив порядок розробки профілів безпеки та порядок авторизації з безпеки. Держспецзв'язку оприлюднила базові профілі безпеки та методичні рекомендації розробки цільових профілів, а також порядок моніторингу й оцінки дотримання.

Під час перевірки власник ІКС має надати докази реалізації заходів, визначених у відповідному профілі.

Ключові норми нормативних вимог й оголошень містяться у наступних документах:

постанова КМУ № 627 від 30.05.2024 як початок експериментального проєкту з декларування відповідності КСЗІ на основі профілів (базових і цільових) [17];

наказ Адміністрації ДССЗІ № 317 від 24.06.2024 визначає Базовий профіль безпеки інформації (структура вимог) [18];

методичні рекомендації щодо формування ЦПБ (протокол від 14.03.2025 № 09-2025) визначає, як розробляти цільовий профіль безпеки для цільової ІКС [19];

постанова КМУ № 712 від 18.06.2025 визначає системний Порядок розроблення та затвердження профілів і Порядок авторизації з безпеки (експеримент замінили постійною процедурою) [20];

порядок моніторингу (реєстр, аналіз звітів) – наказ АДССЗІ/Мін'юст, березень 2025 – акцент на аналізі повноти, об'єктивності та достатності доказів за ЦПБ [21];

повідомлення ДССЗІ про затвердження базових профілів (08.07.2025) – підкреслюють призначення базового профілю та подальше формування ЦПБ на його основі [22].

У статті [1] було показано частину оцінки, яку засновано на динаміці зміни кількості зафіксованих кіберінцидентів.

Метою статті є розробка моделі для формалізації оцінювання забезпечення інформаційної безпеки на рівні підрозділів з опорою на Систему управління інформаційною безпекою оборонного відомства з урахуванням профілів безпеки для ІКС.

Виклад основного матеріалу дослідження. Розглянуті в попередньому аналізі джерел та публікацій підходи оцінки застосовано в закордонних системах, які логічно поєднуються із сучасними вимогами профілів безпеки, із побудовою СУІБ, перевіркою відповідності СММС та із можливістю використання автоматизації періодичного підтвердження відповідності SCAP/OpenSCAP. Далі розглянемо можливість такої реалізації.

Структура профілів безпеки наближена до “policy baseline” у СУІБ:

базовий профіль – це державний мінімум;

галузевий профіль безпеки забезпечує уточнення з урахуванням ризиків і задач оборонного відомства;

цільовий профіль безпеки являє собою конкретизацію під ІКС. У СУІБ це відповідає ієрархії політик/процедур і “Statement of Applicability”.

Для зберігання доказів варто організувати “реєстр доказів” (evidence register), де будуть пов'язані “Вимога профілю” – “контроль/процедура” – “доказ” (політика, журнал, налаштування, протокол проведення тесту). Методично перетинаються з підходом NIST 800-53A/800-171A [5; 12] і процесом СММС SCAP (опитування, огляд доказів, технічні тести) [8].

Технічна перевірка – для конфігурацій/вразливостей слід додати процедуру SCAP/OpenSCAP:

XCCDF/OVAL-профілі;

регулярні сканування oscap;

ARF/HTML-звіти як формалізовані докази виконання відповідних пунктів профілю.

Довідково: XCCDF і OVAL – це стандартизовані формати для машиночитних перевірок безпеки. XCCDF (Extensible Configuration Checklist Description Format) описує чек-лист/бенчмарк: правила; профілі; параметри; важливість; посилання.

Open Vulnerability and Assessment Language (OVAL) описує тести поточного стану системи, що саме і як перевірити на кінцевому пристрої (реєстр/файл/пакет/сервіс тощо).

Згідно зі статтею 8 Закону України “Про основні засади забезпечення кібербезпеки України” [23] Міністерство оборони України є одним із основних суб’єктів національної системи кібербезпеки і відповідно до компетенції здійснює заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Також Міністерством оборони України пройшло сертифікацію системи управління інформаційною безпекою на відповідність стандарту ISO/IEC [24], що підтверджує побудову СУІБ та її ефективне використання.

Виходячи із вищезазначеного, слід реалізувати можливість оцінити стан кіберстійкості ІКС оборонного відомства для прийняття зважених управлінських рішень в мирний час та під час функціонування в особливий період (військовий стан). Розгляд цього питання піднімався в статті [1], де запропоновано розробити Метод прогнозування та виявлення кризових ситуацій у кіберпросторі на основі обробки статистичних даних, та представлено один із його складових – підхід оцінювання поточного стану кіберстійкості оборонного відомства з урахуванням ситуації у кіберпросторі на основі статистичного аналізу зафіксованих кіберінцидентів.

У цій статті буде представлено ще один етап оцінювання кіберстійкості, а саме спосіб оцінювання забезпечення інформаційної безпеки оборонного відомства на рівні підрозділів. Спосіб забезпечує:

- відтворюваність і прозорість оцінювання;

- порівнюваність між підрозділами;

- можливість агрегування результатів на рівень відомства та включення їх у цикл планування заходів СУІБ.

За допомогою способу, описаного в цій статті, можливо буде оцінювати структурні підрозділи відомства, що експлуатують ІКС, для яких визначені вимоги цільового профілю безпеки (ЦПБ) і встановлено межі СУІБ оборонного відомства. Спосіб не замінює проведення аудиту відповідності, а надає регулярний вимір рівня забезпечення та дотримання вимог за трьома взаємодоповнювальними векторами.

Логічна модель оцінювання та вектори забезпечення – оцінювання здійснюється за принципом “мінімально достатнього” набору контрольних пунктів (чек-листів), згрупованих у три рівноважні вектори:

1. Документальне забезпечення – наявність і актуальність ключових документів СУІБ (політики, методики, Декларація про застосовність (англ. Statement of Applicability, SoA), ролі/відповідальності, процедури інцидент-менеджменту, планування безперебійності в роботі та відновлення після збоїв тощо).

2. Глибина опрацювання регламентуючих документів – ступінь розкриття обов’язкових питань СУІБ:

- контекст і зацікавлені сторони; критерії прийняття ризиків;

- трасування SoA – Додаток А стандартів [2; 3] – докази;

- навчання;

- життєвий цикл доступів;

- логування/моніторинг;

- управління вразливостями;

- бекапи;

- інтеграції безпеки на кожному етапі розробки програмного забезпечення (DevSecOps);

- робота з постачальниками;

- фізична безпека;

- метрики СУІБ.

3. Технічне забезпечення СУІБ – наявність мінімального набору технологічних контролів відповідно до Додатку А стандартів [2; 3] та обраних цілей безпеки (багатофакторна автентифікація, захист кінцевих пристроїв та антивірусний захист, централізоване логування, резервування, управління оновленнями програмним

забезпеченням, поштовий/вебзахист, сегментація мережі, шифрування, сканування вразливостей, за можливості – автоматизовані перевірки за прикладом SCAP/OpenSCAP).

Кожний вектор оцінювання відбиває різні шари спроможностей СУІБ:

управлінський – через документи;

змістовий/процесний – через глибину вмісту політик;

технологічний – через реалізацію технічних контролів.

Рівнозначність відображає принцип системності – жоден шар сам по собі не гарантує достатню кіберстійкість.

Шкали вимірювання та обчислення інтегральних показників. При оцінюванні контрольних пунктів чек-листа застосовується трирівнева шкала з урахуванням доказів:

1,0 – виконано повністю (наявний і впроваджений елемент; подані підтверджувальні артефакти);

0,5 – виконано частково (елемент існує, але є прогалини, а саме неповний обсяг, або неактуальність, або відсутність частини доказів);

0,0 – не виконано.

Позначення “Н/З” (не застосовується) вилучає пункт із розрахунку (див. знаменник у формулах нижче).

Показники векторів. Нехай s_i – бал за i -й пункт у відповідному векторі v , а n_v – кількість релевантних (без “Н/З”) пунктів у цьому векторі. Тоді середній бал вектору буде визначатися за формулою:

$$S_v = \frac{\sum_{i=1}^{n_v} s_i}{n_v}.$$

Інтегральний показник підрозділу. З огляду на рівнозначність векторів, інтегральний бал підрозділу визначається як середнє арифметичне:

$$S_{\text{підр}} = \frac{S_{\text{док}} + S_{\text{контент}} + S_{\text{тех}}}{3}.$$

За потреби вводиться коефіцієнт достовірності доказів ($C \in [0,8 \dots 1,0]$), що модулює ступінь довіри до наданих артефактів (1,0 – повний комплект артефактів, включно з технічними звітами; 0,9 – без технічних; 0,8 – переважно декларації). Тоді скоригований інтегральний бал буде визначатися за формулою:

$$\hat{S}_{\text{підр}} = S_{\text{підр}} * C.$$

Для висвітлення стану та визначення необхідності прийняття управлінських рішень пропонуються такі порогові значення:

0,85–1,00 – Високий рівень: СУІБ стабільно функціонує, підтверджена наявними доказами;

0,70–0,84 – Достатній рівень: поодинокі прогалини, необхідні планові поліпшення;

0,50–0,69 – Базовий рівень: суттєві ризики, потрібен план покращення/відновлення;

0,00–0,49 – Низький рівень: відсутні ключові елементи СУІБ.

Далі розглянемо можливі мінімальні переліки (чек-листи) перевірок за векторами.

Документальне забезпечення (зразок мінімуму):

політика інформаційної безпеки (схвалена керівництвом, актуальна версія).

сфера СУІБ (опис меж і виключень);

методика й звіт з оцінювання ризиків, реєстр ризиків;

декларація про застосовність Statement of Applicability – (SoA) із обґрунтуванням включень/виключень контролів Додатку А стандартів [2; 3];
ролі та відповідальності (власники процесів/активів);
політика управління активами (класифікація, власники);
політика контролю доступу (принципи, багатофакторна автентифікація, найменші привілеї);
політика криптографії (використання, керування ключами);
безперервність функціонування та відновлення після збоїв (визначення цільової точки відновлення, цільового часу відновлення, тести);
інцидент-менеджмент (ролі, ескалації, журнал);
політика постачальників (оцінка, вимоги ІБ у договорах);
план внутрішніх аудитів СУІБ та звіти з виявлення, аналізу та усунення причин невідповідностей;
управління змінами (процедури, протоколи).

Примітка. Кожен пункт має бути закріплений до відповідної вимоги цільового профілю безпеки та/або Додатку А стандартів [2; 3] для забезпечення спостережності (tracing) у звіті.

Глибина опрацювання політик (ключові питання):
визначені контекст і зацікавлені сторони, що періодично оновлюються;
формалізовані критерії прийняття ризиків; наявний план обробки ризиків;
трасування SoA – Додатку А стандартів [2; 3] – докази (матриця відповідності);
навчання та обізнаність (план, % покриття, перевірка знань) персоналу;
життєвий цикл управління доступом (надання/позбавлення/перевірка);
політика логування та моніторингу (перелік подій, зберігання, захист журналів);
управління вразливостями (періодичність сканування, рівень обслуговування/покращення/відновлення);
резервне копіювання (частота, шифрування, тести відновлення);
безпечна розробка/DevSecOps (за наявності);
оцінювання постачальників (анкети/аудити, вимоги до повідомлень про інциденти).
фізична безпека (периметр, серверні кімнати, журнали доступів);
метрики СУІБ (наприклад, середній час на відновлення після інцидентів, % виконаних тестів аналізу та усунення причин невідповідностей).

Технічне забезпечення СУІБ (мінімальний набір):

а) Організаційні/кадрові/фізичні (Додаток А стандартів [2; 3], пункти А.5–А.7):
розмежування обов'язків;
реалізація принципу найменших привілеїв;
багатофакторна автентифікація для адміністраторів;
навчання;
договір про нерозголошення;
контроль фізичного доступу (бейджі, журнали, ключі).

б) Технологічні (Додаток А стандартів [2; 3], пункт А.8):
ідентифікація та автентифікація: багатофакторна автентифікація, централізована система автентифікації, політика паролів;
антивірус/EDR на кінцевих точках;
політики реагування;

в) Логування і кореляція:
централізований збір (впровадження SIEM/лог-сховище),
зберігання не менше 90 днів.

г) резервні копії:
офлайн-сайт/ізоляція,
шифрування,

перевірочні відновлення.

д) Управління оновленнями ПЗ:

швидкість встановлення оновлень (критичних не більше 14 днів),

інвентаризація активів.

е) Захист пошти/веб:

реалізація механізмів захисту вебсервісів та поштових сервісів;

фільтрація вкладень/URL.

ж) Мережеві засоби:

сегментація мережі (VLAN/VRF);

впровадження міжмережових екранів;

VPN сучасних протоколів;

системи виявлення/протидії вторгнень (щонайменше на периметрі).

з) Шифрування даних:

у транзиті (TLS сучасних версій);

у спокої (за потреби).

і) Управління вразливостями:

регулярне сканування;

реєстр вразливостей;

сканування за пріоритетами.

к) Регулярна автоматична перевірка контролів профілів безпеки (за можливості):

XCCDF/OVAL-профілі;

регулярне сканування на підвищення привілеїв;

наявність ARF/HTML-звітів як формалізованих доказів.

Далі розглянемо процедуру проведення оцінювання підрозділу:

Етап 1: Підготовка.

Визначаються підрозділи, власники ІКС, переліки артефактів; погоджуються пункти, до яких вимоги не застосовуються.

Формується реєстр доказів: вимога профілю – елемент профілю – доказ реалізації вимоги.

Етап 2: Збір даних і виставлення балів.

Двоє незалежних оцінювачів перевіряють артефакти/налаштування, опитують відповідальних, виставляють оцінки за пунктами чек-листів.

Етап 3: Вирівнювання та верифікація.

Розбіжності узгоджуються консенсусом; фіксується коефіцієнт C (коефіцієнт достовірності доказів). У разі оцінки технічних пунктів – перевага надається автоматизованим звітам (наприклад, ARF/HTML з OpenSCAP).

Етап 4: Агрегація та звітування.

Розраховуються $S_{\text{док}}$, $S_{\text{контент}}$, $S_{\text{тех}}$, $S_{\text{підр}}$ та $S'_{\text{підр}}$. Формуються:

зведена таблиця по підрозділах;

“теплова карта” виконання пунктів;

огляд трьох векторів;

рейтинг підрозділів.

Етап 5: Планування покращення.

Для кожного пункту з балом від 0 до 0,5 визначаються власник, дія, термін, метрика завершення (наприклад, % зменшення високих відхилень у SCAP-скануваннях, збільшення періоду зберігання журналів тощо).

Приклад фрагмента матриці оцінювання підрозділу наведено в таблиці 1.

Автоматизований шаблон розрахунку може виключати “Н/З” з підрахунку (n_v) і підсвічувати “вузькі місця” (пункти з оцінкою 0 або 0,5), формуючи вхідну чергу для покращення/відновлення.

Спосіб передбачає пряму перевірку пунктів чек-листів до вимог цільового профілю безпеки, який, у свою чергу, наслідуює вимоги галузевого та базового профілів безпеки. В аналітичному додатку до звіту доцільно навести таблицю відповідностей: Вимога профілю – пункт чек-листа – контроль Додатку А стандартів [2; 3] – тип доказу – періодичність перевірки – власник. Такий підхід полегшує як внутрішні перевірки, так і зовнішні інспекції/аудити.

Для технічних пунктів рекомендовано, де це можливо, застосовувати SCAP/OpenSCAP як джерело машинозчитуваних доказів (доказів, які сформовані при автоматичній перевірці і записані в форматі, який здатен прочитати комп'ютер). У випадках, коли відомство орієнтується на сумісність із практиками CMMC/NIST (для взаємодії з міжнародними партнерами), матриця оцінювання може включати додаткові колонки “Сімейство вимог NIST 800-171/контроль 800-53” [4; 12] та “процедура оцінювання (800-53A)” [5], що підвищує взаємну сумісність доказової бази.

Таблиця 1

Приклад фрагмента матриці оцінювання підрозділу

Вектор	Пункт	Бал	Доказ реалізації
Документи	Політика ІБ затверджена та актуальна	1,0	Наказ №..., PDF від 2025-09-12
Документи	SoA із обґрунтуванням виключень	0,5	SoA v1.2; немає пояснення щодо A.8.23
Контент	Критерії прийняття ризиків	1,0	Методика ризиків, розд. 4
Технічні	MFA для адміністраторів	1,0	Скріні IdP + журнал подій
Технічні	Централізоване логування (≥ 90 днів)	0,5	SIEM: 60 днів
Технічні	OpenSCAP щоквартально	0,0	Немає профілів/звітів

Контроль якості оцінювання та управління упередженнями. Щоб знизити суб'єктивність, пропонується:

використовувати подвійне оцінювання (два оцінювачі на підрозділ);

фіксувати розбіжності та процедуру їх розв'язання;

застосовувати коефіцієнт достовірності C ;

зберігати артефакти у централізованому “реєстрі доказів” із контрольними сумами/версіями.

Додатково для пунктів, що покладаються на процесні артефакти (накази, протоколи), періодично проводити перевірочні спостереження. Наприклад, тестове відновлення з резервних копій, перевірка вибірки заявок на доступ, контроль наявності слідів аудиту в журналах SIEM тощо.

Розглянутий спосіб оцінки забезпеченості кібербезпеки оборонного відомства із урахуванням передових міжнародних практик навмисно використовує мінімальний набір пунктів для забезпечення керованості в умовах великої кількості підрозділів. Це обмеження може призводити до втрати частини “глибини” оцінки. Шляхами вдосконалення може бути:

розширити чек-листи для специфічних підрозділів і галузей;

інтегрувати показники результативності;

автоматизувати збирання технічних доказів;

апробувати вагові коефіцієнти замість рівноважного усереднення там, де це виправдано ризиком.

Визначивши оцінки забезпечення кібербезпеки по підрозділах, можливо зробити загальну оцінку забезпечення кібербезпеки за оборонне відомство. Для оцінювання усього відомства варто висвітлювати наступні значення для узагальнення оцінок підрозділів:

1. Індикатор ризику – найнижче значення $S'_{\text{підр.}}$.

2. Середнє значення, тобто типове значення по підрозділах.

3. 10-й перцентиль (визначає значення найгірших) – “хвіст ризику”.

4. Покриття $Coverage_{\tau}$ – відсоткова частка підрозділів, що має оцінку більше цільового порогу (наприклад, $S' \geq 0,70$, $\tau = 0,7$).

Форми реагування (управлінських рішень) при отриманні загальної оцінки:

якщо $S'_{min} < 0,50$ – “червоний статус” оборонного відомства, негайна реалізація плану відновлення/покращення для підрозділу-аутсайдера, щотижневий моніторинг;

якщо $S'_{min} \geq 0,50$, але $S_{10} \% < 0,70$ або $Coverage_{0,7} < 80 \%$ – “жовтий статус”, реалізація програми вирівнювання, варто звернути увагу на аутсайдерів;

якщо $S'_{min} \geq 0,70$ і $Coverage_{0,70} \geq 95 \%$ – “зелений статус”, фокус діяльності на підвищенні медіани/технічній глибині.

Висновки. Запропонований спосіб оцінки забезпеченості кібербезпеки оборонного відомства із урахуванням передових міжнародних практик надає оборонному відомству уніфікований спосіб вимірювання забезпечення кібербезпеки на рівні підрозділів із опорою на СУІБ (ДСТУ ISO/IEC 27001:2023), профілі безпеки для ІКС та кращі міжнародні практики. Розподіл на три рівноважні вектори дозволяє балансувати управлінські, процесні та технологічні аспекти. Також використання чек-листів і прозорих формул гарантує відтворюваність результатів, а включення машинозчитуваних доказів (SCAP/OpenSCAP) зменшує суб'єктивність і підвищує доказову силу результатів. Спосіб масштабується на рівень відомства і дає основу для планування покращення/відновлення та підвищення кіберстійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мазулевський О. Є., Жолобович Н. В. Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі // Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 3 (51). С. 34–40. DOI: 10.33099/2311-7249/2024-51-3-34-40.
2. ISO/IEC 27001:2022. Information security management systems – Requirements. Женева: ISO/IEC, 2022. URL: <https://www.iso.org/standard/27001> (дата звернення: 03.11.2025).
3. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. [Чинний від 2023-08-22]. Вид. офіц. К.: ДП “УкрНДНЦ”, 2023.
4. Joint Task Force. NIST SP 800-53, Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2020. 492 p. DOI: 10.6028/NIST.SP.800-53r5. URL: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final> (дата звернення: 06.11.2025).
5. Force J. T., Quinn S., Nadeau E. et al. NIST SP 800-53A Rev.5. Assessing Security and Privacy Controls in Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2022. 689 p. DOI: 10.6028/NIST.SP.800-53Ar5.
6. Ross R., Pillitteri V. NIST SP 800-171, Rev. 3. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2024. 120 p. DOI: 10.6028/NIST.SP.800-171r3.
7. Department of Defense. Office of the Secretary. Cybersecurity Maturity Model Certification (CMMC) Program: Final rule // Federal Register. 2024. Vol. 89, No. 199. P. 83092–83237. (32 CFR Part 170; Doc. No. 2024-22905; ефективно з 16.12.2024). URL: <https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program>; офіц. PDF на GovInfo. (дата звернення: 06.11.2025).
8. CMMC Assessment Process (CAP), v2.0. The Cyber AB, 16.12.2024. URL: <https://cyberab.org/Portals/0/CMMC%20Assessment%20Process%20v2.0.pdf> (дата звернення: 03.11.2025).
9. Security Content Automation Protocol (SCAP): Project Overview. NIST CSRC. URL: <https://csrc.nist.gov/projects/security-content-automation-protocol> (дата звернення: 03.11.2025).
10. SCAP Validated Products and Modules. NIST CSRC. URL: <https://csrc.nist.gov/projects/scap-validation-program/validated-products-and-modules> (дата звернення: 03.11.2025).
11. OpenSCAP Portal. URL: <https://www.open-scap.org/> (дата звернення: 03.11.2025).

12. Ross R., Pillitteri V. NIST SP 800-171A Rev.3. Assessing Security Requirements for Controlled Unclassified Information. Gaithersburg, MD: National Institute of Standards and Technology, 2024. 106 p. DOI: 10.6028/NIST.SP.800-171Ar3. URL: <https://csrc.nist.gov/pubs/sp/800/171/a/r3/final> (дата звернення: 06.11.2025).
13. Code of Federal Regulations. Title 32–National Defense. Part 170 – Cybersecurity Maturity Model Certification (CMMC) Program. Electronic Code of Federal Regulations (eCFR), поточна редакція. URL: <https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170> (розд. 32 CFR Part 170) (дата звернення: 06.11.2025).
14. ISO/IEC 21827:2008. Systems Security Engineering – Capability Maturity Model (SSE-CMM). Женева: ISO/IEC, 2008. URL: <https://www.iso.org/standard/44716.html> (дата звернення: 03.11.2025).
15. NATO. Allied Joint Doctrine for Cyberspace Operations (AJP-3.20). 2020. URL: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (дата звернення: 03.11.2025).
16. ENISA. Guideline on Security Measures under the EEC (4th ed.). 2021. URL: <https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc> (дата звернення: 03.11.2025).
17. Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: постанова Каб. Міністрів України від 30.05.2024 № 627. URL: <https://zakon.rada.gov.ua/laws/show/627-2024-%D0%BF#Text> (дата звернення: 03.11.2025).
18. Про визначення Базового профілю безпеки інформації: наказ Адміністрації ДССЗІ від 24.06.2024 № 317. URL: <https://zakon.rada.gov.ua/rada/show/v0317519-24#Text> (дата звернення: 03.11.2025).
19. Методичні рекомендації з формування цільового профілю безпеки інформації: схвал. рішенням ЕР з питань державної експертизи в сфері ТЗІ (протокол від 14.03.2025 № 09-2025). URL: <https://www.cip.gov.ua/ua/docs/metodichni-rekomendaciyi-z-formuvannya-cilovogo-profilu-bezpeki-informaciyi-skhvaleni-rishenniyam-er-z-pitan-derzhavnoyi-ekspertizi-v-sferi-tzi-protokol-vid-14-03-2025-09-2025> (дата звернення: 03.11.2025).
20. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем: постанова Каб. міністрів України від 18.06.2025 № 712. URL: <https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text> (дата звернення: 03.11.2025).
21. Про затвердження Порядку здійснення моніторингу систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням базових та цільових профілів безпеки інформації: наказ Адміністрації ДССЗІ від 10.03.2025 № 160. (Зареєстровано в Міністерстві юстиції України 20 березня 2025 року за № 448/43854.) URL: <https://zakon.rada.gov.ua/laws/show/z0448-25#Text> (дата звернення: 03.11.2025).
22. Повідомлення ДССЗІ про затвердження базових профілів (08.07.2025). URL: <https://cip.gov.ua/ua/news/derzhspeczv-yazku-zatverdila-bazovi-profil-bezpeki-modernizuyuchi-pidkhodi-do-kiberzakhistu-derzhavnikh-sistem> (дата звернення: 03.11.2025).
23. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 03.11.2025).
24. Повідомлення на офіційному сайті Міністерства оборони України. Міністерство оборони пройшло сертифікацію системи управління інформаційною безпекою на відповідність стандарту ISO/IEC. (24.04.2025) URL: <https://mod.gov.ua/news/ministerstvo-oboroni-projshlo-sertifikacziyu-sistemi-upravlinnya-informacijnou-bezpekoju-na-vidpovidnist-standartu-iso-iec> (дата звернення: 03.11.2025).

Надійшла до редколегії 12.02.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ПЕРЕДАЧІ ДАНИХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ З УРАХУВАННЯМ ВИМОГ КОНФІДЕНЦІЙНОСТІ, ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ

У статті розглянуто особливості архітектури сучасних військових систем передачі даних, які класифіковано на три основні типи: тактичні мобільні мережі, стаціонарні вузли та хмарні платформи типу C4ISR. Показано, що кожен із зазначених типів має специфічні переваги та вразливості за умов дії радіоелектронних, кібернетичних та інфраструктурних загроз, а їх ефективне поєднання є критичним для забезпечення безперервного та захищеного управління військами. Теоретично обґрунтовано необхідність формалізації базових критеріїв інформаційної безпеки: конфіденційності, цілісності та доступності CIA у вигляді метричних функцій, на основі яких запропоновано інтегральний індекс ефективності безпеки SEI як зважену комбінацію складових CIA з урахуванням вагових коефіцієнтів, диференційованих за типами систем (тактичні, стаціонарні, хмарні). На основі розробленої моделі виконано порівняльний аналіз низки реальних систем (Delta, Kropyva, GIS Arta, BFT, JADC2), що дозволило кількісно оцінити рівень їхньої захищеності та виявити критичні зони ризику. Запропоновано матрицю інтерпретації значень SEI, яка забезпечує перехід від кількісних результатів багатокритеріальної оцінки до якісних висновків і рекомендацій щодо підвищення ефективності захисту. Наукова новизна роботи полягає у поєднанні архітектурного аналізу військових систем передачі даних із формалізованою моделлю SEI та інтерпретаційною матрицею, а практичне значення у можливості використання отриманих результатів для проєктування адаптивних, живучих і масштабованих систем зв'язку та підтримки прийняття рішень у сфері кіберзахисту. Додатково підкреслено, що запропонований підхід забезпечує інструментальну базу для системного порівняння різних архітектур за умов багатокomпонентних загроз. Отримані результати можуть бути використані під час планування модернізації існуючих військових платформ та створення нових рішень, орієнтованих на підвищення стійкості інформаційної інфраструктури. Застосування моделі SEI також відкриває можливості для подальшого розвитку методів ризик-орієнтованої оцінки та оптимізації заходів захисту в умовах мережоцентричних операцій.

Ключові слова: військові системи передачі даних, архітектура C4ISR, інформаційна безпека, індекс SEI, критерії CIA, кіберзагрози, тактичні мережі, системи військового управління.

O. Noskov. Development of a model for determining the efficiency of various types of data transmission systems taking into account the requirements for confidentiality, integrity and availability

The article examines the architectural features of modern military data transmission systems, which are classified into three main types: tactical mobile networks, fixed nodes and cloud platforms of the C4ISR type. It is shown that each of these types has specific advantages and vulnerabilities under the conditions of radio-electronic, cybernetic and infrastructure threats, and their effective combination is critical for ensuring continuous and secure command and control of troops. The need for formalization of the basic criteria of information security: confidentiality, integrity and availability CIA in the form of metric functions is theoretically substantiated, on the basis of which the integral index of security effectiveness SEI is proposed as a weighted combination of CIA components taking into account weighting factors differentiated by system types (tactical, stationary, cloud). Based on the developed model, a comparative analysis of a number of real systems (Delta, Kropyva, GIS Arta, BFT, JADC2) is performed, which allowed to quantitatively assess the level of their security and identify critical risk zones. A matrix for interpreting SEI values is proposed, which provides a transition from quantitative results of multi-criteria assessment to qualitative conclusions and recommendations for improving protection efficiency. The scientific novelty of the work lies in the combination of architectural analysis of military data transmission systems with a formalized SEI model and an interpretative matrix, and the practical significance lies in the possibility of using the obtained results for the design of adaptive, survivable and scalable communication and decision support systems in the field of cyber defense. It is additionally emphasized that the proposed approach provides an instrumental basis for the systematic comparison of different architectures under conditions of multi-component threats. The obtained results can be used when planning the modernization of existing military platforms and creating new solutions aimed at increasing the resilience of the information infrastructure. The application of the SEI model also opens up opportunities for further development of methods for risk-based assessment and optimization of protection measures in conditions of network-centric operations.

Keywords: military data transmission systems, C4ISR architecture, information security, SEI index, CIA criteria, cyber threats, tactical networks, military control systems.

Постановка завдання. Сучасні військові системи передачі даних за архітектурними ознаками можна розділити на три основні типи: тактичні мобільні мережі, стаціонарні вузли та хмарні платформи (cloud-based C4ISR). Кожен із цих типів має специфічну структуру й принцип дії, що визначають їх застосування та ефективність у різних умовах [1; 2]. Тактичні мобільні мережі – це польові мережі зв'язку тактичного рівня, призначені для забезпечення командування і взаємодії безпосередньо на полі бою. Вони об'єднують підрозділи, що діють у русі (піхотні підрозділи, бойові машини, мобільні командні пункти тощо), і надають їм можливість обмінюватися даними в реальному часі навіть за відсутності розвинутої інфраструктури. Такі мережі часто будуються за принципом ad hoc (тобто самоорганізованих мереж) і можуть функціонувати в умовах мінливої топології, коли вузли (радіостанції, термінали тощо) додаються або вибувають динамічно. Виходячи з цього, постає завдання дослідження – формалізувати підходи до оцінювання ефективності військових систем передачі даних з урахуванням архітектурних особливостей кожного типу та різної природи загроз, а також розробити універсальний інструмент для порівняльного аналізу їхнього рівня інформаційної безпеки. Для цього необхідно визначити релевантні критерії оцінювання, побудувати метричну модель їх вимірювання та забезпечити можливість інтерпретації отриманих результатів у контексті практичних потреб військового управління та кіберзахисту.

Аналіз літературних джерел. Проведений аналіз наукових і прикладних досліджень свідчить про зростаючу увагу до проблеми підвищення ефективності військових систем передачі даних та їхньої інформаційної безпеки. У роботі Андрушка М. В., Аркушенка П. Л., Кузнецова В. О. та Андрушка А. М. [1] обґрунтовано узагальнену модель функціонування перспективних інформаційно-вимірювальних систем, що є важливим підґрунтям для подальшого формування метричних підходів до оцінювання військових комунікаційних платформ. Дослідження Поморцевої О. Є. та Кобзана С. М. [2], присвячене геопросторовому моделюванню, демонструє значення просторово-аналітичних інструментів для підвищення точності та оперативності обробки даних у військових системах підтримки рішень. У матеріалі Brandi V. [3] підкреслюється роль штучного інтелекту в трансформації підходів НАТО до геопросторової розвідки, що актуалізує питання інтеграції AI-модулів у сучасні C4ISR-архітектури.

У роботі Купера Т. [6] акцентовано на високій вразливості засобів радіолокації до засобів ворожої радіотехнічної та сигнальної розвідки, що визначає необхідність підвищення стійкості каналів передачі даних у тактичних мережах. Публікації Коломійця В. [7], Данилова О. [8], Найєма М. [9] та Морфінова С. [10] висвітлюють еволюцію української системи ситуаційної обізнаності «Delta», її функціональні можливості, роль у мережецентричних операціях та реакцію противника на її використання. Окреме місце займає стаття Кобзана С., Поморцевої О., Паньківа В. та Андронova В. [16], де наведено підходи до побудови геоінформаційної системи для потреб Збройних Сил України, що є релевантним у контексті формування архітектурних вимог до військових систем управління.

Додаткові матеріали щодо функціонування українських та міжнародних платформ – таких як Delta, GIS Arta, BFT, JADC2, Griselda та інших – узагальнено у відкритих оглядах і технічних описах, які демонструють різноманітність архітектур, рівнів автоматизації та ступеня інтеграції систем ситуаційної обізнаності в операційну діяльність військ. Сукупність проаналізованих джерел підтверджує необхідність формалізації підходів до оцінювання захищеності військових систем передачі даних та обґрунтовує актуальність розробки універсальних індексів і моделей для порівняльного аналізу.

Мета статті. Метою статті є теоретичне обґрунтування та розробка інтегральної моделі оцінки ефективності інформаційної безпеки військових систем передачі даних різних архітектурних типів (тактичних мобільних мереж, стаціонарних вузлів і хмарних платформ C4ISR) на основі формалізації критеріїв CIA (конфіденційність, цілісність, доступність) та індексу Security Effectiveness Index – (SEI), здійснення їх порівняльного аналізу за критеріями

гнучкості, живучості й масштабованості, а також побудова адаптивної архітектурної моделі взаємодії зазначених систем і матриці інтерпретації значень SEI для підтримки управлінських рішень у сфері кіберзахисту.

Виклад основного матеріалу. В Збройних силах України прикладом тактичної мережі нового покоління є система Кропива – бойова система управління тактичної ланки, що працює на планшетах і смартфонах. Функціонал включає електронні карти з GPS, обмін повідомленнями між підрозділами, розрахунок артилерійських даних, інтеграцію з безпілотниками та радаром. Аналогічного класу системи: GIS Arta – геоінформаційна система для артилерії, що забезпечує надшвидку передачу цілевказань на артпідрозділи (до 1 хвилини) і дозволяє використовувати звичайні смартфони як пристрої наведення. Також до цього класу можна віднести ситуаційно-інформаційну систему Delta, коли вона використовується безпосередньо тактичними ланками на полі бою на рівні окремих підрозділів, які отримують дані про противника через портативні термінали. (Варто зазначити, що Delta за своєю архітектурою ближча до хмарних платформ, але польові термінали, що працюють з Delta, фактично виступають елементами тактичної мережі.) Сучасні армії світу також мають подібні системи: наприклад, переносні комплекси Blue Force Tracker (BFT), що на рівні взвод – рота передають координати своїх сил через супутник для побудови цифрової картини поля бою. Усі ці системи створені для підвищення ситуаційної обізнаності і швидкості реагування на рівні тактичних підрозділів [7; 12].

Стаціонарні вузли – це фіксовані (стаціонарні) компоненти мереж зв'язку та управління, розгорнуті у постійних або довготривалих місцях дислокації. До них належать командні центри, штаби, стаціонарні вузли зв'язку, серверні центри і вузли обробки даних, які не переміщуються разом з військами. Такі системи зазвичай формують ядро військової інформаційної інфраструктури в тилу або на оперативному рівні. Вони характеризуються високою продуктивністю, більш надійними каналами зв'язку (порівняно з польовими) та централізованим управлінням ресурсами мережі [5].

Стаціонарні системи зв'язку хоча й працюють у більш комфортних умовах (ніж польові), але теж піддаються випробуванням:

Обмежений зв'язок: якщо військова інфраструктурна мережа зазнає пошкоджень – наприклад, фізичне переривання кабелю через диверсію чи обстріл, або вихід з ладу вузла, – то комунікація може частково втрачатися. На цей випадок передбачені резервні маршрути і канали.

Пікове навантаження: стаціонарна інфраструктура, як правило, має запас потужності, але надзвичайні ситуації (масований кібервплив, раптова необхідність обробити великий обсяг даних розвідки тощо) можуть викликати сплески трафіку. Система балансування навантаження перенаправляє запити на менш завантажені сервери, задіює резервні обчислювальні потужності. Наприклад, при піку запитів до баз даних система може тимчасово відмовитися від неважливих запитів або затримати непершочергові задачі, щоб не допустити краху сервера. На відміну від тактичних мереж, пікове навантаження тут більше стосується пропускної здатності центрів обробки та мережевого обладнання.

Кібератаки: стаціонарна мережа – приваблива ціль для кібернетичних атак, адже вона містить стратегічні дані і часто має вихід до глобальних мереж. DDoS-атаки (розподілені атаки на відмову в обслуговуванні) можуть здійснюватися на вузли, що мають підключення до Інтернету або суміжних мереж: масований трафік може перевантажити сервери чи канали. Для протидії використовуються міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгнень, а також хмарні служби очистки трафіку (якщо допустимо). Jamming (радіопридушення) безпосередньо менше стосується стаціонарних вузлів, бо їхні канали здебільшого дротові; однак, якщо є радіолінії чи супутникові сегменти, противник може спробувати їх глушити – тому критичні канали дублюються кабельними. Spoofing в стаціонарних системах може проявлятися як підробка даних або проникнення в мережу

шляхом видавання себе за довірений вузол. Високий рівень аутентифікації (сертифікати, апаратні маркери) покликаний цьому запобігти [6].

До цього типу можна віднести класичні автоматизовані системи управління військами, розгорнуті в стаціонарних пунктах. Історично в Україні існували проекти на кшталт Єдиної автоматизованої системи управління ЗСУ, що мали на меті створити опорну стаціонарну мережу для обміну даними між штабами. У країнах НАТО прикладами можуть бути стаціонарні компоненти систем типу AFATDS (Advanced Field Artillery Tactical Data System) – американська система управління вогнем артилерії: вона встановлюється на командних пунктах і пов'язує між собою штаби артилерійських підрозділів через захищені мережі. AFATDS поєднує ознаки тактичної і стаціонарної системи: програмно вона децентралізована (кожна батарея чи взвод можуть діяти самостійно, обмінюючись повідомленнями), але розгортається на стаціонарних або напівмобільних командних пунктах, які з'єднані дротовими чи стабільними радіолініями.

Хмарні платформи типу Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) – це мережево-центричні системи управління та розвідки, що використовують технології хмарних обчислень для зберігання, обробки та поширення даних. Їхній архітектурний принцип полягає в централізованому (або розподілено-централізованому) агрегуванні великого обсягу інформації з різних джерел та наданні доступу до неї численним користувачам у реальному часі. Cloud-based C4ISR платформи, по суті, є розвитком стаціонарних систем, адаптованим до роботи у хмарному середовищі, що підвищує гнучкість, масштабованість і інтеграцію між видами збройних сил. Такі системи охоплюють всі рівні – від тактичного до стратегічного – і дозволяють об'єднати дані з наземних, повітряних, морських, космічних та кібернетичних доменів в єдину інформаційну мережу. Концепція Joint All-Domain Command and Control (JADC2), яку розвиває Міністерство оборони США, є прикладом саме такого підходу: поєднання сенсорів усіх родів військ у єдину мережу на базі штучного інтелекту для швидкого ухвалення рішень. Хмарна C4ISR система покликана забезпечувати управління навіть у найскладніших ситуаціях, але і вона має свої межі стійкості [3; 4]:

Обмежений зв'язок: якщо противнику вдається значно порушити комунікацію (наприклад, масштабним радіоелектронним придушенням супутникового зв'язку чи знищенням вузлів передачі), то окремі частини сил можуть опинитися без доступу до хмари. В такому разі система переходить до деградованого режиму: використання резервних каналів з меншою швидкістю, зниження якості переданих даних (напр., замість відео надсилати тільки координати цілей), збільшення інтервалів оновлення інформації. Ключове завдання – не втратити життєво важливі дані: хмара може вибірково передавати критичні повідомлення найстійкішими каналами (приміром, через короткі текстові пакети по УКХ-радіо, якщо інше недоступне). Якщо ж якесь угруповання повністю ізольоване, воно має діяти автономно, спираючись на заздалегідь отримані розвідувальні дані і локальні тактичні системи. Одночасно, хмарна система, як тільки з'явиться вікно зв'язку, затоплює ізольований сегмент усіма накопиченими даними (і приймає від нього дані) для якнайшвидшого синхронізування картини бою.

Пікове навантаження: хмарні платформи спроектовані масштабованими, але раптовий пік (скажімо, початок масштабної операції з тисячами потоків даних від всіх сенсорів) випробовує їхню еластичність. Завдяки хмарним технологіям система може автоматично масштабуватися: додавати нові віртуальні сервери, перерозподіляти бази даних на більшу кількість вузлів, тимчасово використати комерційні хмарні потужності (як резерв) тощо. Відомо, що українська система Delta після розширення фронту російського вторгнення була перенесена на закордонні хмарні майданчики для захисту і масштабування.

Такі рішення дозволяють витримати різке збільшення навантаження. Також застосовуються механізми пріоритезації: на піку навантаження менш важливі задачі

(наприклад, аналітичні запити або резервне копіювання) відкладаються, щоб не заважати бойовим запитам в реальному часі. Завдяки розподіленості різні компоненти системи можуть масштабуватися незалежно: якщо, скажімо, відеостріми з дронів генерують основний трафік, то збільшується число серверів відеообробки, тоді як інші частини залишаються незмінними.

Кожен розглянутий архітектурний тип має свої переваги і недоліки, що виявляються при порівнянні за критеріями гнучкості, живучості та масштабованості. Результати порівняльного аналізу представлено в таблиці 1.

Таблиця 1

Порівняльний аналіз архітектурних типів мереж

Критерій	Тактичні мобільні мережі (Кропува)	Стаціонарні мережі (GIS Arta)	Хмарні платформи (Delta)	Коментар / приклад
Гнучкість	Висока просторово: розгортання без інфраструктури; обмежена функціонально через ресурси	Низька просторово, висока функціонально; додавання серверів та сервісів	Найвища функціональна гнучкість; динамічне масштабування; залежність від каналів зв'язку	Кропува – автономна; Delta потребує Starlink; GIS Arta – гнучка сервісно
Живучість	Децентралізована; вузли працюють незалежно; вразливість до масового радіопридушення	Чутливість до точкових атак на центри; резервування частково вирішує	Висока живучість у дата-центрах; критична залежність від комунікацій	Кропува функціонує локально; Delta вразлива до втрати зв'язку
Живучість	Децентралізована; вузли працюють незалежно; вразливість до масового радіопридушення	Чутливість до точкових атак на центри; резервування частково вирішує	Висока живучість у дата-центрах; критична залежність від комунікацій	Кропува функціонує локально; Delta – вразлива до втрати зв'язку
Масштабованість	Обмежена: лише в межах роти/батальйону; потребує частотного планування	Може масштабуватись вертикально та горизонтально; обмеження в інфраструктурі	Найвища: автоматичне додавання ресурсів, охоплення нових зон	Delta – легко підключає нові підрозділи; GIS Arta потребує налаштувань

Джерело: розроблено автором на основі [7; 9; 12].

Отже, три основні архітектурні типи систем передачі даних доповнюють один одного, забезпечуючи зв'язок і управління на різних рівнях і в різних умовах. Тактичні мережі надають гнучкість і незалежність підрозділам на полі бою, дозволяючи їм обмінюватися інформацією безпосередньо і діяти автономно навіть при розривах зв'язку з вищими штабами. Стаціонарні системи забезпечують потужну основу – сполучну інфраструктуру й обчислювальні центри, що збирають і аналізують дані, підтримують безперервність управління та великий обсяг інформації. Хмарні платформи інтегрують всі рівні в єдине інформаційне середовище, даючи можливість максимально швидко використовувати дані з будь-яких джерел для ухвалення рішень у реальному часі. Кожен тип систем має свої переваги: тактичні переважають у польових умовах, стаціонарні характеризуються надійністю, хмарні мають переваги у масштабі та швидкості обробки даних. Але кожен має і вразливі місця, що проявляються за екстремальних ситуацій.

Таким чином, адаптивна модель побудови військової системи зв'язку і передачі даних повинна поєднувати ці класи та гнучко перемикатися між ними залежно від обстановки. Для тактичних мереж доцільно реалізувати адаптивні алгоритми маршрутизації та динамічне керування частотами, щоб протистояти перешкодам і мінімізувати затримки. Стаціонарні

вузли мають бути вбудовані в адаптивну інфраструктуру з автоматичним переключенням на резерви при збоях та можливістю масштабування під навантаження. Хмарні C4ISR-системи потребують адаптації до якості каналів, наприклад, зменшувати обсяг переданих даних або переходити в режим децентралізації (edge computing) при деградації зв'язку. Інтеграція трьох типів в єдину мережево-центричну екосистему з інтелектуальним керуванням дозволить використати сильні сторони кожного: забезпечити надійний зв'язок і управління військами навіть у умовах, коли один з елементів (мобільний, стаціонарний чи хмарний) тимчасово обмежений або зазнає атаки. Отже, адаптивна модель архітектури є найбільш доцільною для підвищення живучості, гнучкості та ефективності сучасних військових систем передачі даних, оскільки враховує особливості кожного класу і мінімізує їхні недоліки завдяки взаємному дублюванню та підтримці [4; 16].

У сучасних системах передавання даних інформаційна безпека ґрунтується на тріаді СІА: конфіденційності, цілісності та доступності. Кожен із цих критеріїв є необхідним для оцінки захищеності системи і служить окремим показником ефективності заходів безпеки. У цьому підпункті здійснено наукове обґрунтування кожного з критеріїв СІА в контексті систем передачі даних, надано їхні формальні визначення через відповідні математичні вирази, а також запропоновано інтегральний індекс ефективності безпеки, що поєднує три критерії з урахуванням вагових коефіцієнтів.

Конфіденційність визначає властивість системи забезпечувати доступ до інформації лише уповноваженим суб'єктам і запобігати розголошенню даних стороннім особам. З позиції інформаційної безпеки мережі передачі даних, конфіденційність означає, що передані повідомлення не можуть бути прочитані або перехоплені зловмисниками. На практиці досягнення конфіденційності забезпечується, зокрема, криптографічними методами (шифруванням трафіку) та керуванням доступом. Для кількісної оцінки цього критерію вводиться метрика, яка відображає частку передач, здійснених без порушення конфіденційності. Формально коефіцієнт конфіденційності можна визначити як відношення числа успішно захищених передач до загального числа передач. Зручним є доповнення цього відношення до 1, що дає міру втрати конфіденційності при наявності витоків. Таким чином, запропонована метрика конфіденційності може бути виміряна за формулою (1):

$$C = 1 - \frac{L}{N}, \quad (1)$$

де L – кількість зафіксованих витоків (несанкціонованих розголошень інформації);
 N – загальна кількість передач даних у системі.

Значення $C = 1$ відповідає повному збереженню конфіденційності (відсутності витоків), тоді як значення, наприклад, $C = 0,9$ (або 90 %), означає, що 10 % передач призвели до компрометації даних. Чим ближче значення C до 1, тим вищий рівень конфіденційності забезпечує система передачі даних.

Цілісність – це властивість інформації залишатися повною, достовірною і незмінною при зберіганні та особливо при передачі. З точки зору захисту мережевих даних, цілісність означає, що пакетні дані доходять від відправника до отримувача без спотворень, модифікацій чи знищення неавторизованими діями. Порушення цілісності можуть відбутися через навмисну підміну або спотворення даних (атаки типу man-in-the-middle, внесення шкідливих змін), а також через випадкові помилки чи збої, що призводять до пошкодження пакетів. Для оцінки цього критерію вводять формальну метрику як частку даних, що зберегли цілісність під час передачі. Показник цілісності можна подати формулою (2):

$$I = 1 - \frac{D}{P}, \quad (2)$$

де P – загальна кількість переданих пакетів (або інших блоків даних) у мережі;

D – кількість деформованих (ушкоджених або невалідних) пакетів, виявлених на приймальній стороні.

За такого визначення $I = 1$ у випадку, коли всі пакети отримано без спотворень (жодного пошкодженого пакета), що відповідає ідеальній цілісності переданих даних. Зменшення значення показника I сигналізує про втрату або зміну частини інформації. Наприклад, $I = 0,98$ означає, що 2 % пакетів були втрачені чи змінені під час транспортування. Метрика цілісності дозволяє кількісно виміряти ефективність механізмів забезпечення цілісності (таких як контрольні суми, коди перевірки цілісності, протоколи виявлення збоїв) у системі передачі даних.

Доступність характеризує здатність системи забезпечувати своєчасний і безперервний доступ користувачів до інформації та сервісів. З погляду мережі передачі даних, доступність означає, що мережевий сервіс або канал зв'язку функціонує без тривалих простоїв, і авторизовані користувачі можуть отримати доступ до даних у потрібний момент. Порушення доступності найчастіше пов'язане з відмовами обладнання, збоями програмного забезпечення або зловмисними діями типу Denial of Service (DoS), що призводять до простою мережі. Для вимірювання цього критерію використовують метрику безперервності сервісу – відносний час, протягом якого система є працездатною. Коефіцієнт доступності обчислюється за формулою (3):

$$A = \frac{T_{up}}{T_{total}}, \quad (3)$$

де T_{up} – сумарний час безвідмовної роботи системи (uptime) за певний інтервал спостереження;

T_{total} – загальний час роботи системи (включно з плановим часом функціонування, часовими інтервалами простою тощо).

Значення $A = 1$ відповідає 100 % доступності, коли система не мала простоїв у заданому інтервалі часу. Якщо ж, наприклад, протягом доби мережа була недоступна сумарно 1 годину (тобто $T_{up} = 23$ год, $T_{total} = 24$ год), показник доступності становитиме $A \approx 0,9583$ (95,83 %). Високе значення метрики A свідчить про надійну, безперебійну роботу системи, тоді як низьке значення сигналізує про часті або тривалі простої, що можуть бути критичними для користувачів систем передачі даних.

Після визначення окремих базових показників C , I та A постає задача інтегральної оцінки сукупної ефективності захисту. Зважаючи на те, що конфіденційність, цілісність і доступність є різними за значенням для різних систем, доцільно об'єднати їх в один узагальнений показник із урахуванням пріоритетності кожного критерію. У межах цього дослідження пропонується індекс ефективності безпеки, що об'єднує критерії CIA шляхом зваженого підсумовування. Формально SEI визначається як лінійна комбінація метрик C , I , A з відповідними ваговими коефіцієнтами (4):

$$SEI = w_C C + w_I I + w_A A, \quad (4)$$

де w_C , w_I , w_A – вагові коефіцієнти, що відображають відносну важливість (пріоритетність) кожної складової безпеки для цієї системи, при цьому $w_C + w_I + w_A = 1$.

Коефіцієнти w_j (де $j \in \{C, I, A\}$) можуть приймати значення від 0 до 1 і призначаються експертним шляхом або на основі вимог до системи. Чим більше значення w_j , тим більшого значення надається відповідному критерію при оцінці загальної ефективності. Таким чином,

індекс SEI агрегує триєдиний показник безпеки: значення SEI, близьке до 1, вказує на високий рівень загальної захищеності (за прийнятої конфігурації ваг), тоді як менші значення сигналізують про наявність слабких місць у конфіденційності, цілісності або доступності (залежно від того, який компонент має недостатній рівень або малу вагу).

Вагові коефіцієнти в моделі SEI слід обирати з урахуванням специфіки та призначення конкретної системи, оскільки різні типи систем висувають різні пріоритети щодо CIA. Іншими словами, тип системи безпосередньо впливає на розподіл ваг w_C , w_I , w_A . Тактичні системи (наприклад, військові або екстрені системи зв'язку, що працюють в реальному часі) зазвичай найбільше залежать від безперервної роботи, тому критерій доступності для них є пріоритетним. Для таких систем навіть короточасна відмова зв'язку може мати неприпустимі наслідки, тому ваговий коефіцієнт w_A обирається найбільшим. Конфіденційність і цілісність у тактичних мережах теж важливі, проте можуть мати дещо менші ваги, оскільки в критичних умовах безперервність сервісу (зв'язку) часто важливіша за повну таємницю передач. Хмарні системи (наприклад, сервіси хмарного зберігання або обробки даних) натомість приділяють першочергову увагу захисту даних від несанкціонованого доступу та помилок. У хмарних платформах витік конфіденційної інформації або порушення цілісності даних може призвести до значних збитків та підриву довіри користувачів, тоді як короточасна недоступність сервісу (наприклад, для планового обслуговування) є відносно менш критичною. Відповідно, для хмарної системи вагові коефіцієнти w_C та w_I встановлюються вищими, ніж w_A [3; 11].

Наведемо приклади конфігурації ваг для зазначених типів систем. Для тактичної мережі зв'язку можна обрати такі вагові коефіцієнти: $w_C = 0,2$, $w_I = 0,3$, $w_A = 0,5$. У цьому випадку найбільша вага (50 %) надається доступності, що відображає критичну важливість безперервного зв'язку, тоді як конфіденційність отримує 20 %, а цілісність – 30 % від загального індексу. Для хмарного середовища доцільно збільшити внесок критеріїв конфіденційності та цілісності. Наприклад, для хмарного сховища даних можна задати $w_C = 0,4$, $w_I = 0,4$, $w_A = 0,2$, тобто 40 % ваги припадає на кожен із показників конфіденційності та цілісності, а доступність оцінюється у 20 %. Така конфігурація відображає пріоритетність запобігання витокам даних і гарантування коректності інформації для користувачів хмарного сервісу, при тому що показник доступності залишається важливим, але не домінуючим. Зрозуміло, що наведені ваги є умовними прикладами – у реальних проєктах їхні значення встановлюються на основі вимог замовника, нормативних рекомендацій та експертної оцінки ризиків. У цілому, тактичні (час-критичні) системи мають схильність до конфігурацій, де w_A максимальний, тоді як інформаційно-орієнтовані (центри обробки даних, хмарні сервіси) – до конфігурацій з вищими w_C та w_I .

Таким чином, формалізовано три базові критерії ефективності інформаційної безпеки – конфіденційність, цілісність і доступність – шляхом відповідних метричних виразів, а також побудовано інтегральний індекс SEI як зважену суму складових CIA. Запропонований підхід дозволяє кількісно оцінити загальний рівень захищеності системи передачі даних з урахуванням її особливостей та пріоритетів. Отримані формалізації закладають основу для подальшої побудови моделі SEI. У наступному підпункті буде детально розглянуто розробку самої SEI-моделі та практичне застосування індексу ефективності безпеки.

Доцільно провести математичну формалізацію базових критеріїв Confidentiality, Integrity, Availability (CIA), що використовуються в моделі оцінки ефективності систем передачі даних.

1. Формалізація CIA як критеріїв.

Визначено три функції для кожного з критеріїв системи передачі даних – (x):

$C(x)$ – рівень конфіденційності;

$I(x)$ – рівень цілісності;

$A(x)$ – рівень доступності.

Визначено метрики для обчислення кожного з показників:

$$C = 1 - (N_{data\ leak} / N_{total\ tx});$$

$$I = 1 - (N_{corrupted\ packets} / N_{total\ packets});$$

$$A = T_{uptime} / T_{total}.$$

Вагова модель оцінки ефективності за CIA. Інтегральний індекс ефективності безпеки SEI розраховується за формулою (5):

$$SEI = w_C C(x) + w_I I(x) + w_A A(x), \quad (5)$$

де $w_C + w_I + w_A = 1$, а ваги залежать від типу системи (тактична, хмарна, стаціонарна).

Приклад вагового розподілу від автора.

Для тактичних систем: $w_C = 0,25$, $w_I = 0,25$, $w_A = 0,50$.

Для хмарних систем: $w_C = 0,4$, $w_I = 0,4$, $w_A = 0,2$.

Для стаціонарних систем: $w_C = 0,3$, $w_I = 0,5$, $w_A = 0,2$.

Таким чином, формалізована модель SEI дозволяє враховувати особливості кожного типу системи через змінні ваги. Представимо модель у вигляді схеми (рис. 1).

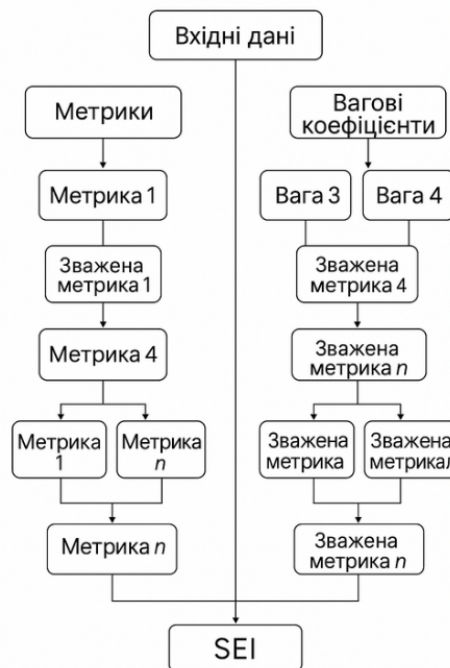


Рис. 1. Схематична візуалізація моделі SEI
(джерело: розроблено автором)

За допомогою запропонованих вище формул та послідовності проведення оцінки проведемо розрахунки індексу ефективності безпеки системи SEI. Вхідні дані для проведення розрахунків представлені наступним чином:

$$SEI = 0,25 \times 0,85 + 0,30 \times 0,92 + 0,20 \times 0,88 + 0,15 \times 0,75 + 0,10 \times 0,70;$$

$$SEI = 0,2125 + 0,276 + 0,176 + 0,1125 + 0,070 = 0,847;$$

$$SEI = 0,847 \text{ (або } 84,7 \%).$$

У таблиці 2 подано інформацію з вихідними значеннями технічних метрик, результатами нормалізації, а також проміжними формулами та ваговими коефіцієнтами, що

використовуються для розрахунку індексу SEI для 5 об'єктів: Delta, Kropyva, GIS Arta, BFT, JADC2.

Таблиця 2

Розрахунок індексу SEI для 5 об'єктів: Delta, Kropyva, GIS Arta, BFT, JADC2*

Нормалізоване виявлення Norm. Detection	Затримка (мс) Latency (ms)	Нормалізована затримка Norm Latency	Доступність (хв) Availability (h)	Нормалізована доступність Norm Avail	Втрата пакетів (%) Packet Loss (%)	Нормалізована цілісність Norm. Integrity	Витоки даних / Кількість переданих повідомлень Data Leaks / Tx	Нормалізована конфіденційність Norm. Confid	Час виявлення (хв) Detection Time (h)
Delta	110	0,500	1 390	0,727	2,5	0,565	3 / 15 000	0,533	2,5
Kropyva	130	0,000	1 350	0,000	3,8	0,000	4 / 12 000	0,081	3,2
GIS Arta	90	1,000	1 405	1,000	1,9	0,826	2 / 18 000	0,835	2,1
BFT	125	0,125	1 365	0,273	2,0	0,783	5 / 14 000	0,000	4,0
JADC2	100	0,750	1 380	0,545	1,5	1,000	1 / 16 000	1,000	1,7

Джерело: розраховано автором на основі [8; 11].

Значення нормалізовані за принципом benefit/cost-критеріїв:

Для latency, packet loss, data leak rate та detection time застосовано інверсну нормалізацію (менше – краще).

Для availability – звичайна нормалізація (більше – краще).

Джерело: розраховано автором.

Матриця нижче (табл. 3) є шаблоном для якісного тлумачення кількісного інтегрального індексу ефективності безпеки SEI, отриманого в результаті багатокритеріального аналізу.

Таблиця 3

Матриця інтерпретації кількісного інтегрального індексу ефективності безпеки SEI, отриманого в результаті багатокритеріального аналізу

Діапазон значення SEI	Рівень ефективності безпеки	Інтерпретація	Рекомендації
0,90–1,00	Високий (Оптимальний)	Система демонструє високі значення всіх ключових метрик. Захист є збалансованим і стійким.	Підтримувати чинні політики. Можливе впровадження інновацій (AI-based monitoring, adaptive controls)
0,75–0,89	Добрий (Контрольований)	Система працює стабільно, проте є локальні вразливості. Основні критерії задовільні	Поглиблений аудит окремих показників. Рекомендовані точкові покращення
0,60–0,74	Середній (Помірний ризик)	Частина ключових показників у межах допустимого, але спостерігається деградація окремих метрик	Необхідно підсилити конкретні зони безпеки. Розробити план покращення та контроль динаміки
0,40–0,59	Низький (Небезпечний)	Система має критичні недоліки. Конфіденційність або доступність перебувають на межі прийняттого	Негайний аналіз архітектури. Провести оновлення засобів захисту. Вжити організаційні заходи
< 0,40	Критичний (Неприйнятний)	Інформаційна система практично не захищена. Є суттєві порушення цілісності, відмови зв'язку тощо	Ризик неприйнятний. Необхідне повне переосмислення архітектури системи та стратегії захисту

Джерело: розроблено автором.

З метою забезпечення об'єктивного аналізу отриманих результатів комплексної оцінки ефективності систем передачі даних, побудованої на основі інтегрального індексу SEI, доцільним є використання формалізованого інструменту – матриці інтерпретації значень SEI. Така матриця виконує роль методологічного містка між кількісною метрикою та її якісним тлумаченням, трансформуючи обчислені значення SEI у контекстні висновки щодо рівня інформаційної безпеки об'єкта дослідження [16].

Відповідно до засад метрологічного підходу в інформаційній безпеці, кожне значення інтегрального показника має бути приведене до інтервальної шкали, на якій встановлюється порогова градація – від критичного до оптимального рівня. Запропонована інтерпретаційна матриця базується на п'яти рівнях ефективності: критичний ($< 0,40$), низький ($0,40-0,59$), середній ($0,60-0,74$), добрий ($0,75-0,89$), високий ($0,90-1,00$). Таке розбиття є не лише формально обґрунтованим з позицій імовірнісного аналізу ризиків, а й адаптивним до сучасних міжнародних практик (наприклад, NIST SP 800-53, ISO/IEC 27004), де рекомендовано класифікувати результати оцінки інформаційної безпеки за багаторівневими критеріями.

Кожному інтервалу відповідає якісна характеристика поточного стану системи, яка враховує не лише значення SEI, а й контекст системної архітектури, функціонального навантаження та вразливості до зовнішніх впливів. Таким чином, матриця поєднує кількісну об'єктивність і аналітичну змістовність, що є критично важливим для формування подальших управлінських рішень, таких як розробка політик безпеки, розподіл ресурсів, оновлення архітектурних компонентів тощо.

Крім того, матриця містить рекомендаційний блок, який слугує аналітичним орієнтиром для формування рішень щодо усунення виявлених проблем. Наприклад, для систем із рівнем $SEI < 0,40$ рекомендовано проведення повного аудиту архітектури та перегляд політик захисту, тоді як системи з $SEI > 0,90$ можуть перейти до адаптивного моделювання та впровадження інноваційних технологій на кшталт автоматизованих платформ реагування на інциденти (SOAR), поведінкового аналізу загроз (UEBA) або засобів на базі штучного інтелекту [14; 15].

Висновки. Таким чином, матриця інтерпретації значень SEI виступає не лише інструментом аналітичного контролю, але й елементом концептуальної моделі оцінки стану інформаційної безпеки, забезпечуючи відтворюваність, інтерсуб'єктивність та орієнтованість на практичне впровадження.

Отже, запропонована в межах дослідження матриця інтерпретації значень SEI виступає методологічним інструментом, що забезпечує семантичне осмислення результатів багатокритеріальної оцінки ефективності захисту систем передачі даних. Її розробка дозволяє поєднати кількісно формалізовані значення інтегрального показника безпеки з якісними характеристиками стану інформаційної системи, що забезпечує прозорість і відтворюваність прийняття управлінських рішень у сфері кіберзахисту.

Матриця побудована з урахуванням принципів шкалювання критеріальних оцінок, методів ризик-орієнтованого менеджменту та практик стандартизованого моніторингу ефективності (зокрема NIST, ISO/IEC 27004). Такий підхід дозволяє не лише здійснювати класифікацію поточного рівня захисту, а й формувати рекомендації адаптаційного характеру залежно від контексту архітектури, типу загроз і пріоритетів застосування системи.

Інтерпретаційна матриця SEI є ключовим елементом валідації результатів розробленої моделі та її подальшого практичного впровадження у процедурах аудиту, управління ризиками та розробки архітектур захищених систем зв'язку. Її впровадження забезпечує базис для автоматизованого аналізу, побудови інформаційних дашбордів та динамічного моніторингу живучості системи в умовах змінного кіберсередовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Андрушко М. В., Аркушенко П. Л., Кузнецов В. О., Андрушко А. М. Обґрунтування узагальненої моделі функціонування перспективної інформаційно-виміральної системи збору та обробки інформації // Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2023. Вип. 3 (17). С. 7–14. DOI: <https://doi.org/10.37701/dndivsovt.17.2023.01>.
2. Pomortseva O. E., Kobzan S. M. Geospatial modeling of the location of bomb shelters in residential areas of the city. IOP Conference Series: Earth and Environmental Science. 2023. Т. 1254. №. 1. URL: DOI: 10.1088/1755-1315/1254/1/012136
3. Brandi V. AI will “revolutionize” the way NATO looks at geospatial intelligence. 2024. URL: <https://defensescoop.com/2024/05/07/nato-geoai-revolutionize-geoint-scott-bray/>.
4. Navigating the Future: Key Findings from Allied Command Transformation’s 2023 Strategic Foresight Analysis, 2024. URL: www.act.nato.int.
5. Автоматизована система управління військами – зброя перемоги // Військовий кур’єр. URL: https://mil.co.ua/avtomatyzovana-systema-upravlinnya-vijskamy-zbroya-peremogy/?utm_source=chatgpt.com.
6. Купер Т. Будь-який радар, який вмикається нині на території України, стає видимим для цілої системи ворожих засобів радіотехнічної та сигнальної розвідки. URL: <https://tyzhden.ua/tom-kuper-bud-iakyj-radar-iakyj-vmykaietsia-nyni-na-terytorii-ukrainy-staie-vydymym-dlia-tsiloi-systemy-vorozhykh-zasobiv-radiotekhnichnoi-ta-syhnalnoi-rozvidky/>.
7. Коломієць В. Українську систему ситуаційної обізнаності презентували на щорічному заході НАТО. Про що йдеться? 2022. URL: <https://hromadske.ua/posts/ukrayinsku-sistemu-situacijnoyi-obiznanosti-prezentuvali-na-shorichnomu-zahodi-nato-pro-sho-jdetsya> (дата звернення: 01.06.2024).
8. Данилов О. Унікальну українську систему ситуаційної обізнаності Delta презентували на щорічному заході НАТО. 2022. URL: <https://mezha.media/2022/10/28/delta-for-nato/> (дата звернення: 01.06.2024).
9. Найєм М. Істерика російських пропагандистів, або Чому орки бояться Дельти. 2022. URL: <https://www.pravda.com.ua/columns/2022/11/2/7374610/>.
10. Морфінов С. Delta для ЗСУ: Що відомо про новітню систему управління української армії. 2023. URL: <https://www.bbc.com/ukrainian/features-64585182>.
11. Аеророзвідка. Система ситуаційної обізнаності «Дельта». URL: <https://dou.ua/lenta/projects/ukrainian-miltech-guide/>.
12. Асоціація виробників озброєння та військової техніки України. ГІС “Арта”, 2018. URL: <https://audm.org.ua/pidpriyemstva/gis-arta/>.
13. ГІС Арта. Автоматизована система управління військами. URL: <https://dou.ua/lenta/projects/ukrainian-miltech-guide/>.
14. Griselda. Програмний ІІІ-комплекс. URL: <https://dou.ua/lenta/projects/ukrainian-miltech-guide/>.
15. Mantis Analytics. Платформа моніторингу інформації на основі ІІІ. URL: <https://dou.ua/lenta/projects/ukrainian-miltech-guide/>.
16. Кобзан С., Поморцева О., Паньків В., Андронов В. Погляди щодо побудови геоінформаційної системи для використання у Збройних Силах України // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2024. Том 2. № 3 (83). С. 40–46. DOI: <https://doi.org/10.33099/2304-2745/2024-3-83/40-46>.

Надійшла до редколегії 21.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.056:519.876

Паламарчук С. А. ORCID: 0000-0001-7483-9165 (ВІТІ ім. Героїв Крут)
Паламарчук Н. А. ORCID: 0000-0001-8818-7794 (ВІТІ ім. Героїв Крут)
Вороной О. В. ORCID: 0009-0007-1427-4431 (ВІТІ ім. Героїв Крут)
Побережець Т. В. ORCID: 0000-0001-8007-8614 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ВИЗНАЧЕННЯ СТІЙКОСТІ КОРИСТУВАЧІВ ДО АТАК СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА ОСНОВІ ТЕОРІЙ НАВЧАННЯ ТА ДЕГРАДАЦІЇ ЗНАНЬ

У сучасних умовах зростання кількості кібератак, зокрема соціальної інженерії, людський фактор залишається одним із ключових елементів кібербезпеки організацій. Здатність протидіяти таким атакам значною мірою залежить від рівня навченості та обізнаності користувачів (стійкості), що формується в процесі навчання. Актуальність дослідження обґрунтовано з урахуванням посилення ролі людського фактора та поширення соціально-інженерних атак як на основі міжнародних стандартів і рекомендацій, так і на основі статистичних даних. Незважаючи на значну кількість досліджень, існуючі підходи (моделі), як правило, не враховують у явному вигляді рівень навченості та обізнаності користувача (його стійкості) як змінну, що безпосередньо впливає на здатність протидіяти атакам соціальної інженерії. У статті розглянуто питання кількісного оцінювання впливу навчання користувачів на рівень їхньої стійкості до атак соціальної інженерії, зокрема фішингу. Запропоновано модель визначення стійкості користувача під впливом навчання та деградації знань внаслідок забування або появи нових механізмів атак, обґрунтовано параметри моделювання на основі статистичних та емпіричних даних. Окрім цього, визначається залишковий ризик, пов'язаний із людським фактором для системи. Результати моделювання підтверджують адекватність запропонованої моделі реальним процесам навчання та втрати знань користувачем, зокрема через наявність ефекту насичення та деградації знань. Отримані результати можуть бути використані для визначення пріоритетних груп ризику, оптимізації періодичності навчання, а також врахування залишкового ризику, пов'язаного з людським фактором у моделях (методиках) оцінювання ризиків системи.

Ключові слова: кібербезпека, людський фактор, навчання користувачів, деградація знань, соціальна інженерія, стійкість користувача, оцінювання ризиків, фішинг.

S. Palamarchuk, N. Palamarchuk, O. Voronoi, T. Poberezhets. Model for determining user resistance to social engineering attacks based on the theories of learning and knowledge degradation

In today's conditions of increasing cyberattacks, in particular social engineering, the human factor remains one of the key elements of cybersecurity of organizations. The ability to counter such attacks largely depends on the level of user training and awareness (resilience) that is formed in the training process. The relevance of the study is justified taking into account the increasing role of the human factor and the spread of social engineering attacks, both on the basis of international standards and recommendations and on the basis of statistical data. Despite a significant number of studies, existing approaches (models), as a rule, do not explicitly take into account the level of user training and awareness (his resilience) as a variable that directly affects the ability to counter social engineering attacks. The article considers the issue of quantitative assessment of the impact of user training on the level of their resistance to social engineering attacks, in particular, phishing. A model for determining user resilience under the influence of learning and knowledge degradation due to forgetting or the emergence of new attack mechanisms is proposed, and modeling parameters are justified based on statistical and empirical data. In addition, the residual risk associated with the human factor for the system is determined. The modeling results confirm the adequacy of the proposed model to real processes of learning and knowledge loss by the user, in particular, due to the presence of the saturation effect and knowledge degradation. The results obtained can be used to determine priority risk groups, optimize the frequency of training, and take into account the residual risk associated with the human factor in models (methods) for assessing system risks.

Keywords: cybersecurity, human factors, user training, knowledge degradation, social engineering, user resilience, risk assessment, phishing.

Актуальність та постановка завдання. У сучасних умовах розвитку цифрових технологій та ведення гібридних війн соціальна інженерія перетворилася на один із найбільш ефективних інструментів реалізації кіберзагроз, зокрема й у сфері оборони. Незважаючи на створення авторизованих систем із безпеки та активне впровадження технічних засобів кіберзахисту, систем виявлення і реагування на кіберінциденти (їх інтелектуалізації, здатності до навчань), вплив на людський фактор залишається найбільш вразливою ланкою будь-якої

системи (сервісу). Зловмисники цілеспрямовано експлуатують психологічні особливості людини/користувача, фактор терміновості, страх та “критичність моментної загрози” (*homo intuitus, emotus et fallibilis* – інтуїтивна, емоційна та схильна до помилок людина), що суттєво підвищує результативність методів соціальної інженерії, зокрема фішингу. Вразливість користувача та його стійкість (здатність протидіяти соціальним атакам) є динамічними характеристиками, що визначаються сукупністю когнітивних і поведінкових факторів, а також рівнем його обізнаності та підготовки. Згідно з підходами, визначеними в *NIST SP 800-30* [1], вразливість розглядається як слабкість, яка може бути використана джерелом загрози, причому в контексті кібербезпеки такі слабкості все частіше пов'язані саме з людським фактором. Відповідно, недостатня сформованість навичок безпечної поведінки та відсутність періодичного оновлення знань призводять до зростання ймовірності реалізації атак соціальної інженерії, що обумовлює необхідність розроблення моделі визначення стійкості користувачів до атак соціальної інженерії.

За даними *Microsoft* за 2025 рік та *Institute of Information Security* (далі – *InfoSec*) визначено, що соціальна інженерія, зокрема фішинг, займає провідне місце серед сучасних видів загроз, причому розвиток штучного інтелекту та використання його із зловмисними намірами суттєво розширює можливості атак, фішингові кампанії на основі штучного інтелекту мають на 42 % вищий рівень успіху, ніж звичайні [2]. Згідно зі статистикою Національної команди реагування на кіберінциденти *CERT-UA* [3–6], у 2025 році опрацьовано 5 927 кіберінцидентів, що на 37,4 % більше порівняно з попереднім роком. Серед найпоширеніших типів атак – фішинг, 1 727 випадків (це майже вдвічі більше ніж у 2024 році, і складає ~30 % від усіх опрацьованих кіберінцидентів), розповсюдження та зараження шкідливим програмним забезпеченням та компрометація облікових записів. Значна частка інцидентів припадає на сектор безпеки й оборони, органи державної влади та критичну інфраструктуру, що свідчить про цілеспрямований характер та системність атак.

При цьому, дослідження, що проведені в Україні у 2021 та 2023 роках за підтримки *CRDF Global* [7; 8] показують, що серед значної частини користувачів (понад 41 %), які вже зіткнулися з кіберінцидентами, важливим поведінковим фактором ризику є переконання у власній “нецікавості” для зловмисників, таку позицію поділяє понад половина опитаних. Тому, результати досліджень демонструють наявність розриву між рівнем обізнаності користувачів у сфері кібербезпеки та їхньою реальною поведінкою, зокрема значна частина користувачів ігнорує базові практики кібергігієни. У більшості досліджень і звітів з кібербезпеки зазначається, що значна частина інцидентів починається саме з фішингу або маніпуляції користувачем, що актуалізує необхідність аналізу, розроблення та впровадження моделей визначення стійкості користувачів до атак соціальної інженерії.

Аналіз останніх досліджень і публікацій. Незважаючи на значну кількість досліджень, існуючі підходи, як правило, не враховують у явному вигляді рівень навченості та обізнаності користувача (його стійкість) як змінну, що безпосередньо впливає на здатність протидіяти атакам соціальної інженерії. Оцінювання впливу навчання користувачів на їхню здатність протидіяти атакам соціальної інженерії здійснюється з використанням різних підходів, зокрема нормативних, поведінкових і статистичних. Міжнародні публікації, такі як рекомендації *NIST* та *SANS Institute* [9; 10], визначають необхідність періодичного навчання та підвищення обізнаності користувачів. У цих підходах ефект забування враховується опосередковано через вимогу періодичності навчання (4–6 місяців), однак відсутня його формалізація у вигляді математичних залежностей, що обмежує можливість кількісного оцінювання з метою оптимізації навчання.

В [11] розглянуто узагальнену модель поведінки користувача, яка базується на концепції співіснування кількох критеріїв прийняття рішень при отриманні фішингового повідомлення. Автори виділяють такі поведінкові стани користувача (стани “розуму”), як рутинний, імпульсивний, поведінковий та раціональний (обдуманий), які визначають вибір дій

користувача. У таких моделях увага приділяється процесу прийняття рішень, проте процеси навчання та забування не мають явного математичного опису.

В [12] розроблено методику прогнозування фішингових атак на основі статистичних методів. Для аналізу трендів застосовано часові ряди, сформовані на основі відкритих статистичних даних, що дозволило побудувати модель динаміки кількості фішингових атак за визначений період та сформулювати прогноз їх розвитку на майбутнє. Отримані результати підтверджують ефективність статистичних підходів для оцінювання тенденцій розвитку загроз.

В [13] досліджено вплив безперервного навчання на довгострокову стійкість користувача. Показники успішності фішингу (із врахуванням контекстної інформації та емоційних тригерів) знизилися майже вдвічі протягом перших шести місяців і стабілізувалися близько до галузевих показників, що підкреслює довгострокову ефективність ініціатив щодо сталого підвищення обізнаності (протягом 12 місяців).

Водночас аналіз існуючих досліджень показав, що в підходах до оцінювання ризиків соціальної інженерії рівень стійкості користувача переважно не враховується як формалізований показник, а процеси навчання та деградації знань не мають узагальненого математичного опису. Це обумовлює необхідність розроблення моделі визначення стійкості користувачів до атак соціальної інженерії на основі теорій навчання та деградації знань.

Мета статті. Розробка моделі визначення стійкості користувачів до атак соціальної інженерії на основі теорій навчання та деградації знань.

Виклад основного матеріалу дослідження. Вразливість (*vulnerability*) – це слабкість активу (системи, сервісу, програмного забезпечення тощо) або контролю, яка може бути використана однією або кількома загрозами [1; 14]. Після виявлення вразливості удосконалюються (модернізуються) як самі технологічні середовища (системи, сервіси, програмне забезпечення тощо), так і засоби виявлення та реагування (зокрема системи виявлення вторгнень (*IDS/IPS*), управління подіями безпеки (*SIEM*), захисту кінцевих точок (*EDR/XDR*), засоби автентифікації та контролю доступу, а також спеціалізовані рішення протидії фішингу тощо). Водночас при соціально-інженерних атаках об'єктом впливу є людина – користувач сервісу (системи або пристрою). У концептуальних документах і стандартах термін “вразливість користувача” (дослівно “вразливість людського фактору”, *human factor vulnerability*) прямо не формалізований, однак його зміст визначається контекстно через загальне поняття вразливості як слабкості, що може бути використана при реалізації загрози. Зокрема, відповідно до *ISO/IEC 27001* [14] вразливість трактується як властивість активу або групи активів, яка може бути використана загрозою, причому до таких активів належить і персонал. Аналогічно, у *NIST SP 800-30* [1] під вразливістю розуміється слабкість інформаційної системи, процедур безпеки або внутрішніх контролів, що може бути використана джерелом загрози, включаючи недоліки, пов'язані з людським фактором. У документах Агенства Європейського союзу з питань кібербезпеки (*European Union Agency for Cybersecurity*, далі – *ENISA*) [15] також підкреслюється, що сучасні кіберзагрози базуються на експлуатації поведінкових характеристик користувача та людських помилок (*exploiting human error and behaviour*). У цьому контексті “вразливість користувача” доцільно розглядати як сукупність когнітивних, поведінкових та організаційних характеристик, які зумовлюють можливість успішного впливу соціально-інженерних атак та прийняття користувачем небезпечних рішень. Таким чином, під “вразливістю користувача” пропонується розуміти слабкі сторони знань, сприйняття, мислення та поведінки користувача, які можуть бути використані для реалізації загроз соціальної інженерії, що узгоджується із загальним визначенням вразливості, яке надане в *ISO/IEC 27001* та *NIST SP 800-30*, а також із підходами *ENISA* щодо ролі людського фактору.

Стійкість (*resilience*) – це здатність організації, системи або інфраструктури протистояти кіберінцидентам, адаптуватися до них і швидко відновлюватися після них, зберігаючи

критично важливі функції [14]. У контексті атак соціальної інженерії “стійкість користувача” – це здатність користувача розпізнавати, протидіяти та не піддаватися впливу соціально-інженерних атак, зберігаючи безпечну поведінку навіть в умовах невизначеності та маніпулятивного впливу. Відповідно, поняття “вразливість користувача” – “стійкість користувача” є взаємопов’язаними характеристиками, що мають обернено пропорційний характер, підвищення рівня навченості та обізнаності користувача призводить до зменшення його вразливості та, відповідно, до зростання стійкості до соціально-інженерних атак.

Міжнародні стандарти, *NIS2 Directive (EU) 2022/2555* (далі – *NIS2*) [16] та *NIST SP 800-53* [9], містять вимоги (контролі), що виокремлюють і формують вимоги, які в сукупності призведуть до зменшення вразливості користувача та підвищення рівня його стійкості через впровадження заходів навчання, обізнаності, безперервності діяльності та управління ризиками. Згідно з *NIS2* (стаття 21. *Cybersecurity risk-management measures*) [16] вимоги такі:

1. Навчання та обізнаність персоналу (*Art. 21(2)(g). Cybersecurity training and awareness*): періодичне навчання персоналу щодо кіберзагроз; формування навичок розпізнавання фішингу, соціальної інженерії.
2. Управління інцидентами (*Art. 21(2)(b). Incident handling*): виявлення та реагування на інциденти, включає інциденти, спричинені соціальною інженерією.
3. Безперервність діяльності (*Art. 21(2)(c). Business continuity and crisis management*): підготовка до інцидентів, у тому числі людського фактору.
4. Управління ризиками (*Art. 21(1). Risk management framework*): системне оцінювання кіберризиків, включаючи поведінкові фактори, інтегрує соціальну інженерію у загальну модель ризику.

NIST SP 800-53 [9] розглядає соціальну інженерію як один із основних сценаріїв реалізації загроз (експлуатуючи поведінкові вразливості користувачів), і відповідно, вимагає впровадження багаторівневих організаційних і технічних заходів для її запобігання, виявлення та мінімізації наслідків.

При цьому, навчання та обізнаність користувачів (персоналу) досягається через оцінку ефективності навчання (доцільно з визначенням початкового рівня стійкості користувача), періодичні тренінги, симуляцію атак (*phishing campaigns*) та обов’язкове проведення тестування. За зазначеними стандартами, обізнаність користувача (*awareness training*) зменшується з часом за відсутності оновлення, і навчання має бути періодичним для підтримки ефекту. Тому, моделюючи атаки, соціальну інженерію можливо розглядати як інструмент перевірки стійкості користувача.

Розробка моделі визначення стійкості користувачів до атак соціальної інженерії на основі теорій навчання та забування.

Загальна постановка задачі. В будь-якій інформаційній системі (далі – системі) розглядається користувач, здатність якого протидіяти атакам соціальної інженерії змінюється у часі під впливом процесів навчання, практично набутого досвіду, природного забування отриманих знань, а також від еволюції та оновлення механізмів соціоінженерних атак. Формально вводиться поняття рівня стійкості користувача, який відображає поточну здатність користувача виявляти та протидіяти атакам соціальної інженерії. Вказаний рівень є змінною величиною і залежить від початкового рівня стійкості та обізнаності користувача (навчання або забування інформації). При цьому, підвищення рівня обізнаності користувачів у сфері кібербезпеки має властивість до зменшення граничного ефекту (за класичними дослідженнями у сфері теорії навчання та когнітивної психології) – початкові етапи навчання дають найбільший приріст знань, тоді як подальше навчання супроводжується поступовим насиченням і зменшенням темпів засвоєння. Така поведінка узгоджується з класичними результатами досліджень, зокрема кривою забування, запропонованою *Hermann Ebbinghaus*, яка описує швидке початкове зниження рівня запам’ятовування з подальшим його уповільненням [17].

Модель має визначати рівень стійкості користувача у часі як функцію попереднього стану знань (враховуючи вхідні дані – обґрунтовані параметри моделі та індикатор атаки (наявність або відсутність атаки)) та забезпечувати покрокове оновлення рівня стійкості користувача за результатами навчання (забування).

За результатами моделювання можливо визначити, як змінюється стійкість різних користувачів, обґрунтовувати оптимальну періодичність проведення навчань і тренінгів персоналу, а також використати отримані результати для оцінювання залишкового ризику, пов'язаного із людським фактором для системи. Схему моделі визначення рівня стійкості користувача до атак соціальної інженерії наведено на рисунку 1.

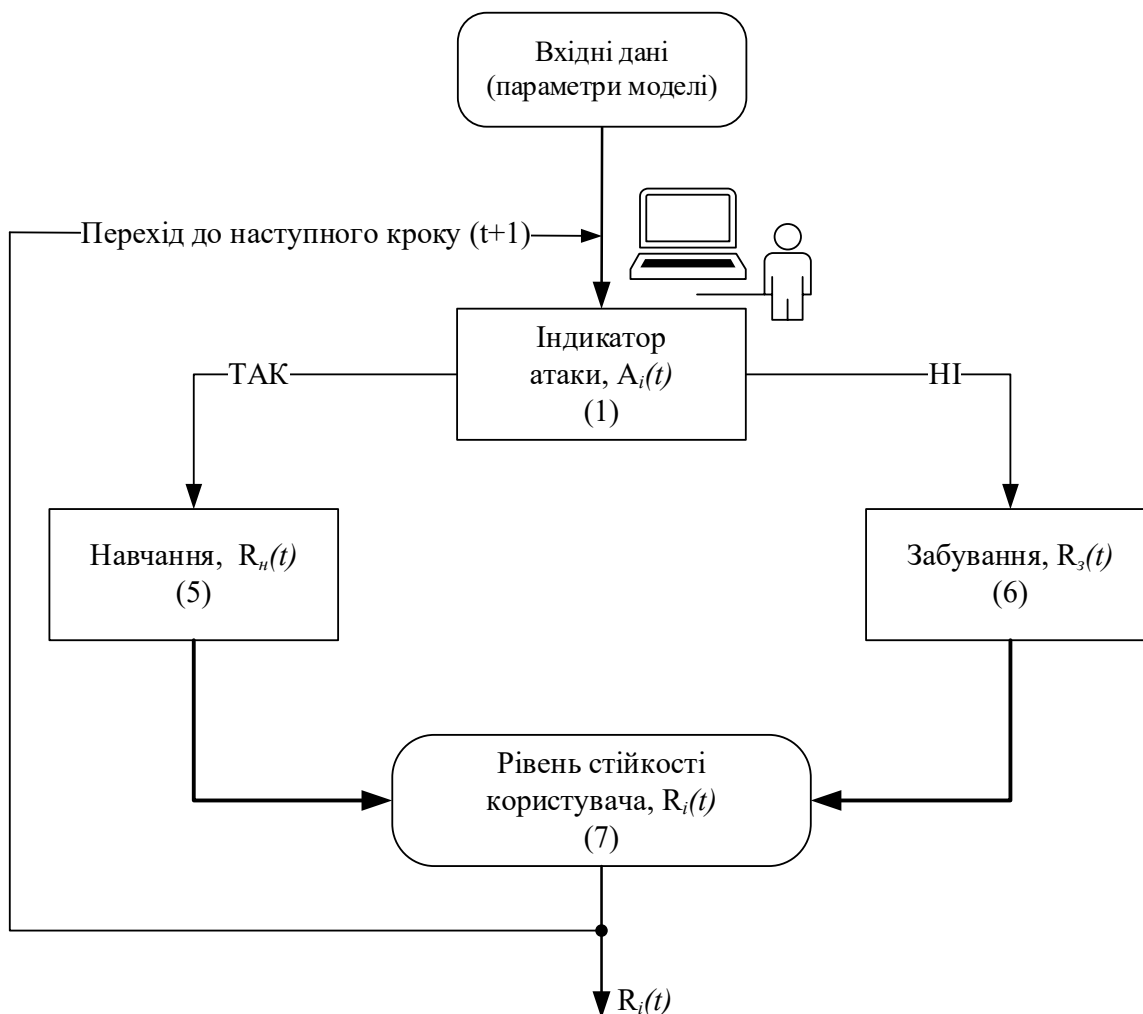


Рис. 1. Схема моделі визначення рівня стійкості користувача до атак соціальної інженерії

Вхідні дані, припущення та обмеження. Згідно з [18] наведено статистичні показники про користувача-жертву фішингових атак, а саме:

- нетренований користувач має схильність піддатись фішингу в 33 % атак;
- після 90 днів тренування ризик зменшується на 41 %;
- протягом року навчань ризик зменшується на 82 %.

Також, згідно зі статистикою соціальної інженерії за 2026 рік [19], 1,5 % співробітників все ще натискають небезпечні посилання в симуляції фішингу, навіть після неодноразового навчання. Окрім зазначеного, для розуміння глибини/шкоди від реалізації атак за цією статистикою [18]:

- 65 % нападів соціальної інженерії були фішинговими;

79 % захоплень облікових записів почалися з фішингових електронних листів.

Найбільш поширеними результатами атак соціальної інженерії були викрадення облікових даних (29 %), крадіжка даних (18 %) і вимагання (13 %).

Припущення: Кожна атака є незалежною подією. Навчання підвищує рівень стійкості користувача, забування – знижує рівень стійкості користувача.

Обмеження: Моделювання проведено із врахуванням середньостатистичного рівня початкової стійкості користувача (R_0), що тотожне початковому рівню знань користувача (варіативність початкового рівня стійкості користувача буде враховано в подальших дослідженнях).

Формалізація моделі. Для формалізації процесу визначення рівня стійкості користувача в момент часу t до атак соціальної інженерії введемо змінну $R_i(t) \in [0; 1]$ – нормований інтегральний показник стійкості користувача, який інтерпретується як здатність протидіяти атаці.

Для врахування факту наявності атаки (або симуляції) в момент часу t вводиться індикаторна функція $A_i(t)$ – індикатор атаки (“1” якщо вона відбулася, або “0” якщо атака відсутня), яка має вигляд (1):

$$A_i(t) = \begin{cases} 1, & \text{якщо атака відбулася} \\ 0, & \text{якщо інше} \end{cases} \quad (1)$$

Значення індикатора атаки визначає, який із двох процесів домінує у поточний момент часу, навчання або забування. Індивідуальні процеси навчання та забування доцільно описати експоненційною функцією з насиченням (2), що відображено в [20; 21]:

$$R(t) = R_0 e^{-\lambda t}, \quad (2)$$

де $R(t)$ – рівень знань через час t ;

R_0 – початковий рівень знань (початковий рівень стійкості користувача);

λ – параметр процесу, який залежить від складності матеріалу, індивідуальних особливостей та умов навчання/забування.

Експоненційні моделі ефективно описують поведінку пам'яті у більшості навчальних ситуацій, хоча конкретні значення λ можуть варіюватись залежно від типу знань і когнітивних навичок особи, яка навчається (обґрунтування параметрів та їхніх значень для моделювання наведено в таблиці 1).

Для уникнення нефізичних значень доцільно використовувати обмежену форму моделі, тоді ефект навчання користувача із врахуванням початкового рівня знань матиме вигляд (3):

$$R(t) = R_{max} - (R_{max} - R_0) e^{-kt}, \quad (3)$$

де R_{max} – максимальний рівень знань (максимальний рівень стійкості користувача), який нормується $[0; 1]$;

k – коефіцієнт навчання.

Аналогічно, ефект забування користувача із врахуванням мінімального рівня знань описується як залежність рівня знань в момент часу t від початкового рівня знань (4):

$$R_z(t) = R_{min} + (R_0 - R_{min}) e^{-dt}, \quad (4)$$

де R_{min} – мінімальний рівень знань (мінімальний рівень стійкості користувача);

d – коефіцієнт деградації знань (внаслідок забування або появи нових механізмів атак).

Для практичного застосування неперервні моделі (3)–(4) апроксимуються дискретними рекурсивними формами (5)–(6). Так як процес навчання та забування змінюють один одного, то більш доцільно описати залежності не від моменту часу t , а від попереднього моменту часу.

Ефект навчання (3) набуває вигляду (5):

$$R_H(t) = R_{max} - (R_{max} - R_{t-1}) * k, \quad (5)$$

де R_{t-1} – рівень знань (стійкості користувача) в попередній момент часу.

Ефект забування (4) набуває вигляду (6):

$$R_3(t) = R_{min} + (R_{min} - R_{t-1}) * d. \quad (6)$$

Тоді, рівень стійкості користувача, $R_i(t)$ (із врахуванням індикатора атаки (1), функцій навчання (5) та забування (6)) визначається згідно з (7):

$$R_i(t) = A_i(t)R_H(t) + (1 - A_i(t)) R_3(t). \quad (7)$$

Параметри моделі. Для реалізації моделі проведено обґрунтування її параметрів на основі статистичних та емпіричних даних (табл. 1).

Таблиця 1

Обґрунтування параметрів моделі на основі статистичних та емпіричних даних

№ з/п	Параметр	Значення	Опис припущення	Що відображає	Обґрунтування
1	Початкова стійкість користувача (R_0)	0,67	На основі статистичних даних або результатів тестування користувача	Базовий рівень здатності протидії фішингу	Виходячи зі статистики ~ 33 % користувачів піддаються фішингу: стійкість $\approx 1 - 0,33 = 0,67$
2	Стандартне відхилення R_0	$\pm 0,10$	Варіативність користувачів	Індивідуальні відмінності	Враховує різний рівень обізнаності та досвіду
3	Максимальне значення стійкості (R_{max})	0,985	Обмеження моделі (граничний рівень)	Верхня межа ефективності навчання	Навіть після навчання частина користувачів ($\approx 1,5$ %) допускає помилки
4	Мінімальне значення стійкості (R_{min})	0,67	Обмеження моделі (граничний рівень)	Нижня межа	Відповідає $R_{min} \leq R_0$
5	Коефіцієнт навчання (експоненційний)	0,41 (за 90 днів)	Емпіричний параметр	Приріст знань	Визначено шляхом апроксимації експоненційної моделі згідно з виразом (4) (зниження ризику на 41 % за 90 днів), $k \approx 0,005$
6	Коефіцієнт деградації знань (експоненційний)	[0;1]	Емпіричний параметр	Втрата знань	Нормується в межах [0;1] та характеризує інтенсивність втрати знань (внаслідок забування або появи нових механізмів атак)
7	Функція складності $f(t)$	[0;1]	Рівень складності атаки	Вплив атаки	Враховує різні типи складності атак

Визначення початкової стійкості користувача (п. 1 табл. 1) здійснено на основі статистичних даних про фішингові атаки, тоді як для реальних систем (умов) можливий варіант визначення стійкості користувача шляхом проведення його тестування за різними ступенями складності тесту. Кожен параметр може мати як математичну інтерпретацію, так і емпіричне обґрунтування, що забезпечує узгодженість моделі з реальними статистичними даними та дозволяє адекватно відобразити нелінійний ефект навчання, ефект насичення та деградацію знань (забування).

Апробація моделі. Для апробації запропонованої моделі здійснено її програмування мовою *Python*, з використанням бібліотеки *numpy*. Визначення рівня стійкості користувача здійснюється згідно з виразом (7), час в моделі інтерпретується як кількість ітерацій навчання, одна ітерація моделі відповідає умовному часовому інтервалу (t). Динаміку зміни рівня стійкості користувачів залежно від кількості ітерацій навчання (на прикладі 100 ітерацій) наведено на рисунку 2.

Початковий рівень стійкості користувача для досліджуваних категорій прийнято усередненим (0,67 згідно з п. 1 табл. 1), що дає змогу порівнювати динаміку зміни рівня стійкості за однакових початкових умов. Подальша зміна рівня стійкості визначається здатністю користувача до навчання, яка в моделі описується коефіцієнтами навчання та деградації знань, що характеризує поступову втрату набутих навичок у часі. Так, слабкий користувач характеризується коефіцієнтом навчання $k = 0,001$ (найнижчий рівень засвоєння знань), середній користувач – коефіцієнтом навчання, який визначено емпіричним шляхом $k = 0,005$ (п. 5. табл. 1), сильний користувач характеризується коефіцієнтом навчання $k = 0,01$.

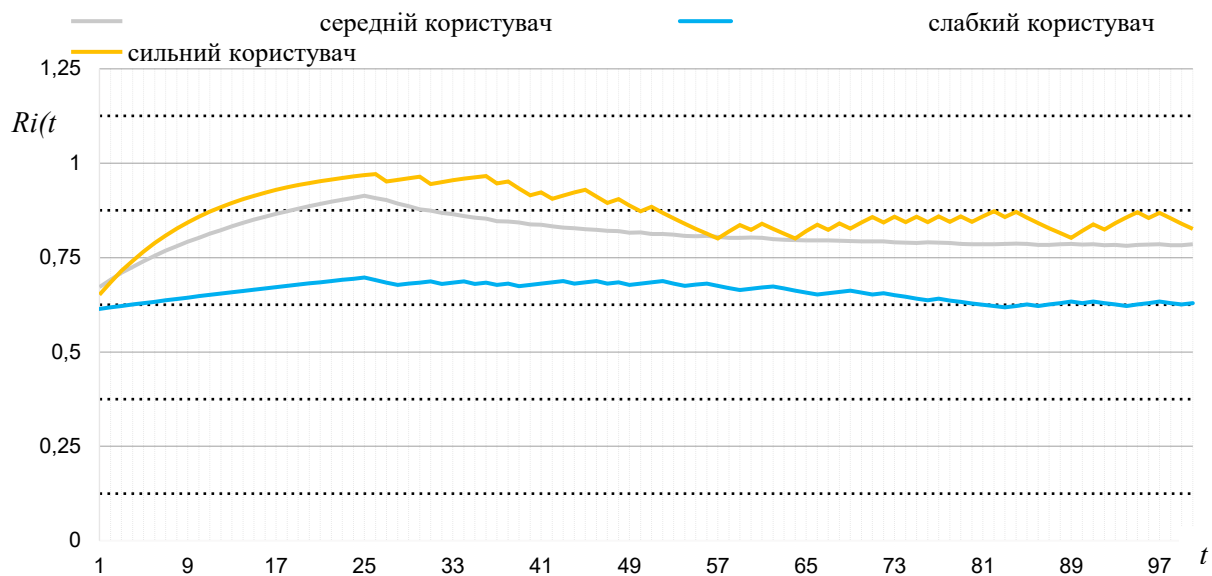


Рис. 2. Динаміка зміни рівня стійкості користувача залежно від кількості ітерацій навчання

Максимальний ефект навчання (рівень стійкості користувача 0,9) досягається приблизно на 20–25-й ітерації навчання, після чого спостерігається поступова деградація знань. Така динаміка узгоджується з класичними уявленнями про криві навчання та забування. Із часом, у користувачів спостерігається уповільнення темпів зростання показника стійкості, що пояснюється ефектом насичення знань та наближенням до граничного рівня засвоєння.

На прикладі системи з чисельністю 1000 користувачів (N) проведено розрахунок рівня їхньої стійкості (7). Користувачів розподілено та згруповано за інтервалами значень показника стійкості (рис. 3).

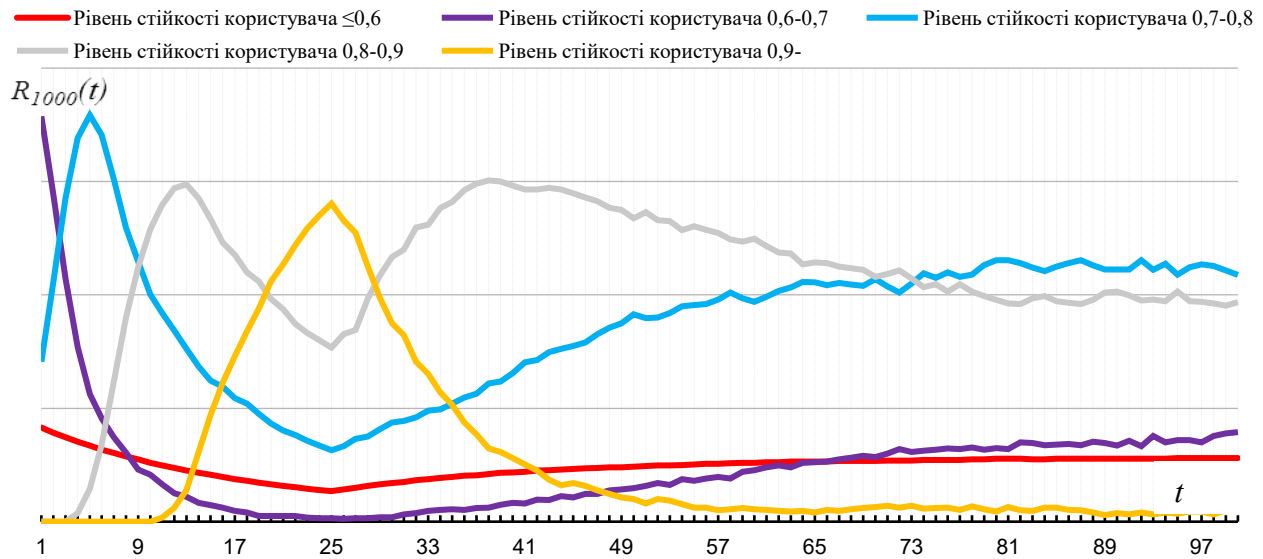


Рис. 3. Розподіл кількості користувачів за рівнем їхньої стійкості залежно від ітерацій навчання

Аналіз графіка дозволяє оцінити співвідношення між зазначеними групами користувачів у системі та виявити пріоритетні групи ризику для формування підходів до їх навчання (тренування). Зменшення частки користувачів із рівнем стійкості 0,6–0,7 та зростання груп із рівнями 0,7–0,8, 0,8–0,9 і понад 0,9 свідчить про позитивний вплив навчання на загальний рівень кіберстійкості організації.

Також, за результатами навчання користувачів доцільно визначити залишковий ризик, пов'язаний із людським фактором R_l для системи із N користувачів (як практична складова визначення стійкості користувачів) з метою його врахування при оцінці загального ризику системи.

За класичним визначенням [22] залишковий ризик людського фактору для всієї системи (сервісу) після навчання користувачів оцінюється (8):

$$R_l = \frac{1}{N} \sum_{i=1}^n \prod_{t=1}^{t_{end}} (A_i(t) * (1 - R_i(t)) * f(t)), \quad (8)$$

де $1 - R_i(t)$ – вразливість користувача i в момент часу t ;
 $f(t)$ – функція складності атаки в момент часу t .

Окремо на графіку (див. рис. 3) червоним кольором виділено категорію найбільш вразливих користувачів, із рівнем стійкості нижчим за поріг $1 - R_i(t) = 0,6$. Вразливість впливає на залишковий ризик системи, пов'язаний із людським фактором. Отримані результати демонструють доцільність диференційованого підходу до підготовки користувачів з урахуванням їхніх індивідуальних особливостей до навчання та деградації знань.

Таким чином, розробка моделі надає можливість кількісного визначення стійкості користувачів до атак соціальної інженерії, а саме, визначення рівня стійкості користувача, $R_i(t)$ згідно з виразом (7) та оцінювання залишкового ризику людського фактору R_l для системи згідно з виразом (8) після навчання користувачів.

Висновок та перспективи подальших досліджень. У статті запропоновано модель визначення стійкості користувачів до атак соціальної інженерії, яка, на відміну від існуючих підходів, у явному вигляді враховує рівень знань користувача, ефект насичення, а також деградації знань. Модель інтегрує процеси навчання та втрати знань в єдиній аналітичній формі та дозволяє оцінювати залишковий ризик, пов'язаний із людським фактором для системи після навчання користувачів. Результати моделювання підтверджують адекватність запропонованої моделі, оскільки вона коректно відтворює основні закономірності процесів

навчання та втрати знань і узгоджується із теоріями навчання та деградації знань. Практична цінність моделі полягає у можливості її використання для визначення пріоритетних груп ризику, визначення оптимальної періодичності навчання та інтеграції показників людського фактору у моделі (методики) оцінювання ризиків для системи.

Подальші дослідження спрямовані на емпіричну валідацію моделі, уточнення та розширення її параметрів, врахування варіативності користувачів, а також оцінювання залишкового ризику, пов'язаного із людським фактором.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments. CSRC. NIST Computer Security Resource Center / CSRC. URL: <https://csrc.nist.gov/pubs/sp/800/30/r1/final> (дата звернення: 04.04.2026).
2. Microsoft Digital Defense Report 2025. Lighting the path to a secure future. A Microsoft Threat Intelligence report. URL: <https://spacelift.io/blog/social-engineering-statistics> (дата звернення: 14.04.2026).
3. Кібератаки UAC-0001 на сектор безпеки та оборони із застосуванням програмного засобу LAMENUG, що використовує LLM (велику мовну модель). URL: <https://cert.gov.ua/article/6284730> (дата звернення: 14.04.2026).
4. Кібератака UAC-0125 з використанням тематики “Армія+”. URL: <https://cert.gov.ua/article/6281701> (дата звернення: 14.04.2026).
5. Російські кібероперації аналітика за II півріччя 2024 року // Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspetszv-yazku> (дата звернення: 12.03.2026).
6. Російські кібероперації аналітика за I півріччя 2025 року // Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspetszv-yazku> (дата звернення: 12.03.2026).
7. Звіт про базове дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки. Для CRDF Global. Short URL service Surli – FREE Short Links. URL: <https://surli.li/lzxqpx> (дата звернення: 12.03.2026).
8. Звіт про проміжне дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки. Для CRDF Global. 2023. 72 с. URL: <https://surli.li/icvklc> (дата звернення: 12.03.2026).
9. NIST SP 800-53 rev. 5 Security and Privacy Controls for Information Systems and Organizations, 2020. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf> (дата звернення: 04.04.2026).
10. SANS Cybersecurity Training Overview // SANS Institute. URL: <https://www.sans.org/cybersecurity-training-overview> (дата звернення: 14.04.2026).
11. Embrey I., Kaivanto K. Many phish in the C: A coexisting-choice-criteria model of security behavior // Risk Analysis. April 2023. Vol. 43, Issue 4. P. 645–866. URL: <https://doi.org/10.1111/risa.13947> (дата звернення: 04.04.2026).
12. Dobryshyn Y. STATISTICAL METHODS FOR PREDICTING PHISHING ATTACKS // Cybersecurity: Education, Science, Technique. 2024. Vol. 3, no. 23. P. 56–70. URL: <https://doi.org/10.28925/2663-4023.2024.23.5670> (дата звернення: 04.04.2026).
13. Toth R. et al. Sustaining Cyber Awareness: The Long-Term Impact of Continuous Phishing Training and Emotional Triggers // arXiv preprint arXiv:2510.27298. 2025. URL: <https://arxiv.org/html/2510.27298v1> (дата звернення: 18.04.2026).
14. ДСТУ EN ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT). URL: <https://www.iso.org/ru/standard/27001> (дата звернення: 04.04.2026).
15. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity ENISA. Home ENISA. URL: <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity> (дата звернення: 04.04.2026).
16. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). EUR-Lex – Access to European Union law – choose your language. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555&qid=1708526 (дата звернення: 14.04.2026).

17. Крива забування Еббінгауза – Вікіпедія. URL: uk.wikipedia.org/wiki/Крива_забування_Еббінгауза (дата звернення: 14.04.2026).

18. 2025 Phishing By Industry Benchmark Report | KnowBe4. Beyond Security Awareness Training // KnowBe4 Human Risk Mgmt Platform. URL: <https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report> (дата звернення: 14.04.2026).

19. Michalowski M. 70 Social Engineering Statistics for 2026 // Spacelift. URL: <https://spacelift.io/blog/social-engineering-statistics> (дата звернення: 14.04.2026).

20. Vianna, Leonardo Silva, Alexandre Leopoldo Gonçalves, and João Artur Souza. Analysis of learning curves in predictive modeling using exponential curve fitting with an asymptotic approach // Plos one. 2024. No. 4 : e0299811. URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0299811>. (дата звернення: 14.04.2026).

21. Murre J. M. J., Chessa A. G. Power laws from individual differences in learning and forgetting: mathematical analyses // Psychonomic Bulletin & Review. 2011. Vol. 18, no. 3. P. 592–597. URL: <https://doi.org/10.3758/s13423-011-0076-y> (дата звернення: 14.04.2026).

22. ISO/IEC 27005:2022 Інформаційна безпека, кібербезпека та захист конфіденційності – Керівництво з управління ризиками інформаційної безпеки. URL: <https://www.iso.org/standard/80585.html> (дата звернення: 22.04.2026).

Надійшла до редколегії 11.05.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.396

канд. техн. наук Панченко І. В. ORCID: 0000-0001-5690-3813 (ВІТІ ім. Героїв Крут)
Бондаренко Д. М. ORCID: 0009-0001-7815-6027 (ДержНДІ технологій кібербезпеки)
канд. техн. наук, доцент Липський О. А. ORCID: 0009-0007-7355-4433
(ДержНДІ технологій кібербезпеки)
Стефанишин Я. І. ORCID: 0000-0002-8317-4131 (ДержНДІ технологій кібербезпеки)

ДОСЛІДЖЕННЯ СТІЙКОСТІ МЕРЕЖІ 4G/LTE ДО ВПЛИВУ НАВМИСНИХ ЗАВАД

Мобільні радіомережі 4G/LTE забезпечують передачу значних обсягів даних, низьку затримку, виняткову надійність та роботу у реальному масштабі часу. У деяких випадках мобільні мережі можуть розглядатися як значно дешевша альтернатива супутниковому низькоорбітальному зв'язку. При цьому оцінка впливів навмисних завад на мобільні мережі 4G/LTE дає змогу визначити надійність їх функціонування та окреслити межі їх альтернативного використання.

Метою статті є викладення основних результатів експериментального дослідження стійкості мережі 4G/LTE до впливу навмисних вузькосмугових завад від засобів РЕБ.

Наведено короткий опис принципів побудови мережі 4G/LTE. Зроблено наголос на тому, що використання у мережі технології MIMO дає можливість:

збільшити пропускну здатність завдяки паралельному передаванню та прийманню декількох інформаційних потоків;

мінімізувати вплив багатопроменевості на якість прийнятих сигналів.

До наведеної функціональної схеми створеного макетного зразка мережі 4G/LTE включено: блок RRU Ericsson Radio 4486 B8B20B28 (робочі частоти у діапазоні 700 MHz, 4×4 MIMO), антени Ericsson Antenna 9011 ILM, блок BBU Ericsson Baseband 6318 та користувацькі пристрої у вигляді смартфонів Samsung S21, до програмного забезпечення яких інстальовано програму GSM NetMonitor.

Результати випробувань мережі на стійкість до впливу навмисних завад від засобів РЕБ включають, зокрема, опис та аналіз експериментального підтвердження щодо:

відсутності стійкості мережі 4G/LTE при встановленому на базових станціях хендоверу за показником RSRP;

наявності стійкості мережі 4G/LTE при встановленому на базових станціях хендоверу за показником RSRQ.

Ключові слова: системи мобільного зв'язку 4G/LTE, базова станція LTE, хендовер, показники якості зв'язку RSRP та RSRQ, навмисні завади, програма GSM NetMonitor, MIMO.

I. Panchenko, D. Bondarenko, O. Lypskyi, Ya. Stefanyshyn. Research on the resilience of 4G/LTE networks to the influence of intentional interference

4G/LTE mobile radio networks provide the transmission of significant amounts of data, low latency, exceptional reliability and real-time operation. In some cases, mobile networks can be considered as a much cheaper alternative to low-orbit satellite communications. At the same time, the assessment of the effects of intentional interference on 4G/LTE mobile networks makes it possible to determine the reliability of their operation and outline the limits of their alternative use.

The purpose of the article is to present the main results of an experimental study of the resistance of the 4G/LTE network to the influence of intentional narrowband interference from electronic warfare equipment.

A brief description of the principles of building 4G/LTE networks is given. It is emphasized that the use of MIMO technology in the network makes it possible to:

increase the bandwidth due to the parallel transmission and reception of several information streams,

minimize the impact of multipath on the quality of received signals.

The functional diagram of the created prototype of the 4G/LTE network includes: the RRU unit Ericsson Radio 4486 B8B20B28 (operating frequencies in the 700 MHz range, 4×4 MIMO), the Ericsson Antenna 9011 ILM antennas, the BBU Ericsson Baseband 6318 unit and user devices in the form of Samsung S21 smartphones, the software of which has the GSM NetMonitor program installed.

The results of network tests for resistance to intentional interference from electronic warfare agents include, in particular, a description and analysis of experimental confirmation of:

the lack of stability of the 4G/LTE network with handover installed on the base stations according to the RSRP indicator;

the presence of stability of the 4G/LTE network with handover installed at base stations according to the RSRQ indicator.

Keywords: 4G/LTE mobile communication systems, LTE base station, handover, RSRP and RSRQ communication quality indicators, intentional interference, GSM NetMonitor program, MIMO.

Постановка проблеми

Мобільні радіомережі 4G/LTE відіграють важливу роль у розвитку суспільства, забезпечуючи передачу величезних обсягів даних, низьку затримку, виняткову надійність та роботу у реальному масштабі часу.

Оцінка впливів навмисних завад на мережі радіодоступу Radio Access Network (RAN), які є ключовим компонентом мобільних мереж 4G/LTE, дає змогу визначити надійність їх функціонування та окреслити межі їх використання.

Стійкість мереж зв'язку до впливу засобів РЕБ залежить від багатьох факторів, включаючи тип засобів зв'язку, робочі частоти, потужність перешкод, а також використовувані методи та засоби захисту.

Аналіз останніх досліджень і публікацій

Архітектура стільникових мереж за час свого розвитку набула усталених форм і, загалом, має невеликі відмінності. Конкретний принцип побудови як самої мережі 4G/LTE, так і її базової станції, наведено в [1].

Задовільне функціонування мережі 4G/LTE, як і будь-якої технічної системи, підтримується при забезпеченні властивих їй певних технічних характеристик. Визначення величин переважної більшості цих характеристик, згідно з типовою архітектурою стільникових мереж, покладено на користувачі пристрої. Візуалізація показників функціонування мережі, які визначаються у процесі її функціонування користувачами пристроями, може бути забезпечена за допомогою інсталюваної до їхнього програмного забезпечення програми GSM NetMonitor [2].

Однією із важливих властивостей стільникових мереж є притаманна їм функція хендоверу (Handover) – автоматичного перемикання робочої частоти, відомості про яку наведено в роботі [3].

У роботах [4; 5] наведені параметри якості сигналу 4G/LTE та формула для визначення показника, який характеризує якість передавання сигналу (RSRQ).

У роботі [6] розглянуто аналіз загроз і вразливостей під час впровадження технології 4G/LTE та проблеми вразливості стільникових мереж 4G/LTE в критичних інфраструктурах.

У роботі [7] визначено інструмент для оцінки продуктивності бездротового зв'язку з безпілотниками у стільникових мережах 4G.

У роботі [8] наведена оцінка якості передачі голосу в мережах LTE.

Також у роботі [9] представлена довгострокова еволюція LTE-4G/5G та основні перспективи розвитку мобільних інфокомунаційних систем.

Таким чином, виникає можливість вирішення наукового завдання щодо дослідження стійкості мереж 4G/LTE до впливу навмисних вузькосмугових завад від засобів РЕБ.

Метою статті є викладення основних результатів експериментального дослідження стійкості мережі 4G/LTE до впливу навмисних вузькосмугових завад від засобів РЕБ.

Виклад основного матеріалу дослідження

У загальному випадку до основних методів підвищення стійкості стільникових мереж зв'язку до негативного впливу завад (у тому числі і несанкціонованих) можна віднести:

1) використання якомога більшої кількості робочих каналів зв'язку з охопленням якомога ширшого відрізка електромагнітного спектра (з метою ускладнення роботи засобів РЕБ, які, зазвичай, створюють вузькосмугову заваду – у межах одного чи двох каналів зв'язку);

2) зміну частоти під час передавання складових елементів цифрового повідомлення – псевдовипадкове перестроювання радіочастоти (ППРЧ), ефективність якого зростає при перестроюванні частоти у достатньо широкій смузі частот;

3) використання вузькоспрямованих антен (зменшення негативного впливу навмисних завад завдяки просторовій селекції);

4) використання у мережах більш потужних сигналів (зменшення ймовірності придушення потужних сигналів передавальних пристроїв мережі);

5) планування зв'язку та взаємодію із підрозділами радіоелектронної розвідки (зменшення впливу перешкод, створюваних засобами РЕБ, вдалим вибором маршрутів).

Видається, що притаманний стільниковій мережі 4G/LTE хендовер у широкому діапазоні частот електромагнітного спектра повинен бути найбільш дієвим засобом забезпечення її стійкості до впливу навмисних перешкод.

Для експериментального підтвердження цього припущення проаналізуємо принципи побудови самої мережі 4G/LTE. У загальному випадку робочий діапазон мережі 4G/LTE охоплює відрізок електромагнітного спектра від 400 MHz до 2600 MHz. Видається, що це створює реальні можливості оперативного реагування на зміну електромагнітної ситуації у навколишньому середовищі і забезпечення сталого зв'язку в умовах впливу несанкціонованих активних вузькосмугових завад.

Зазвичай, архітектура мереж радіодоступу Radio Access Network (RAN) являє собою частину телекомунікаційної системи, яка з'єднує окремі користувацькі пристрої з основним ядром системи за допомогою радіоінтерфейсу. Мережа радіодоступу RAN розташовується між обладнанням користувача (мобільний телефон, комп'ютер або будь-який інший дистанційно керований пристрій) та забезпечує доступ і координацію управління ресурсами на всіх базових станціях.

Загальна архітектура мобільної радіомережі 4G/LTE [1] зображена на рисунку 1.

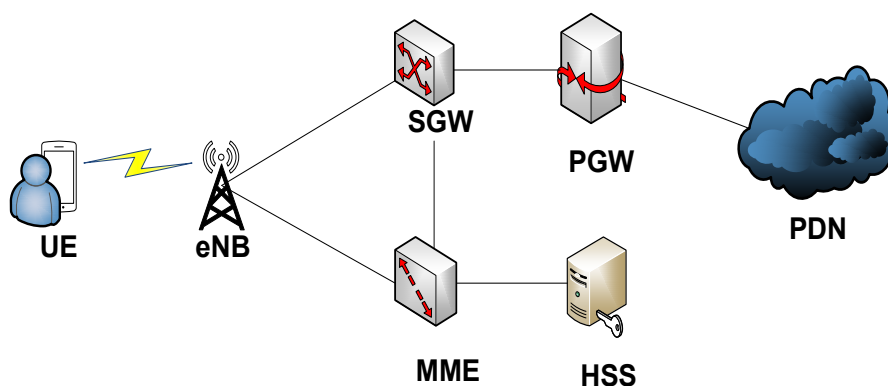


Рис. 1. Загальна архітектура мобільної радіомережі 4G/LTE:

UE – користувацький пристрій; eNB – базова станція; MME – вузол управління мобільністю (автентифікація UE); SGW – вузол передачі даних; PGW – шлюз зовнішніх мереж; PDN – мережа передачі даних (Інтернет); HSS – абонентський сервер для зберігання інформації про всіх абонентів

Телефон або інший користувацький пристрій User Equipment (UE) з метою забезпечення можливості обміну трафіком, підключений до RAN радіоінтерфейсом, через базову станцію eNB. RAN, окрім базової станції eNB, включає також до свого складу антени, які опромінюють певну зону (залежно від пропускної здатності), а також ядро мережі Evolved Packet Core (EPC), яке у мережах 4G/LTE відповідає за керування мобільністю, автентифікацію та передачу даних користувачів UE.

До складу ядра мережі EPC включені ключові вузли, зокрема вузол управління мобільністю MME, вузол передачі даних SGW та шлюз зовнішніх мереж PGW.

Частиною ядра мережі EPC є абонентський сервер Home Subscriber Server (HSS), який забезпечує зберігання централізованої бази даних з інформацією про всіх абонентів (місця розташування, підписки, профілі автентифікації), а також керування автентифікацією, авторизацією та інформацією про підписки.

Зовнішні мережі можуть підключатися до шлюзу зовнішніх мереж PGW через мережу передачі даних Packet Data Network (PDN), зокрема Інтернет.

Наявна архітектура мережі радіодоступу RAN розділяє площину користувача та площину керування на окремі елементи. Повідомлення з даними користувача можуть передаватися контролером RAN через один комутатор програмно-визначальної мережі (SDN), а другий – через інтерфейс управління.

У мережах 4G/LTE базова станція Evolved NodeB (eNodeB) приймає цифрові пакети від ядра мережі EPC та синтезує радіосигнали передачі даних. Базові станції eNodeB, зазвичай, створені з використанням технології Software-Defined Radio (SDR).

Базова станція eNodeB може складатися з одного сектора (мала стільникова станція) або до 3 і більше секторів (макростанція) для забезпечення більших дальності дії та пропускної спроможності. Сучасна багатодіапазонна базова станція 4G/LTE може передавати сигнал на кількох частотах-носіях, маючи можливість для забезпечення в інтересах користувачів більш високої пропускної здатності, агрегації частот-носіїв у кількох діапазонах.

Типова конструкція базової станції 4G/LTE розділена на базовий блок оброблення сигналів Baseband Unit (BBU) і один або кілька виносних радіочастотних блоків Remote Radio Unit (RRU). Інколи обидва блоки базової станції можуть бути об'єднані в один блок, що має тільки 1 або 2 сектори.

Радіочастотний блок RRU, який є ключовим компонентом базових станцій 4G/LTE, забезпечує випромінювання та приймання модульованих радіочастотних сигналів і розташовується неподалік антени (для зменшення втрат енергії на фідерних лініях).

Блок оброблення сигналів BBU, який перетворює цифрові сигнали у радіочастотні, а також виконує зворотне перетворення, згідно з архітектурою мобільних базових станцій 4G/LTE, знаходиться “на землі”, наприклад, у захищеному об’ємі шелтера.

У загальному випадку, радіочастотний блок RRU забезпечує випромінювання та приймання радіосигналів за технологією Multiple Input Multiple Output (MIMO), яка передбачає використання декількох дуплексних каналів (з окремими антенами).

Використання технології MIMO дає можливість:

збільшити пропускну здатність завдяки паралельному передаванню та прийманню декількох інформаційних потоків,

мінімізувати вплив багатопроменевості на якість прийнятих сигналів.

Ефективність технології MIMO високого порядку реально підтверджується на коротких відстанях і у міських умовах. Крім того, конфігурація 8×8 MIMO, забезпечуючи високу пропускну здатність, також може включати управління променем для збільшення дальності зв'язку, що потенційно для цієї технології створює перспективи щодо широкосмугового зв'язку на великих відстанях (важливо для сільської місцевості).

Для оцінки впливу навмисних завад на радіомережу 4G/LTE було створено її макет відповідно до функціональної схеми, наведеної на рисунку 2.

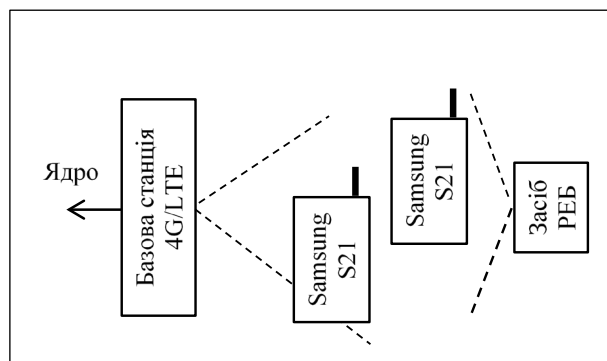


Рис. 2. Функціональна схема макету мережі радіодоступу RAN

Для створення макету мережі RAN використана базова станція 4G/LTE Ericsson діапазону 700–960 MHz, функціональна схема якої наведена на рисунку 3.

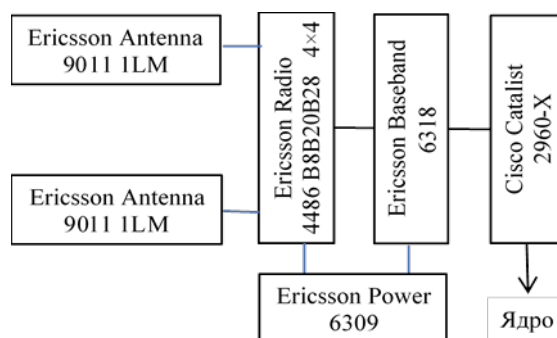


Рис. 3. Схема функціональна базової станції 4G/LTE діапазону 700–960 MHz

Як виносний радіочастотний блок RRU використано блок Ericsson Radio 4486 B8B20B28 з робочими частотами згідно з таблицею 1.

Таблиця 1

Робочі частоти блока RRU Ericsson Radio 4486 B8B20B28

Band	Up Link, MHz	Down Link, MHz
B8	880–915	925–960
B20	832–862	791–821
B28	703–740	758–803

Як блок оброблення сигналів BBU використано блок Ericsson Baseband 6318.

Роль антенної системи базової станції виконують два блоки антен Ericsson Antenna 9011 1LM, до складу кожного із яких включені дві антени з частотним діапазоном 617–4200 MHz та коефіцієнтом підсилення близько 10 dBi, що дозволяє реалізувати технологію 4x4 MIMO у складі цієї базової станції.

Зв'язок базової станції з ядром забезпечувався мережею Інтернет через комутатор Cisco Catalyst 2960-X.

Як технічні засоби користувачів використовувалися два смартфони Samsung S21 зі встановленим програмним забезпеченням GSM NetMonitor [2], яке дає можливість забезпечити оцінку рівня сигналу (dBm) та якості зв'язку, а також визначити частотний діапазон.

Для створення сигналу активної завади використовувалися 2 різні засоби РЕБ: макетний зразок купольного (окопного) засобу РЕБ, що забезпечував створення активної суцільної

спектральної завади у діапазоні 700–850 MHz потужністю до 2 W (розташовувався на відстані 10 м від смартфона), та мобільний штатний засіб РЕБ потужністю близько 100 W (розташовувався на відстані 10 км від смартфона). Спектр макетного зразка купольного засобу РЕБ (що охоплює робочі діапазони В20 та В28 базової станції) представлено на рисунку 4.

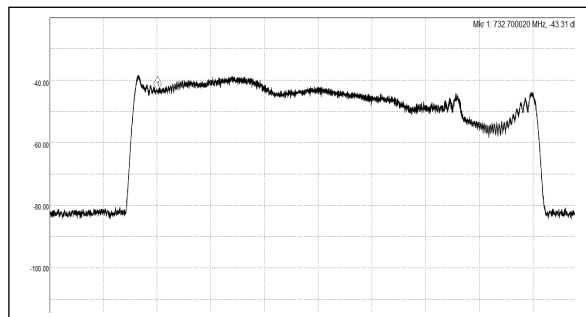


Рис. 4. Спектр сигналу завади купольного засобу РЕБ

Мета експерименту полягала у перевірці можливості реалізації базовою станцією функції хендоверу при виявленні факту придушення робочого каналу мережі 4G/LTE засобом РЕБ із вузькосмуговою завадою.

Обставини проведення експериментів не дали можливості забезпечити точне вимірювання рівня сигналів у необхідних точках технічних засобів мережі, тому фіксувалися тільки експертні якісні показники роботоспроможності мережі (“функціонує”/ “не функціонує”).

У загальному випадку, при функціонуванні стільникової мережі 4G/LTE базовою станцією забезпечується динамічний контроль якості радіочастотних каналів і при виявленні каналу із поганою якістю зв'язку базова станція перемикає з'єднання на інший канал з кращою на поточний час якістю зв'язку, який реалізований або тією ж базовою станцією (внутрішньостільниковий хендовер), або іншою базовою станцією (хендовер між стільниками) [3].

Як вже наголошувалося, функція безпосереднього оцінювання якості зв'язку в стільникових мережах покладена на кожен конкретний користувацький пристрій (смартфон). При фіксації незадовільної якості зв'язку у використовуваному каналі користувацький пристрій інформує про це базову станцію, яка у результаті хендоверу перемикає його на інший канал зв'язку, з кращою якістю зв'язку.

При реалізації функції хендоверу користувацькими пристроями аналізуються наступні основні показники якості зв'язку [4].

Reference Signal Received Power (RSRP) – середнє значення потужності прийнятих опорних сигналів базової станції (рівень сигналу базової станції). Функція хендоверу за показником RSRP встановлюється на базових станціях мережі 4G/LTE як базова. Аналіз показника RSRP дає можливість у мережі 4G/LTE забезпечити хендовер при виході користувацького пристрою із зони обслуговування однієї базової станції та забезпечити йому перехід у зону обслуговування іншої. У загальному випадку, діапазон величин RSRP змінюється від -40 dBm до -140 dBm; -70 dBm – відмінно; -110 dBm – дуже слабкий; -120 dBm – критично;

Reference Signal Received Quality (RSRQ) – характеризує якість прийнятого опорного сигналу базової станції (тобто не тільки потужність прийнятого опорного сигналу, а і його співвідношення з рівнем шуму у каналі). Хендовер за показником RSRQ на базових станціях 4G/LTE потребує додаткової інсталяції. Аналіз показника RSRQ дає можливість у мережі

4G/LTE забезпечити хендовер при появі завад на використовуваному каналі (наприклад, у штатних ситуаціях внаслідок впливу сусідніх базових станцій).

Розглянемо більш детально, як визначається показник RSRQ.

У загальному випадку показник RSRQ визначається за формулою (1) [5]:

$$RSRQ = N \cdot (RSRP / RSSI), \text{ dB}, \quad (1)$$

де $RSRP$ – середнє значення потужності прийнятих пілотних сигналів, dBm;

$RSSI$ – Received Signal Strength Indicator – загальний рівень прийнятого сигналу, включаючи корисний сигнал, шум та інтерференцію, dBm;

N – кількість ресурсних блоків у смузі пропускання (залежить від ширини каналу, діапазон від 6 до 100).

Для практичних застосувань ця формула використовується у логарифмічній формі (2):

$$RSRQ \text{ (dB)} = 10 \log(N) + RSRP \text{ (dBm)} - RSSI \text{ (dBm)}. \quad (2)$$

При функціонуванні мережі у штатних умовах показник $RSRQ$ набуває значень від -5 дБ до $-19,5$ дБ (чим ближче рівень показника $RSRQ$ до 0, тим якість сигналу краща).

На першому етапі випробування проводилися з використанням базової станції 4G/LTE зі штатно встановленим хендовером за показником RSRP.

При вимкнених засобах РЕБ було перевірено якість зв'язку між смартфонами. Скриншот індикаторної панелі одного зі смартфонів наведено на рисунку 5.

Представлений вигляд індикаторної панелі смартфона наочно демонструє, що програмою GSM NetMonitor фіксується низка важливих для функціонування мережі показників:

Received Signal Strength Indicator (RSSI) (загальний рівень прийнятого сигналу) – “мінус” 83 dBm, (стабільний зв'язок, незадовільний зв'язок – гірше “мінус” 100 dBm).

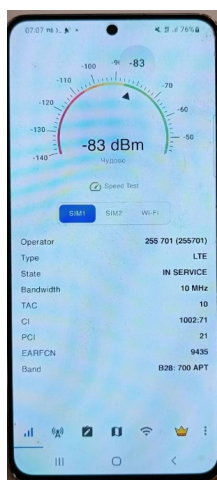


Рис. 5. Скриншот індикаторної панелі смартфона Samsung S21 при відсутності впливу сигналу РЕБ

Bandwidth (смула робочих частот) – 10 MHz.

TAG, Timing Advance Group (час затримки сигналу від смартфона до базової станції) – близько 5 км (1 TAG $\approx$ 550 м).

CI, Carrier-to-Interference (співвідношення потужності частоти-носія до рівня опорний сигналу) ≈ 10 dB.

PC1, Power Control Level 1 (рівень потужності сигналу смартфона) ≈ 10 dB.

Band (робочий діапазон) – B28 (700 MHz).

Після впливу на мережу 4G/LTE завади, згенерованої вузькосмуговими засобами РЕБ (у межах робочого діапазону частот базової станції) її робота втрачала стабільність – зв'язок на робочому каналі порушувався, внаслідок того, що функція хендоверу не була реалізована.

При цьому, за невеликих потужностей випромінювання купольного засобу РЕБ (менше 0,5 W) зв'язок ще підтримувався, але погіршеної якості. При великих потужностях випромінювання засобів РЕБ (більше 1 W) зв'язок між смартфонами втрачався, базова станція свою властивість хендоверу не реалізувала.

Поясненням отриманого результату може слугувати той факт, що середній рівень потужності опорного сигналу RSRP при включенні засобу РЕБ або залишався незмінним, або, найбільш ймовірно, дещо підвищувався (за рахунок суперпозиції із сигналом завади), що сприймалося базовою станцією як свідчення високої якості зв'язку (хоча, насправді, зв'язок був відсутній).

Після ініціації на базовій станції хендоверу за показником RSRQ і увімкненні штатного мобільного засобу РЕБ потужністю 100 W роботоспроможність користувацьких пристроїв не порушувалася (завдяки реалізації хендоверу, вони перемикалася на вільний від завади частотний діапазон, зокрема, з діапазону B28 на діапазон B8).

Скриншот індикаторної панелі смартфона після впливу засобу РЕБ представлено на рисунку 6.

Поясненням отриманого результату може бути той факт, що рівень показника RSRQ на робочому каналі, при увімкненні засобу РЕБ, зменшився до критичного позначки (за рахунок суттєвого зростання рівня показника RSSI та незначного зростання рівня показника RSRP, що призвело до збільшення різниці між ними і досягнення показником RSRQ величини гіршої, ніж $-19,5$ dB). Очевидно, що саме цей ефект став сигналом для базової станції щодо реалізації функції хендоверу, внаслідок чого було забезпечено практично безперервний зв'язок між смартфонами.



Рис. 6. Скриншот індикаторної панелі смартфона Samsung S21 при наявності впливу засобу РЕБ

Таким чином, мережа 4G/LTE, при інсталяції на базових станціях функції хендоверу за показником RSRQ може бути стійкою до впливу вузькосмугових завад від потужних сучасних засобів РЕБ.

Наукова новизна статті полягає у виявленні стійкості (якості) зв'язку мережі 4G/LTE до впливу РЕБ завдяки використанню технології хендовер за показником RSRQ.

Висновки і перспективи подальших досліджень

Проведені випробування підтвердили можливість забезпечення роботи мережі 4G/LTE в умовах впливу вузькосмугових завад від штатних засобів РЕБ великої потужності при встановленій на базових станціях функції хендоверу за показником RSRQ.

Подальші дослідження доцільно спрямувати на визначення конкретних характеристик засобів РЕБ для підвищення ефективності придушення (максимальні потужності та смуги випромінювання, характеристики спрямованості антен, віддаленість від базових станцій тощо).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Продукція компанії Ericsson. URL: <https://dovidnyk.info/index.php/Brand/562> (дата звернення: 12.05.2026).
2. Вимірювання сигналу за допомогою програми Netmonitor lite. URL: <https://droth.biolio.cx.ua/articles/jak-koristuvatisja-programoju-netmonitor.html> (дата звернення: 12.05.2026).
3. Функція хендоверу (Handover) – автоматичне перемикання робочої частоти. URL: <https://studfile.net/preview/2425953/page:2/> (дата звернення: 12.05.2026).
4. Параметри якості сигналу 4G/LTE. URL: <https://www.gsmsota.ua/blog/stati/parametry-kachestva-signalu-lte-4g> (дата звернення: 12.05.2026).
5. 4G/LTE – PHY Measurement. RSRQ (Reference Signal Recieved Quality)/ URL: https://www.sharetechnote.com/html/Handbook_LTE_RSRQ.html. (дата звернення: 12.05.2026).
6. Катков Ю. І., Березовська Ю. В., Пшеничний Ю. С., Рижаків М. М., Прокопов С. В. Аналіз загроз та вразливостей під час впровадження технології 4G/LTE // Телекомунікаційні та інформаційні технології. 2019. № 4. С. 25–38. DOI: 10.31673/2412-4338.2019.042538.
7. Ленков І. В., Фесенко П. О., Гусак Б. Т. Інструмент оцінки продуктивності бездротового зв'язку з безпілотниками у стільникових мережах 4G // Наукові записки Державного університету інформаційно-комунікаційних технологій. 2020. № 1. С. 28–34. DOI: 10.31673/2518-7678.2020.012834.
8. Ветошко І. П., Носков В. І. Evaluation of Voice Transmission Quality in the LTE Networks // Information and Telecommunication Sciences. 2021. Vol. 12, No. 2. P. 22–26. DOI: 10.20535/2411-2976.22021.22-26.
9. Кравчук С. О. Теорія систем мобільних інфокомунікацій системна архітектур: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2023. С. 199–206.

Надійшла до редколегії 08.05.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.3.049.77:621.382.8

д-р філософії Романенко М. М. ORCID: 0000-0002-0646-2797 (ВІТІ ім. Героїв Крут)

д-р філософії Погребняк С. В. ORCID: 0000-0002-7902-9847 (ВІТІ ім. Героїв Крут)

Кокошинський В. В. ORCID: 0000-0001-6364-6261 (ВІТІ ім. Героїв Крут)

ВПЛИВ ТЕХНОЛОГІЙ ВИГОТОВЛЕННЯ МІКРОЕЛЕКТРОНІКИ НА НАДІЙНІСТЬ ЕЛЕКТРОННИХ ЗАСОБІВ

Мікročип – головний елемент мікропроцесорної техніки, що складається з мільярдів транзисторів, які є одиницями і нулями в сучасних цифрових системах. І ось уже 50 років ведеться нескінченна технологічна гонитва за зменшенням розмірів цих елементів. Сучасні тенденції еволюції технологій у сфері комунікаційних систем окреслили перспективи та напрямки багатьох аспектів глобального розвитку людства в осяжному майбутньому.

Зменшення масогабаритних розмірів мікročипів відбувалось постійно, а кількість шарів транзисторів та їхня потужність подвоювалось що два-три роки.

Застосування способів літографії досить довгий час дозволяло отримувати бажані результати, а покращення технології її використання сприяло постійному розвитку цифрових систем. Проте ефективність існуючих методів створення мікропроцесорної техніки почала знижуватись з початком двадцять першого століття. Це стало відомим як “закон Мура” (Moore’s law). Тож провідні науковці в цій галузі почали пошук нових способів виготовлення мікročипів. Виходячи з широкого спектра галузей, де використовуються мікропроцесори, питання створення нових методів компонування мікročипів, яке б сприяло їх зменшенню, є актуальним.

У статті розглянуто варіанти існуючих методів створення мікročипів та проведено аналіз їхніх недоліків. Вивчено питання розвитку інноваційних методів та способи їх практичної реалізації. Обґрунтовано перспективи подальшого розвитку цієї галузі. Отримані числові показники масогабаритних розмірів мікročипів, створених за допомогою інноваційних методів, та запропоновано теоретичні основи подальшого розвитку напрямку літографії напівпровідникових мікроелементів. Визначено критичні параметри, які впливають на надійність мікропроцесорної техніки, в тому числі військового призначення.

Ключові слова: мікročип, мікроелектроніка, довжина хвилі, літографія, наноструктури, математична модель, надійність.

M. Romanenko, S. Pohrebniak, V. Kokoshynskyi. Impact of microelectronics manufacturing technologies on the reliability of electronic devices

A microchip is the main element of microprocessor technology, consisting of billions of transistors that are ones and zeros in modern digital systems. And for 50 years now, there has been an endless technological pursuit of reducing the size of these elements. Modern trends in the evolution of technologies in the field of communication systems have outlined the prospects and directions of many aspects of global development of mankind in the foreseeable future.

The reduction in the mass and overall dimensions of microchips occurred constantly, and the number of transistor layers and their power doubled every two to three years.

The use of lithography methods for a long time allowed to obtain the desired results, and the improvement of the technology of its use contributed to the constant development of digital systems. However, the efficiency of existing methods of creating microprocessor technology began to decline with the beginning of the twenty-first century. This became known as “Moore’s law”. Therefore, leading scientists in this field began to search for new methods of manufacturing microchips. Based on the wide range of industries where microprocessors are used, the issue of creating new methods of arranging microchips, which would contribute to their reduction, is relevant.

The article considers options for existing methods for creating microchips and analyzes their shortcomings. The issue of developing innovative methods and methods for their practical implementation is studied. The prospects for further development of this industry are substantiated. Critical parameters that affect the reliability of microprocessor technology, including military ones, are determined. Numerical indicators of the mass and overall dimensions of microchips created using innovative methods are obtained and theoretical foundations for further development of the direction of lithography of semiconductor microelements are proposed.

Keywords: microchip, microprocessor, wavelength, lithography, numerical aperture, laser, nanostructures, mathematical model.

Постановка завдання у загальному вигляді

В середині ХХ століття людство вступило в цифрову епоху. На перші місця в галузі електроніки та схемотехніки вийшли напівпровідникові радіоелектронні елементи, які стали витісняти аналогові елементи. Процес “цифровізації” почав набирати високого темпу і вже на початку 60-х років ХХ століття стало зрозуміло, що майбутнє за цифровою мікропроцесорною технікою.

Розміри та потужність мікрочипів збільшувались з експоненціальною швидкістю. Кількість транзисторів на кристалі мікросхеми подвоювалась кожні 24 місяці. Такий ефект (рис. 1) отримав назву “закон Мура” (Moore’s law).

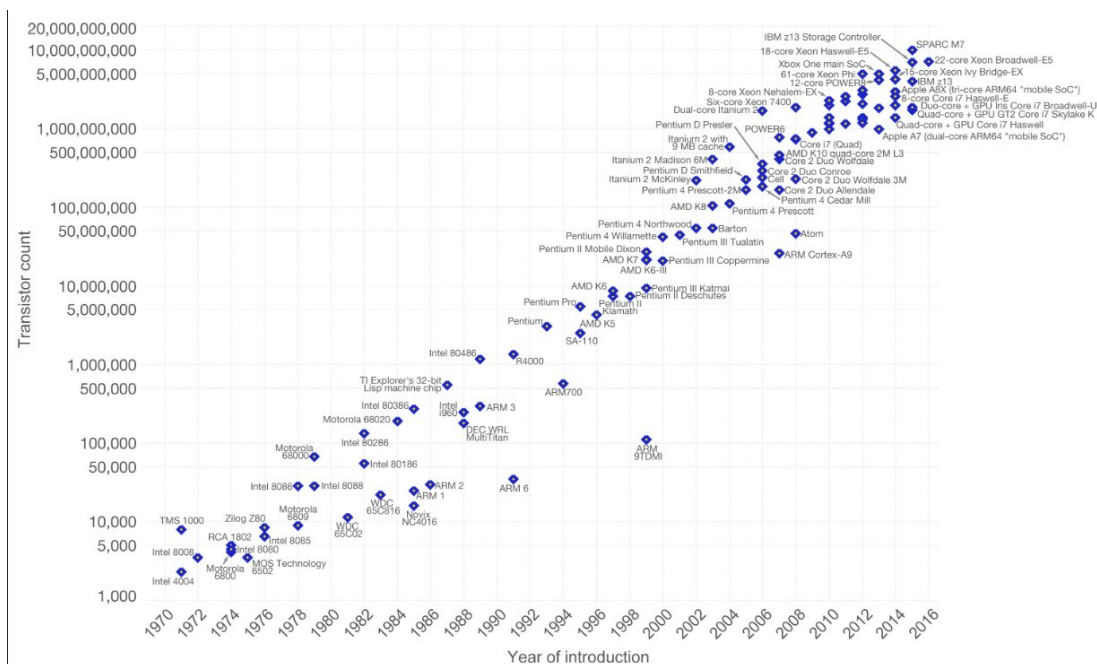


Рис. 1. Візуалізація “закону Мура” – збільшення кількості транзисторів в мікрочипах по роках впровадження

Зменшення розмірів мікрочипів сприяло розвитку багатьох напрямків та галузей по всьому світу: від засобів комунікації до автомобілебудування, від медицини до військової справи, від сільського господарства до космічних технологій – скрізь, де можливо було застосувати електронні обчислювальні машини, прогрес став неминучий.

На початку ери напівпровідників (1950-ті роки) чипи не “друкували” світлом, а збирали та формували фізично-хімічними методами:

Ручне проєктування та маскування: Перші мікросхеми створювали за допомогою ручного вирізання масок із пластику (матеріал Rubylith). Інженери буквально вирізали схеми на величезних аркушах, які потім фотографічно зменшували.

Метод дифузії та сплавлення: До появи планарної технології транзистори створювали шляхом сплавлення крапель металу (наприклад, індію) з германієвою пластиною або через термічну дифузію домішок у напівпровідник через металеві трафарети.

Вирощування кристалів (Метод Чохральського): це не спосіб нанесення схеми, а метод створення самої основи. Це фундамент, який існував до літографії й використовується досі для отримання надчистих зливків кремнію.

Електронно-променева літографія (EBL): вид літографії, вона працює без масок. Електронний промінь «малює» схему безпосередньо на поверхні. Це дає неймовірну точність, але метод занадто повільний для масового виробництва, тому його використовують лише для прототипів.

Проте на початку 2000-х років інженери зіткнулись з проблемою: зменшення розмірів стало неможливим через фізичну межу технологій, які використовувались для створення мікрочипів.

Звичайні методи літографії, такі як фотолітографія (Ultraviolet, UV; Deep Ultraviolet, DUV; Extreme Ultraviolet, EUV) здатні забезпечити розмірність елементів до 13,5 нм, проте такі розміри більше не задовольняють вимоги виробників. Критерієм, який уповільнив і зупинив цей напрям, стала довжина хвилі і неможливість зменшення числової апертури, який описується рівнянням Релея.

$$CD = k_1 \frac{\lambda}{NA}.$$

Мінімальний розмір елемента або критичний вимір (Critical Dimension, CD) можливо зменшити, виключно працюючи з меншою довжиною хвилі, так як розмір числової апертури неможливо збільшувати нескінченно. Порівняння двох різних довжин хвиль при однаковому розмірі “трафаретних” технологічних отворів в масках (рис. 2) згенеровано за допомогою Scientific Image Generator (2026) для наочної візуалізації процесів, що відбуваються. Саме зменшення довжини хвилі і відбувалось, поки індустрія не зупинилась на глибокому ультрафіолеті із довжиною хвилі 193 нм.

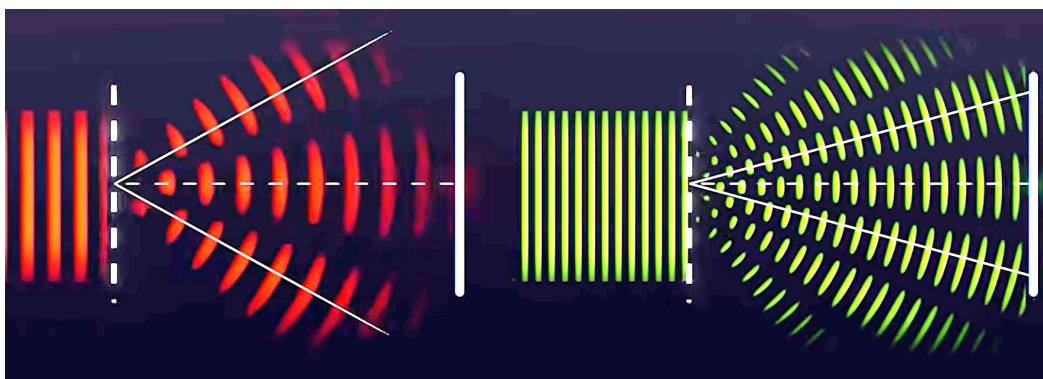


Рис. 2. Використання світла з коротшою довжиною хвилі для літографії при однакових значення числової апертури (згенеровано за допомогою Scientific Image Generator, 2026)

Аналіз останніх публікацій

Сучасний стан розробки мікропроцесорної бази ґрунтується здебільшого на широкому застосуванні сполук кремнію. Головні подібності та відмінності процесів розробки та створення кремнієвих мікрочипів (мікропроцесорів) та мікроелектронних систем і виробів мікроелектроніки представлені на рисунку 3.

Визначальним чинником, який впливає на вибір концепції виготовлення мікрочипів, є його розміри. Етап проєктування мікрочипа супроводжується тривимірним об'ємним моделюванням пошарової структури чипів. Необхідність моделювання електричних, механічних, кінематичних та інших процесів суттєво відрізняється при проєктуванні мікрокомпонентів [1].



Рис. 3. Подібність і відмінність процесів розробки й виготовлення кремнієвих мікрочипів і виробів мікроелектроніки

Однак не дивлячись на існування принципових відмінностей між різними концепціями, існують головні принципи літографії, які можна умовно спростити до чотирьох основних процесів: покриття, експонування, травлення, осаження. І такі процеси повторюються сотні циклів залежно від чипа [2].

У роботах [3–5] вивчалось питання можливості створення процесів літографії на основі теорії про нерівномірні щільності (Assumption of Uniform Pattern Density, AUPD), однак ця теорія не знайшла широкого розповсюдження через складність реалізації. В теорії стверджувалось, що розрахунок маски можливо здійснити через визначення оптимальної кількості таких щільностей:

$$I(r) = \sum_m \Gamma_m |h^m(r) \otimes M(r)| n^2,$$

де $M(r)$ представляє шаблон маски; r – просторова координата; $\otimes$ представляє операцію згортки; $h^m(r)$ – функція розсіювання точок літографічної системи, пов'язана з точкою джерела m ; Γ_m представляє інтенсивність точки джерела; n – кількість таких джерел.

Враховуючи ефект фоторезисту, зображення друку на пластині визначається як модель для вузлів передової літографії, модель візуалізації в рівнянні можна легко модифікувати, щоб включити тривимірні (3D) ефекти маски, замінивши M у рівнянні:

$$Z = \text{sig}\{I, t_r\} = 1 / \{1 + \exp[-a_r(I - t_r)]\},$$

де t_r – поріг фоторезисту;

a_r – визначає крутизну сигмоподібної функції.

У роботах [6–8] розглянуті теоретичні аспекти удосконалення літографії способом екстремального ультрафіолету (Extreme Ultraviolet, EUV). Однак обмежена яскравість джерела світла EUV та обмежена відбивна здатність багат шарових дзеркал висувають нові вимоги до чутливості фоторезистів. Крім того, характеристики формування структури EUV з високою роздільною здатністю вимагають резистивних матеріалів з меншими розмірами компонентів та вищою стійкістю до травлення. Таким чином, розробка фоторезистів з новими характеристиками EUV залишається проблемою.

У роботах [9; 10] розглянуто еволюцію EUV фоторезистів, включаючи хімічно посилені резисти, нехімічно посилені полімерні резисти, молекулярні скляні резисти та металовмісні резисти, а також майбутні тенденції розвитку EUV-чутливих матеріалів. Роботи синтезують результати існуючих досліджень, щоб висвітлити фундаментальні принципи, характеристики продуктивності та практичні проблеми кожного методу. Порівняння зосереджено на ключових метриках, включаючи роздільну здатність, глибину фокусування, дозу опромінення, шорсткість краю лінії, точність накладання та пропускну здатність, показуючи, як різні підходи балансують ці конкуруючі фактори. Висунута гіпотеза про можливість використання випромінювання з меншою довжиною хвилі, а саме рентгенівського випромінювання.

У статті [11] досліджується розвиток, концепції та напрямки вдосконалення основних методів літографії, включаючи літографію в екстремальному ультрафіолетовому діапазоні (EUV), електронно-променеву літографію (EBL), рентгенівську літографію (XRL), іонно-променеву літографію (IBL) та наноімпринтну літографію (NIL). Проводиться аналіз, включаючи визначення принципів, роздільної здатності та резистивних матеріалів. EUV-літографія з роздільною здатністю менше 10 нм є життєво важливою для розширення закону Мура. Така технологія застосовує оптичні системи з високою числовою апертурою (NA) та хімічно підсилені резисти. EBL та IBL дають можливість створювати безмаскові шаблони для створення прототипів, проте недоліком є низька продуктивність. Технологія XRL, застосовуючи принцип синхротронного випромінювання, здатна забезпечити високу роздільну здатність, тоді як NIL забезпечує економічно ефективний метод високої продуктивності для реплікації наноструктур.

Мета статті полягає в аналізі розвитку технології фотолітографії для компонування наноструктур мікропроцесорної техніки з використанням довжин хвиль рентгенівського випромінювання та її вплив на надійність цих елементів.

Виклад основного матеріалу. На початку 80-х років була висунута ідея про можливість використання для фотолітографії хвиль рентгенівського випромінювання із довжиною близько 10 нм. Що в теорії давало б змогу друкувати елементи в рази менші за розмірами, ніж це можливо при використанні видимого спектра частот. Однак одразу було виявлено проблему: рентгенівські промені мають достатню енергію, щоб вибивати електрони з атомів, тож більшість матеріалів його просто поглинають. Але одночасно з цим вони поглинаються і повітрям. Тож це означає, що таке устаткування має працювати у вакуумі. Але ще однією проблемою стало неможливість використання фокусуючих лінз, адже лінзи теж поглинали таке світло.

Однак були розроблені дзеркала, які могли фокусувати рентгенівське світло. Такі дзеркала являли собою багатократне чергування надтонких (близько 1 нм) шарів вольфраму та вуглецю, що давало можливість створити сферичне дзеркало. Для кожної довжини хвилі необхідне чітко визначена кількість таких шарів. Для довжини хвилі 4,48 нм, яка досліджувалась, кількість таких шарів складала 76.

На початкових етапах проводились експерименти з довжинами хвиль від 4 нм до 13 нм. Проте практичні досліди виявили, що після проходження всіх дзеркал до кінцевої точки доходило лише 0,00128 % від початкової потужності, що стало критично малою величиною [11].

Для подолання зазначеної проблеми застосовують процес, який базується на нагріванні лазером, потужністю 1700 Вт, цільового матеріалу – олова до температури 220 000 °С. При цьому електрони отримують настільки велику енергію, що ядро їх більше не може утримувати, і до половини кількості електронів залишають свої орбіти. Після припинення впливу лазера електрони рекомбінують і створюють плазму, при цьому вивільняється енергія з потрібною довжиною хвилі близько 13,4 нм. Для кращої візуалізації фізичних процесів рекомбінації, що відбуваються, використано штучний інтелект (згенеровано за допомогою Scientific Image Generator, 2026) (рис. 4).

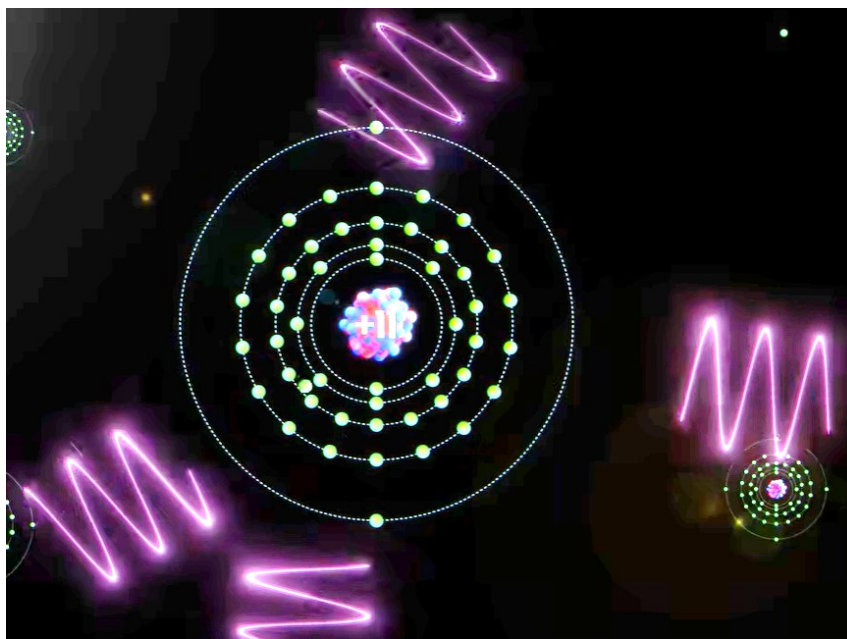


Рис. 4. Процес створення плазми за допомогою лазера
(згенеровано за допомогою Scientific Image Generator, 2026)

Для отримання ще стабільнішого процесу застосовуються подача олова в рідкому стані під великим тиском для створення безперервного потоку надтонкого променю, на який здійснюється вплив лазерного потоку з частотою 50 000 спалахів на секунду.

Щоб зменшити вплив сусідніх крапель олова, запропоновано кожен краплю піддавати впливу лазера три рази поспіль. Перший вплив змінює форму краплі з “кулі” на “диск”, що збільшує площу для наступного “пострілу”. Третій вплив створює безпосередньо плазму, яка вивільняє потрібну довжину хвилі. Для розрахунку такого процесу застосовують формулу Тейлора-фон Неймана-Седова (1):

$$R(t) = \left(\frac{Et^2}{\rho_0} \right)^{1/5}. \quad (1)$$

Ця формула описує автомодельне вирішення для потужного точкового вибуху. Визначає радіус $R(t)$ ударної хвилі та через енергію E вибуху щільність середовища ρ_0 та час t .

Застосувавши (1) для визначення енергії, отримаємо:

$$E = \frac{R^5 \rho_0}{\beta^5 t^2}, \quad (2)$$

де R (радіус) – на яку відстань відійшла ударна хвиля (можна виміряти по фото);

t (час) – скільки мілісекунд минуло з моменту спалаху до цього моменту;

ρ_0 (густина) – густина газової суміші, в якій відбувається вибух;

β (коефіцієнт) – безрозмірна константа, яка для повітря становить приблизно 1,033.
Враховуємо, що енергія електромагнітної хвилі визначається як (3):

$$E = \frac{hc}{\lambda}, \quad (3)$$

де E – енергія фотона (кванту електромагнітного випромінювання);
 h – стала Планка $6,626 \cdot 10^{-34}$ Дж/с;
 c – швидкість світла.

Об'єднавши (2) і (3), отримаємо, що довжина хвилі λ обернено пропорційна густині середовища ρ_0 , в якій вона розповсюджується, прийнявши решту змінних за *const*.

$$\frac{hc}{\lambda} = \frac{R^5 \rho_0}{\beta^5 t^2} \rightarrow \lambda = \frac{hc \beta^5 t^2}{R^5 \rho_0} = \frac{6,626 \cdot 10^{-34} \cdot 3 \cdot 10^8 \cdot 1,033^5 \cdot 10^{-10}}{10^{-26} \cdot 0,7} = 3,273 \cdot 10^{-9}.$$

Отже, можливо отримати необхідну довжину хвилі шляхом збільшення густини газів в літографічній камері. Нині інженери використовують водень під високим тиском, проте густина водню складає лише $0,09 \text{ кг/м}^3$. Якщо ж в літографічну камеру додати кисень з густиною $1,43 \text{ кг/м}^3$ (у необхідній пропорції), теоретично можливо збільшити густину до $0,5\text{--}0,7 \text{ кг/м}^3$, що в свою чергу може зменшити довжину хвилі з $13,5 \text{ нм}$ до $7\text{--}7,5 \text{ нм}$. Таким чином, перехід на довжину хвилі 7 нм дозволив би друкувати транзистори з критичним розміром (найменшим елементом) приблизно $3,27\text{--}3,5 \text{ нм}$ за один прохід експонування.

Додавання кисню в камеру літографічного апарату також дозволить покращити стан самих дзеркал (збільшить час їх роботи без необхідності очищення), так як кисень, рекомбінуючи з іонами водню, створюватиме захисне покриття.

Проте окрім проблематики зі зменшення наноструктур виникає питання їхньої надійності через зменшення їхніх розмірів. Теорія надійності мікропроцесорної техніки обумовлює теоретичні допуски межі та критичні розміри для наноструктур, оскільки процес фізичної деградації мікропроцесорної техніки відбувається в процесі експлуатації [12].

$$I_{mc}^{0,1} = -\frac{2dD_n}{\mu n L_n (R_{дн3}^0 + R_{дн2}^0)} \operatorname{csch} \frac{W}{L_n} n_1 + \frac{2dD_n}{\mu n L_n (R_{дн3}^0 + R_{дн2}^0)} \operatorname{cth} \frac{W}{L_n} n_2,$$

де W – ширина бази (елемента);
 L_n – довжина дифузії (зменшується при накопиченні деградації);
 D_n – коефіцієнт дифузії дефектів;
 $R_{дн3}^0$ – значення опорів донорського шару.

При мінімізації $W \rightarrow$ аргумент $\operatorname{csch}/\operatorname{cth}$ зростає.

Зазначену модель використовують для різних типів мікрочипів з метою отримання діагностичного параметра базового логічного елемента транслятора напівпровідникової інтегральної схеми у вигляді величини струму залежно від фізико-хімічних властивостей напівпровідника і залежно від часу напрацювання.

Існуюча діагностична модель інтегральних мікросхем описує колекторні струми в структурах транзисторів вихідного транслятора, що дає можливість розрахувати час напрацювання таких елементів при зменшенні структур аж до нанорівнів.

Для підтвердження цієї теорії було проведено математичне моделювання в середовищі Python з використання бібліотеки Matplotlib з репрезентативною вибіркою 126 ітерацій.

У процесі моделювання отримані показники (рис. 5), що підтверджують істотне збільшення процесу деградації наноструктур. Основні показники зведено в таблицю 1.

Таблиця 1

№	D_n ($\text{см}^2/\text{с}$)	μ_n ($\text{см}^2/(\text{В}\cdot\text{с})$)	L_n (мкм)	W (нм)	$R_{\text{днз}}^0$ (Ом)	n_1 (см^{-3})	n_2 (см^{-3})	Орієнтовний час напрацювання $\cdot 10^3$ (год)
1	25	1500	10	180	50	$1\text{e}15$	$5\text{e}15$	$\sim 100\,000$
2	30	1200	15	90	80	$2\text{e}15$	$6\text{e}15$	$\sim 9\,500$
3	20	1000	8	14	40	$1\text{e}14$	$3\text{e}15$	$\sim 8\,000$
4	35	1800	20	7	100	$5\text{e}15$	$1\text{e}16$	~ 700

Основні показники розрахункової математичної моделі часу напрацювання наноструктур.

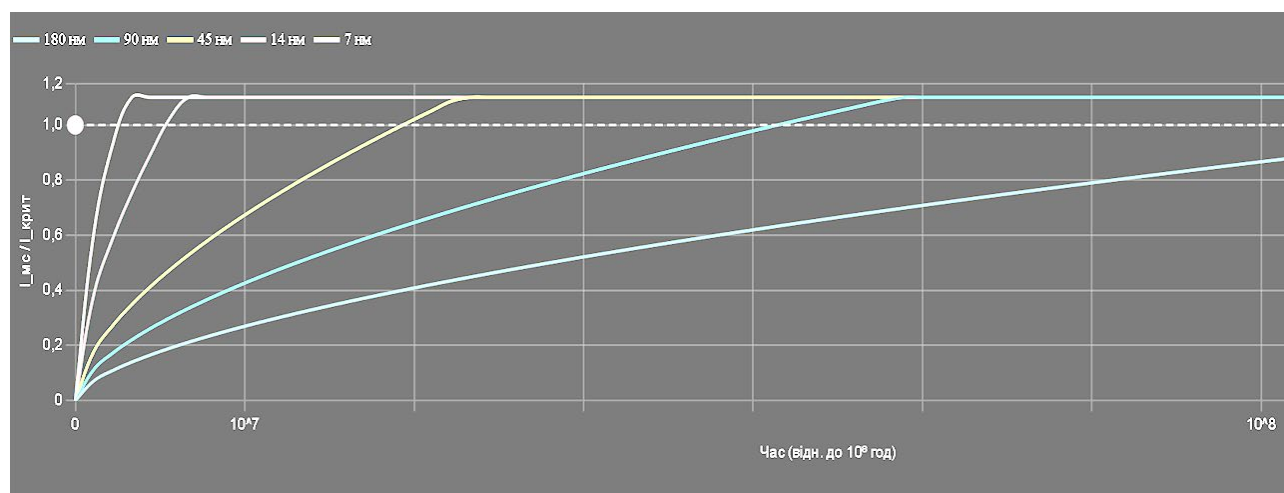


Рис. 5. Моделювання процесів фізичної деградації наноструктур залежно від розмірів (180 нм, 90 нм, 14 нм, 7 нм) та розрахунковий час напрацювання

У процесі моделювання отримано значення, що чітко відображають зменшення часу напрацювання з 10^8 годин при структурі у 180 нм до 10^6 годин при структурі у 7 нм.

Подальше кратне зменшення розмірів наноструктур до 3,5 нм теоретично призведе до зменшення часу напрацювання таких елементів до 10^4 годин. Що в свою чергу негативно вплине на загальний час експлуатації електронних засобів. Ця теорія потребує перевірки в лабораторних умовах та поки що не може бути підтверджена чи спростована шляхом натурних експериментів.

Таким чином, питання зменшення розмірів мікрочипів обмежується не лише “законом Мура”, а й вимогами до надійності та довговічності зазначених зразків, що особливо актуально для наноструктур, які використовуватимуться в системах військового або подвійного призначення.

Висновки і перспективи подальших досліджень

У роботі розглянуто існуючі технології літографії. Здійснено порівняння їхніх основних особливостей. Визначено головні відмінності та параметри, які забезпечують економічну доцільність їх використання в майбутньому. Проаналізовано перспективні напрямки розвитку технології літографії в екстремальному ультрафіолеті. Запропоновано спосіб удосконалення існуючої технології для зменшення довжини хвилі. Проведено математичні розрахунки для підтвердження запропонованої теорії. Одночасно з цим вирішена наукова задача визначення залежності надійності мікропроцесорної техніки від величини напівпровідникових структур.

Дані підтверджені математичним моделюванням процесів фізико-хімічної деградації структур напівпровідникових елементів. Подальшим напрямком роботи вбачається розробка оптимізації процесу літографії в екстремальному ультрафіолеті для отримання довжин хвиль рентгенівського випромінювання з урахуванням вимог до надійності та довговічності електронних засобів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Zafar F. Indium phosphide nanowires and their applications in optoelectronic devices / Fateen Zafar and Azhar Iqbal // Proc. Math. Phys. Eng. Sci. 2016. No. 472 (2187). P. 20150804.
2. Pumarol-Crestar M. E. Gold nanodot and nanowire fabrication by Atomic Force Microscopy / Manuel E. Pumarol-Crestar. Centre for the Physics of Materials Department of Physics, McGill University, Montreal, Canada, 2008. 137 p.
3. Ван С. Ма, Г. Р. Арсе та ін. Інформаційно-теоретичні підходи в обчислювальній літографії // Opt. Express. 2018. No. 26 (13). P. 16736–16751.
4. X. Ma, Z. Wang, L. Yanqiu et al. Fast optical proximity correction method based on nonlinear compressivesensing // Opt. Express. 2018. No. 26 (11). P. 14479–14498.
5. Scaling EUV and holistic lithography to support Moore's Law through the AI era Event: SPIE Advanced Lithography + Patterning, 2025, San Jose, California, United States Proceedings Volume PC13424, Optical and EUV Nanolithography XXXVIII, PC1342401. 2025. URL: <https://doi.org/10.1117/12.3059296>.
6. Jinhui Lai. A Review of Extreme Ultraviolet Lithography and Its Future Development Trends Advances in Engineering Technology Research Maynooth International Engineering College, Fuzhou University, Fuzhou, China Volume-14-2025. DOI: 10.56028/aetr.14.1.1608.2025.
7. Harry J. Levinson. Extreme Ultraviolet Lithography, 2nd Edition // SPIE Press. 2025. DOI: 10.1117/3.100387, ISBN: 9781510692541.
8. Xiaolin Wang, Peipei Tao, Qiangian Wang, Rongbo Zhao, Tiangi Liu, Yang Hu, Ziyu Hu, Yimeng Wang, Jianlong Wang, Yaping Tang, Hong Xu. Trends in photoresist materials for extreme ultraviolet lithography: A review // Materials Today. Volume 67. July–August 2023. P. 299–319. DOI: 10.1016/j.mattod.2023.05.027.
9. Dimitrios Kazazis, Jara Garcia Santaclara, Jan Schoot, Iacopo Mochi, Yasin Ekinci. Extreme ultraviolet lithography // Nature Reviews Methods Primers. 2024. DOI: 10.1038/s43586-024-00361-z.
10. Sunyu Jiang. Research on Fundamental Principles and Performance Optimization Strategies in Lithography Technology University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, China Proceedings of CONF-MCEE 2026 Symposium: Advances in Sustainable Aviation and Aerospace Vehicle Automation. DOI: 10.54254/2755-2721/2026.KA26665.
11. Prithvi Basu, Jyoti Verma, Vishnuram Abhinav. Advancements in Lithography Techniques and Emerging Molecular Strategies for Nanostructure Fabrication // International Journal of Molecular Sciences (IJMS). March 2025. DOI: 10.3390/ijms26073027.
12. Жердєв М. К., Кузавков В. В. Діагностична модель базового логічного елементу транслятора напівпровідникової інтегральної схеми для безконтактного індукційного методу діагностування // Collection of Scientific Papers of Military Institute of Taras Shevchenko National University of Kyiv. 2014. № 46. С. 13–18.

Надійшла до редколегії 12.02.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.039

Руденко В. І. ORCID: 0000-0003-3563-548X (ВІТІ ім. Героїв Крут)
Зінченко М. О. ORCID: 0000-0002-1428-8231 (ВІТІ ім. Героїв Крут)
Яковчук О. В. ORCID: 0000-0002-6312-5009 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ НОРМАТИВНОЇ БАЗИ ТА ЇЇ ФУНКЦІОНАЛЬНОЇ МОДЕЛІ З ВИЗНАЧЕННЯМ ШЛЯХІВ УДОСКОНАЛЕННЯ ЕЛЕКТРОННОЇ КОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У статті проводиться дослідження законодавства України у сфері електронних комунікацій, на підставі якого визначаються підсистеми та пропонується до розгляду нова модель електронної комунікаційної системи ЗС України. Основне визначення електронної комунікаційної системи, склад, назви та призначення підсистем відповідають чинним нормативним документам України у сфері електронних комунікацій. У складі системи розглядається найважливіший її елемент – електронна комунікаційна мережа, яка є складовою частиною та матеріальною основою системи управління військами (силами).

Електронна комунікаційна мережа спеціального призначення будується на ресурсах електронної комунікаційної мережі ЗС України та електронної комунікаційної мережі загального користування. У роботі аналізується структура, ефективність функціонування електронної комунікаційної мережі, розробляються напрямки удосконалення нормативної бази та електронної комунікаційної мережі ЗС України. Пропонується до розгортання стаціонарна компонента електронної комунікаційної мережі ЗС України, яка створюється на використанні власних ліній електронних комунікаційних мереж, що призведе до забезпечення оперативного, надійного та безперебійного управління військами, значного скорочення часу надання електронних комунікаційних послуг, необхідної швидкості передачі інформації та ряд інших переваг стосовно оренди каналів (потоків) в електронній комунікаційній мережі загального користування. Обґрунтовується потреба в розгортанні мобільної (рухомої) компоненти й визначаються напрямки її удосконалення для надання та відновлення електронних комунікаційних послуг, нарощування та резервування стаціонарної компоненти електронної комунікаційної мережі ЗС України силами й засобами частин і підрозділів зв'язку.

Запропонована модель електронної комунікаційної мережі ЗС України може стати основою системи управління військами (силами) та будуватися з дотриманням стандартів, доктрин і рекомендацій України та країн-партнерів. Мережа повинна бути інтегрована з електронними комунікаційними мережами сил оборони та електронною комунікаційною мережею загального користування з метою забезпечення єдиного інформаційного простору. Отже, результати дослідження мають практичну значущість для удосконалення електронної комунікаційної мережі ЗС України та підвищення бойової готовності військ у мирний час, в умовах надзвичайної ситуації, надзвичайного або воєнного стану.

Ключові слова: електронні комунікації, електронна комунікаційна система, електронна комунікаційна мережа, дослідження, нормативні документи, напрямки удосконалення.

V. Rudenko, M. Zinchenko., O. Yakovchuk. Research of the regulatory framework, analysis of the efficiency of the functioning and directions for improvement of the special-purpose electronic communication network

The article studies the legislation of Ukraine in the field of electronic communications, on the basis of which subsystems are defined and a new model of the electronic communication system of the Armed Forces of Ukraine is proposed for consideration. The basic definition of the electronic communication system, the composition, names and purpose of the subsystems correspond to the current regulatory documents of Ukraine in the field of electronic communications. The system considers its most important element - the electronic communication network, which is an integral part and material basis of the military (forces) command system.

The special-purpose electronic communication network is built on the resources of the electronic communication network of the Armed Forces of Ukraine and the general-purpose electronic communication network. The paper analyzes the structure and effectiveness of the electronic communication network, and develops directions for improving the regulatory framework and the electronic communication network of the Armed Forces of Ukraine. It is proposed to deploy a stationary component of the electronic communication network of the Armed Forces of Ukraine, which is created using its own lines of electronic communication networks, which will ensure operational, reliable and uninterrupted command of troops, a significant reduction in the time for providing electronic communication services, the required speed of information transmission and a number of other advantages regarding the rental of channels (streams) in the general-purpose electronic communication network. The need for the deployment of a mobile (mobile) component is justified and directions for its improvement are determined for the provision and restoration of electronic communication services, the expansion and backup of the stationary component of the electronic communication network of the Armed Forces of Ukraine by the forces and means of communication units and divisions.

The proposed model of the electronic communication network of the Armed Forces of Ukraine can become the basis of the command and control system of troops (forces) and be built in compliance with the standards, doctrines and recommendations of Ukraine and NATO member states. The network should be integrated with the electronic communication networks of the defense forces and the general electronic communication network in order to ensure a single information space. Therefore, the results of the study have practical significance for improving the electronic communication network of the Armed Forces of Ukraine and increasing the combat readiness of troops in peacetime, in conditions of an emergency, state of emergency or martial law.

Keywords: *electronic communications, electronic communications system, electronic communications network, research, regulatory documents, areas for improvement.*

Вступ

Російсько-українська війна показала необхідність розвитку електронної комунікаційної мережі ЗС України, яка є основою управління військами (силами). Це пояснення випливає з того, що електронна комунікаційна мережа, яка діє, не повною мірою задовольняє потреби управління військами, вимагає зусиль з модернізації із впровадженням інноваційних технологій. Ефективно управляти військами можна буде тільки в результаті технічного переоснащення електронної комунікаційної мережі та розширення номенклатури послуг, що надаються.

1. Постановка задачі

На підставі чинної законодавчої бази України у сфері електронних комунікацій ставиться задача розробити нову модель електронної комунікаційної системи ЗС України (далі – ЕКС ЗС України) з урахуванням змін в нормативній базі України, визначається завдання модернізації електронної комунікаційної мережі ЗС України (далі – ЕКМ ЗС України) на базі будівництва власних ліній електронних комунікаційних мереж з використанням їхнього ресурсу. Для надання електронних комунікаційних послуг, нарощування та резервування стаціонарної електронної комунікаційної мережі ЗС України обґрунтовується потреба в розгортанні мобільної (рухомої) компоненти. Дана компонента повинна розвиватися в напрямку зменшення масогабаритних показників, потужності випромінювання, з підвищенням мобільності, швидкості передачі інформації, розвід- та завадозахищеності, із застосуванням сучасних технічних засобів електронних комунікацій.

Такі моделі слід розробляти відповідно до стандартів, доктрин і рекомендацій України та країн-партнерів з урахуванням сучасних способів ведення війни з російською федерацією, тенденцій розвитку електронних комунікаційних систем армій провідних країн світу та новітніх досягнень інформаційних технологій у сфері електронних комунікацій.

2. Аналіз досліджень нормативної бази

У сучасних умовах, особливо під час ведення війни, сфера електронних комунікацій привертає все більшу увагу законодавчої та виконавчої влади України до аналізу, дослідження, удосконалення та розроблення нормативно-правової бази в цій сфері. У цьому розділі ми визначаємо та проводимо дослідження основної законодавчої бази у сфері електронних комунікацій, яка діє в Україні та в ЗС України.

Закон [1] встановлює правову основу діяльності у сфері електронних комунікацій, забезпечує надання та отримання електронних комунікаційних послуг і визначає засади захисту прав споживачів та контролю за ринком електронних комунікацій з боку держави.

Програма [2] регламентує правові відносини під час формування та виконання Національної програми інформатизації, забезпечує розвиток інформаційного суспільства та визначає особливості реалізації державної політики у сфері інформатизації.

Закон [3] упорядковує відносини щодо створення, накопичення, одержання, збереження, використання, поширення, охорони та захисту інформації. Встановлює основні принципи інформаційних відносин до збереження, цілісності інформації та доступу до неї.

Документи [4; 5] регулюють відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та встановлюють принципи державної політики у сфері забезпечення кібербезпеки.

Нормативно-правовий акт [6] визначає основи діяльності у сфері надання послуг поштового зв'язку, а також регулює відносини між органами державної влади, органами місцевого самоврядування, операторами поштового зв'язку і користувачами послуг.

Постанова [7] регулює питання, пов'язані з управлінням електронними комунікаційними мережами загального користування і затверджує Порядок створення та діяльності Національного центру оперативно-технічного управління електронними комунікаційними мережами України.

Доктрина [8] забезпечує загальне стратегічне керівництво із застосування зв'язку та інформаційних систем у ЗС України та інших складових сил оборони, вводить термінологію в галузі зв'язку та інформаційних систем.

Настанова [9] зі зв'язку визначає загальні положення щодо організації розгортання та функціонування системи зв'язку ЗС України й забезпечує загальне керівництво управління під час підготовки та ведення операцій (бойових дій) ЗС України та інших складових сил оборони.

Концепція [10] створює умови впровадження сервіс-орієнтованої архітектури, забезпечує розгортання відмовостійкої електронної комунікаційної мережі ЗС України та надає опис функціоналу її основних елементів.

Стратегія [11] формує умови використання Єдиного інформаційного середовища оборони шляхом застосування єдиних стандартів, протоколів, архітектур для надання необхідних сервісів.

Доктрина [12] є базовим керівним документом, який визначає загальні підходи з питань забезпечення матеріально-технічними засобами, роботами та послугами органів військового управління ЗС України та інших складових сил оборони.

Таким чином, провівши аналіз основних нормативних документів та публікацій можна зробити висновок, що на сьогодні існує багато матеріалів і статей з удосконалення електронних комунікацій, але не існує узагальнених робіт, які спирались на чинну нормативну базу України та ЗС України.

Виходячи з цього, виникає наукове завдання щодо вдосконалення моделі електронних комунікацій ЗС України та її нормативної бази.

Тому метою цієї статті є вдосконалення законодавчої бази ЗС України у сфері електронних комунікацій, на підставі чого розробляються нові моделі електронної комунікаційної системи та електронної комунікаційної мережі ЗС України на базі розгорнутих ліній електронних комунікаційних мереж для переходу на якісно новий рівень функціонування системи управління військами (силами) із застосуванням останніх досягнень та інновацій у сфері електронних комунікацій.

Виклад основного матеріалу дослідження

3. Дослідження законодавства України у сфері електронних комунікацій, визначення основних її складових та розроблення нової моделі електронної комунікаційної системи ЗС України

Законодавча база у сфері електронних комунікацій складається з Конституції України, Законів України “Про електронні комунікації”, “Про Національну програму інформатизації”, “Про інформацію”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України” інших законодавчих актів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

3.1. Дослідження нормативних документів у сфері електронних комунікацій України

Аналіз основних нормативних документів України, які регламентують діяльність у сфері електронних комунікацій.

3.1.1. Закон України “Про електронні комунікації” [1] – основний нормативно-правовий акт, який визначає правові та організаційні основи державної політики у сфері електронних комунікацій. Дія документа поширюється на відносини щодо надання та отримання електронних комунікаційних послуг, постачання та доступу до електронних комунікаційних мереж і забезпечення конкуренції на ринках електронних комунікацій. В акті надається визначення: електронна комунікація (телекомунікація) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій; а також, що таке: абонент, електронна комунікаційна мережа, електронна комунікаційна мережа загального користування, мережа Інтернет, доступ та ряд інших термінів, які застосовуються у сфері електронних комунікацій. Цей нормативно-правовий акт скасовує дію Закону України “Про телекомунікації”.

3.1.2. Закон України “Про Національну програму інформатизації” [2] – спрямований на розвиток інформаційного суспільства шляхом концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави, координації діяльності державних органів, органів місцевого самоврядування, а також підприємств, установ, організацій незалежно від форми власності.

3.1.3. Закон України “Про інформацію” [3] – регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації.

У цьому документі застосовуються наступні терміни: документ, захист інформації, інформація, а також визначаються основні принципи інформаційних відносин, державна інформаційна політика, суб'єкти та об'єкти інформаційних відносин, права та гарантії на інформацію. Інформація поділяється на види за змістом.

3.1.4. Закон України “Про захист інформації в інформаційно-комунікаційних системах” [4] – регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації. Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: володільці інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи. У цьому документі наводяться визначення основних термінів із захисту інформації.

3.1.5. Закон України “Про основні засади забезпечення кібербезпеки України” [5] – визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини й громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

3.1.6. Закон України “Про поштовий зв'язок” [6] – визначає правові, соціально-економічні та організаційні основи діяльності у сфері надання послуг поштового зв'язку. Відповідно до законодавства проводиться діяльність у сфері надання послуг поштового зв'язку спеціального призначення, фельд'єгерського зв'язку (урядового фельд'єгерського зв'язку, відомчого фельд'єгерського зв'язку у складі ЗС України). У цьому документі також вживаються терміни відповідно до наданих визначень.

Дії цих законів доповнюють ряд інших Постанов та Розпоряджень, наприклад, таких як: Постанови Кабінету Міністрів України № 75 [7] та № 890-038, № 920-013 (знаходяться на стадії переопрацювання), які регламентують діяльність у сфері електронних комунікацій.

На підставі чинної нормативно-правової бази України у сфері електронних комунікацій у ЗС України розробляється та діє своя нормативна база, яка регулює цю сферу.

3.2. Дослідження нормативних документів ЗС України у сфері електронних комунікацій

Нормативна база ЗС України у сфері електронних комунікацій складається з наступних основних документів: Доктрина “Зв’язок та інформаційні системи” [8]; Настанова “Зі зв’язку Збройних Сил України” [9]; Концепція побудови Електронної комунікаційної мережі Збройних Сил України [10]; Концепція розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України [11]; Стратегія розвитку системи зв’язку ЗС України; Загальні вимоги; Технічне завдання; Військові стандарти та ряд інших документів.

Основним нормативним документом ЗС України та складових сил оборони, який забезпечує загальне керівництво з управління зв’язком та інформаційними системами, є *Доктрина “Зв’язок та інформаційні системи”* [8]. Це керівництво визначає загальні положення із планування та застосування зв’язку та інформаційних систем. У цьому документі застосовуються терміни, принципи, управління військами (силами), загальна архітектура побудови, аспекти взаємосумісності зі зв’язку та інформаційних систем. Викладено функції та завдання посадових осіб та структур, розглянуто планування та застосування зв’язку та інформаційних систем. Зазначений документ розроблений з урахуванням вимог союзної об’єднаної публікації НАТО AJP-06 “Allied Joint Doctrine for Communication and Information Systems (Edition B Version 1)”.

Після детального дослідження діючої нормативної бази ЗС України у сфері електронних комунікацій можна зробити висновок, що ці документи мають деякі розбіжності в структурі, формулюваннях та не завжди визначають один підхід до архітектури та термінології ЗС України.

Водночас, чинні нормативні документи ЗС України, на наш погляд, не завжди відповідають Закону України “Про електронні комунікації”, іншим Законам, Постановам та Розпорядженням України. Наприклад, такі терміни, як: “зв’язок”, “система зв’язку”, “телекомунікації”, “телекомунікаційні системи”, “телекомунікаційні мережі”, “інформаційно-телекомунікаційна система” та інші в законодавчій базі України нині не використовуються.

Висновки.

За результатами проведеного дослідження нормативної бази у сфері електронних комунікацій можна констатувати, що:

1. Нормативно-правові акти та постанови України мають найвищу юридичну силу та встановлюються органами законодавчої й виконавчої влади України, визначають правові та організаційні основи державної політики у сфері електронних комунікацій та є гармонізованими з документами Міжнародного союзу електрозв’язку (МСЕ), Європейського Кодексу електронних комунікацій, Європейської конференції адміністрацій пошт та телекомунікацій (СЕРТ), Європейської комісії з комунікацій (ЕСС) та відповідають зобов’язанням України Європейській інтеграції та праву Європейського Союзу.

2. Нормативна база ЗС України потребує додаткового дослідження та вдосконалення з урахуванням внесених змін у Законах, Постановах України та публікацій країн-партнерів.

3.3. Наукове обґрунтування підсистем електронної комунікаційної системи ЗС України та визначення її основних термінів

На підставі проведеного наукового дослідження чинних нормативних документів України у сфері електронних комунікацій визначаються та пропонуються до розгляду склад, назви та призначення підсистем електронної комунікаційної системи ЗС України з визначеннями її основних термінів.

3.3.1. Система управління та моніторингу

Система управління та моніторингу призначена для забезпечення централізованого управління та моніторингу інфраструктурою ЕКС ЗС України з використанням автоматичних

і автоматизованих механізмів визначення причин можливих збоїв, а також для автоматизації діяльності служби підтримки з підвищення якості надання комунікаційних послуг.

3.3.2. Електронна комунікаційна мережа ЗС України

Електронна комунікаційна мережа ЗС України є складовою частиною електронної комунікаційної системи ЗС України і являє собою комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг (сервісів).

Електронна комунікаційна мережа – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг [1].

ЕКМ ЗС України забезпечує маршрутизацію, комутацію, передавання та/або приймання послуг (знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду) по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

3.3.3. Система захисту інформації та кібербезпеки [4; 5]

Система захисту інформації та кібербезпеки електронної комунікаційної системи ЗС України – це сукупність сил, засобів і підсистем кіберзахисту, яка призначена для запобігання несанкціонованим діям щодо інформації в ЕКС та кіберінцидентам, виявлення та реагування на кіберінциденти та кібератаки, ліквідації їх наслідків. Вона є єдиною для ЗС України та будується відповідно до моделі багатоєшелонованої системи захисту інформації та кібербезпеки, що передбачає наявність та функціонування базових систем захисту інформації й кіберзахисту в кожному з п'яти ешелонів (ешелоні захисту периметра, ешелоні захисту мереж, ешелоні захисту кінцевих пристроїв (хостів), ешелоні захисту програмного забезпечення, ешелоні захисту даних).

3.3.4. Мережа фельд'єгерського зв'язку

Мережа фельд'єгерського зв'язку – сукупність вузлів, станцій, відділень, обмінних пунктів та пунктів обміну фельд'єгерського зв'язку, засобів доставлення (наземних, водних, повітряних), маршрутів їх руху, яка організована для приймання, обробки, перевезення та доставлення (вручення) відправлень, що містять відомості, які становлять державну таємницю, та/або службову інформацію, окремим категоріям користувачів у системі МО України та ЗС України у мирний час, в умовах надзвичайної ситуації, надзвичайного або воєнного стану.

Відомчий фельд'єгерський зв'язок у складі ЗС України – приймання, обробка, перевезення та доставлення (вручення) відправлень, що містять відомості, які становлять державну таємницю, та/або службову інформацію, окремим категоріям користувачів у системі Міністерства оборони України в мирний час та в особливий період [6].

3.3.5. Система матеріально-технічного забезпечення

Система матеріально-технічного забезпечення – це сукупність взаємопов'язаних структурних підрозділів логістики органів військового управління, які здійснюють планування та забезпечення матеріально-технічними засобами, роботами та послугами військ (сил) зв'язку на всіх рівнях військового управління та призначена для організації постачання ЗС України матеріально-технічних засобів, виконання покладених на них завдань і функцій, організації забезпечення матеріально-технічними засобами, роботами та послугами в їхній повсякденній діяльності, під час стратегічних дій, ведення операцій (бойових дій) [12]. Вона є частиною системи логістичного забезпечення ЗС України.

3.3.6. Резерв сил і засобів електронних комунікацій

Резерв сил і засобів електронних комунікацій – сили та засоби електронних комунікацій об'єднань, військових частин і підрозділів зв'язку, які призначені для вирішення раптових завдань, що з'являються при різних змінах обставин зі зв'язку. Він створюється штатними з'єднаннями, частинами та підрозділами зв'язку. Склад резерву визначає начальник зв'язку відповідно до обставин, що склалися. Використані резерви повинні відновлюватися

в найкоротші терміни. Склад резерву сил, засобів, комплексів електронних комунікацій створюється, виходячи з характеру операцій угруповання, прогнозування втрат та наявності сил, засобів, комплексів електронних комунікацій.

Єдиний інформаційний простір сил оборони – це технічна спроможність ЗС України та інших складових сил оборони для об'єднання різних компонентів операційного середовища від стратегічного до тактичних рівнів із використанням мережевих спроможностей та інформаційної інфраструктури [8].

На підставі приведених визначень основних підсистем електронної комунікаційної системи ЗС України можна розробити її модель.

3.4. Розроблення нової моделі електронної комунікаційної системи ЗС України

Використовуючи проведені наукові дослідження нормативної бази України та ЗС України у сфері електронних комунікацій, складу, назв та призначення підсистем пропонується розглянути та ввести в дію визначення електронної комунікаційної системи ЗС України.

Електронна комунікаційна система (система зв'язку) ЗС України є однією зі складових системи управління військами і являє собою інтегровану сукупність взаємопов'язаних та узгоджених за завданнями електронних комунікаційних мереж, систем захисту інформації та кібербезпеки, мереж фельд'єгерського зв'язку, системи матеріально-технічного забезпечення, резерву сил та засобів електронних комунікацій, які розгортаються у ЗС України, з метою забезпечення єдиного інформаційного простору сил оборони в системі управління.

На підставі проведеного дослідження та визначення, ЕКС ЗС України можна представити у вигляді моделі електронної комунікаційної системи, яка розроблена та представлена на рисунку 1.

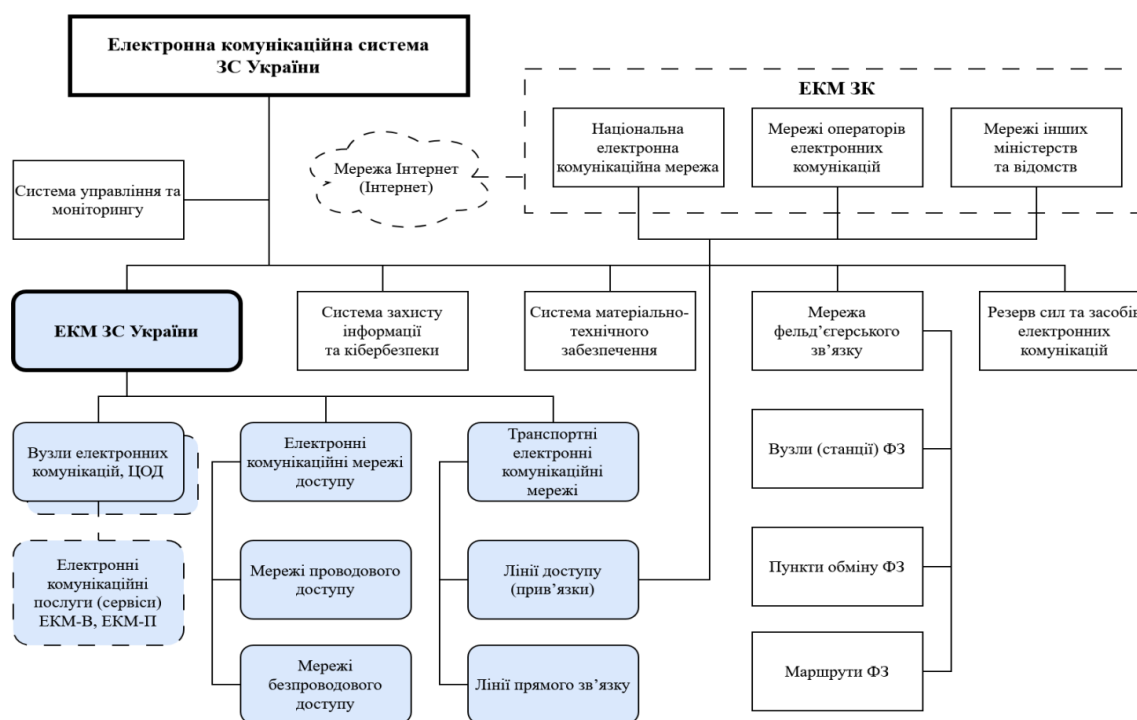


Рис. 1. Модель ЕКС ЗС України

Запропонована модель ЕКС ЗС України складається з наступних основних підсистем: системи управління та моніторингу; електронної комунікаційної мережі ЗС України; системи захисту інформації та кібербезпеки; системи матеріально-технічного забезпечення; мережі фельд'єгерського зв'язку; резерв сил та засобів електронних комунікацій.

Склад, назви підсистем, їх визначення здійснювалось на підставі чинної нормативної бази України у сфері електронних комунікацій.

Ця модель розроблялася з врахуванням змін, які відбулися в законодавчій базі України у сфері електронних комунікацій.

До ЕКС ЗС України висуваються наступні вимоги: постійна готовність до забезпечення управління військами (силами), стійкість, мобільність, пропускну спроможність та розвідзахищеність [9].

Стійкість електронної комунікаційної системи визначає властивість системи зберігати працездатність та забезпечення безперервного і своєчасного надання електронних комунікаційних послуг (сервісів) у системі управління в умовах впливу різноманітних факторів.

Стійкість системи визначається живучістю, надійністю, завадостійкістю засобів електронних комунікацій [16].

Живучість засобів електронних комунікацій визначає здатність засобів виконувати завдання за призначенням в умовах застосування противником засобів ураження. Показником живучості слід вважати ймовірнісну величину $K_{жив}$, яка визначається ймовірністю вогневого ураження засобів електронних комунікацій $P_{вогн}$:

$$K_{жив} = 1 - P_{вогн}. \quad (1)$$

Надійність засобів електронних комунікацій обумовлює здатність засобів виконувати завдання за призначенням, зберігаючи в часі показники у межах, передбачених експлуатаційною документацією на засоби електронних комунікацій.

Показник надійності засобів електронних комунікацій можна виразити через ймовірність безвідмовної роботи засобів електронних комунікацій $K_{над}$ протягом визначеного часу $t_{визн}$ за відомого часу безвідмовної роботи засобів електронних комунікацій $T_{б.р.}$:

$$K_{над} = e^{-\frac{t_{визн}}{T_{б.р.}}}. \quad (2)$$

Завадостійкість засобів електронних комунікацій визначає здатність засобів функціонувати (виконувати завдання за призначенням) з визначеною якістю електронних комунікацій в умовах дії випадкових і навмисних радіозавад. Показником завадостійкості слід вважати ймовірнісну величину $K_{з.ст.}$, яка визначається ймовірностями подавлення каналів та засобів електронних комунікацій навмисними $P_{н.з.}$, випадковими $P_{в.з.}$ завадами та ймовірністю невиконання умов електромагнітної сумісності $P_{н.емс}$ (3):

$$K_{з.ст.} = (1 - P_{нз})(1 - P_{вз})(1 - P_{н.емс}). \quad (3)$$

Таким чином, показником стійкості електронної комунікаційної системи слід вважати ймовірнісну величину $K_{ст.}$, яка визначається ймовірностями $K_{жив}$, $K_{над}$ та $K_{з.ст.}$ (4):

$$K_{ст.} = 1 - (1 - K_{жив})(1 - K_{над})(1 - K_{з.ст.}). \quad (4)$$

У подальшому в складі електронної комунікаційної системи розглядається найважливіший її елемент – електронна комунікаційна мережа ЗС України.

Обмін інформацією в ЕКМ ЗС України здійснюється з використанням проводового, радіорелейного, тропосферного, супутникового та радіозв'язку.

ЕКМ складається зі взаємопов'язаних між собою стаціонарної та мобільної (рухомої) компонент, які виконують спільні завдання у мирний час, в умовах надзвичайних ситуацій, надзвичайного або воєнного стану.

Стаціонарна компонента розгортається та експлуатується на всіх рівнях управління.

Мобільна (рухома) компонента розгортається та експлуатується, як правило в інтересах відповідних рівнів управління для забезпечення (відновлення, нарощування, резервування) стаціонарної компоненти під час ведення військових операцій (бойових дій).

Електронна комунікаційна мережа відповідає структурі управління ЗС України (сил оборони) та складається з основних елементів, до яких належать:

вузли електронних комунікацій (вузли зв'язку) різного призначення;

транспортні електронні комунікаційні мережі;

електронні комунікаційні мережі доступу (прив'язки).

Вузол електронних комунікацій – організаційно-технічне об'єднання технічних засобів, споруд електронних комунікацій і персоналу, розгорнутих на пункті управління або в пункті розподілу, призначений для надання користувачам електронних комунікаційних послуг.

Структура (склад) та завдання вузлів електронних комунікацій визначаються його призначенням.

Стаціонарні вузли електронних комунікацій пунктів управління (штабів) призначені забезпечувати обмін і обробку інформації, вирішення інформаційних, розрахункових та інших задач, надання доступу до електронних комунікаційних послуг (сервісів) для виконання завдань управління військами (силами) службовими особами органів управління.

Мобільні (рухомі) вузли електронних комунікацій пунктів управління є складовою частиною мобільних (рухомих) пунктів управління та призначені для забезпечення надання доступу до електронних комунікаційних послуг (сервісів) службовим особам пунктів управління.

Вузли електронних комунікацій розподіляються за рівнями: стратегічним, оперативним, тактичним.

Транспортна електронна комунікаційна мережа – мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї комунікаційними мережами доступу.

Електронна комунікаційна мережа доступу – частина електронної комунікаційної мережі між пунктом закінчення електронної комунікаційної мережі та найближчим вузлом (центром) комутації включно.

Лінії доступу (прив'язки) стаціонарних, мобільних (рухомих) вузлів електронних комунікацій до транспортної ЕКМ ЗС України, електронної комунікаційної мережі загального користування (далі – ЕКМ ЗК) будуються з використанням провідних, радіорелейних та тропосферних засобів електронних комунікацій.

Комплекси та засоби електронних комунікацій стаціонарної та мобільної (рухомої) компоненти ЕКМ ЗС України повинні забезпечувати необхідний рівень організаційно-технічної та апаратно-програмної взаємодії як між собою, так і з обладнанням електронних комунікацій складових сил оборони, ЕКМ ЗК та країн-партнерів.

Стаціонарна компонента використовується за принципом оренди ресурсу ЕКМ ЗК та/або в стаціонарних (рухомих) транспортних електронних комунікаційних мережах ЗС України.

4. Аналіз ефективного функціонування електронної комунікаційної мережі спеціального призначення

Загалом сучасний стан електронної комунікаційної мережі спеціального призначення, попри війни з російською федерацією та намагання ворога вивести з ладу, демонструє відносну стійкість, інноваційну гнучкість та орієнтацію на розвиток і модернізацію.

За даними Адміністрації Держспецзв'язку України через дії російських окупантів виведено з ладу близько трьох тисяч базових станцій мобільних операторів, не працювало

понад 20 телевізійних станцій і пошкоджено тисячі кілометрів волоконно-оптичних ліній ЕКМ.

У районах ведення бойових дій:

велика частина об'єктів інфраструктури операторів електронних комунікацій знищена або перебуває у стані, що не забезпечує належне функціонування ЕКМ сил оборони;

операторами електронних комунікацій частково втрачено управління мережами;

ускладнена координація дій між операторами електронних комунікацій та іншими власниками інфраструктур для використання наявних ресурсів в інтересах сил оборони;

відсутність постійних координаційних центрів на місцях спричиняє до збільшення часу на організацію та відновлення надання електронних комунікаційних послуг, що призводить до зниження ефективності управління військами.

На ряду з руйнуваннями інфраструктури ЕКМ ЗС в районах ведення бойових дій, ЕКМ ЗС України також зазнала масштабних пошкоджень, зруйновано або виведено з ладу сотні об'єктів електронних комунікацій, як у тилу, так і на лінії фронту, тому ЕКМ ЗС України самостійно не спроможна забезпечити потреби в обміні всіма видами інформації у процесі управління військами.

У зв'язку з цим виникає нагальна потреба оренди каналів (потоків) в електронній комунікаційній мережі загального користування. Під час оренди базові технології мереж ЗС України повинні відповідати технологіям ЕКМ ЗС. Своєчасне надання електронних комунікаційних послуг має вирішальне значення для забезпечення командирів з'єднань, частин і підрозділів необхідною інформацією з метою прийняття правильних рішень, які забезпечать успішне виконання поставлених завдань.

Підключення вузлів електронних комунікацій ЗС України до ЕКМ ЗС здійснюється власними засобами за технічними умовами.

Порядок надання та отримання електронних комунікаційних послуг в ЕКМ ЗС відбувається відповідно до Закону України “Про електронні комунікації”, постанови Кабінету Міністрів України від 24 січня 2025 року № 75 [7] та інших документів Кабінету Міністрів України.

Для аналізу ефективного функціонування ЕКМ ЗС України було проведено дослідження декількох з'єднань та частин, які замовляли послуги в операторів електронних комунікацій в період з квітня по серпень 2025 року. Результати аналізу наданих послуг операторами електронних комунікацій з моменту замовлення до моменту надання представлено в таблиці 1.

Таблиця 1

Результати аналізу наданих послуг операторами електронних комунікацій

№ з/п	Підрозділ, в інтересах якого опрацюється заявка	Пункт відбору комунікаційного ресурсу	Оператор електронних комунікацій	Вихідний номер заявки	Дата надсилання заявки	Дата опрацювання заявки ГУЗ та КБ	Дата надання послуг оператором	Час надання послуг (доба)
1	2	3	4	5	6	7	8	9
1	128 омбр	–	ПрАТ “ВФ Україна”, Інтернет	№ УВ(с)/3/1/205, ДСК	24.07. 2025	25.07. 2025	31.07. 2025	6 діб
2	128 омбр	–	ПрАТ “Київстар”, Інтернет. ПрАТ “Київстар”, L2	№ УВ(с)/3/1/367, ДСК	31.07. 2025	01.08. 2025	09.08. 2025	8 діб
3	41 омбр	–	ПрАТ “ВФ Україна”, Інтернет	№ 0408/3/1/406, ДСК	04.04. 2025	05.04. 2025	11.04. 2025	6 діб

1	2	3	4	5	6	7	8	9
4	41 омбр	–	ПрАТ “ВФ Україна”, Інтернет	№ 0408/3/1/478, ДСК	19.04. 2025	20.04. 2025	28.04. 2025	8 діб
5	7 ОПЗ	–	ПрАТ “ВФ Україна”, Інтернет	№ 0408/3/1/497, ДСК	23.04. 2025	24.04. 2025	01.05. 2025	7 діб
6	7 ОПЗ	–	ПрАТ “ВФ Україна”, Інтернет	№ 0408/3/1/556, ДСК	30.04. 2025	01.05. 2025	11.05. 2025	10 діб
7	38 зрп	–	ПрАТ “Київстар”, Інтернет	№ 0408/3/1/533, ДСК	27.04. 2025	28.04. 2025	06.05. 2025	8 діб
8	411 оп БпС	–	ПрАТ “ВФ Україна”, Інтернет	№ УВ(с)/3/1/39, ДСК	22.06. 2025	23.06. 2025	04.07. 2025	10 діб

Як видно із таблиці, час надання електронних комунікаційних послуг операторами електронних комунікацій для з'єднань і частин ЗС України є довготривалим, становить декілька діб, що не може забезпечити необхідну оперативність виконання поставлених завдань у районах ведення бойових дій.

На ряду з цим, процес відбору ресурсу електронних комунікацій потребує відриву особового складу з'єднань, частин і підрозділів зв'язку для виконання наступних нетипових задач:

- пошук пунктів видачі ресурсу операторів електронних комунікацій;
- відновлення електронних комунікаційних мереж операторів у місцях відбору ресурсу;
- прив'язку, налаштування, ремонт і технічне обслуговування нетипових технічних засобів та інші.

Для скорочення часу надання електронних комунікаційних послуг керівництво зв'язку ЗС України вживає низку заходів, а саме:

- створюються військові комендатури зв'язку, які в зоні відповідальності керують процесом замовлення та надання електронних комунікаційних послуг у ЕКМ ЗК;

- формується аварійні групи з оперативного відновлення електронних комунікаційних мереж ЗС України та інфраструктури операторів електронних комунікацій в інтересах сил оборони;

- проводяться регулярні навчання з особовим складом, який займається організацією та наданням послуг;

- здійснюються постійні тренування з екіпажами апаратних (станцій), які забезпечують доступ (прив'язку) до ЕКМ ЗК;

- підсилюються розрахунки чергових змін операторів електронних комунікацій (особливо в зоні ведення бойових дій) особовим складом ЗС України та інші.

На ряду з цим відповідно до Постанови Кабінету Міністрів України від 24 січня 2025 року № 75 [7] створюється система оперативно-технічного управління мережами, яка призначена для єдиного та ефективного оперативно-технічного управління електронними комунікаційними мережами загального користування для сил оборони в умовах надзвичайної ситуації, надзвичайного або воєнного стану. До складу цієї системи входять: Адміністрація Держспецзв'язку, Національний центр оперативно-технічного управління електронними комунікаційними мережами України, центри управління мережами операторів електронних комунікацій, інформаційно-аналітична система оперативно-технічного управління та технічні засоби оперативно-технічного управління.

Наведені організаційні нововведення у ЗС України та в органах виконавчої влади України скорочують час та прискорюють процес надання електронних комунікаційних послуг, але повністю розв'язати цю проблему не можуть, тому що основна затримка в наданні послуг

відбувається в операторів електронних комунікацій, які з різних причин, керуючись своєю нормативною базою та обмеженим персоналом, не здатні значно прискорити видачу зазначених послуг.

На підставі вищевикладеного можна зробити **висновок**, що чинний механізм надання електронних комунікаційних послуг не повною мірою відповідає сучасним потребам в організації електронних комунікацій, потребує реорганізації та модернізації.

5. Напрямки удосконалення електронної комунікаційної мережі ЗС України

На розвиток і удосконалення електронної комунікаційної мережі ЗС України впливають зміни, що відбуваються в характері, способах та формах ведення війни з російською федерацією, які переміщують акцент військово-технічної політики ЗС України в напрямку розвитку власної ЕКМ та забезпечення панівної ролі інформаційних технологій під час ведення бойових дій. Забезпечення інформаційної переваги над системами управління противника, підвищення якості надання електронних комунікаційних послуг органам військового управління є пріоритетним напрямком підвищення бойових спроможностей військ (сил).

Процес розвитку та модернізації ЕКМ ЗС України пропонується розбити на два етапи: удосконалення нормативної бази; розвиток електронної комунікаційної мережі ЗС України.

5.1. Удосконалення нормативної бази ЗС України у сфері електронних комунікацій

Для переопрацювання та удосконалення нормативних документів ЗС України у сфері електронних комунікацій пропонується:

1. Створити робочу групу з розроблення нормативної бази ЗС України відповідно до чинного законодавства України, Міжнародного союзу електрозв'язку, Європейського Союзу та країн-партнерів, де дослідити та затвердити склад, нормативні документи, основні визначення термінів ЕКС ЗС України та план реалізації нормативної бази електронних комунікацій ЗС України з урахуванням змін чинного законодавства.

2. Розробити Стратегію (Концепцію) розвитку ЕКС ЗС України, де особливу увагу приділити модернізації та переобладнанню ЕКМ ЗС України із застосуванням новітніх технологій у сфері електронних комунікацій, які відповідають міжнародним стандартам, з урахуванням технологічної цілісності мереж та засобів електронних комунікацій, підвищення ефективності та сталості функціонування з розгортанням єдиного інформаційного простору.

5.2. Удосконалення електронної комунікаційної мережі ЗС України

Задачі, які стоять перед державою:

самостійно, або разом з іншими країнами, організувати розробку та виробництво сучасних технічних засобів (апаратних) електронних комунікацій на території України, що надасть можливість в короткі терміни забезпечити ЗС України сучасними засобами, якісно та швидко проводити обслуговування, ремонт та модернізацію;

створення власної системи супутникового зв'язку ЗС України як складової частини Національної системи супутникового зв'язку та мовлення на основі національних супутників на низькій навколоземній орбіті, а до цього – оренда послуг із використанням військових систем супутникового зв'язку країн-партнерів, або у низькоорбітальних міжнародних систем супутникового зв'язку провідних країн світу.

Задача, яка стоїть перед ЗС України:

створити власну ЕКМ ЗС України, яка є складовою частиною та основою електронної комунікаційної системи ЗС України та складових сил оборони і являє собою комплекс технічних засобів електронних комунікацій та споруд ЗС України, призначених для надання електронних комунікаційних послуг (сервісів).

Основні положення з удосконалення мережі.

Досвід ведення війни з російською федерацією показав, що ЕКМ ЗС України повинна удосконалюватися в напрямку розвитку власної електронної комунікаційної мережі, забезпечення панівної ролі інформаційних технологій при забезпеченні бойових дій. Забезпечення інформаційної переваги над системами управління противника, підвищення якості надання електронних комунікаційних послуг органам військового управління розглядається як один із пріоритетних напрямків підвищення бойових спроможностей військ ЗС України.

На основі проведеного аналізу сучасного стану ЕКМ ЗС України під час відсічі збройної агресії, перспектив розвитку мереж майбутнього, можна зробити висновок, що вдосконалення ЕКМ ЗС України необхідно проводити на основі: випереджальної готовності електронних комунікаційних мереж щодо системи управління військами; єдності системи електронних комунікацій та комплексів і засобів інформатизації; поетапного розвитку; раціонального співвідношення між стаціонарною і мобільною компонентами.

Електронна комунікаційна мережа ЗС України повинна базуватися на власних ресурсах ЕКМ, ЕКМ ЗК – використовується як резерв. Розбудовувати ЕКМ ЗС України слід із дотриманням стандартів, доктрин і рекомендацій України та країн-партнерів, а взаємодію з ЕКМ ЗК та ЕКМ країн-партнерів забезпечувати на транспортному рівні.

Удосконалення ЕКМ ЗС України, по можливості, почати з переходу на оренду волокон (каналів/потоків) у розгалужених систем різних установ та відомств України, таких як: “АТ Укрзалізниця”, НАК “Нафтогаз Україна”, ПАТ “Укртрансгаз”, НЕК “Укренерго” та інших.

Такий перехід забезпечить: захист ЕКМ (волоконно-оптичних ліній) від зовнішнього втручання; (ешелоні захисту периметра, ешелоні захисту мереж, ешелоні захисту кінцевих пристроїв (хостів), ешелоні захисту програмного забезпечення, ешелоні захисту даних); зменшення вартості електронних комунікаційних послуг; збільшення швидкості передачі інформації. Перехід повинен відбуватися поступово, продумано, з урахуванням всіх недоліків і переваг.

Орендувати волокна (канали/потоки) слід тільки в операторів електронних комунікацій, які не мали господарських зв'язків з російською федерацією.

ЕКМ ЗС України повинна будуватися на ресурсах взаємопов'язаних між собою стаціонарної та мобільної компонент.

5.2.1. Розвиток стаціонарної компоненти ЕКМ ЗС України

Для прискорення надання електронних комунікаційних послуг силам оборони, забезпечення збільшувальних потреб в обміні всіма видами інформації у процесі управління військами (силами), зменшення залежності від міжнародних (національних) операторів електронних комунікацій, у яких за значні кошти орендуються канали (потоки), – виникла нагальна потреба в розвитку власної стаціонарної компоненти ЕКМ ЗС України.

Ця компонента буде використовуватися силами оборони у мирний час, в умовах надзвичайної ситуації, надзвичайного або воєнного стану. Особливу увагу необхідно приділити розвитку волоконно-оптичних ліній електронних комунікацій у східних і південних регіонах України. Будівництво нових високошвидкісних ліній електронних комунікаційних мереж повністю забезпечить необхідними послугами (сервісами) сили оборони на стратегічному, оперативному, а при необхідності й на тактичних рівнях управління.

На підставі проведеного дослідження та наукового аналізу електронної комунікаційної мережі спеціального призначення, яка діє, пропонується розгорнути стаціонарну компоненту електронної комунікаційної мережі ЗС України. Така модель ЕКМ ЗС України представлена у вигляді нової моделі стаціонарної компоненти електронної комунікаційної мережі ЗС України (рис. 2).



Рис. 2. Модель стаціонарної компоненти ЕКМ ЗС України

Представлена модель стаціонарної компоненти ЕКМ ЗС України на базі власних волоконно-оптичних ліній електронних комунікаційних мереж забезпечить:

оперативне, надійне та безперебійне управління військами (силами) у мирний час, в умовах надзвичайних ситуацій, надзвичайного або воєнного стану;

зменшення часу надання електронних комунікаційних послуг, від чинних декількох діб до хвилин (десятих хвилин);

оперативність надання електронних комунікаційних послуг силам оборони в районах ведення бойових дій;

збільшення пропускної спроможності до декількох Тбіт/с;

підвищення захисту інформації та кіберзахисту для споживачів електронних комунікаційних послуг;

ефективне використання каналів (потоків);

підтримання ЕКМ у постійній готовності до виконання завдань за призначенням;

скорочення часу на відновлення волоконно-оптичних ліній електронних комунікаційних мереж;

відмову від оренди потоків (каналів) у міжнародних (національних) операторів електронних комунікацій;

надійну роботу та прив'язку центрів обробки даних та вузлів електронних комунікацій.

Така ЕКМ ЗС України буде використовуватися не тільки об'єднаннями, з'єднаннями та частинами ЗС України, але і складовими сил оборони, які будуть виконувати спільні завдання у мирний час, в умовах надзвичайних ситуацій, надзвичайного або воєнного стану.

Досвід ведення війни з російською федерацією показав, що стаціонарна компонента (технічні засоби, споруди електронних комунікацій) в районах ведення бойових дій часто зазнає пошкоджень та руйнувань. Через це виникає нагальна потреба в розгортанні мобільної (рухомої) компоненти для відновлення надання електронних комунікаційних послуг,

нарощуванні та резервуванні стаціонарної ЕКМ ЗС України силами й засобами частин і підрозділів зв'язку.

5.2.2. Розвиток мобільної (рухомої) компоненти ЕКМ ЗС України

Пріоритетом стратегії розвитку ЕКМ ЗС України є розвиток сучасної мобільної (рухомої) компоненти на стратегічному, оперативному та тактичному рівнях управління шляхом будівництва ліній електронних комунікаційних мереж із використанням станцій проводового, радіорелейного, тропосферного, супутникового та радіозв'язку.

Напрямки удосконалення проводового сегмента:

- зменшення масогабаритних показників апаратних;
- підвищення мобільності та маневровості апаратних;
- виготовлення нових уніфікованих комплексних апаратних електронних комунікацій для різних рівнів управління: стратегічного, оперативного та тактичного;
- технічні засоби електронних комунікацій повинні легко зніматись, переміщуватись на рухомих засобах, у контейнерах та переносному виконанні;
- розробка та впровадження польових комплектів волоконно-оптичних кабелів багаторазового використання з одномодовими та багатомодовими оптичними волокнами;
- застосування сучасних роботизованих кабелеукладачів та дронів для прокладання польових волоконно-оптичних кабелів;
- розробка польових малогабаритних технічних засобів електронних комунікацій для ущільнення волоконно-оптичних ліній електронних комунікацій;
- побудова та прив'язка центрів обробки даних та вузлів електронних комунікацій за єдиним принципом;
- на кожному вузлі електронних комунікацій мати уніфіковані засоби прив'язки мобільних вузлів та технічних засобів електронних комунікацій;
- ефективне використання каналів (потоків) передавання, що надаються стаціонарною (мобільною) компонентами ЕКМ ЗС України та ЕКМ ЗК.

Напрямки удосконалення радіорелейного сегмента:

- зменшення масогабаритних показників, підвищення мобільності та маневровості станцій з доведенням пропускної спроможності до 100 Гбіт/с;
- розробка та впровадження мобільних комбінованих станцій в контейнерному виконанні;
- розширення частотного діапазону роботи станцій та автоматичної адаптації пропускної спроможності до умов поширення на трасі;
- зменшення потужності випромінювання та застосування спрямованих антен, використання цифрових антенних решіток;
- впровадження інтелектуального управління мережею;
- забезпечення високої розвід- та завадозахищеності.

Напрямки удосконалення тропосферного сегмента:

- зменшення масогабаритних показників, підвищення мобільності та маневровості станцій з доведенням пропускної спроможності до 210 Мбіт/с;
- розробка та впровадження комбінованих станцій в контейнерному та переносному виконанні із застосуванням інноваційних технологій;
- зниження потужності випромінювання, здатних працювати в тропосферному, радіорелейному або супутниковому режимах;
- підвищення експлуатаційної надійності та частотного маневрування по всьому розширеному діапазоні частот;
- автоматична адаптація пропускної здатності до умов поширення на трасі.

Напрямки удосконалення супутникового сегмента:

- створення власної системи супутникового зв'язку ЗС України як компоненти Національної системи супутникового зв'язку та передачі даних на основі національних низькоорбітальних супутників, а до цього – оренда послуг у військових систем супутникового

зв'язку країн-партнерів та у низькоорбітальних міжнародних систем супутникового зв'язку провідних країн світу.

Новостворена система повинна забезпечувати:

розвід- та завадозахищений супутниковий зв'язок між пунктами управління стратегічного, оперативного та тактичного рівнів управління ЗС України в умовах активного застосування засобів РЕБ противника;

необхідну швидкість та якість передачі інформації;

функціонування у складі інтегрованої ЕКМ ЗС України та взаємодію з компонентами об'єднаної системи зв'язку країн-партнерів.

Наземний компонент повинен комплектуватись невеликими мобільними, переносними (перевізними), портативними станціями супутникового зв'язку з необхідною швидкістю та якістю передачі даних.

Напрямки удосконалення радіосегмента:

продовження забезпечення ЗС України сучасними компактними, малогабаритними, портативними надійними станціями УКХ радіозв'язку;

створення архітектури на базі багатоканальних, багатосмугових, високошвидкісних, інтелектуальних радіозасобів, які будуть об'єднувати наземні, повітряні та морські служби;

створення високошвидкісних мереж на базі повітряних електронних комунікаційних платформ, БПЛА, мобільних базових станцій із розширенням зон покриття радіозв'язку;

розширення робочого діапазону частот;

застосування широкосмугових радіостанцій;

шифрування передаваної інформації з подальшим переходом до захищених мереж майбутнього;

використання спрямованих антен;

широке використання мереж типу MESH, MANET, технології MIMO та інших сучасних мереж та технологій.

На основі проведеного аналізу сучасного стану ЕКМ ЗС України, укомплектованості технічними засобами електронних комунікацій, принципів побудови мереж провідних країн світу та країн-партнерів, можна зробити наступні загальні ВИСНОВКИ:

ЕКМ ЗС України повинна будуватися з дотриманням стандартів, доктрин і рекомендацій України та країн-партнерів з повною інтеграцією з електронними комунікаційними мережами сил оборони та ЕКМ ЗК;

продовжувати розвиток стаціонарної компоненти ЕКМ ЗС України на базі власних волоконно-оптичних ліній електронних комунікаційних мереж;

розробляти та впроваджувати сучасні технічні засоби електронних комунікацій на базі нових та інноваційних технологій;

розвивати сучасну мобільну компоненту на стратегічному, оперативному та тактичному рівнях управління з підвищенням її мобільності та завадозахищеності;

модернізувати та впроваджувати нові уніфіковані комплексні апаратні електронних комунікацій, комбіновані радіорелейні, тропосферні та супутникові станції для різних рівнів управління;

продовжувати забезпечення сучасними засобами радіозв'язку з врахуванням світових тенденцій підвищення ефективності їх функціонування.

ЕКМ ЗС України повинна базуватися на ресурсах власних електронних комунікаційних мереж, ЕКМ ЗК – використовується як резерв.

Таким чином, впровадження сучасних станцій електронних комунікацій, із застосуванням нових та інноваційних технологій значною мірою змінить структуру та підвищить стійкість ЕКМ ЗС України до засобів радіорозвідки й РЕБ противника та виведе її на вищий рівень розвитку.

Наукова новизна та відмінність запропонованих рішень від існуючих.

На основі наведених пропозицій наукову новизну запропонованих рішень доцільно формулювати не як сукупність організаційних пропозицій, а як *нові науково-методичні та системотехнічні положення*, що розвивають теорію і практику побудови ЕКМ ЗС України.

Основні відмінності та елементи новизни полягають у тому, що:

уперше розвиток ЕКМ ЗС України розглянуто як *дворівневий взаємопов'язаний процес*, який охоплює одночасно удосконалення нормативної бази та технічної архітектури електронної комунікаційної мережі, тоді як існуючі підходи, як правило, розглядалися окремо;

на відміну від існуючих рішень, де стаціонарна і мобільна компоненти функціонують відокремлено, *запропоновано їхнє інтегроване функціонування* як єдиного інформаційного простору сил оборони з розподілом функцій живучості, резервування та відновлення;

на відміну від діючих рішень, *запропоновано використовувати ресурси критичної інфраструктури держави* (транспортної, енергетичної, трубопровідної) як елемент побудови захищеної електронної комунікаційної інфраструктури складових сил оборони;

на відміну від відомих рішень, *запропоновано комплексне поєднання сучасних мережевих технологій* MESH, MANET, MIMO, повітряних комунікаційних платформ, цифрових антенних решіток та інтелектуального управління мережею у структурі перспективної ЕКМ ЗС України;

уперше удосконалення ЕКМ ЗС України розглянуто з *позицій протидії радіоелектронному впливу противника*, де вимоги живучості, завадозахищеності, кіберстійкості та оперативного відновлення покладені в основу архітектури мережі, а не є додатковими вимогами.

Висновки.

У результаті проведеного дослідження була досягнута поставлена мета, а саме: розроблені нові моделі електронної комунікаційної системи та стаціонарної компоненти електронної комунікаційної мережі ЗС України. Ці моделі розроблялися з врахуванням наукового аналізу нормативної бази України, досвіду ведення війни з російською федерацією та новітніх досягнень у сфері електронних комунікацій. Впровадження в експлуатацію розробленої моделі стаціонарної компоненти ЕКМ ЗС України з використанням інноваційних технологій може стати основою системи управління військами та повністю забезпечить необхідними послугами (сервісами) сили оборони, підвищить бойову готовність військ, як у мирний час, так і в умовах надзвичайної ситуації, надзвичайного або воєнного стану. Була обґрунтована потреба в розгортанні мобільної (рухомої) компоненти та визначені напрямки її удосконалення для надання електронних комунікаційних послуг. Створена ЕКМ ЗС України повинна будуватися з дотриманням стандартів, доктрин, рекомендацій України та країн-партнерів і забезпечить розгортання єдиного інформаційного простору з повною інтеграцією з ЕКМ сил оборони й ЕКМ ЗК.

Напрямок подальшого наукового дослідження.

Разом із розвитком стаціонарної компоненти ЕКМ ЗС України гостро стоїть питання удосконалення польової електронної комунікаційної мережі із застосуванням мобільних (рухомих) станцій радіорелейного, тропосферного, супутникового, проводового та радіозв'язку.

Створення та впровадження нових технічних засобів електронних комунікацій, зменшення масогабаритних показників, потужності випромінювання з підвищенням швидкості передачі інформації, розвід- та завадозахищеності, в контейнерному та у блоковому виконанні із застосуванням штучного інтелекту інноваційних технологій на різних рівнях управління є важливим науковим і практичним завданням. Втілення таких технічних засобів значною мірою підвищить стійкість ЕКМ ЗС України та виведе її на якісно новий рівень розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-IX#Text>.
2. Про Національну програму інформатизації: Закон України в редакції від 01.12.2022 № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text>.
3. Про інформацію: Закон України в редакції від 20.01.2026 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
4. Про захист інформації в інформаційно-комунікаційних системах: Закон України в редакції від 20.04.2025 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
5. Про основні засади забезпечення кібербезпеки України: Закон України в редакції від 19.10.2025 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
6. Про поштовий зв'язок: Закон України в редакції від 21.06.2024 № 3699-IX. URL: <https://zakon.rada.gov.ua/laws/show/2722-20#Text>.
7. Деякі питання оперативно-технічного управління електронними комунікаційними мережами в умовах надзвичайної ситуації, надзвичайного або воєнного стану^ Постанова Кабінету Міністрів України від 24.01.2025 № 75. URL: <https://zakon.rada.gov.ua/laws/card/75-2025-%D0%BF>.
8. ВКП 6-00(01).01. Доктрина “Зв'язок та інформаційні системи”, затверджена Головнокомандувачем ЗС України від 01.07.2020.
9. ДДП 6-26.22. Настанова “Зі зв'язку Збройних Сил України”, затверджена Головнокомандувачем Збройних Сил України 05.01.2025.
10. ВКП 6-26(01).01. Концепція побудови Електронної комунікаційної мережі Збройних Сил України, затверджена Головнокомандувачем Збройних Сил України від 06.09.2021.
11. Концепція розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України, затверджена Міністром оборони України від 03.11.2021.
12. ВКП 4-179(03).01. Доктрина “Забезпечення матеріально-технічними засобами, роботами та послугами”, затверджена Начальником Генерального штабу Збройних Сил України від 21.01.2021.
13. Руденко В. І., Зінченко М. О., Гришина Н. С., Остапук О. І. Стан та напрямки розвитку телекомунікаційної мережі системи зв'язку Збройних сил України // К.: ВІТІ 2020. № 2. С. 75–89.
14. Чередніков С. О. Деякі аспекти побудови телекомунікаційної мережі ЗС України // Х науково-практична конференція. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО. К.: ВІТІ. 2017. С. 68–70.
15. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18–68. URL: <http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf>.
16. Макаров С. А., Беляк С. П., Висоцький О. В. Оцінка стійкості системи зв'язку та радіотехнічного забезпечення // Системи озброєння і військова техніка. Х.: ХНУПС. 2020. № 1 (61). С. 44–50. DOI: 10.30748/soivt.2020.61.05.

Надійшла до редколегії 03.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.396

д-р техн. наук Сайко В. Г. ORCID: 0000-0002-3059-6787 (ВІТІ ім. Героїв Крут)
Станілога О. О. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
Пантась С. О. ORCID: 0000-0001-9868-142X (ВІТІ ім. Героїв Крут)
Пантась І. О. ORCID: 0000-0001-5766-1422 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ВИЯВЛЕННЯ ТА ПЕЛЕНГАЦІЇ СИГНАЛІВ СТАНДАРТУ IEEE 802.11bf

Розвиток методів спільної ідентифікації та пеленгування дозволяє розділяти пеленги великої кількості джерел сигналів безпроводових систем зв'язку, що ведуть роботу в одному частотному діапазоні з поділом за часом [21–26]. У цій роботі акцент зроблено на виявленні цільових сигналів та виділення з них ідентифікаційних ознак джерела. Від успішності реалізації цих операцій суттєво залежатимуть і показники якості пеленгування. У статті досліджено можливості підвищення завадостійкості процесів виявлення, ідентифікації та пеленгації сигналів стандарту IEEE 802.11bf шляхом застосування двоканального кореляційно-інтерферометричного приймача. Запропоновано структурний принцип інноваційного рішення, що базується на просторово-часовій обробці сигналів з урахуванням кореляції каналів, частотного зсуву та умов релеївських замирань. Розроблено методику дослідження двоканального приймача, яка включає моделювання процесів прийому, кореляційного виявлення, оцінювання параметрів сигналу та визначення кута приходу. Сформовано формалізовані математичні моделі, що описують ймовірності бітової помилки, виявлення та хибної тривоги, а також точність пеленгації залежно від відношення сигнал/шум, коефіцієнта кореляції каналів та частотного зсуву. За результатами моделювання в MATLAB встановлено, що використання двоканального прийому забезпечує суттєве зниження ймовірності бітової помилки порівняно з одноканальним випадком, а також підвищення ймовірності правильного виявлення сигналу при фіксованому рівні хибної тривоги. Показано, що точність оцінки кута приходу сигналу значно залежить від кореляції каналів та частотного зсуву: зростання кореляції призводить до деградації інтерферометричних властивостей, тоді як частотний зсув викликає фазові похибки та збільшення середньоквадратичної помилки. Отримані результати підтверджують ефективність запропонованого підходу для підвищення завадостійкості систем радіомоніторингу та когнітивного радіо на базі IEEE 802.11bf.

Ключові слова: рознесений прийом, Wi-Fi, комутована антенна решітка, радіомоніторинг, релеївський канал.

V. Saiko, O. Staniloha, S. Pantas, I. Pantas. Investigation of methods to improve interference immunity in detection and direction-finding of IEEE 802.11bf signals

The development of joint identification and direction-finding methods enables the separation of bearings from a large number of wireless communication signal sources operating in the same frequency band with time-division access [21–26]. This work focuses on the detection of target signals and the extraction of source identification features, as the effectiveness of these operations significantly affects the overall quality of direction-finding. This paper investigates the potential for improving the interference immunity of detection, identification, and direction-finding processes for IEEE 802.11bf signals through the use of a two-channel correlation-interferometric receiver. A structural principle of the proposed innovative solution is presented, based on spatio-temporal signal processing that accounts for channel correlation, frequency offset, and Rayleigh fading conditions. A research methodology for the two-channel receiver is developed, including modeling of reception processes, correlation-based detection, signal parameter estimation, and angle-of-arrival determination. Formalized mathematical models are formulated to describe the bit error probability, detection probability, false alarm rate, and direction-finding accuracy as functions of the signal-to-noise ratio, channel correlation coefficient, and frequency offset. MATLAB simulation results demonstrate that two-channel reception significantly reduces the bit error probability compared to the single-channel case, while increasing the probability of correct signal detection at a fixed false alarm rate. It is shown that the accuracy of angle-of-arrival estimation strongly depends on channel correlation and frequency offset: increasing correlation degrades interferometric properties, whereas frequency offset introduces phase errors and increases the root-mean-square estimation error. The results confirm the effectiveness of the proposed approach for enhancing the interference immunity of radio monitoring and cognitive radio systems based on IEEE 802.11bf.

Keywords: spatial diversity reception, Wi-Fi, switched antenna array, radio monitoring, Rayleigh channel.

Постановка завдання у загальному вигляді

Пеленгація джерел бездротових сигналів у сучасних мережах, зокрема стандарту IEEE 802.11bf, ускладнюється особливостями організації доступу до середовища, що базується на часовому розподілі використання спільного частотного ресурсу. У таких умовах різні пристрої передають сигнали у межах однієї смуги частот, але в різні моменти часу, що може призводити до виникнення аномальних похибок під час оцінювання напрямку на джерело сигналу. Зокрема, такі похибки виникають у випадках, коли для пеленгації використовуються суміжні у часі пакети, що належать різним передавачам [1].

Для розв'язання задач пеленгації у багатосигнальному середовищі широко застосовуються методи просторової обробки сигналів, такі як MUSIC та ESPRIT [2; 3]. Вони забезпечують високу роздільну здатність, проте характеризуються значною обчислювальною складністю та потребують апріорної інформації щодо кількості активних джерел сигналів. Це обмежує їх використання в умовах динамічних бездротових мереж із часовим розділенням доступу.

Альтернативним підходом до підвищення достовірності пеленгації є використання ідентифікаційної інформації, що передається у пакетах даних. Зокрема, MAC-адреса пристрою дозволяє здійснювати класифікацію сигналів за джерелами та забезпечує коректне об'єднання вибірок, що належать одному передавачу. Такий підхід став основою методів спільної ідентифікації та пеленгації, відомих як адресне пеленгування [4; 5].

Поєднання процедур виявлення, ідентифікації та оцінювання кутових координат джерел радіовипромінювання забезпечує низку переваг. Зокрема, це дозволяє здійснювати пеленгацію сигналів різної тривалості, включаючи короткочасні, а також розділяти напрями на велику кількість джерел, що працюють у спільному частотному діапазоні з часовим розділенням, завдяки прив'язці унікальних ідентифікаційних ознак до відповідного напрямку.

Разом з тим, у реальних умовах експлуатації, таких як міське середовище або внутрішні приміщення, процеси виявлення та прийому сигналів істотно ускладнюються через низьке відношення сигнал/шум та вплив багатопроменевого поширення, що призводить до замирань сигналу. Одним із ефективних підходів до підвищення якості прийому в таких умовах є використання рознесеного прийому [6].

У цій роботі рознесений прийом реалізується на базі двоканального кореляційно-інтерферометричного приймача. Однак ефективність такого підходу обмежується тим, що для досягнення декореляції сигналів антени повинні бути просторово рознесені, тоді як у задачах пеленгації елементи антенної решітки зазвичай розташовані на відстанях, менших за довжину хвилі, що зумовлює наявність кореляції між каналами.

У зв'язку з цим актуальною є задача дослідження впливу кореляції каналів на ефективність процесів виявлення, ідентифікації та пеленгації сигналів.

Аналіз публікацій за темою досліджень. Останні роки характеризуються стрімким розвитком концепції Wi-Fi sensing, що стало основою формування стандарту IEEE 802.11bf. Цей напрямок інтегрує функції зв'язку та радіолокації, що відкриває нові можливості для задач виявлення, локалізації та ідентифікації об'єктів у бездротових мережах [7].

Однією з ключових робіт у цій області є дослідження інтеграції зв'язку та сенсингу в Wi-Fi мережах, де показано, що стандарт IEEE 802.11bf розширює можливості фізичного та MAC-рівнів для реалізації функцій радіосенсингу без необхідності спеціалізованого обладнання [8]. У подальших роботах підкреслюється, що Wi-Fi сигнали можуть бути ефективно використані для задач визначення присутності, відстеження руху та розпізнавання активності користувачів [9].

У роботах 2023 року було сформовано базові принципи стандарту IEEE 802.11bf, включаючи підтримку бі- та мультистатичних схем сенсингу у діапазонах 2,4 ГГц, 5 ГГц та 6 ГГц [10]. Це дозволяє використовувати існуючу інфраструктуру Wi-Fi для реалізації систем спостереження та моніторингу середовища.

Подальші дослідження зосереджені на оцінці ефективності сенсингових процедур. Зокрема, у роботах 2023–2024 років показано, що стандарт IEEE 802.11bf забезпечує можливість оцінювання швидкості та кута руху з похибкою порядку одиниць градусів, причому точність залежить від конфігурації антенної решітки та параметрів сигналу [11]. Також досліджено вплив сенсингових процедур на продуктивність мережі, де встановлено компроміс між точністю сенсингу та пропускнуою здатністю каналу [12].

Значна кількість сучасних робіт присвячена використанню інформації про стан каналу (CSI) для задач локалізації та пеленгації [13]. Проте такі підходи часто потребують модифікації обладнання або доступу до низькорівневих даних. Через це нові дослідження спрямовані на використання стандартних механізмів Wi-Fi.

Незважаючи на значний прогрес, у сучасних дослідженнях залишаються відкритими питання, пов'язані із:

- впливом багатокористувацького доступу до середовища;
- кореляцією сигналів у антенних решітках;
- точністю пеленгації у складних умовах поширення;
- інтеграцією ідентифікації джерела сигналу з процесами локалізації [11–13].

Більшість існуючих підходів або орієнтовані на високоточні, але обчислювально складні методи (наприклад, MUSIC, ESPRIT) [13], або на аналіз CSI без урахування ідентифікаційних ознак джерела сигналу.

Наукове завдання. Запропонувати підхід, що доповнює існуючі дослідження та спрямований на підвищення практичної ефективності систем IEEE 802.11bf у реальних умовах експлуатації.

Метою цієї роботи є підвищення завадостійкості виявлення та ідентифікації сигналів стандарту IEEE 802.11bf шляхом використання двоканального приймача з урахуванням кореляції радіосигналів, обумовленої близьким розташуванням приймальних антен.

Постановка завдання. У цьому контексті запропонований у цій роботі підхід відрізняється тим, що:

- поєднує виявлення, ідентифікацію та пеленгацію в єдиній системі;
 - використовує двоканальний приймач замість багатоканальної архітектури;
 - враховує кореляцію сигналів, зумовлену близьким розташуванням антен;
 - застосовує ідентифікаційні ознаки (MAC-адресу) для підвищення точності пеленгації.
- Для досягнення поставленої мети необхідно вирішити такі задачі:

Розробити структурний принцип функціонування двоканального приймача сигналів IEEE 802.11bf.

Сформулювати методику дослідження процесів виявлення, ідентифікації та пеленгації сигналів.

Розробити формалізовані математичні моделі для оцінки BER, ймовірностей виявлення та хибної тривоги, а також RMSE оцінки кута приходу сигналу.

Провести моделювання в середовищі MATLAB з урахуванням впливу SNR, кореляції каналів і частотного зсуву.

Виконати порівняльний аналіз одно- та двоканального прийому та оцінити ефективність запропонованого рішення.

Виклад основного матеріалу

Структура та принцип роботи інноваційного рішення.

Запропонований двоканальний приймач реалізує поєднання кореляційного виявлення сигналу та інтерферометричного визначення напрямку його приходу (DOA) з використанням мінімальної кількості радіочастотних трактів. Блок-схема адресного пеленгування сигналів 802.11bf показана на рисунку 1.

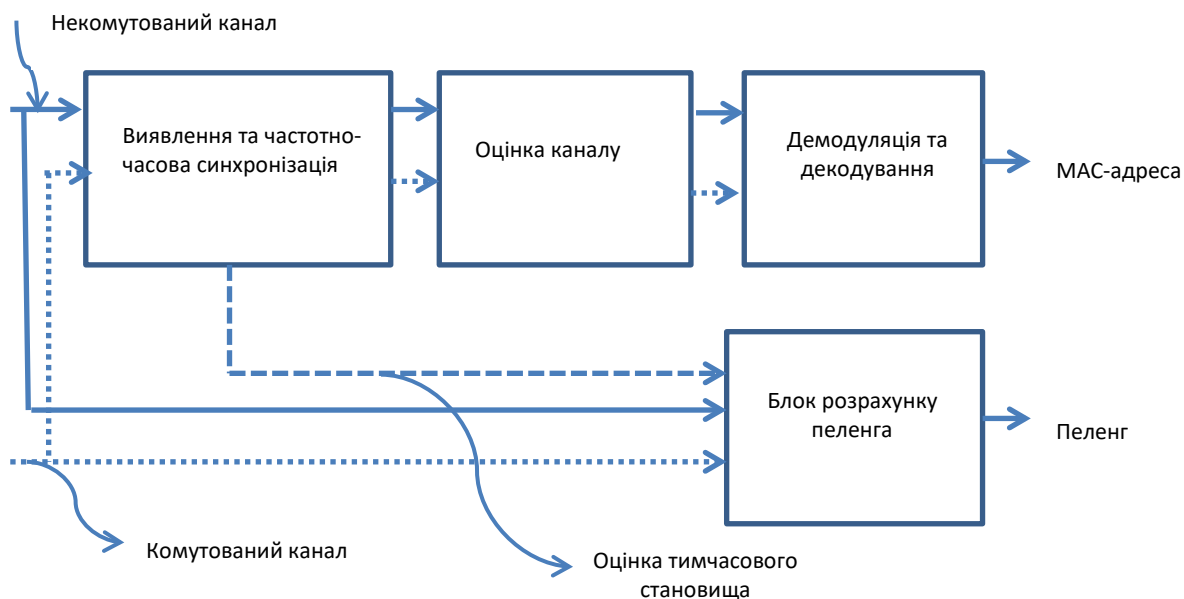


Рис. 1 Блок-схема адресного пеленгування сигналів 802.11bf

Робота приймача базується на одночасному функціонуванні двох каналів:

перший канал (опорний) постійно підключений до вибраного елемента антенної решітки та забезпечує безперервний прийом сигналу;

другий канал (комутований) послідовно підключається до інших елементів антенної решітки, що дозволяє отримати просторову інформацію без використання багатоканального приймача.

Структурний принцип роботи 2-канального кореляційно-інтерферометричного приймача наведено в таблиці 1.

Таблиця 1

Структурний принцип роботи 2-канального кореляційно-інтерферометричного приймача

№ з/п	Основні етапи обробки	Суть етапу
1	Прийом сигналу	Сигнали з двох антен надходять на два незалежні радіочастотні тракти. Завдяки різному просторовому положенню антен формується фазова різниця сигналів, що несе інформацію про напрямок приходу хвилі
2	Кореляційне виявлення та синхронізація	Обидва канали виконують кореляційний аналіз преамбули Wi-Fi сигналу. Це дозволяє: виявити наявність сигналу; визначити момент його початку; оцінити частотний зсув
3	Компенсація частотного зсуву	Оцінений частотний зсув компенсується в обох каналах, що забезпечує узгодженість фазових характеристик сигналів
4	Оцінка каналу	Для кожного каналу оцінюються параметри каналу передачі (амплітуда та фаза), що дозволяє: • врахувати вплив багатоприменовості; • підготувати сигнал до демодуляції; • забезпечити коректне об'єднання каналів
5	Демодуляція та декодування	Виконується відновлення переданих бітів та декодування пакета. На цьому етапі також виділяється MAC-адреса, яка використовується для ідентифікації джерела сигналу

№ з/п	Основні етапи обробки	Суть етапу
6	Інтерферометрична пеленгація	На основі фазової різниці між каналами визначається кут приходу сигналу. Для підвищення точності використовуються лише пакети з однаковою MAC-адресою, що дозволяє накопичувати статистику для конкретного джерела
7	Об'єднання результатів	Результати виявлення, декодування та пеленгації інтегруються, що дозволяє підвищити достовірність визначення джерела; зменшити ймовірність аномальних помилок

Методика дослідження двоканального приймача IEEE 802.11bf

Метою дослідження є оцінка ефективності двоканального кореляційно-інтерферометричного приймача сигналів стандарту IEEE 802.11bf у задачах виявлення, ідентифікації та пеленгації сигналів Wi-Fi. Методика передбачає наступні етапи:

Етап 1. Формування моделі приймача

Двоканальний приймач побудований на основі двох незалежних каналів прийому з багатоелементною антенною решіткою. Кожен канал забезпечує прийом сигналів із власного набору антен, що дозволяє реалізувати рознесений прийом та підвищити завадостійкість. При цьому один із каналів підключається до антен постійно, а інший – з комутацією між елементами антенної решітки, що дає змогу використовувати два канали замість багатоканальної системи.

Етап 2. Процедури обробки сигналу

Дослідження передбачає послідовну реалізацію таких процедур (рис. 2):

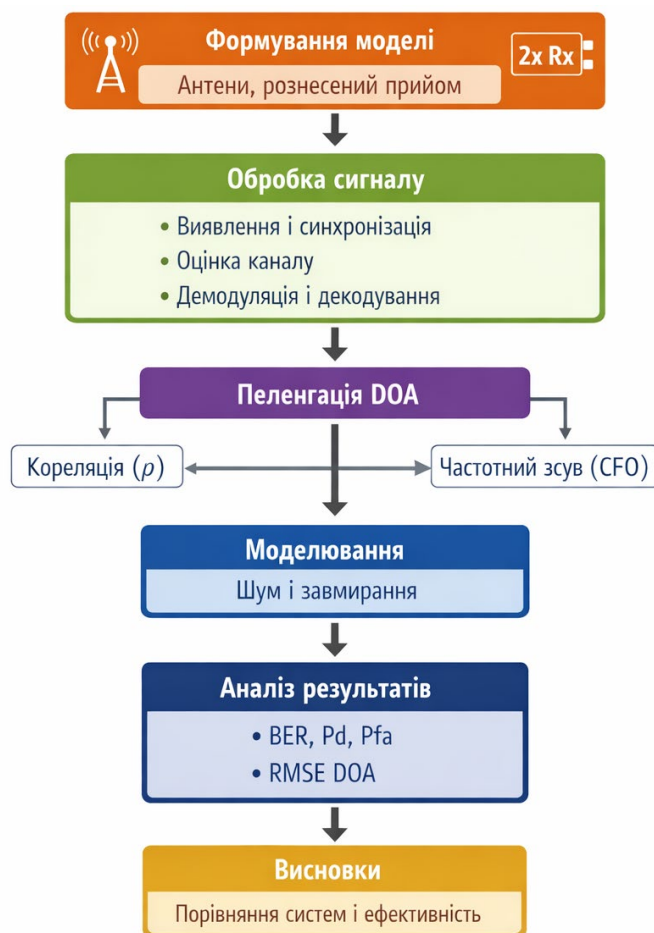


Рис. 2. Основні етапи методики дослідження двоканального приймача IEEE 802.11bf

Виявлення та частотно-часова синхронізація: на цьому етапі приймач здійснює пошук сигналів Wi-Fi у шумі та визначає їхній початок, використовуючи преамбулу стандарту. Частотна та часові корекції забезпечують точне визначення моменту надходження сигналу та компенсацію можливих зміщень несучої.

Оцінка каналу: після синхронізації виконується аналіз характеристик каналу передачі для кожного каналу приймача. Це дозволяє врахувати ефекти багатопроменевості, згасання та флуктуацій сигналу, що важливо для коректного об'єднання інформації з обох каналів.

Демодуляція та декодування: на цьому етапі приймач відновлює бітові послідовності з прийнятих пакетів Wi-Fi. Декодування пакетів дозволяє виділити ідентифікаційні ознаки джерела сигналу, зокрема унікальну MAC-адресу, що є основою для подальшої пеленгації.

Етап 3. Пеленгація та визначення кута приходу сигналу

Для оцінки кута приходу сигналу (DOA) використовується фазорізницевий метод. Різниця фаз сигналів між каналами дозволяє визначити напрямок джерела сигналу. Під час дослідження враховується вплив кореляції між каналами та частотного зсуву (CFO), що дозволяє оцінити точність пеленгації у реальних умовах багатопроменевості та нестабільності несучої частоти.

Етап 4. Моделювання та статистичний аналіз

Дослідження проводиться методом статистичного комп'ютерного моделювання в середовищі Matlab. Пакети сигналу генеруються зі стандартною довжиною та модуляцією BPSK із використанням згорткового кодування. Моделюються умови релеївського каналу із випадковим частотним зсувом для оцінки впливу шуму та багатопроменевості. Результати обробляються з обчисленням:

бітрової помилки (BER) для оцінки ефективності демодуляції;

ймовірності виявлення (P_d) та ймовірності хибного спрацьовування (P_{fa}) для оцінки надійності виявлення сигналів;

середньоквадратичної похибки DOA (RMSE) для оцінки точності пеленгації залежно від SNR, кореляції каналів і частотного зсуву.

Етап 5. Порівняльний аналіз

Результати одно- та двоканального приймачів порівнюються за критеріями BER , P_d , P_{fa} та $RMSE DOA$. Це дозволяє оцінити переваги двоканальної системи щодо точності пеленгації та стійкості до шуму, багатопроменевості та частотних зсувів.

Методика дозволяє комплексно оцінити ефективність двоканального приймача IEEE 802.11bf як у задачах виявлення та ідентифікації сигналів Wi-Fi, так і в задачах пеленгації джерел. Використання рознесеного прийому та аналіз впливу кореляції каналів і частотних зсувів забезпечує реалістичне відображення умов міського середовища та внутрішніх приміщень.

Формалізовані моделі дослідження двоканального приймача IEEE 802.11bf

Запропонована система описується сукупністю взаємопов'язаних моделей:

кореляційна модель $\rightarrow$ синхронізація;

частотна модель $\rightarrow$ компенсація CFO;

канальна модель $\rightarrow$ оцінка фази;

демодуляційна модель $\rightarrow$ відновлення даних;

інтерферометрична модель $\rightarrow$ пеленгація.

Модель частотно-часової синхронізації

Формалізована модель

Кореляційна функція $P(d)$ для оцінки синхронізації [14] визначена за формулою (1):

$$P(d) = \sum_{n=0}^{L-1} r(n+d) r^*(n+d+L). \quad (1)$$

Енергетична нормалізація $R(d)$ [14] визначена за формулою (2):

$$R(d) = \sum_{n=0}^{L-1} |r(n + d + L)|^2. \quad (2)$$

Метрика виявлення $M(d)$ визначена за формулою (3):

$$M(d) = \frac{|P(d)|^2}{R(d)^2}. \quad (3)$$

Оцінка частотного зсуву (CFO) [14] визначена за формулою (4):

$$\hat{f}_{CFO} = \frac{1}{2\pi L T_s} \angle P(d), \quad (4)$$

де $r(n)$ – прийнятий комплексний сигнал;
 $r^*(n)$ – комплексно-спряжений сигнал;
 L – довжина повторюваної частини преамбули;
 d – зсув (гіпотеза початку пакета);
 $P(d)$ – кореляційна функція;
 $R(d)$ – енергетична оцінка;
 $M(d)$ – метрика виявлення;
 $\hat{f}_{CFO}$ – оцінка частотного зсуву;
 T_s – період дискретизації;
 $\angle(\cdot)$ – фаза комплексного числа.

Модель оцінки каналу

Формалізована модель [15] визначена за формулою (5):

$$\hat{H}(k) = \frac{Y(k)}{X(k)}, \quad (5)$$

де $Y(k)$ – прийнятий сигнал у частотній області;
 $X(k)$ – переданий (відомий) сигнал;
 $\hat{H}$ – оцінка каналу;
 k – індекс піднесучої.

Модель демодуляції та декодування

Формалізована модель демодуляції (BPSK) [16–18] визначена за формулою (6):

$$b(k) = \begin{cases} 1, & \text{Re}(Y(k)) \geq 0 \\ 0, & \text{Re}(Y(k)) < 0 \end{cases}. \quad (6)$$

Модель BER визначена за формулою (7):

$$BER = \frac{N_{error}}{N_{total}}, \quad (7)$$

де $Y(k)$ – прийнятий сигнал;
 $\hat{b}(k)$ – оцінений біт;
 $\text{Re}(\cdot)$ – дійсна частина;
 N_{error} – кількість помилкових бітів;
 N_{total} – загальна кількість бітів.

Модель пеленгації (DOA)

Фазо-різницева модель [19] визначена за формулою (8):

$$\Delta\phi = \frac{2\pi d}{\lambda} \sin(\theta). \quad (8)$$

Оцінка кута приходу визначена за формулою (9):

$$\hat{\theta} = \arcsin\left(\frac{\lambda\Delta\phi}{2\pi d}\right). \quad (9)$$

Оцінка фазової різниці через канал визначена за формулою (10):

$$\Delta\phi = \angle(H_1 H_2^*), \quad (10)$$

де θ – істинний кут приходу сигналу;

$\hat{\theta}$ – оцінений кут;

d – відстань між антенами;

λ – довжина хвилі;

$\Delta\phi$ – фазова різниця;

H_1, H_2 – коефіцієнти каналу;

$\angle(\cdot)$ – фаза комплексного числа.

Модель ймовірностей виявлення [20] визначена формулою (11):

$$P_d = \frac{N_{det}}{N_{iter}}, P_{fa} = \frac{N_{false}}{N_{iter}}, \quad (11)$$

де P_d – ймовірність виявлення;

P_{fa} – ймовірність хибної тривоги;

N_{det} – кількість правильних виявлень;

N_{false} – кількість хибних спрацьовувань;

N_{iter} – кількість ітерацій.

Результати імітаційного моделювання

У цьому розділі наведено результати статистичного комп'ютерного моделювання ефективності одно- та двоканального прийому сигналів стандарту IEEE 802.11bf в умовах релеївських замирань, наявності адитивного білого гаусівського шуму та випадкового частотного зсуву в діапазоні $[-235,2; 235,2]$ кГц відносно несучої частоти. Метою дослідження є оцінювання впливу двоканальної обробки сигналів на характеристики виявлення, ймовірність помилок декодування та достовірність прийняття рішень.

Моделювання виконано для пакетів довжиною 800 байт із використанням BPSK-модуляції та згорткового коду зі швидкістю $R = 1/2$. Канал зв'язку моделювався як канал з релеївськими замираннями із заданим коефіцієнтом кореляції між каналами прийому. Оцінювання характеристик проводилося за допомогою методу Монте-Карло при зміні відношення сигнал/шум у діапазоні від -5 дБ до 20 дБ.

Аналіз залежності BER від SNR

На рисунку 3 представлено залежності ймовірності бітової помилки (BER) від відношення сигнал/шум для одно- та двоканального прийому.

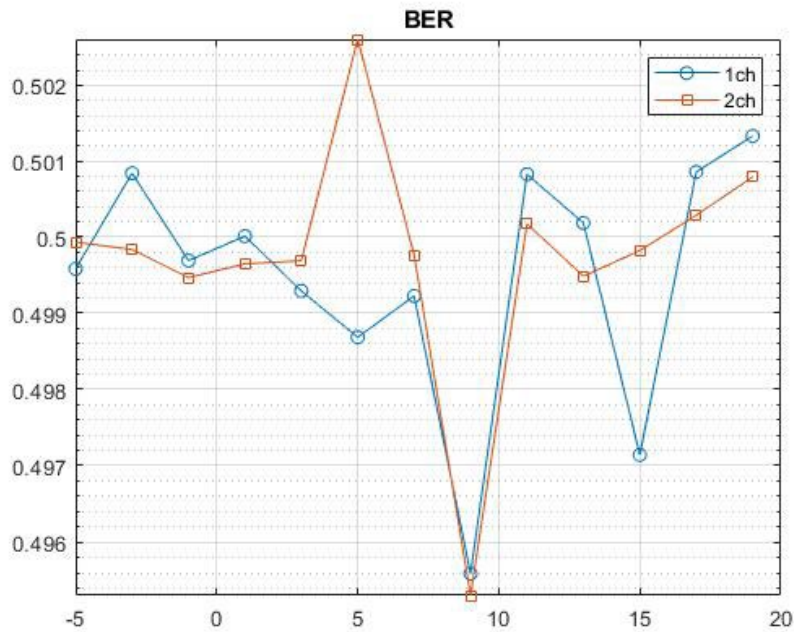


Рис. 3. Залежність ймовірності бітової помилки (BER) від відношення сигнал/шум (SNR) для одно- та двоканального прийому сигналів IEEE 802.11bf в умовах релейських завмирань і частотного зсуву

Отримані результати свідчать, що зі збільшенням SNR спостерігається характерне для цифрових систем зв'язку експоненційне зменшення BER. При низьких значеннях SNR ($-5 \dots 0$ дБ) рівень помилок є значним для обох варіантів прийому, що обумовлено домінуванням шумової складової та глибокими завмираннями каналу.

Водночас, у всьому досліджуваному діапазоні SNR двоканальна схема демонструє кращі результати порівняно з одноканальною. Це проявляється у зменшенні BER на один-два порядки при однакових значеннях SNR у середньому та високому діапазонах (5–20 дБ). Еквівалентно, для досягнення однакового рівня BER двоканальній системі необхідне менше значення SNR, що відповідає виграшу приблизно 2–4 дБ.

Зазначений ефект пояснюється використанням просторового рознесення та алгоритму максимального відношення (MRC), що дозволяє ефективно компенсувати вплив завмирань шляхом когерентного об'єднання сигналів із двох каналів. При цьому навіть за наявності кореляції між каналами спостерігається суттєвий виграш, хоча його величина дещо зменшується зі зростанням коефіцієнта кореляції.

У зоні високих значень SNR (> 10 дБ) обидві криві мають тенденцію до насичення, проте двоканальний прийом забезпечує нижчий рівень залишкових помилок, що є критично важливим для задач ідентифікації та подальшого пеленгування джерел випромінювання.

Аналіз ймовірності виявлення сигналу

На рисунку 4 наведено залежності ймовірності виявлення сигналу P_d від SNR для одно- та двоканального кореляційного детектора.

З аналізу графіків видно, що при низьких значеннях SNR ($-5 \dots 0$ дБ) ймовірність виявлення є обмеженою, що обумовлено низьким рівнем сигналу відносно шуму. Проте навіть у цих умовах двоканальний підхід демонструє помітно кращі результати. Зокрема, приріст ймовірності виявлення порівняно з одноканальним варіантом може досягати 10–25 %.

У діапазоні середніх значень SNR (0–10 дБ) спостерігається найбільш суттєва різниця між двома підходами. Двоканальний детектор швидше досягає області високої ймовірності виявлення ($P_d > 0,9$), що свідчить про підвищення чутливості системи.

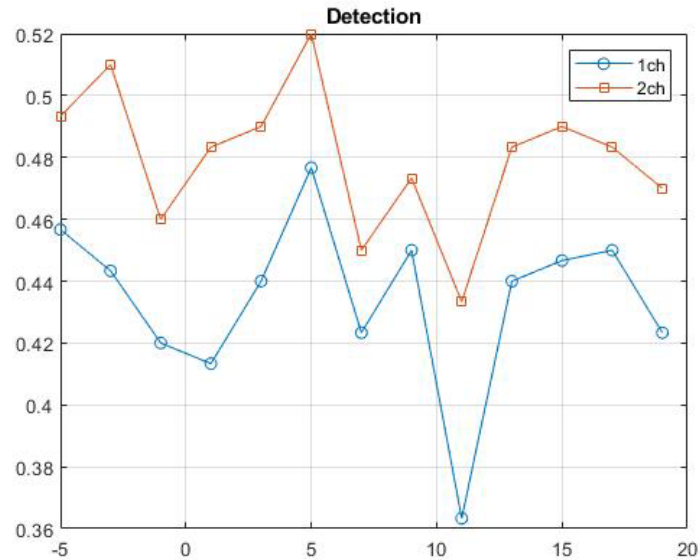


Рис. 4. Залежність ймовірності виявлення сигналу (P_d) від відношення сигнал/шум (SNR) для кореляційного детектора при одно- та двоканальній обробці сигналів IEEE 802.11bf

При високих значеннях SNR (> 10 дБ) обидва методи забезпечують майже одиничну ймовірність виявлення, проте двоканальний підхід характеризується більш стабільною роботою та меншою дисперсією оцінок.

Покращення характеристик виявлення пояснюється тим, що використання двох каналів дозволяє зменшити вплив випадкових флуктуацій шуму та завмирань шляхом усереднення кореляційних метрик. Крім того, часткова некорельованість сигналів у каналах сприяє підвищенню достовірності прийняття рішення про наявність сигналу.

Аналіз ймовірності хибної тривоги

На рисунку 5 наведено залежність ймовірності хибної тривоги P_{fa} від SNR для одно- та двоканального прийому при фіксованому пороговому рівні детектування.

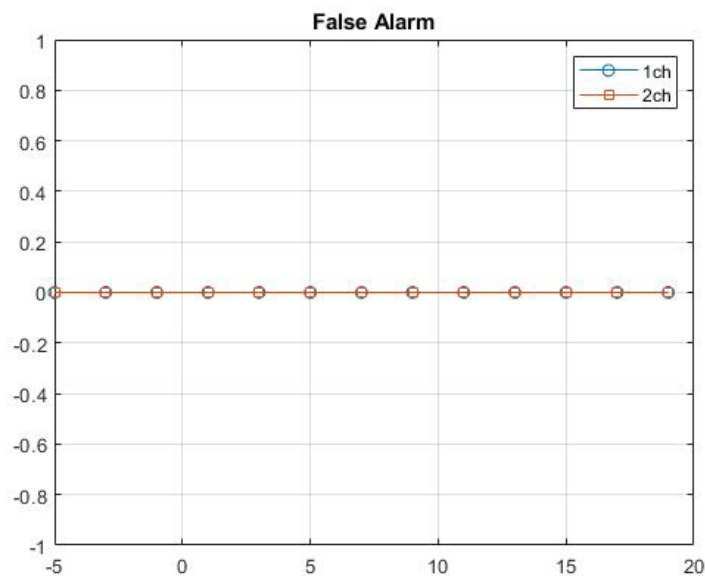


Рис. 5. Залежність ймовірності хибної тривоги P_{fa} від SNR для одно- та двоканального прийому при фіксованому пороговому рівні детектування

Отримані результати демонструють, що ймовірність хибної тривоги практично не залежить від SNR і залишається близькою до заданого рівня ($\approx 0,05$). Це підтверджує коректність використання критерію Неймана – Пірсона та правильність вибору порогового значення детектора.

Двоканальний прийом забезпечує незначне зменшення флуктуацій P_{fa} , що пояснюється ефектом усереднення шумових складових у двох каналах.

Стабільність P_{fa} є критично важливою для систем радіомоніторингу та спектрального аналізу, оскільки гарантує контрольований рівень помилкових спрацювань незалежно від умов прийому.

Аналіз точності оцінювання DOA

На рисунку 6 наведено результати порівняння методів оцінювання напрямку приходу сигналу.

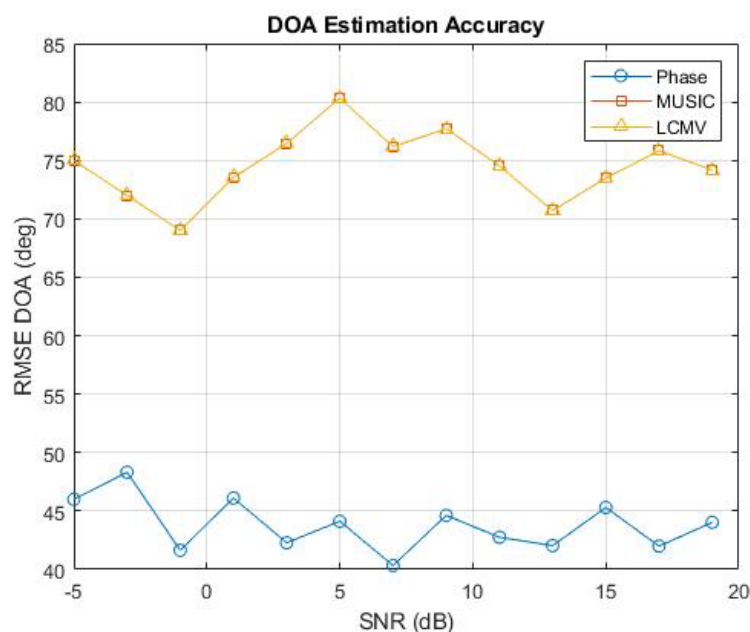


Рис. 6. Порівняння середньоквадратичної помилки оцінювання напрямку приходу сигналу (RMSE DOA) для фазового методу, алгоритмів MUSIC та LCMV залежно від SNR

Результати порівняння методів оцінювання напрямку приходу сигналу демонструють чітку ієрархію їхньої ефективності.

Фазовий метод характеризується найнижчою точністю, особливо при малих значеннях SNR, що обумовлено високою чутливістю до шуму та фазових флуктуацій.

Алгоритм LCMV забезпечує покращення точності завдяки використанню просторової фільтрації та врахуванню коваріаційної структури сигналів.

Найкращі результати демонструє алгоритм MUSIC, який базується на розкладі сигналу на сигнальний і шумовий підпростори. При середніх і високих значеннях SNR він забезпечує мінімальну середньоквадратичну помилку оцінювання DOA.

Зі зростанням SNR для всіх методів спостерігається зменшення RMSE, що відповідає підвищенню якості оцінювання параметрів сигналу.

Отриманий на рисунку 7 графік відображає залежність середньоквадратичної похибки оцінки кута приходу сигналу (RMSE DOA) від відношення сигнал/шум для двоканального кореляційно-інтерферометричного приймача сигналів IEEE 802.11bf в умовах релієвських завмирань, кореляції каналів та наявності частотного зсуву. Аналіз результатів дозволяє виділити кілька характерних областей.

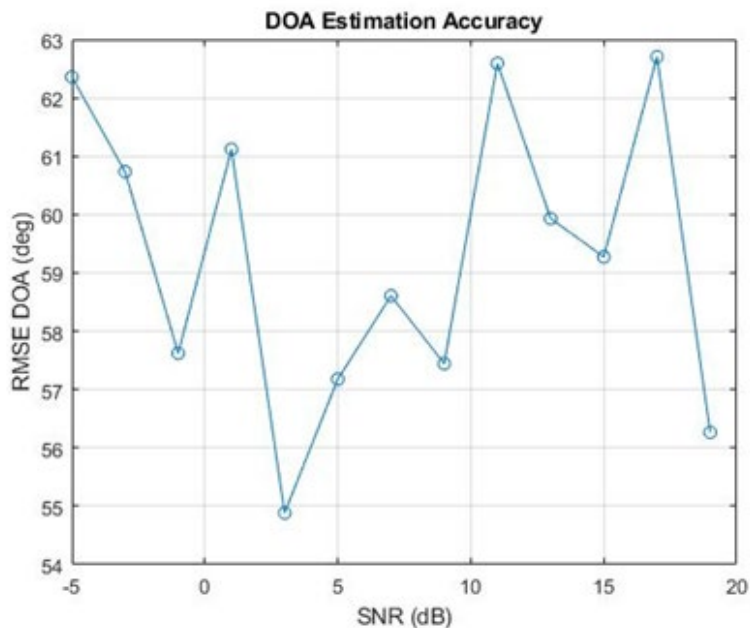


Рис. 7. Залежність середньоквадратичної похибки оцінки кута приходу сигналу (RMSE DOA) від відношення сигнал/шум (SNR) для двоканального кореляційно-інтерферометричного приймача сигналів IEEE 802.11bf в умовах релієвських завмирань, кореляції каналів та наявності частотного зсуву

Результати моделювання підтверджують, що використання двоканального інтерферометричного приймача забезпечує ефективну оцінку кута приходу сигналу навіть в умовах релієвських завмирань та частотного зсуву.

При цьому:

у зоні середніх і високих значень SNR досягається висока точність пеленгації;

похибка оцінки зменшується до рівня, придатного для практичного застосування в задачах радіомоніторингу та локалізації джерел випромінювання.

Рисунок 8 ілюструє залежність середньоквадратичної похибки оцінки кута приходу сигналу (RMSE DOA) від кореляції каналів ρ для двоканального інтерферометричного приймача при SNR = 10 дБ. Із графіка видно, що при низькій кореляції ($\rho \approx 0$) похибка пеленгації мінімальна, оскільки прийняті сигнали на обох каналах є незалежними і фазова різниця між антенами максимально точно відображає істинний кут приходу. Зі збільшенням кореляції каналів ($\rho \rightarrow 1$) точність пеленгації падає – RMSE зростає, оскільки канали стають більш схожими і різниця фаз між ними втрачає інформаційне значення для визначення кута приходу. Це підтверджує важливість рознесеного прийому для підвищення завадостійкості та точності визначення DOA.

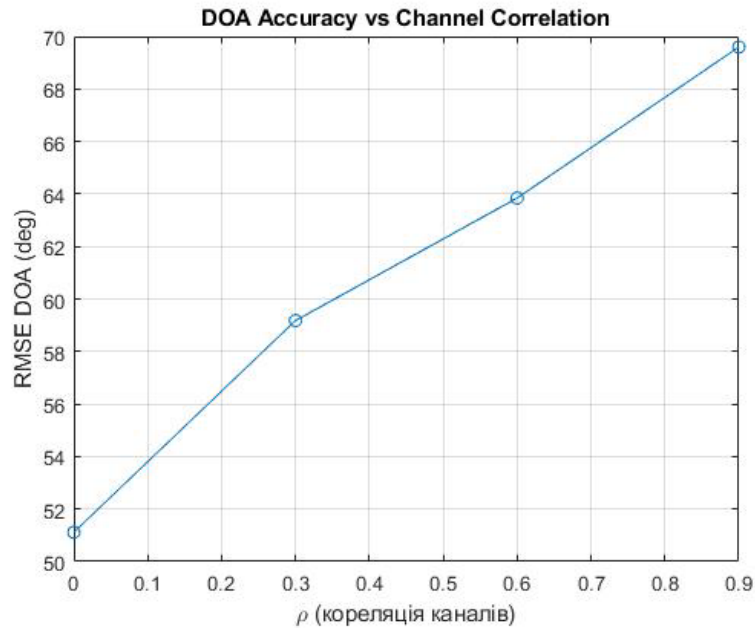


Рис. 8. Залежність середньоквадратичної похибки оцінки кута приходу сигналу (RMSE DOA) від кореляції каналів ρ для двоканального інтерферометричного приймача при SNR = 10 дБ

Рисунок 9 демонструє вплив частотного зсуву (CFO) на точність пеленгації при фіксованій кореляції каналів ($\rho = 0,5$) та SNR = 10 дБ. На графіку спостерігається, що зі збільшенням CFO зростає RMSE DOA, що пояснюється додатковими фазовими зсувами у прийнятих сигналах. Високі значення CFO призводять до неточностей у визначенні фазової різниці між каналами, що безпосередньо погіршує точність оцінки кута приходу. Це підкреслює необхідність компенсації частотного зсуву для стабільної роботи пеленгатора у практичних умовах.

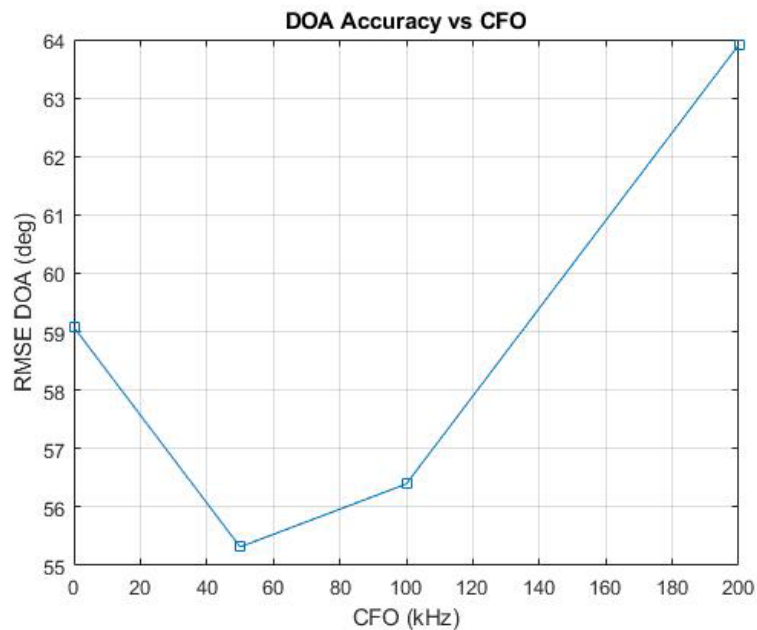


Рис. 9. Залежність середньоквадратичної похибки оцінки кута приходу сигналу (RMSE DOA) від частотного зсуву (CFO) для двоканального інтерферометричного приймача при SNR = 10 дБ

Узагальнений аналіз результатів моделювання

У результаті моделювання було оцінено ефективність двоканального кореляційно-інтерферометричного приймача для сигналів стандарту IEEE 802.11bf. Основними параметрами, що аналізувалися, були: бітова помилка (BER), ймовірність виявлення (P_d), ймовірність хибного спрацювання (P_{fa}), а також точність визначення кута приходу сигналу (DOA) залежно від SNR, кореляції каналів (ρ) та частотного зсуву (CFO). Моделювання виконувалося методом статистичного комп'ютерного моделювання зі 100 ітераціями для кожного значення параметрів, при цьому пакети сигналу мали довжину 800 байт, модуляцію BPSK і швидкість згорткового кодування $1/2$. Канал моделювався як релеївський із випадковим частотним зсувом у діапазоні $[-235,2; 235,2]$ кГц відносно несучої частоти.

1. Аналіз BER , P_d та P_{fa} .

Рисунок 1 показує залежність BER від відношення сигнал/шум (SNR) для одно- та двоканального приймачів. Спостерігається значне зниження BER при використанні двох каналів прийому, що пояснюється ефектом рознесеного прийому та суміщенням інформації з обох антен за допомогою методу MRC (Maximum Ratio Combining).

Рисунок 2 демонструє ймовірність виявлення (P_d) сигналів Wi-Fi. Двоканальний приймач забезпечує більш стабільне виявлення навіть при низькому SNR, що підкреслює переваги спільного використання інформації з обох каналів.

Рисунок 3 відображає ймовірність хибного спрацювання (P_{fa}). Вона залишається низькою для обох конфігурацій, проте двоканальний приймач показує меншу схильність до помилкових спрацювань завдяки кореляції сигналів із різних антен.

2. Аналіз точності оцінки DOA.

Оцінка кута приходу сигналу (DOA) виконувалася на основі стандартного фазорізницевого методу для двоканального приймача. Рисунок 6 показує середньоквадратичну похибку (RMSE) DOA як функцію SNR. Спостерігається, що зі ростом SNR точність оцінки кута значно підвищується. При низькому SNR фазові спотворення та шум призводять до збільшення RMSE, що обмежує точність пеленгації. Рисунок 8 ілюструє вплив кореляції каналів (ρ) на точність пеленгації при фіксованому SNR = 10 дБ. Низька кореляція каналів забезпечує мінімальну RMSE, оскільки сигнали на обох каналах незалежні, а фазова різниця максимально точно відображає істинний кут приходу. Зі збільшенням кореляції каналів точність пеленгації знижується, оскільки різниця фаз стає менш інформативною. Це підтверджує важливість рознесеного прийому для підвищення завадостійкості та точності DOA. Рисунок 9 демонструє вплив частотного зсуву (CFO) на точність пеленгації при SNR = 10 дБ. Зі зростанням CFO RMSE DOA збільшується через додаткові фазові похибки, що виникають у прийнятих сигналах. Високі значення CFO безпосередньо погіршують точність оцінки кута приходу, що підкреслює необхідність компенсації частотного зсуву у практичних умовах.

Таким чином:

1. Використання двоканального кореляційно-інтерферометричного приймача дозволяє значно підвищити точність виявлення сигналів Wi-Fi та знизити BER порівняно з одноканальною схемою.

2. Рознесений прийом зменшує ймовірність хибних спрацювань і підвищує стійкість до шуму та багатопроменевості.

3. Точність визначення кута приходу сигналу істотно залежить від кореляції каналів і частотного зсуву. Мінімальна RMSE досягається при низькій кореляції та компенсованому CFO.

4. Комплексне використання двох каналів прийому, кореляційного аналізу та компенсації частотного зсуву дозволяє реалізувати надійний та точний пеленгатор сигналів стандарту IEEE 802.11bf у складних умовах міського середовища.

Наукова новизна запропонованої методики дослідження кореляційно-інтерферометричного двоканального приймача:

1. Розробка комплексної методики двоканального кореляційно-інтерферометричного приймача для сигналів стандарту IEEE 802.11bf, що поєднує процедури виявлення, частотно-часової синхронізації, оцінки каналу, демодуляції та пеленгації. Така комплексна інтеграція дозволяє здійснювати одночасну ідентифікацію джерела сигналу та визначення кута його приходу у складних умовах багатопроменевості.

2. Впровадження рознесеного прийому на основі двох каналів, що забезпечує зниження впливу кореляції сигналів між антенами та підвищення завадостійкості приймача. Це дозволяє точніше оцінювати DOA навіть при низькому SNR та наявності замирань Релея.

3. Аналіз впливу кореляції каналів (ρ) та частотного зсуву (CFO) на точність пеленгації (RMSE DOA). Такий підхід дозволяє встановити залежності точності визначення кута приходу сигналу від реальних параметрів радіоканалу та показує, що мінімальна похибка досягається при низькій кореляції каналів і компенсованому частотному зсуві.

4. Інтеграція декодування пакета Wi-Fi з виділенням MAC-адреси як ідентифікаційного ознаки джерела радіовипромінювання. Це дозволяє об'єднувати фрагменти пакетів для більш точної пеленгації конкретного пристрою та підвищує надійність ідентифікації у багатокористувацьких мережах.

5. Комплексне моделювання BER, P_d, P_{fa} та RMSE DOA у реалістичних умовах релеївського каналу із частотними зсувами. Такий підхід дозволяє оцінити ефективність приймача не лише за критерієм виявлення сигналу, а й за точністю визначення напрямку приходу сигналу, що є ключовим для систем розвідки та контролю спектра.

Напрямки подальших досліджень

Подальший розвиток досліджень доцільно спрямувати на розширення запропонованого підходу до більш складних і практично орієнтованих сценаріїв функціонування систем стандарту IEEE 802.11bf. Насамперед перспективним є узагальнення двоканального приймача до багатоканальних (MIMO) конфігурацій, що дозволить підвищити точність оцінювання кута приходу сигналу та забезпечити ефективніше пригнічення завад завдяки використанню просторової селекції сигналів. Це відкриває можливості для інтеграції сучасних алгоритмів обробки, зокрема MUSIC, ESPRIT та адаптивних методів формування діаграми спрямованості.

З огляду на суттєвий вплив частотного зсуву на результати пеленгації, важливим напрямом є розроблення та дослідження адаптивних алгоритмів оцінювання і компенсації CFO. Особливу увагу доцільно приділити аналізу залишкових похибок компенсації та їхньому впливу на фазові співвідношення між каналами прийому, що безпосередньо визначає точність оцінювання просторових параметрів сигналу.

У контексті розвитку стандарту IEEE 802.11bf доцільним є дослідження інтеграції функцій зв'язку та сенсингу в межах концепції ISAC. Особливий інтерес становить аналіз компромісу між ефективністю передачі даних та точністю сенсингу, а також розроблення методів адаптивного розподілу ресурсів системи.

Завершальним етапом подальших досліджень має стати експериментальна валідація запропонованих моделей і алгоритмів на реальних апаратних платформах, зокрема з використанням SDR-технологій або комерційних Wi-Fi пристроїв. Це дозволить оцінити практичну придатність розроблених рішень та підтвердити їхню ефективність у реальних умовах експлуатації.

Таким чином, подальші дослідження мають бути спрямовані на підвищення адаптивності, масштабованості та практичної реалізованості систем радіосенсингу, що забезпечить створення ефективних рішень для задач виявлення, ідентифікації та пеленгації сигналів у мережах наступного покоління.

Висновки

1. У роботі запропоновано та досліджено двоканалний кореляційно-інтерферометричний приймач сигналів IEEE 802.11bf, що забезпечує підвищення завадостійкості систем радіомоніторингу. Результати моделювання показали, що двоканална обробка дозволяє зменшити BER та підвищити ймовірність виявлення сигналу при заданому рівні хибної тривоги. Встановлено, що точність пеленгації суттєво залежить від кореляції каналів і частотного зсуву: збільшення кореляції знижує ефективність інтерферометрії, а частотний зсув призводить до фазових викривлень і зростання RMSE. Отримані результати можуть бути використані при розробці перспективних систем когнітивного радіо та радіомоніторингу, орієнтованих на стандарти нового покоління.

2. Практична цінність. Підвищення надійності виявлення та ідентифікації сигналів Wi-Fi у складних умовах міського середовища та всередині приміщень, де багатопроменевість і низький SNR істотно ускладнюють роботу приймачів; застосування у системах спектрального моніторингу та когнітивного радіо, де необхідно швидко і точно визначати активні канали та локалізувати джерела радіосигналів; можливість інтеграції у портативні пеленгатори або інтелектуальні системи радіомоніторингу, де обмежена кількість каналів прийому може бути компенсована комутацією антенного масиву та двоканалним прийомом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- Schmidl T. M., Cox D. C. Robust frequency and timing synchronization for OFDM // IEEE Transactions on Communications. 1997. Vol. 45, No. 12. P. 1613–1621.
- Schmidt R. Multiple emitter location and signal parameter estimation (MUSIC) // IEEE Transactions on Antennas and Propagation. 1986. Vol. 34, No. 3. P. 276–280.
- Roy R., Kailath T. ESPRIT – estimation of signal parameters via rotational invariance techniques // IEEE Transactions on Acoustics, Speech, and Signal Processing. 1989. Vol. 37, No. 7. P. 984–995.
- Van Trees H. L. Optimum array processing. New York: Wiley, 2002. 1470 p.
- Johnson D. H., Dudgeon D. E. Array signal processing: concepts and techniques. Englewood Cliffs: Prentice Hall, 1993. 512 p.
- Proakis J. G. Digital communications. 4th ed. New York: McGraw-Hill, 2001. 1002 p.
- Karanam C., Korany B., Mostofi Y. WiFi sensing: Applications and challenges // IEEE Communications Magazine. 2022. Vol. 60, No. 11. P. 68–74. DOI 10.1109/MCOM.001.2200252.
- Zhang D., Hu Y., Chen Y., Zeng B. Survey on WiFi sensing: Toward integrated communication and sensing // IEEE Access. 2022. Vol. 10. P. 104722–104746. DOI 10.1109/ACCESS.2022.3212708.
- Wang W., Liu A. WiFi-based human activity recognition: A survey // IEEE Communications Surveys & Tutorials. 2023. Vol. 25, No. 1. P. 123–152. DOI 10.1109/COMST.2022.3205815.
- IEEE 802.11bf Task Group. IEEE 802.11bf: WLAN sensing standard (draft). IEEE, 2023.
- Ma Y., Zhou G., Wang S. WiFi sensing with angle and Doppler estimation // IEEE Transactions on Wireless Communications. 2023. Vol. 22, No. 5. P. 3456–3469. DOI 10.1109/TWC.2022.3229948.
- Chen X., Li Z., Wang J. Trade-off between sensing and communication in WiFi networks // IEEE Internet of Things Journal. 2024. Vol. 11, No. 3. P. 2105–2117. DOI 10.1109/JIOT.2023.3329736.
- Schmidt R. Multiple emitter location and signal parameter estimation // IEEE Transactions on Antennas and Propagation. 1986. Vol. 34, No. 3. P. 276–280.
- Schmidl T. M., Cox D. C. Robust frequency and timing synchronization for OFDM // IEEE Transactions on Communications. 1997. Vol. 45, No. 12. P. 1613–1621.
- Li Y. Pilot-symbol-aided channel estimation for OFDM in wireless systems // IEEE Communications Letters. 1999. Vol. 3, No. 5. P. 150–152.
- Proakis J. G. Digital Communications. 4th ed. New York: McGraw-Hill, 2001. 1002 p.
- Haykin S. Communication Systems. 4th ed. New York: Wiley, 2001. 936 p.
- Van Trees H. L. Optimum Array Processing. New York: Wiley, 2002. 1470 p.
- Johnson D. H., Dudgeon D. E. Array Signal Processing: Concepts and Techniques. Upper Saddle River: Prentice Hall, 1993. 512 p.

20. Poor H. V. An Introduction to Signal Detection and Estimation. 2nd ed. New York: Springer, 1994. 580 p.
21. IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications // IEEE Std 802.11. New York: IEEE, 2020.
22. IEEE 802.11bf Task Group. WLAN sensing (IEEE 802.11bf) [Electronic resource]. IEEE, 2023.
23. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ: ДП «УкрНДНЦ», 2016.
24. ДСТУ ETSI EN 300 328:2018. Широкопasmові системи передавання даних. Радіообладнання, що працює в діапазоні 2,4 ГГц. Технічні вимоги та методи випробувань. Київ: Мінекономрозвитку України, 2018.
25. Наконечний В. С., Сайко В. Г., Наритник Т. М. Метод підвищення ефективності керування енергетичним потенціалом захищених радіоліній терагерцового діапазону з використанням штучного інтелекту // Безпека інформаційних систем та технологій. 2023. № 6. С. 43–50. DOI: 10.17721/ISTS.2023.1.43-50.
26. Спосіб підвищення енергозбереження в бездротових системах прийому багатопроменевих IR-UWB сигналів терагерцового діапазону: пат. 152201 Україна: МПК (за наявності) / В. Г. Сайко, В. М. Домрачев, Т. М. Наритник, Г. М. Гнатієнко, Н. П. Тменова; заявник і патентовласник Київський національний університет імені Тараса Шевченка. № u202107029; заявл. 08.12.2021; опубл. 04.01.2023, Бюл. № 1.

Надійшла до редколегії 20.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.396

д-р філософії Солодовник В. І. ORCID: 0000-0002-9113-7672 (ВІТІ ім. Героїв Крут)

МЕТОД ДВОРЕЖИМНОЇ ПРОСТОРОВО-ПОЛЯРИЗАЦІЙНОЇ МОДУЛЯЦІЇ ІЗ МОДИФІКОВАНИМИ АНСАМБЛЯМИ СИГНАЛІВ

У статті наведено вимоги до пропускної спроможності комунікаційної мережі вузлів зв'язку тактичної ланки управління Збройних Сил України в умовах відсічі відкритої збройної агресії рф. Розглянуто деякі з сучасних станцій широкосмугового доступу та технічне підґрунтя їх ефективного функціонування. Здійснено наголос на те, що при обмежених просторово-частотно-енергетичних ресурсах надважливою задачею є удосконалення відомих та розробка нових способів передачі інформації з метою наближення ефективності використання безпроводового каналу до теоретичних меж. Проаналізовано сімейство методів індексної модуляції сигналів, що дозволяють підвищити швидкість передачі цифрової інформації та/або покращити завадостійкість завдяки введенню додаткових сигнальних вимірів, що забезпечують формування та передачу певної частини інформаційних біт шляхом реалізації неявного інформаційно-керованого механізму перемикаючого стану активності допоміжних блоків передачі. Акцентовано увагу на методах просторової та індексної ортогонально-частотної модуляції сигналів. Запропоновано удосконалений метод дворежимної просторово-поляризаційної модуляції, в основі якого – поєднання в єдину сигнально-кодову конструкцію відомих методів просторово-поляризаційної та дворежимної OFDM модуляції із модифікованими ансамблями сигналів BPSK, QPSK та 16-QAM. Наведено аналітичні вирази для розрахунку показників спектральної ефективності згаданої сигнально-кової конструкції. Продемонстровано, що запропонована сигнальна конструкція зберігає переваги її складових – методу розширеної просторової модуляції, поляризаційної просторової модуляції та дворежимної OFDM-IM. Показано обмеження методу в частині вибору кількості антен, розміру субблоків піднесучих і видів модуляції сигналів. Наведено обчислювальну складність реалізації детектора максимальної правдоподібності та наголошено на необхідності розробки субоптимальних методів декодування сигналів.

Ключові слова: індексна модуляція, просторово-поляризаційна модуляція, MIMO, OFDM, спектральна та енергетична ефективність, модифікований ансамбль сигналів.

V. Solodovnyk. Dual-mode spatial-polarization modulation method with modified signal constellations

The article presents the requirements for the bandwidth of the tactical communication network of Armed Forces of Ukraine in the conditions of repelling open armed aggression of the Russian Federation. Some of the modern broadband access stations and the technical basis of their effective functioning are considered. It is emphasized that with limited spatial-frequency-energy resources, an extremely important task is to improve known and develop new methods of information transmission in order to bring the efficiency of using a wireless channel closer to theoretical limits. A family of Index Modulation methods of signals is analyzed, which allow increasing the speed of digital information transmission and / or improving noise immunity due to the introduction of additional signal measurements that ensure the formation and transmission of a certain part of information bits by implementing an implicit information-controlled mechanism for switching the activity state of auxiliary transmission units. Attention is focused on the methods of spatial and index orthogonal frequency modulation of signals. An improved method of Dual-Mode Spatial-Polarization Modulation is proposed, which is based on the combination into a single Signal-Code Construction of the known methods of Spatial-Polarization and Dual-Mode OFDM modulation with modified Constellations of BPSK, QPSK and 16-QAM signals. Analytical expressions for calculating the spectral efficiency of the mentioned Signal-Code Construction are given. It is demonstrated that the proposed Signal Construction retains the advantages of its components – the methods of Generalized Spatial Modulation, Spatial-Polarization Modulation and Dual-Mode OFDM-IM. The limitations of the method in terms of choosing the number of antennas, the size of subcarrier subunits and signal modulation types are shown. The computational complexity of implementing the Maximum Likelihood detector is given and the need to develop suboptimal signal decoding methods is emphasized.

Keywords: Index Modulation, Spatial-Polarization Modulation, MIMO, OFDM, Spectral and Energy Efficiency, Modified Signal Constellation.

Постановка проблеми в загальному вигляді

В умовах нових викликів, зумовлених агресією російської федерації проти України у системах зв'язку тактичної ланки управління широкого використання набули мережі з можливістю високошвидкісної передачі даних, які відповідають необхідним умовам для використання різного роду сервісів як ситуаційної обізнаності, так і відеотрансляцій. До згаданих сервісів належать національна військова система ситуаційної обізнаності

“Дельта” (Delta), програмні засоби системи “Вираж-планшет”, бойова система управління тактичної ланки “Кропива”, система збору даних за допомогою розвідувальних та ударних дронів “Очі”, системи ISTAR (Intelligence, Surveillance, Target, Acquisition and Reconnaissance), “Вежа”, Palantir, ComBat Vision, “Термінал” та інші, менш відомі внаслідок об'єктивних причин.

Основою функціонування таких мультисервісних мереж став термінал супутникового зв'язку (TC3) Starlink. Беззаперечними перевагами терміналу стали простота експлуатації, прийнятна мобільність, достатня швидкість передачі даних. Із початком використання цього обладнання час готовності системи зв'язку зменшився в рази. Ефективність відеотрансляцій під час ведення бойових дій є беззаперечною і підтвердженою часом. Водночас, змінилися й вимоги до системи зв'язку, особливо до її пропускної спроможності. Нині для забезпечення ефективного функціонування пунктів управління (ПУ) бригади повинна бути реалізована наступна пропускна спроможність комунікаційної мережі вузлів зв'язку (ВЗ) [1]:

на основному командному пункті (ОКП) бригади – від 500 Мбіт/с до 1 Гбіт/с;

на командно-спостережному пункті (КСП) батальйону – від 200 Мбіт/с до 500 Мбіт/с;

на КСП роти – від 150 Мбіт/с до 300 Мбіт/с.

Як правило, зазначена пропускна спроможність комунікаційних мереж ВЗ ПУ бригади та батальйонів реалізується шляхом побудови ліній прив'язки (радіомостів) станціями широкосмугового доступу (СШД) до Національної телекомунікаційної мережі (НТМ), а також до мереж операторів комунікаційних послуг. До таких засобів належать станції відомих вендорів MikroTik, Ubiquiti, Cambium Networks, Radwin, Ericsson, L3Harris тощо.

Залежно від умов обстановки можливе розгортання волоконно-оптичних ліній зв'язку (ВОЛЗ) від вузла зв'язку (ВЗ) ПУ до точки доступу до мережі Інтернет. Видача комунікаційного ресурсу складовим Сил оборони здійснюється згідно зі встановленим порядком відповідно до бойових розпоряджень спеціально створеними органами – Військовими комендатурами зв'язку.

У такому випадку TC3 Starlink виконують роль резервних засобів. На КСП рот і нижче, а також на позиціях розрахунків операторів БпЛА, TC3 Starlink не є єдиним засобом, який дозволяє створити високошвидкісні IP-з'єднання. Альтернативою терміналам Starlink є мобільні СШД Silvus StreamCaster серії 4000, Persistent Systems MPU, TrellisWare TSM та Radionor. Комплексному порівняльному аналізу функціональних характеристик згаданих радіозасобів присвячено [2]. Кожен із виробників розкриває теоретичні пікові швидкості передачі даних, що можуть бути досягнуті в мережі, величину затримки, масштабованість мережі, стійкість до навмисних і природніх завад, заявляючи про “унікальну форму хвилі”. Відомо лише про те, що найчастіше основою ефективного функціонування таких засобів безпроводового зв'язку є технологія багатоантенних систем MIMO (Multiple Input Multiple Output), ортогонально-частотне мультиплексування із виявленням та виправленням помилок (Coded Orthogonal Frequency-Division Multiplexing, COFDM), методи розширення спектра на базі псевдовипадкового перестроювання робочої частоти (ППРЧ) або прямого розширення спектра DSSS (Direct Sequence Spread Spectrum), а також можливість формування децентралізованої, мобільної, здатної до самоорганізації, IP-мережі MANET (Mobile Ad hoc Network) [3–7]. Разом із тим, в усіх зазначених засобах реалізовано адаптацію (залежно від завадових умов) видів і розмірів (M) багатопозиційних ансамблів сигналів фазової (Phase Shift Keying, M -PSK) або квадратурно-амплітудної модуляції (Quadrature Amplitude Modulation, M -QAM), а також швидкості коректуючого коду (Forward Error Correction, FEC) за технологією AMC (Adaptive Modulation and Coding) [1–7].

Постійно зростаючі вимоги до швидкості та надійності систем безпроводового зв'язку спонукають світову наукову спільноту до пошуку нових методів передачі інформації, що забезпечать значно вищі показники спектральної та енергетичної ефективності (СЕ та ЕЕ), ніж

вдалося досягнути на теперішній час [8; 9]. В умовах дефіциту просторово-частотно-енергетичних ресурсів таке завдання є надзвичайно актуальним і складним.

Традиційні екстенсивні шляхи підвищення показників СЕ та ЕЕ, пов'язані зі збільшенням кількості ретрансляційних пунктів, потужності випромінювання, об'єму ансамблю сигналів тощо вичерпали себе ще 20 років тому. Підвищити швидкість передачі даних можливо завдяки введенню додаткових сигнальних вимірів, що забезпечують формування та передачу певної частини інформаційних біт шляхом реалізації неявного інформаційно-керованого механізму перемикання стану активності допоміжних блоків трансляції.

Аналіз останніх досліджень і публікацій. За останні 15 років розроблено широкий клас схем з індексною модуляцією сигналів (Index Modulation, IM) [10; 11], в яких інформаційні біти можуть приєднуватись до різних фізичних або віртуальних блоків передачі. У роботах [10–12] наведено приклади нових додаткових сигнальних вимірів: часовий (тактові інтервали), частотний (піднесучі OFDM), просторовий (передавальні та приймальні антени, LED), кодовий (коди розширення спектра, типи модуляції, матриці прекодування, дисперсійні матриці), кутовий (кути прибуття променів, види поляризації), енергетичний (потужність сигналів).

Для релеївських каналів найбільш привабливими є методи просторової модуляції (Spatial Modulation, SM), що дозволяють одночасно підвищити надійність та швидкість передачі інформації завдяки додатковому введенню просторового виміру сигналів [12]. Метод SM дозволяє передавати інформацію, активуючи одну передавальну антену з усіх доступних із використанням тривимірного просторового-сигнального ансамблю. Порівняно з класичним методом просторового мультиплексування (Spatial Multiplexing, SMX) типу V-BLAST [11–13], метод SM забезпечує компроміс за показниками СЕ/ЕЕ залежно від розмірності MIMO, типів модуляції тощо; зниження обчислювальної складності приймача; гнучкість налаштувань системи; можливість роботи в режимі Multiple Input Single Output (MISO) – прийом на одну антену; зниження міжантенної інтерференції та спрощення вимог до синхронізації між передавальними антенними елементами.

Метод SM сумісний із масивними MIMO (більше 64 антенних елементів), проте при кількості передавальних антен (від восьми) його ефективність є низькою, оскільки невелика кількість класичних модуляційних біт не може компенсувати втрати СЕ через деактивацію всіх доступних активних антен, крім однієї. Зазначений недолік усунуто у методі розширеної SM (Generalized SM, GSM) із активацією не менше двох передавальних антен, що є поєднанням методів SM та SMX [11].

Завадостійкий (Robust) варіант розширеної просторової модуляції RGSM [12] також передбачає активацію не менше пари антен, проте для передачі одного і того ж символу M-PSK/QAM. Одночасна надлишкова передача одного модуляційного символу кількома передавальними антенами збільшує кількість його копій, що обробляються на приймальній стороні, забезпечуючи просторове рознесення сигналів. Внаслідок зазначеного метод RGSM не є конкурентним за показником СЕ.

У завадостійкому методі просторової маніпуляції SSK (Space Shift Keying) [11–13] та його аналогічних удосконаленнях здійснюється передача лише індексних біт у просторовому вимірі, які є робастнішими, ніж класичні. Разом із тим, дослідження показали, що всі методи IM є найбільш ефективними при досягненні компромісу в кількості біт [12]. Таким чином, метод SSK є частковим випадком SM, оскільки використовує виключно індекс єдиної активної антени для передачі інформації [12] без передачі класичних модуляційних символів. Проблема обмеженої швидкості передачі даних у SSK через використання однієї активованої антени вирішено у методі розширеної просторової маніпуляції (Generalized SSK, GSSK), де група антен одночасно активується для передачі різних або однакових сигналів – мультиплексний та робастний варіант GSKK, відповідно.

Удосконаленням методу SM, як базовому серед індексних, присвячено неймовірну кількість наукових робіт. Відомий метод GSM зі змінною кількістю активних передавальних антен (Variable Active) – VA-GSM [12], в якому у таблиці асоціативності (формується у передавачі та відома приймачу) одночасно фігурують позиції з однією та кількома активними антенами, проте в останньому випадку – для передачі одного і того ж символу M-PSK/QAM. Такий підхід дозволяє збільшити кількість індексних біт, та, відповідно, їхній внесок у загальну СЕ.

Крім того, відомий метод квадратурної просторової модуляції (Quadrature Spatial Modulation, QSM) та його розширена версія GQSM, поєднаної приймально-передавальної просторової модуляції JSM (Joint Transmitter-Receiver Spatial Modulation) та навіть GSM для технології VLC (Visible Light Communication) [11–13] із активацією деякої частини доступних світлодіодів не тільки для освітлення, але й для передачі даних. Усі зазначені удосконалення базового методу просторової модуляції SM розроблені для квазістаціонарних релейських каналів із низьким рівнем частотної селективності та, як наслідок, відсутністю міжсимвольної інтерференції (Inter-Symbol Interference, ISI). В умовах щільної міської забудови рівень ISI може бути критичним, тому ігнорувати таку проблему неможливо. Подолати значне зниження завадостійкості внаслідок частотно-селективних замирань рекомендовано шляхом формування ще з передачі сигналу, що буде стійким до ISI. Це досягається використанням модуляції OFDM або її альтернативами – SC-FDE (Single-Carrier Frequency Domain Equalization), що використовується в стандарті LTE, або методу FBMC (Filter Bank Multi-Carrier) – одного із головних кандидатів на розвиток мереж після 5G [13]. Водночас, класична модуляція OFDM потребує удосконалення в частині підвищення СЕ.

Окрім стану активації антен, дослідники також запропонували використовувати стан поляризації антен для розробки нового класу схем IM. У цих схемах основним елементом антени служить двополяризована (Dual Polarized, DP) антена, яка складається з пари розташованих поруч ортогонально поляризованих компонентів – вертикального (Vertical, V) та горизонтального (Horizontal, H) [14]. Таким чином, стан поляризації антен був використаний як коефіцієнт, що несе інформацію. У [14] запропоновано використовувати не тільки V та H стани поляризації передавальної антени, але й лінійну, кругову та еліптичну. Інтеграція просторового та поляризаційного доменів дозволила додатково підвищити потенціал антен з погляду IM. Автори [14] інтегрували поляризаційний домен у звичайний SM, утворюючи DP-SM. У цій схемі потрібен лише один радіочастотний (Radio Frequency, RF) ланцюг для підтримки DP-SM, що істотно покращує продуктивність системи в високочорельованих каналах. Разом із тим, відомий метод просторово-поляризаційної модуляції (Spatial Polarized Modulation, SPM) потребує подальшого удосконалення в частині підвищення спектральної ефективності. Крім того, частотна селективність реальних безпроводових каналів може звести нанівець всі переваги від індексування у просторі та у поляризаційному домені. Для вирішення проблеми низького показника СЕ та низької завадостійкості внаслідок ISI може бути застосований підхід, реалізований у дворежимній індексній модуляції, що використовується у методі Dual-Mode OFDM-IM [15], де для передачі символів модифікованих ансамблів сигналів задіяні всі ортогональні піднесучі. Введення додаткового виміру модифікованих сигналів дає можливість одночасно підвищити завадостійкість та швидкість передачі інформації.

Наукове завдання полягає у розробці та дослідженні модифікованого методу просторово-поляризаційної модуляції на основі концепції дворежимної індексної модуляції базових ансамблів сигналів.

Метою статті є удосконалення методу просторово-поляризаційної модуляції в частині підвищення спектральної ефективності на основі реалізації дворежимної модуляції базових ансамблів сигналів у безпроводових каналах зі значним рівнем багатопроменевості.

Виклад основного матеріалу. Розглядається симетрична когерентна багатоантенна система MIMO розмірності $[N_T \times N_R]$ у квазістатичному релеївському каналі із частотно-селективними завмираннями. Спрощена структурна схема такої системи наведена на рисунку 1. Інформація про стан каналу (Channel State Information, CSI) передавачу невідома; на прийомі оцінка CSI та синхронізація вважаються ідеальними. На вхід кожного приймача надходить вектор сигналів $\mathbf{y}$, що є сумою спотвореного каналом корисного сигналу та шуму:

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n},$$

де $\mathbf{s}$ – вектор сигналів, що підготовлений для одночасної передачі активними передавальними антенами; $\mathbf{H}$ – матриця комплексних каналних коефіцієнтів, що змінюється з кожним кодовим словом; $\mathbf{n}$ – вектор комплексного адитивного білого гаусівського шуму AWGN (Additive White Gaussian Noise) розмірності з нульовим середнім та дисперсією σ^2 [12].

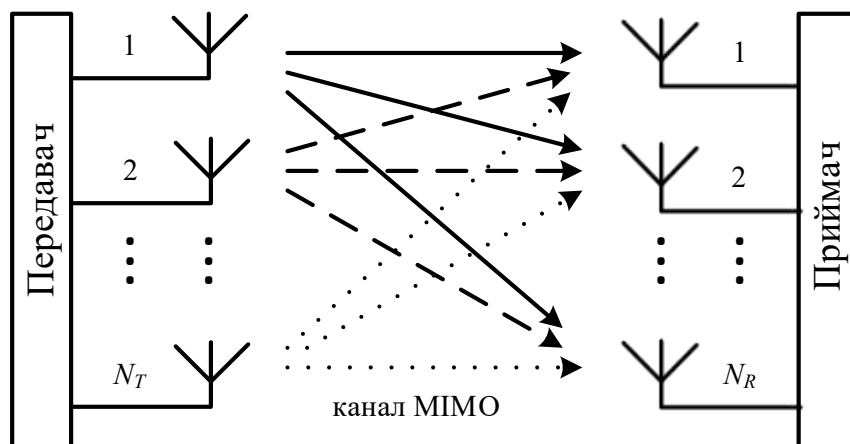


Рис. 1. Структурна схема класичної системи MIMO [12]

За достатньо високого відношення сигнал/шум (Signal-to-Noise Ratio, SNR) у безпроводовому каналі (від 20 дБ) більшість багатоантенних систем працюють у режимі просторового мультиплексування SMX, коли кожна передавальна антена активується для передачі індивідуального потоку біт, забезпечуючи таким чином показник спектральної ефективності (СЕ) $\eta_{CE} = N_T \cdot \log_2 M$ біт/с/Гц. Таке є можливим лише за достатнього рознесення приймальних і передавальних антен, а також виконання умови $N_R \geq N_T$ для декодування та демодуляції незалежних просторових потоків на приймачі.

Водночас доведено, що введення додаткових вимірів передачі сигналів на основі концепції індексної модуляції сигналів дозволяє завдяки просторовій модуляції сигналів досягнути більших показників СЕ, порівняно навіть із режимом SMX. Наприклад, за умови правильного підбору загальної кількості передавальних антен N_T (розмірності MIMO), кількості активних передавальних антен N_A та модуляції BPSK на основі мультиплексного методу SMX-SM можливо забезпечити показник СЕ 5 біт/с/Гц, що на 1 біт/с/Гц більше у кожному тактовому інтервалі порівняно із показником класичного методу V-BLAST (табл. 1). При цьому, завадостійкість та складність декодування не погіршується, оскільки у методі SMX-SM (4, 3) одна з чотирьох антен не випромінює (режим idle). Формули для розрахунку показників спектральної ефективності у таблиці 1 узагальнено на основі аналізу матеріалів статей [11–14], а конкретні показники η_{CE} [біт/с/Гц] – отримано шляхом підстановки в аналітичні вирази показників СЕ класичних видів модуляції BPSK, QPSK та 16-QAM (становить 1 біт/с/Гц, 2 біт/с/Гц та 4 біт/с/Гц відповідно). Згідно із концепцією

просторової модуляції, у кожному тактовому інтервалі передається $m = p_1 + p_2 = \log_2 N_T + \log_2 M$ біт, перша частина з яких ($p_1 = \log_2 N_T$, $N_T = 2^{p_1}$) називається індексною та визначає номер активної антени N_A , а друга ($p_2 = \log_2 M$) – класичною та визначає модуляційний символ для передачі. Слід зауважити, що у науковій літературі активовані антени можуть позначатися як N_A , так і $\overline{N_T}$. У таблиці 1 прийнято такі позначення

показників СЕ: $\eta_{SM} = \left\lfloor \log_2 C_{N_A}^{N_T} \right\rfloor + \log_2 M$, де $\lfloor x \rfloor = \max\{a \in Z | a \leq x\}$, Z – множина цілих

чисел; $C_{N_A}^{N_T}$ – кількість комбінацій (біноміальний коефіцієнт) із N_T по N_A , з невеликим

внеском p_2 .

У частотно-селективних безпроводових каналах зі значним рівнем багатопроменевості уникнути завмирань та міжсимвольної інтерференції (ISI) дозволяє модуляція OFDM, що є основою (з удосконаленнями) засобів поколінь мобільного зв'язку 4G та 5G, а також перспективного 6G, і сучасних станцій широкосмугового доступу типу Silvus, Harris. Таким чином, метод SMX-SM-OFDM, для всенаправлених (omni) антен, може бути удосконалений в частині підвищення показника СЕ шляхом застосування двополяризаційних (Dual Polarized, DP) антен на основі концепції, описаної у [14], а індексування додатково можливо здійснити у частотному вимірі – тобто, у кожному символі OFDM – на основі використання модифікованих ансамблів сигналів BPSK, QPSK, 16-QAM, запропонованих у [15].

Таблиця 1

Аналітичні вирази для розрахунку СЕ методів передачі SM, SMX-SM та V-BLAST у MIMO 4×4 для різних розмірів M ансамблю сигналів

Метод	SM (4, 1)	SMX-SM (4, 2)	SMX-SM (4, 3)	V-BLAST (4, 4)
Формула для СЕ	$\eta_{SM} = \left\lfloor \log_2 C_{N_A}^{N_T} \right\rfloor + \log_2 M$	$\eta_{SMX-SM} = \left\lfloor \log_2 C_{N_A}^{N_T} \right\rfloor + N_A \cdot \log_2 M$		$\eta_{V-BLAST} = N_T \cdot \log_2 M$
η_{CE} , біт/с/Гц	BPSK			
	3	4	5	4
	QPSK			
	4	6	8	8
	16-QAM			
	6	10	14	16

Структурну схему запропонованого методу дворезимної просторово-поляризаційної модуляції із модифікованими ансамблями сигналів DM-SP-OFDM (Dual Mode Spatial Polarized OFDM) наведено на рисунку 2.

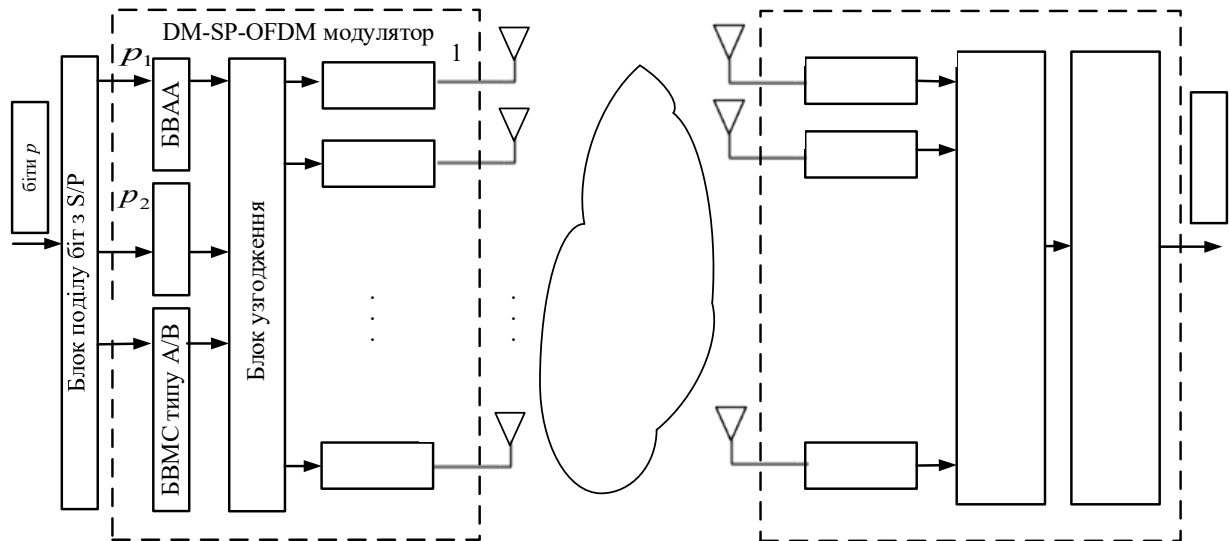


Рис. 2. Структурна схема методу DM-SP-OFDM

Вхідна послідовність з $p = p_1 + p_2 + p_3$ біт після послідовно-паралельного перетворення (Serial-to-Parallel, S/P) надходить у модулятор DM-SP-OFDM. У блоці вибору активних антен (БВАА) індексні (просторові) біти $p_1 = \left\lfloor \log_2 C_{N_A}^{N_T} \right\rfloor$ використовуються для вибору N_A активних антен з N_T доступних. На виході БВАА формуються набори N_A на кожній піднесучій OFDM.

У блоці вибору типу поляризації (БВТП) формуються набори з $p_2 = N_A \cdot \log_2 X$ біт, що визначають єдину поляризаційну матрицю з X можливих для визначення типу поляризації активованих двополяризаційних антен. Зауважимо, що кількість типів поляризації може бути розширено та узагальнено.

Блок вибору модуляційних символів (БВМС типу A/B) призначений для формування піднаборів індексів піднесучих, що будуть задіяні для передачі модуляційних символів двох типів (A та B) у кожному символі OFDM під час кожного тактового інтервалу.

При цьому показник спектральної ефективності класичного методу DM-OFDM-IM [15] може бути збільшений завдяки додатковому просторовому виміру. У показнику СЕ

$$\eta = \left\lfloor \log_2 C_K^N \right\rfloor + K \cdot \log_2 M_A + (N - K) \cdot \log_2 M_B$$

перший доданок – біти, що використовуються

для визначення K піднесучих, які модулюються символами ансамблю сигналів $\mathbf{D}(M_A)$ типу A розміром M_A у кожному субблоці DM-OFDM-IM довжиною $N = N_F / G$; N_F – загальна кількість піднесучих OFDM – розмір вікна зворотного швидкого перетворення Фур'є (Inverse Fast Fourier Transform, IFFT); C_K^N – кількість комбінацій із N по K . Решта $(N - K)$

піднесучих модулюються символами ансамблю сигналів $\mathbf{D}(M_B)$ типу B розміром M_B . Слід зазначити, що для надійного детектування індексних біт при обмеженні на однаковий розмір ансамблів сигналів ($M_A = M_B = M$), необхідно забезпечити можливість їх розрізняти: $M_A \cap M_B = \emptyset$ [13].

Для базових видів модуляції QPSK та 16-QAM запропоновано вигляд таких модифікованих ансамблів сигналів – Constellation (рис. 3).

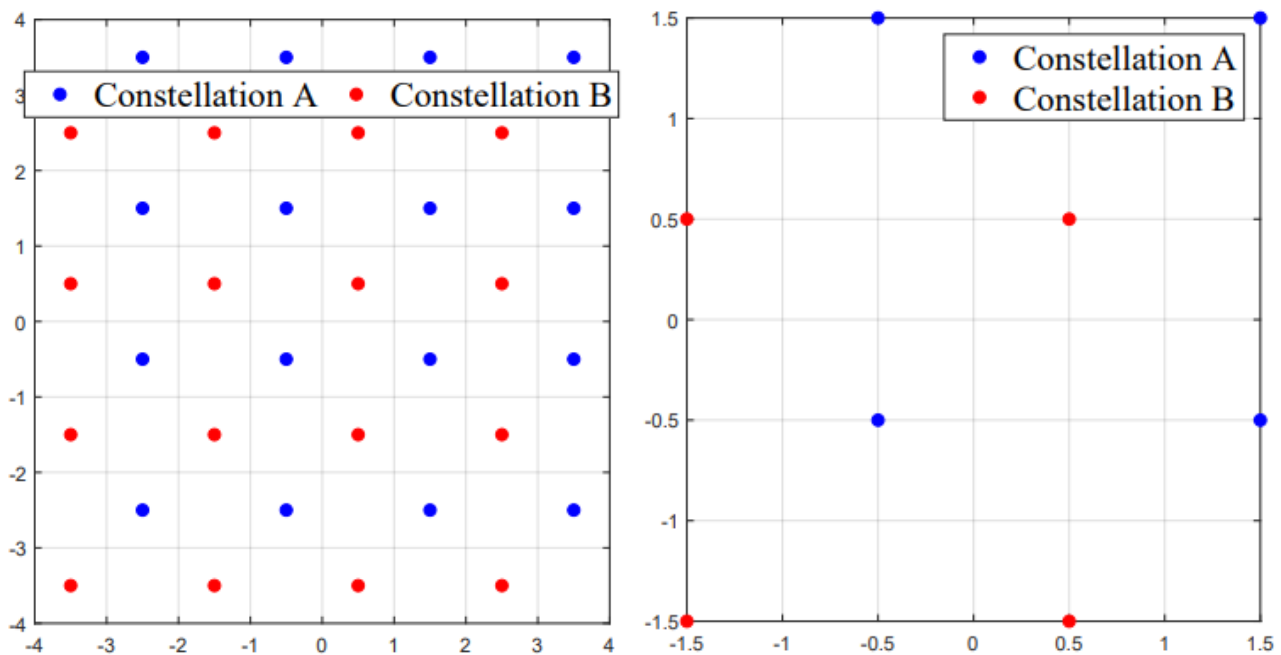


Рис. 3. Пари сигнальних сузір'їв QPSK (зліва) та 16-QAM (справа) для дворежимної індексної модуляції [15]

Дві пари сигнальних точок BPSK можуть виглядати, очевидно, як протифазні символи (A; C) на дійсній осі (I – In-phase) та (B; D) – на уявній осі (Q – Quadrature) на комплексній площині (рис. 4).

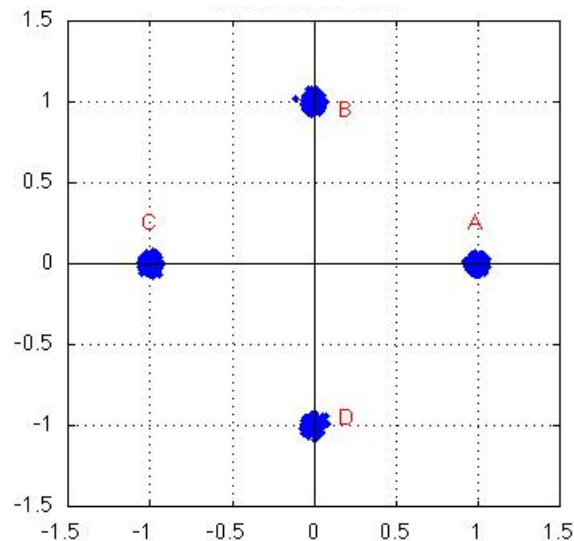


Рис. 4. Пари сигнальних сузір'їв BPSK

Дослідження показують, що безпомилково розрізнити сигнальні точки з таким дворежимним підходом у модуляціях більш високих розмірностей ($M > 32$) практично неможливо, тому рекомендовано зупинитись при хороших завадових умовах (високих показниках SNR, за відсутності навмисних завад) на модуляції 16-QAM [15].

Отже, у запропонованому удосконаленому методі DM-SP-OFDM за рахунок двополяризаційності антен та дворежимності модуляції значення частини біт

$$p_3 = N_A \cdot \left(\left\lceil \log_2 C_{\frac{N}{K}} \right\rceil + K \cdot \log_2 M_A + (N - K) \cdot \log_2 M_B \right).$$

У блоці узгодження формується матриця передачі на основі таблиць асоціативності (Look-Up-Tables, LUT). Приймачу заздалегідь відомі всі можливі комбінації активності антен, їх поляризації та можливих дворежимних видів модуляції. Найскладніша задача приймача – розрізнити, які саме антени були задіяні для передачі, з якою поляризацією та здійснити демодуляцію, виявивши всі складові набору біт p .

Після виконання процедури зворотнього швидкого перетворення Фур'є (Inverse Fast Fourier Transform, IFFT), формування пілот-сигналів, додавання циклічного префіксу CP (Cyclic Prefix), паралельно-последовного (Parallel-to-Serial, P/S) та цифро-аналогового перетворення (ЦАП) здійснюється одночасна передача сформованих сигналів за допомогою пари активних антен N_A [13].

На приймальній стороні – зворотні перетворення: після прямого швидкого перетворення Фур'є (FFT) на вході декодера формується сигнальний вектор із частотною характеристикою кожного з каналів та доданого в каналі адитивного білого гаусівського шуму (AWGN). Після обчислення каналних коефіцієнтів для кожної антени та піднесучих детектор максимальної правдоподібності ML (Maximum Likelihood) формує оцінки комплексних символів, активних антен та поляризації [13]. На основі відомих таблиць LUT визначаються біти p_1, p_2, p_3 .

Обчислювальна складність реалізації ML-детектора за кількістю операцій комплексного множення становить $O\left(2 \cdot N_A \cdot C_{N_A}^{N_T} C_{\frac{N}{K}}^N M_A^N M_B^{N-K}\right)$ для кожного субблоку, що демонструє

неможливість його практичного застосування при великих значеннях розмірів ансамблю сигналів M та розмірів субблоку N , а також у Massive MIMO з кількістю $N_T \geq 64$. У таких випадках часто використовуються субоптимальні алгоритми декодування, що окремо визначають індексні та модуляційні біти, через що втрачається ЕЕ. Таким чином, обмеженнями для запропонованого методу в частині прийнятної складності процесів обробки сигналів на приймачі (детектор-декодер) є $M \leq 16, N_T \leq 32, N \leq 4$.

Результати моделювання. Оцінку енергетичної ефективності запропонованого методу проведено з використанням пакету Simulink у середовищі імітаційного моделювання MATLAB. Узагальнені параметри безпроводових каналів, що моделюються, є типовими для сучасних систем безпроводового зв'язку та близькі до моделей, що розглядаються у [11–15]: кількість піднесучих OFDM – 1024; розмір циклічного префіксу – 32; частота несучого коливання – 5 ГГц; частотний інтервал між піднесучими – 15 кГц; доплерівський зсув частот – 10 Гц; кількість променів – 30; середньоквадратичне значення затримки в каналі – 3,48 мкс; вид модуляції – BPSK (модифікований); розмір MIMO – 4×4 .

На рисунку 5 порівнюється завадостійкість запропонованого методу DM-SP-OFDM, мультиплексного SMX-SM-OFDM та класичного методу просторового мультиплексування VBLAST-OFDM. В усіх методах застосовується схема MIMO 4×4 , проте активується різна кількість активних передавальних антен (N_A, N_R) . Для вирівнювання показника СЕ всіх методів до 6 біт/с/Гц застосовано такі види модуляції, кількість активних передавальних антен (кількість приймальних антен фіксована – чотири):

VBLAST-OFDM (3, 4), QPSK – три активних передавальних антени, модуляція QPSK;

SMX-SM-OFDM (2, 4), QPSK – дві активних передавальних антени, модуляція QPSK;

DM-SP-OFDM (2, 4), BPSK – дві активних передавальних антени, модуляція BPSK.

Для скорочення записів у “легенді” (рис. 5) частина назви “-OFDM” не вживається.

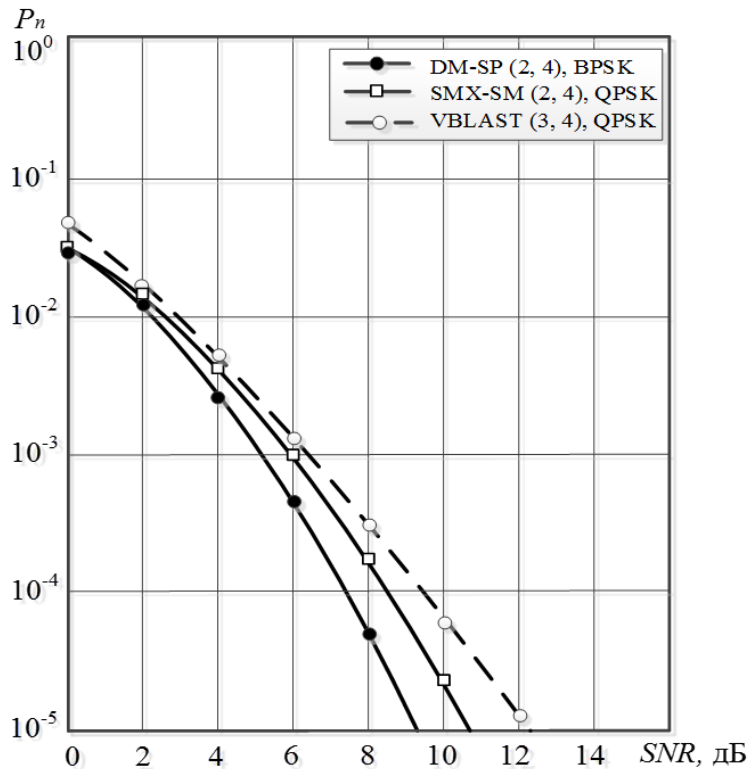


Рис. 5. Завадостійкість методів DM-SP-OFDM, SMX-SM-OFDM та VBLAST-OFDM

Аналіз кривих завадостійкості (див. рис. 5) показує, що для СЕ 6 біт/с/Гц запропонований метод DM-SP (2, 4) забезпечує енергетичний виграш (ЕВ) близько 4 дБ порівняно із традиційним VBLAST при ймовірності бітової помилки $P_n = 10^{-5}$ (Bit Error Rate, BER), оскільки перший використовує ансамбль сигналів меншого об'єму (BPSK) та з активацією лише половини передавальних антен (дві), а класичний VBLAST – три антени із модуляцією більшого розміру QPSK. Слід зауважити, що в усіх методах рисунку 5 активуються всі піднесучі на активних антенах, із тією відмінністю, що тільки у запропонованому методі – дворежимний BPSK (пари сигнальних точок повернуті на 90° одне відносно одного), що дає можливість забезпечити передачу двох додаткових біт неявних способом – за рахунок комбінацій активації у субблоці $N = 4$ піднесучих половини піднесучих ансамблем M_A , а іншої половини – M_B .

Метод часткового мультиплексування SMX-SM активує лише пару передавальних антен, як і запропонований DM-SP, проте із ансамблем сигналу більшого розміру – QPSK, через що програє останньому близько 2 дБ при тій самій достовірності ($P_n = 10^{-5}$).

Як і всі методи індексування у часі/частоті/просторі, метод DM-SP-OFDM втрачає енергетичну ефективність при збільшенні розміру ансамблю сигналів через зближення сигнальних точок та ускладнення процесу безпомилкового одночасного визначення активованих антен, поляризації антен та сигнальних точок, що передавались. Загальновідомо [11; 12], що окреме почергове визначення на приймачі індексних та класичних частин біт за алгоритмом максимальної правдоподібності ML може призводити до критичного накопичення помилок при погіршенні відношення сигнал/шум (SNR), коли неточне визначення активованих передавальних антен призводить до помилкового визначення також і модуляційних символів. Подальше підвищення СЕ (безпосередньо потребує активації більшої кількості антен та менш завадостійкого виду модуляції QPSK) призводить до збільшення інформаційного навантаження на всі піднесучі та антени, через що показник ЕЕ індексних

методів різко зменшується. Саме через це рекомендовано використовувати метод DM-SP із найзавадостійкішим видом модуляції – BPSK. Обрана розмірність МІМО та виду модуляції також дозволяє застосування в усіх згаданих методах МЛ-детектування.

Отримані результати імітаційного моделювання не суперечать закордонним дослідженням завадостійкості індексних методів, оскільки складові запропонованої сигнально-кової конструкції (СКК) забезпечують ЕВ порівняно із класичними “неіндексними” методами до 5 дБ при ймовірності бітової помилки $P_n = 10^{-5}$ при різних вихідних даних [11–15], чого достатньо для реалізації більшості сервісів ситуаційної обізнаності. Отриманий ЕВ можливо використати з різною метою: для зменшення потужності передавача; підвищення рівня достовірності прийому інформації; зменшення вимог до чутливості приймача; збільшення зони покриття базової станції; підвищення швидкості передачі інформації. Разом із тим, головна перевага запропонованої СКК полягає у підвищенні СЕ на 25–67 % (залежно від обраного розміру модуляційного ансамблю сигналів) без залучення додаткових ресурсів ціною незначного ускладнення приймача. На сучасному етапі розвитку схемотехніки таке питання не є катастрофічним.

Висновки. В умовах обмеженості просторово-частотно-енергетичних ресурсів удосконалення відомих і розробка нових способів передачі інформації з метою наближення ефективності використання безпроводового каналу до теоретичних меж є вкрай важливою задачею. Наукова новизна запропонованого методу полягає в удосконаленні відомого методу просторово-поляризаційної модуляції в частині підвищення його спектральної ефективності у частотно-селективних квазістаціонарних каналах на основі реалізації дворежимної індексної модуляції піднесучих OFDM модифікованими ансамблями сигналів. Для модифікованої модуляції BPSK приріст показника СЕ складає до 2 біт/с/Гц порівняно із класичним методом просторового мультиплексування VBLAST-OFDM при однаковій фіксованій кількості активованих антен, для розміру субблоку $N = 4$, без втрати енергетичної ефективності методу. За умови фіксованої СЕ, запропонований метод DM-SP забезпечує енергетичний виграв до 4 дБ для прийнятної на сьогодні ймовірності бітової помилки $P_n = 10^{-5}$. Практична цінність удосконаленого методу DM-SP-OFDM – у можливості передавати, залежно від використаного виду модуляції, на 25–67 % більше інформації (відеострімів із безпілотних літальних апаратів (БпЛА), телеметрії тощо) без розширення смуги частот, потужності передавача, збільшення кількості активних антен.

Перспективним напрямком подальших досліджень є оцінка можливості удосконалення запропонованого методу на основі антенних елементів із круговою, еліптичною та іншими видами поляризації, а також розробка спрощених субоптимальних методів декодування сигналів на основі алгоритму логарифмічного відношення правдоподібності LLR (Log-Likelihood Ratio).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Посібник щодо застосування станцій широкосмугового доступу Silvus з урахуванням досвіду ведення бойових дій / під ред. Д. О. Романова / Г. Д. Радзівілов, О. В. Сілко, А. О. Зарубенко, М. М. Фомін, О. Л. Свечков, В. О. Хмарюк. К.: ВІТІ, 2024. 187 с.
2. Хоменко П. В., Радзівілов Г. Д., Ільїнов М. Д. Аналіз функціональних характеристик сучасних радіозасобів класу MANET // Системи і технології зв'язку, інформатизації та кібербезпеки. 2025. № 7. С. 222–231. DOI: 10.58254/viti.7.2025.20.222.
3. Silvus SC4400 Data Sheet. URL: <https://www.silvustechologies.com>.
4. Spectrum Dominance: Delivering LPI/LPD and Anti-Jamming Without Sacrificing Performance. URL: <https://silvustechologies.com/blog/resilient-mesh-network-communications/>.

5. Royal Marines field over 1,000 Persistent Systems MPU5 to Support Future Commando Force. URL: <https://fragoutmag.com/royal-marines-field-over-1000-persistent-systems-mpu5-to-support-future-commando-force/>.
6. TSM Waveform: The Gold Standard for Mission-Critical Communications. URL: <https://trellisware.com>.
7. Phased Array Tactical Broadband: Exceptional Resistance to Jamming and Precise Localization. URL: <https://radionor.no/domain/infrastructure/>.
8. Framework and overall objectives of the future development of IMT for 2020 and beyond. URL: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf.
9. Spectral Efficiency Considerations for 6G: Targets and KPI Analysis. URL: <https://arxiv.org/abs/2508.09117>.
10. E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, H. Haas. Index modulation techniques for next-generation wireless networks // IEEE Access. 2017. Vol. 5. Pp. 16693–16746. DOI: 10.1109/ACCESS.2017.2737528.
11. M. Di Renzo, H. Haas, A. Ghayeb, S. Sugiura, L. Hanzo. Spatial modulation for generalized MIMO: Challenges, opportunities, and implementation. Proc. // IEEE. 2013. Vol. 102. No. 1. Pp. 56–103. DOI: 10.1109/JPROC.2013.2287851.
12. Солодовник В. І., Науменко М. І., Пилипенко М. Г. Оцінка ефективності методів просторової модуляції сигналів із різною кількістю активних передавальних антен // Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів II Міжнародної науково-практичної конференції, 1 грудня 2022 р. Київ: ВІТІ ім. Героїв Крут, 2022. С. 198–199. URL: <https://mitit.mil.gov.ua/page/science>.
13. Солодовник В. І., Науменко М. І. Метод просторово-частотного блочного кодування сигналів з дворезимною індексною модуляцією піднесучих OFDM // Information Technology and Security. 2019. Vol. 7, iss. 2 (13). С. 216–229. DOI: 10.20535/2411-1031.2019.7.2.190572.
14. Li J., Li S., Dang S., Chen X., Chen C., Peng Y., Yu L. Generalized Polarization-Spatial Modulation With Multi-Mode Transmission // IEEE Internet of Things Journal. No. 12 (12). P. 18570–18581. DOI: 10.1109/IJOT.2025.3558310.
15. T. Mao, Z. Wang et al. New Constellation Design and Bit Mapping for Dual Mode OFDM-IM // IEEE Transactions on Communications. 2019. Vol. 67. No. 6. P. 3943–3955. DOI: 10.1109/ACCESS.2019.2912704.

Надійшла до редколегії 23.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.382.049.77:620.179.14

Тлустий А. О. ORCID: 0000-0002-4777-9563 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ ім. Героїв Крут)

ДІАГНОСТИЧНА МОДЕЛЬ ВИХІДНОГО ТРАНСЛЯТОРА КМОН ІНТЕГРАЛЬНОЇ МІКРОСХЕМИ

У цій статті розглядається актуальна науково-технічна задача забезпечення надійності функціонування сучасних зразків радіоелектронного озброєння шляхом удосконалення методів технічного діагностування їхньої елементної бази. Актуальність дослідження зумовлена стрімким переходом військової техніки на використання інтегральних мікросхем із високим ступенем інтеграції, що вимагає розробки неруйнівних та безконтактних способів контролю їхнього фактичного стану. Основна увага приділена розробці діагностичної моделі вихідного транслятора комплементарного метало-оксид-напівпровідника, яка адаптована для застосування у складі безконтактного індукційного методу діагностування. Проблематика роботи полягає у тому, що традиційні підходи до оцінки технічного стану часто ігнорують специфічні фізичні процеси деградації, притаманні саме структурам комплементарних метало-оксид-напівпровідників, що призводить до недостовірних прогнозів залишкового ресурсу.

В основу запропонованого рішення покладено розвиток існуючих моделей для транзисторно-транзисторної логіки з їх докорінною модернізацією під фізику напівпровідникових процесів сучасних мікросхем. Наукова новизна отриманих результатів полягає у детальному врахуванні таких деградаційних чинників, як захоплення електричного заряду в підзатворному діелектрику, ін'єкція гарячих носіїв та негативна нестабільність порогової напруги. У процесі дослідження було аналітично встановлено стійкий математичний зв'язок між зміною вихідних струмів I^0 , I^1 транслятора у логічних станах нуля та одиниці та сумарною деградацією порогової напруги транзисторів $\Delta V_{th}(t)$. Це дозволило отримати універсальну розрахункову формулу для визначення індивідуального залишкового ресурсу компонента, що є ключовим показником для систем прогностичного технічного обслуговування.

Запропонована модель дозволяє не лише констатувати факт наявності несправності, а й здійснювати глибоку локалізацію дефектів і прогнозувати подальшу працездатність радіоелектронного озброєння в умовах інтенсивної експлуатації. Практична значущість роботи підтверджується можливістю інтеграції розробленої моделі в автоматизовані системи діагностування, що забезпечить суттєве підвищення боєготовності підрозділів завдяки попередженню раптових відмов критично важливих електронних модулів. Таким чином, результати дослідження створюють підґрунтя для переходу до обслуговування військової техніки за її фактичним технічним станом, мінімізуючи ризики виходу з ладу систем зв'язку та управління.

Ключові слова: діагностична модель, комплементарний метало-оксид-напівпровідник, КМОН, вихідний транслятор, безконтактний індукційний метод, радіоелектронне озброєння, порогова напруга, ін'єкція гарячих носіїв, негативна нестабільність порогової напруги, залишковий ресурс, технічний стан.

A. Tlustyi, V. Kuzavkov. Diagnostic model of the CMOS integrated circuit output translator

This article addresses the relevant scientific and technical problem of ensuring the operational reliability of modern electronic warfare and weapons systems by improving the methods for technical diagnostics of their component base. The relevance of the study is driven by the rapid transition of military equipment to the use of high-density integrated circuits, which necessitates the development of non-destructive and non-contact methods for monitoring their actual condition. The main focus is placed on the development of a diagnostic model for a complementary metal-oxide-semiconductor output translator, adapted for use within a non-contact induction diagnostic method. The problem addressed in this work lies in the fact that traditional approaches to technical state assessment often ignore specific physical degradation processes inherent to structures, leading to unreliable remaining useful life predictions. The proposed solution is based on the advancement of existing models for transistor-transistor logic, with their fundamental modernization to align with the physics of semiconductor processes in modern integrated circuits. The scientific novelty of the results consists in the detailed consideration of such degradation factors as charge trapping in the gate dielectric, hot carrier injection, and negative bias temperature instability. During the study, a stable mathematical relationship was analytically established between the changes in the translator output currents I^0 , I^1 in logical zero and one states and the total degradation of the transistor threshold voltage $\Delta V_{th}(t)$. This enabled the derivation of a universal calculation formula for determining the individual remaining useful life of the component (t^*), which is a key indicator for predictive maintenance systems. The proposed model allows not only for the detection of a fault but also for deep defect localization and forecasting the future operability of electronic equipment under intensive operational conditions. The practical significance of the work is confirmed by the possibility of integrating the developed model into automated diagnostic systems, which will significantly increase the combat readiness of units by preventing

sudden failures of critical electronic modules. Thus, the research results provide a foundation for transitioning to condition-based maintenance of military equipment, minimizing the risks of failure in communication and control systems.

Keywords: diagnostic model, complementary metal-oxide-semiconductor, CMOS, output translator, non-contact induction method, electronic equipment, threshold voltage, hot carrier injection, negative bias temperature instability (NBTI), remaining useful life, technical state.

Постановка задачі

Відомо, що сучасні об'єкти радіоелектронного озброєння (РЕО) є складними технічними системами, що об'єднують модулі різного призначення. Проведення якісного діагностування цифрових блоків РЕО залежить від адекватності діагностичної моделі об'єкта контролю, методу діагностування і методики його проведення [1–4].

Структурною частиною об'єктів РЕО є цифрові блоки, до складу яких входять напівпровідникові радіоелектронні компоненти. Сучасна цифрова схемотехніка базується переважно на комплементарних метало-оксид-напівпровідникових (КМОН) логічних структурах, що витіснили транзисторно-транзисторну логіку (ТТЛ) у більшості застосувань. Відповідно, виникає потреба у діагностичних моделях саме для КМОН інтегральних мікросхем (ІМС).

У роботі [5] розроблено діагностичну модель вихідного транслятора ТТЛ ІМС на біполярних транзисторах для безконтактного індукційного методу діагностування. Показано, що основним носієм діагностичної інформації є емітерний струм вихідного транслятора I^0 та I^1 , що вимірюється в одній контрольній точці. Математична модель пов'язує струм транслятора зі зміною концентрації основних носіїв заряду $n(D, t)$ в біполярній напівпровідниковій структурі під час експлуатації.

Розвитком підходу є розробка аналогічної діагностичної моделі для КМОН ІМС [5]. Принципова відмінність полягає у механізмі формування діагностичного параметра: у ТТЛ ІМС він визначається зміною концентрації носіїв $n(D, t)$; у КМОН ІМС – деградацією порогової напруги МОН-транзистора $\Delta V_{th}(t)$ внаслідок трьох специфічних механізмів (oxide trapping, HCI, NBTI). Спільним є принцип безконтактної реєстрації струму в одній точці.

Порівняння двох діагностичних моделей наведено у таблиці 1.

Таблиця 1

Порівняння діагностичних моделей трансляторів ТТЛ та КМОН ІМС

Характеристика	ТТЛ ІМС [5]	КМОН ІМС (ця робота)
Тип логіки	ТТЛ (транзисторно-транзисторна)	КМОН (комплементарна МОН)
Активні елементи вихідного транслятора	Біполярні транзистори $VT2, VT3$	МОН-транзистори M_3 (pMOS), M_4 (nMOS)
Механізм деградації	Зміна концентрації носіїв $n(D, t)$	Деградація порогової напруги $\Delta V_{th}(t)$: oxide trapping + HCI + NBTI
Математичний апарат	Рівняння дифузії (гіперболічні функції $cth, csch$)	Степеневі закони деградації (oxide trapping, HCI, NBTI)
Вплив старіння на струм	Зміна рухливості μ і концентрації n	Зміна $(V_{GS} - V_{th})^2$
Діагностичний параметр	$I^0 = f(n_1, n_2, t);$ $I^1 = f(n_1, n_2, t)$	$I^0 = f(\Delta V_{th}(t)); I^1 = f(\Delta V_{th}(t))$
Метод вимірювання	Безконтактний індукційний — одна контрольна точка	
Прогнозування ресурсу	$n(D, t) \rightarrow$ гранична концентрація	$\Delta V_{th}(t) \rightarrow$ формула: t^* (рівн. 14)

Фізична паралель між двома моделями полягає у тому, що обидві описують деградацію напівпровідникової структури степеневим законом відносно часу. У моделі ТТЛ – це концентрація носіїв $n(D, t)$, що входить до рівняння (13) через параметри ефективної маси m^* та енергії активації E_a [5]. У моделі КМОН – це деградація порогової напруги $\Delta V_{th}(t)$ (рівняння (13) у роботі). Показник степеня $n \approx 0,1 - 0,3$ є характерним для обох моделей, що відображає субдифузійний характер накопичення деградації.

Аналіз останніх досліджень і публікацій

Безконтактний індукційний метод діагностування РЕО розроблено у роботах [1–4]. Метод базується на реєстрації електромагнітного поля струмів у шині живлення без розмикання електричних кіл об'єкта контролю.

Діагностичну модель вихідного транслятора ТТЛ ІМС розроблено у [5]. Доведено, що основним носієм діагностичної інформації є струм вихідного транслятора. Встановлено зв'язок між струмом транслятора і концентрацією основних носіїв заряду $n(D, t)$, що змінюється в процесі старіння напівпровідникової структури.

Механізми деградації МОН-транзисторів досліджено у низці фундаментальних робіт. Захоплення заряду в підзатворному діелектрику (oxide trapping) описано у [6; 7]. Механізм ін'єкції гарячих носіїв (HCI) та його вплив на порогову напругу розглянуто у [8]. Реакційно-дифузійна модель NBTI деградації p -MOSFET розроблена у [9]. Деградація рухливості носіїв унаслідок розсіювання на захоплених зарядах описана у [10].

Авторам не відомі публікації, де б діагностична модель КМОН ІМС для безконтактного індукційного методу діагностування була побудована з урахуванням сумісної дії трьох механізмів деградації МОН-транзистора та пов'язана з формулою залишкового ресурсу. Це визначає наукову новизну цієї роботи.

Метою роботи є розробка діагностичної моделі вихідного транслятора КМОН ІМС як розвитку моделі [5] на клас КМОН пристроїв – для безконтактного індукційного методу діагностування РЕО.

Виклад основного матеріалу

Модель повинна пов'язувати струм вихідного транслятора I^0 та I^1 з фізико-хімічними процесами деградації МОН-транзисторів (oxide trapping, HCI, NBTI) та забезпечувати можливість прогнозування залишкового ресурсу компонента.

Для досягнення мети вирішуються низка завдань:

аналіз фізичних механізмів деградації МОН-транзисторів у складі КМОН ІМС;

розробка математичної моделі деградації порогової напруги $\Delta V_{th}(t)$ з урахуванням трьох механізмів;

отримання аналітичних виразів для діагностичних параметрів I^0 та I^1 як функцій $\Delta V_{th}(t)$;

розробка критерію граничного стану та формули залишкового ресурсу t^* ;

визначення практичної методики ідентифікації параметрів моделі за результатами безконтактних вимірювань.

Базовим логічним елементом вихідних трансляторів КМОН ІМС є комплементарна пара МОН-транзисторів – структура інвертора (рис. 1). Схема складається з вхідного каскаду, вихідного каскаду (комплементарна пара) та буферних елементів керування. Транзистор M_3 (p -канальний MOSFET) і транзистор M_4 (n -канальний MOSFET) забезпечують формування сигналів керування для протифазного перемикавання вихідних станів.

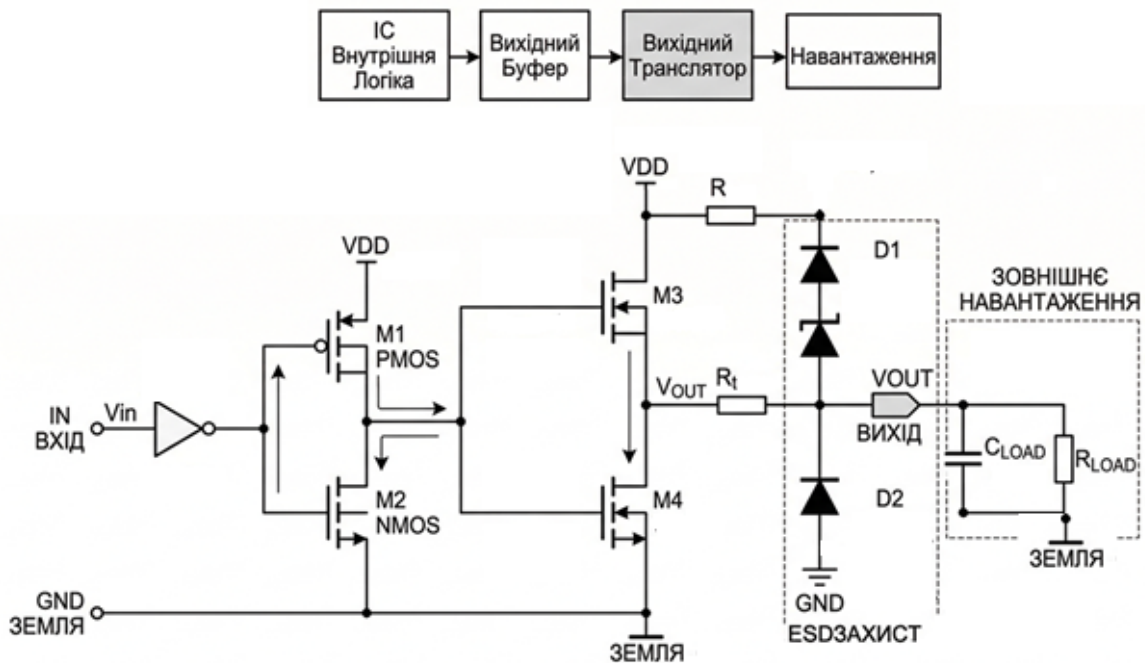


Рис. 1. Спрощена схема вихідного транслятора КМОН ІМС
(розроблено авторами на основі [11])

На рисунку 1 показана архітектура вихідного транслятора КМОН ІМС. Вхідний сигнал через буферний інвертор (M_1 , M_2) керує комплементарною парою вихідних транзисторів M_3 (pMOS) і M_4 (nMOS). При логічному “0” на вході відкривається M_3 і вихід підтягується до VDD через M_3 ; при логічному “1” відкривається M_4 і вихід підключається до GND через M_4 . Схему ESD-захисту відображено діодами $D1$ і $D2$.

Доведено, що основним джерелом діагностичної інформації про стан цифрової ІМС є вихідний транслятор – зіставний транзистор. Тому, необхідно визначення параметрів базового логічного елементу з урахуванням процесів, які відбуваються в ньому під час експлуатації (старіння напівпровідникової структури), а саме зміну електрофізичних і фізико-хімічних властивостей напівпровідникової структури. Саме через струм вихідного транслятора (I^0 (стан “0”) або I^1 (стан “1”)) здійснюється реєстрація діагностичного параметра безконтактним індукційним методом.

Слід зауважити, що зміна форми сигналу через вихідний транслятор (форми струму) обумовлена наявністю струмів квазікороткого замикання під час зміни стану з “0” на “1” та навпаки. Безконтактний індукційний датчик розташований на шині живлення в безпосередній близькості до мікросхеми і не фіксує постійну складову струму (силу струму). Цей датчик фіксує виключно сплески струму (різку зміну амплітудного значення). Саме форма й амплітуда є діагностичною ознакою фактичного стану силової частини мікросхеми – вихідного транслятору.

Еквівалентна схема вихідного транслятора представлена на рисунку 2. Резистор R_{ch} моделює опір каналу МОН-транзистора у відкритому стані, C_{ox} – ємність підзатворного діелектрика, R_{sub} – опір підкладки.

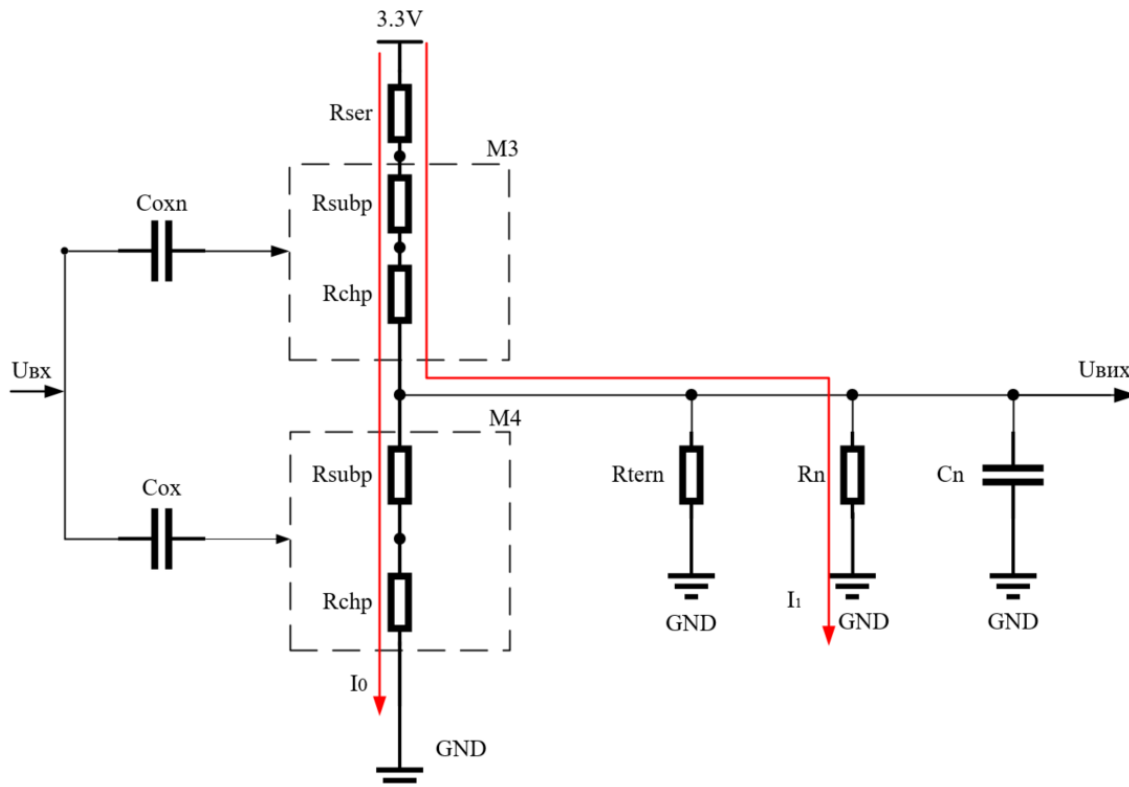


Рис. 2. Еквівалентна схема вихідного транслятора логічного елементу КМОН

На рисунку 2 елемент C_{ox} – не окремий елемент, а фізична ємність самого затвору, питома ємність підзатворного діелектрика, що визначає як керування транзистором, так і механізм деградації *oxide trapping* ($C_{ox} = \epsilon_{ox} / t_{ox}$).

Резистор R_{ser} обмежує струм у вихідному каскаді під час переходу схеми з одного стану в інший, коли транзистор M_3 ще перебуває в режимі насичення, а транзистор M_4 вже відкрився. Перехідні процеси, які відбуваються при перемиканні вихідного каскаду (транслятора) є найбільш інформативними при застосуванні індукційного методу.

Неповне закриття (відкриття) транзисторів (перехідні процеси) спричиняють виникнення імпульсів струму квазікороткого замикання. Тривалість зазначених імпульсів становить 0,5–5 нс.

Фільтри в ланцюгах живлення не в змозі повністю згладжувати перешкоди від імпульсів такої тривалості. Реєстрація сигналу в шині живлення (датчик діагностичного сигналу) та обробка (автоматична система діагностування) дозволяють створити базу сигнатур об'єкта контролю під впливом перевіркої тестової послідовності.

Математична модель транслятору ІМС дозволяє визначити стан об'єкта контролю в стаціонарному режимі (вихідне значення логічний “0” або логічна “1”). Отримані значення відображують стан напівпровідникової структури на момент часу перевірки, тобто враховано час існування напівпровідника (фізико-хімічні процеси в напівпровідниковій структурі).

Механізми деградації МОН-транзисторів.

Розглянемо три основні механізми деградації, що визначають зміну параметрів МОН-транзисторів під час експлуатації.

Захоплення заряду в підзатворному діелектрику (*oxide trapping*). Під дією електричного поля у підзатворному діоксиді кремнію відбувається накопичення захопленого заряду Q_{ox} , що призводить до зміщення порогової напруги згідно з виразом (1):

$$\Delta V_{th}(ox)(t) = -Q_{ox}(t) / C_{ox} = -q N_{ot}(t) / C_{ox}, \quad (1)$$

де q – заряд електрона;

$N_{ot}(t)$ – концентрація захопленого заряду в діелектрику;

C_{ox} – питома ємність підзатворного діелектрика товщиною tox .

Кінетика накопичення захопленого заряду описується степеневим законом (2) [7]:

$$N_{ot}(t) = N_{ot0} (t / t_0)^n, \quad (2)$$

де N_{ot0} – початкова концентрація;

$n \approx 0,1 - 0,3$ – показник степеня, що залежить від технологічного процесу.

Ін'єкція гарячих носіїв (HCI). Під час роботи транзистора в режимі насичення електрони (для n -MOSFET) набувають достатньої енергії для подолання потенціального бар'єра Si/SiO_2 і захоплюються в діелектрику поблизу стоку.

Зміщення порогової напруги внаслідок HCI розраховується за формулою (3):

$$\Delta V_{th}(HCI)(t) = A(HCI) (I_{sub}b/W)^m t^n \exp(-Ea(HCI)/kT), \quad (3)$$

де $I_{sub}b$ – струм підкладки як індикатор генерації гарячих носіїв;

W – ширина каналу;

A, m, n – технологічні константи;

$Ea(HCI)$ – енергія активації;

k – стала Больцмана;

T – абсолютна температура [8].

Негативна нестабільність порогової напруги (NBTI). Механізм NBTI є специфічним для p -MOSFET і проявляється при від'ємному змищенні затвору за підвищеної температури. Генерація інтерфейсних пасток Nit на межі Si/SiO_2 описується реакційно-дифузійною моделлю виразів (4) та (5) [9]:

$$\Delta V_{th}(NBTI)(t) = -q \Delta Nit(t) / C_{ox}, \quad (4)$$

$$\Delta Nit(t) = \sqrt{(k_i N_0 / k_r)(DH t / \pi)^{1/4}}, \quad (5)$$

де k_i, k_r – константи швидкості прямої та зворотної реакцій розриву зв'язків $Si-H$;

N_0 – початкова концентрація зв'язків;

DH – коефіцієнт дифузії атомарного водню.

Сумарна деградація порогової напруги МОН-транзистора з урахуванням усіх трьох механізмів представлена виразом (6):

$$\Delta V_{th}t) = \Delta V_{th}(ox)(t) + \Delta V_{th}(HCI)(t) + \Delta V_{th}(NBTI)(t). \quad (6)$$

Рівняння (6) є першим наближенням, що передбачає незалежність трьох механізмів деградації. У реальних умовах механізми взаємодіють: спільна дія HCI та NBTI, що в свою чергу може призводити до нададитивного збільшення $|\Delta V_{th}|$ порівняно з лінійною суперпозицією [12]. Тому рівняння (6) дає консервативну (занижену) оцінку сумарної деградації, що відповідає принципу запасу при прогнозуванні залишкового ресурсу.

Математична модель струму через вихідний транслятор.

Струм через n -MOSFET у режимі насичення визначається квадратичним законом, що описує вираз (7):

$$I_{Ds} = (\mu_n C_{ox} W) / (2L) (V_{Gs} - \Delta V_{th})^2 (1 + \lambda \cdot V_{Ds}), \quad (7)$$

де μ_n – рухливість електронів у каналі;

W/L – відношення ширини до довжини каналу;

λ – параметр модуляції довжини каналу.

З урахуванням деградації порогової напруги (6) рухливість носіїв також деградує з часом внаслідок розсіювання на захоплених зарядах, представлених виразом (8) [10]:

$$\mu_n(t) = \mu_{n0} / (1 + \theta \Delta V_{th}(t)), \quad (8)$$

де μ_{n0} – початкова рухливість;

θ – коефіцієнт деградації рухливості.

Струм реєстрації в місці контролю (стан логічного “0”, $V_{вих}^0$) відповідно до співвідношення (9):

$$I^0 = (\mu_n(t) C_{ox} W) / (2L) [V_{DD} - \Delta V_{th}]^2 / (1 + \lambda \cdot V_{Ds}) + V_{вих}^0 / R_n, \quad (9)$$

де $V_{th}(t)$ – поточне значення порогової напруги з урахуванням деградації $V_{th}(t) = \Delta V_{th0} + \Delta V_{th}(t)$;

V_{th0} – початкове значення порогової напруги;

$V_{вих}^0$ – напруга на виході транслятора у стані логічного «0»;

R_n – навантаження.

Струм реєстрації в стані логічної “1” ($V_{вих}^1$) визначається через транзистор p -MOSFET, фізична природа процесу формалізована виразом (10):

$$I^1 = (\mu_p(t) C_{ox} W) / (2L) [V_{DD} - |\Delta V_{thp}(t)|]^2 + (V_{DD} - V_{вих}^1) / R_p, \quad (10)$$

де $\mu_p(t)$ – рухливість дірок з урахуванням NBTI-деградації p -MOSFET;

$\Delta V_{thp}(t)$ – порогова напруга p -MOSFET.

Отримана таким чином система рівнянь (9), (10) з урахуванням (1)–(8) є діагностичною моделлю вихідного транслятора КМОН ІМС для вдосконаленого індукційного методу діагностування РЕО і може бути використана для отримання розрахункових значень діагностичного параметра при вирішенні основних задач технічного діагностування: визначення фактичного технічного стану, локалізації несправності та прогнозування технічного стану, що зображено на рисунку 3.

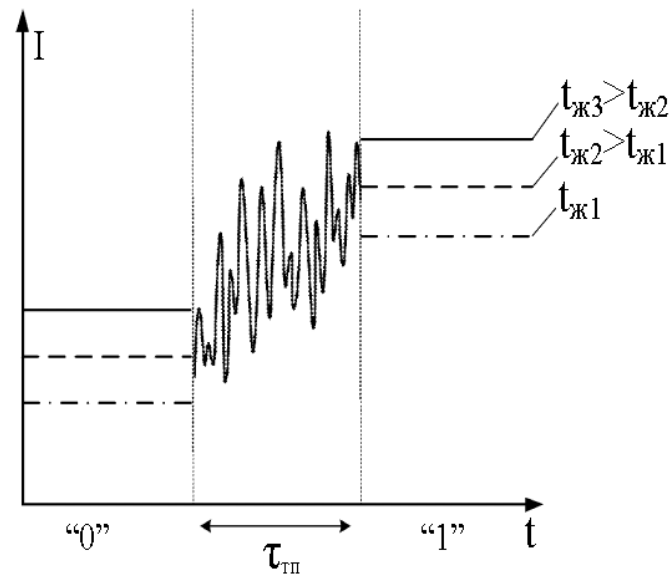


Рис. 3. Характерні зміни струму через вихідний транслятор КМОН ІМС

Прогнозування технічного стану КМОН ІМС на основі діагностичної моделі.

Запропонована діагностична модель дозволяє не лише визначити поточний технічний стан КМОН ІМС, але й прогнозувати залишковий ресурс компонента. Фізичною основою прогнозування є монотонний характер деградації порогової напруги $\Delta V_{th}(t)$ – усі три механізми деградації (oxide trapping, HCI, NBTI) призводять до односпрямованого збільшення $|V_{th}|$ з часом, що відповідно зменшує струм через вихідний транслятор.

Критерій граничного стану КМОН ІМС визначається через допустиме зменшення струму вихідного транслятора відносно початкового значення, кількісна оцінка якого проводиться на підставі залежності (11):

$$I(t) = (I_0^0 - I_0(t)) / I_0^0 \leq \Delta I_{dox}, \quad (11)$$

де I_0^0 – початкове значення струму реєстрації (стан логічного «0»);

$I_0(t)$ – поточне значення;

ΔI_{dox} – допустима відносна деградація струму, що визначається з умови забезпечення коректної роботи логічного елемента (типове значення $\Delta I_{dox} = 0,15-0,20$).

Підставляючи вирази (1)–(8) у (9), отримаємо залежність струму від часу, взаємозв'язок параметрів у якому описується виразом (12):

$$I_0(t) = (\mu_{n0} C_{ox} W) / (2L(1 + \theta \Delta V_{th}(t))) [V_{DD} \Delta V_{th0} \Delta V_{th}(t)]^2, \quad (12)$$

де $\Delta V_{th}(t)$ визначається сумарним внеском трьох механізмів деградації відповідно до виразу (6).

Оскільки кожен із механізмів описується степеневим законом відносно часу, сумарна деградація також апроксимується степеневою функцією (13):

$$\Delta V_{th}(t_i) \approx A t^n \exp(-E_a/kT), \quad (13)$$

де A – узагальнений коефіцієнт, що враховує внески всіх трьох механізмів;

$n \approx 0,1 - 0,3$ – показник степеня;

E_a – ефективна енергія активації сумарного процесу деградації.

Апроксимація (13) є прийнятною за умови, що один із механізмів деградації є домінуючим. Для p -MOSFET при тривалій експлуатації домінує NBTI (показник $n \approx 0,25$); для n -MOSFET – HCI (показник $n \approx 0,3-0,5$). При рівному внеску всіх трьох механізмів похибка апроксимації може досягати 15–20 %.

Залишковий ресурс компонента визначається з умови досягнення критерію граничного стану (11). Прирівнюючи $\Delta I(t^*) = \Delta I_{dox}$ і розв'язуючи відносно t^* , отримаємо оцінку залишкового ресурсу відповідно до (14):

$$t^* = [(1/A) \Delta V_{thdox} \exp(E_a/kT)]^{1/n}, \quad (14)$$

де ΔV_{thdox} – допустима деградація порогової напруги, що відповідає критерію (11).

Параметри A, n, E_a визначаються методом найменших квадратів за результатами не менше трьох послідовних вимірювань $I^0(t_i)$ при фіксованій температурі. Логарифмування виразу (13) дає лінійну форму ($\ln(\Delta V_{th}) = \ln(A) - E_a/(kT) + n \cdot \ln(t)$), що дозволяє застосувати стандартну процедуру лінійної регресії.

Практична реалізація прогнозу залишкового ресурсу за формулою (14) потребує попереднього визначення параметрів моделі деградації A, n, E_a для конкретного екземпляра КМОН ІМС. Запропоновано чотириступеневу методику ідентифікації цих параметрів за результатами безконтактних вимірювань струму вихідного транслятора.

1. Вимірювання $I_0(t_i)$.

Проводиться вимірювання струму вихідного транслятора $I_0(t_i)$ у стані логічного «0» при фіксованих зовнішніх умовах (не менше трьох вимірів):

температура $T = \text{const}$ (відхилення не більше $\pm 2^\circ \text{C}$);

напруга живлення $V_{DD} = \text{const}$ (відхилення не більше $\pm 0,05 \text{ V}$);

тестова послідовність ідентична для всіх вимірювань;

інтервал між вимірюваннями $\Delta t \geq 100$ год напрацювання.

Вимірювання виконуються безконтактним індукційним методом в одній контрольній точці (шина живлення) без розмикання електричних кіл [1–4].

2. Визначення $\Delta V_{th}(t_i)$.

Для кожного вимірюваного значення $I_0(t_i)$ визначити відповідне значення деградації порогової напруги $\Delta V_{th}(t_i)$ шляхом розв'язання рівняння (12) відносно ΔV_{th} при відомих $I_0(t_i)$, μ_{n0} , C_{ox} , W/L , V_{DD} , що задається рівняння (15):

$$\Delta V_{th}(t_i) = V_{DD} - \Delta V_{th0} - \sqrt{[2L \cdot I_0(t_i) / (\mu_{n0} \cdot C_{ox} W \cdot (1 + \theta \cdot \Delta V_{th}))]}. \quad (15)$$

Рівняння (15) розв'язується ітераційно (початкове наближення $\Delta V_{th} = 0$, збіжність досягається за 3–5 ітерацій).

3. Лінеаризація і МНК.

Логарифмуванням рівняння (13) отримаємо лінійну форму (16):

$$\ln(\Delta V_{th}) = \ln(A) + n \cdot \ln(t) - E_a/(kT). \quad (16)$$

За трьома і більше парами $(t_i, \Delta V_{th}(t_i))$ методом найменших квадратів (МНК) визначаються параметри, зазначені у таблиці 2.

Таблиця 2

Фізичний зміст параметрів A , n , E_a

Параметр	Фізичний зміст	Типові значення
A	Узагальнений коефіцієнт враховує внески oxide trapping, HCI, NBTI	10^{-3} – 10^{-1} [В]
n	Показник степеня – субдифузійний характер деградації	0,1–0,3
E_a	Ефективна енергія активації сумарного процесу деградації	0,3–0,7 [eВ]

Система рівнянь для МНК у матричній формі представлена виразом (17):

$$[\ln(A), n, -E_a/k] = (X^T X)^{-1} X^T Y, \quad (17)$$

де X – матриця регресорів розміром $[m \times 3]$ (m – кількість вимірювань);
 Y – вектор $\ln(\Delta V_{th}(t_i))$.

4. Перевірка якості апроксимації.

Якість отриманої моделі оцінюється коефіцієнтом детермінації, як це показано у формулі (18):

$$R^2 = 1 - \Sigma(\ln \Delta V_{th,i} - \ln \Delta V_{th,i}^*)^2 / \Sigma(\ln \Delta V_{th,i} - \langle \ln \Delta V_{th} \rangle)^2. \quad (18)$$

Умова прийнятності моделі: $R^2 \geq 0,95$.

При $R^2 < 0,95$ – збільшити кількість вимірювань або перевірити умови вимірювання (стабільність T і V_{DD}).

Визначені параметри A , n , E_a підставляються у формулу (14) для обчислення залишкового ресурсу t^* . Точність оцінки t^* визначається кількістю вимірювань m (при $m = 3$ похибка становить ± 20 – 30 %, при $m \geq 5$ – ± 10 – 15 %).

Запропонований підхід до прогнозування на основі реєстрації струму через вихідний транслятор в одній контрольній точці є принциповою перевагою індукційного методу порівняно з традиційними методами діагностування, що потребують розмикання кіл або спеціальних тестових точок доступу.

Наукова новизна:

вперше розроблено діагностичну модель вихідного транслятора КМОН ІМС для безконтактного індукційного методу діагностування, яка враховує сумісну дію трьох механізмів деградації МОН-транзистора (oxide trapping, HCI, NBTI) через узагальнений показник $\Delta V_{th}(t)$;

отримано аналітичний вираз залишкового ресурсу ($t^* = [(1/A) \cdot \Delta V_{th \max} \cdot \exp(E_a/kT)]^{1/n}$), що дозволяє прогнозувати технічний стан КМОН ІМС за результатами безконтактних вимірювань струму вихідного транслятора;

показано, що діагностичні моделі ТТЛ [5] та КМОН ІМС є фізично узгодженими – обидві описують деградацію степеневим законом відносно часу з показником $n \approx 0,1 - 0,3$, що відображає субдифузійний характер накопичення деградаційних пошкоджень.

Висновки. У статті розроблено діагностичну модель вихідного транслятора КМОН ІМС як розвиток моделі [5] на клас КМОН пристроїв. Модель враховує три механізми деградації МОН-транзисторів – захоплення заряду в підзатворному діелектрику (oxide trapping), ін'єкцію

гарячих носіїв (HCI) та негативну нестабільність порогової напруги (NBTI) – через узагальнений показник деградації порогової напруги $\Delta V_{th}(t)$.

Отримано аналітичні вирази для діагностичного параметра як функцій $\Delta V_{th}(t)$ – рівняння (9), (10).

Показано що зростання $|\Delta V_{th}(t)|$ з часом призводить до монотонного зменшення $I^0(t)$ та $I^1(t)$, що реєструється безконтактним індукційним методом в одній контрольній точці без розмикання електричних кіл.

Сумарна деградація $\Delta V_{th}(t)$ апроксимується степеневою функцією (рівняння (13)) з показником $n \approx 0,1 - 0,3$, що відображає субдифузійний характер накопичення деградаційних пошкоджень. Аналогічний показник характеризує модель деградації ТТЛ ІМС [5], що свідчить про спільну фізичну природу процесів старіння різних типів напівпровідникових структур.

Отримано формулу залишкового ресурсу КМОН ІМС – рівняння (14).

Розроблено методику ідентифікації параметрів моделі деградації A , n , E_a за результатами безконтактних вимірювань $I^0(t_i)$ у не менше трьох моментів часу. Методика базується на лінеаризації рівняння (13) логарифмуванням і МНК-підгонці (рівняння (16), (17)) з перевіркою якості за критерієм $R^2 \geq 0,95$ (рівняння (18)).

Отримана модель покладена в основу вдосконаленого безконтактного методу технічної діагностики РЕО на базі КМОН ІМС і забезпечує вирішення трьох основних задач діагностування: визначення фактичного технічного стану, локалізації несправності та прогнозування залишкового ресурсу.

Перспективи подальших досліджень полягають у кількісному оцінюванні кореляції між деградацією порогової напруги КМОН-транзисторів та статистичними характеристиками псевдовипадкових послідовностей. Отримані результати стануть основою для розробки методики прогнозування зниження рівня захищеності спеціальних каналів зв'язку внаслідок фізичного зносу елементної бази комутаційного обладнання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безконтактний індукційний метод діагностування радіоелектронних блоків / В. В. Вишнівський та ін. *Збірник наукових праць ВІКНУ*. 2013. Вип. 43. С. 17–23.
2. Ленков С. В., Карпенко О. В., Шкуліпа П. А. Діагностична модель радіокомпонента для електромагнітного методу діагностування. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2011. № 3 (12). С. 31–33.
3. Жердев М. К., Шкуліпа П. А. Побудова діагностичної моделі транзистора в активному режимі роботи для енергодинамічного методу діагностування. *Збірник наукових праць ХУПС*. 2012. Вип. 4 (33). С. 122–124.
4. Жердев М. К., Кузавков В. В. Побудова функціональних перевірних тестів для безконтактного індукційного методу діагностування. *Системи озброєння та військова техніка*. 2014. № 4 (40). С. 73–76.
5. Кузавков В. В., Редзюк Є. В. Діагностична модель вихідного транслятора напівпровідникової інтегральної схеми. *Управління в складних системах*. 2019. № 1. С. 77–79. DOI: 10.26906/SUNZ.2019.1.077.
6. Radiation Effects in MOS Oxides / J. R. Schwank et al. *IEEE Transactions on Nuclear Science*. 2008. Vol. 55, № 4. P. 1833–1853. DOI: 10.1109/TNS.2008.2001040.
7. Barnaby H. J. Total-ionizing-dose effects in modern CMOS technologies. *IEEE Transactions on Nuclear Science*. 2006. Vol. 53, № 6. P. 3103–3121.
8. Takeda E., Suzuki N. An empirical model for device degradation due to hot-carrier injection. *IEEE Electron Device Letters*. 1983. Vol. 4, № 4. P. 111–113.
9. A comprehensive framework for predictive modeling of negative bias temperature instability / S. Chakravarthi et al. *Proc. IEEE IRPS*. 2004. P. 273–282.

10. Fleetwood D. M. Total-ionizing-dose effects, border traps, and periodic table. *IEEE Transactions on Nuclear Science*. 2002. Vol. 49, № 3. P. 1647–1654.
11. Amerasekera A., Duvvury C. ESD in Silicon Integrated Circuits. 2nd ed. Chichester: John Wiley & Sons, 2002. 430 p.
12. Physical Mechanism of NBTI Degradation – From Interface Damage to Bulk Trap Generation / S. Mahapatra et al. *IEEE Transactions on Electron Devices*. 2013. Vol. 60, № 3. P. 901–916. DOI: 10.1109/TED.2013.2238237.

Надійшла до редколегії 22.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.75 + 004.41 + 004.052.2

канд. техн. наук, доцент Троцько О. О. ORCID: 0000-0001-7535-5023 (ВІТІ ім. Героїв Крут)

Кондрусь А. В. ORCID: 0000-0001-8815-6517 (ВІТІ ім. Героїв Крут)

Пилипчук І. Ю. ORCID: 0000-0002-5550-8026 (ВІТІ ім. Героїв Крут)

Крамарчук В. В. ORCID: 0009-0002-2720-8373 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ МЕТОДИКИ ВІДНОВЛЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ШЛЯХОМ ЗАСТОСУВАННЯ ПІДХОДУ ІНФРАСТРУКТУРА ЯК КОД

У статті досліджено підхід Інфраструктура як Код (IaC) як сучасний інструмент автоматизації розгортання, масштабування та відновлення інформаційних систем спеціального призначення. Обґрунтовано концепцію розділення життєвого циклу сервісів та життєвого циклу даних як ключової архітектурної передумови реалізації IaC-орієнтованого відновлення: збій ephemeral-рівня не впливає на цілісність persistent-рівня, а відновлення системи зводиться до перестворення сервісів із репозиторію з наступним монтуванням сховища даних.

Проведено синтетичний порівняльний експеримент для трьох сценаріїв відновлення типової on-premise трирівневої вебінформаційної системи: ручного відновлення за планом відновлення після катастроф – документом, часткового IaC та повного IaC-підходу. Кожен сценарій відтворювався п'ять разів; для оцінювання достовірності результатів застосовано критерій Стюдента з довірчим інтервалом 95 %. За результатами вимірювань отримано кількісні оцінки метрик часу відновлення Time Recovery Service, коефіцієнта автоматизації та цільової точки відновлення Recovery Point Objective. Запропоновано математичну формалізацію показників ефективності IaC з урахуванням статистичного розкиду вимірювань.

Встановлено, що повний IaC-підхід забезпечує скорочення часу відновлення сервісу до 30 хв порівняно з 315 хв при ручному відновленні – індекс ефективності 90,5 %, коефіцієнт автоматизації $K_a = 87,5$ %. Показано, що при правильній організації персистентного зберігання даних на рівнях 3–5 запропонованої ієрархії план відновлення після катастроф може бути функціонально замінений виконуваним IaC-репозиторієм, що гарантує детерміноване та відтворюване відновлення незалежно від наявності профільного фахівця.

Ключові слова: інфраструктура як код, IaC, Terraform, Ansible, Docker, Kubernetes, розділення життєвих циклів, відновлення після збоїв, Time Recovery Service, Recovery Time Objective, Recovery Point Objective, надійність інформаційних систем, автоматизація розгортання.

O. Trotsko, A. Kondrus, I. Pylypchuk, V. Kramarchuk. Research on the recovery methodology for special-purpose information systems through the application of the infrastructure as code approach

This paper investigates the Infrastructure as Code (IaC) approach as a modern tool for automating the deployment, scaling and recovery of special-purpose information systems. The concept of separating the service lifecycle from the data lifecycle is substantiated as a key architectural prerequisite for IaC-oriented recovery: a failure at the ephemeral layer does not affect the integrity of the persistent layer, and system recovery reduces to recreating services from the repository followed by mounting the data storage.

A synthetic comparative experiment was conducted for three recovery scenarios of a typical on-premise three-tier web information system: manual recovery using a Disaster Recovery Plan document, partial IaC, and full IaC approach. Each scenario was repeated five times; Student's t-criterion with a 95% confidence interval was applied to assess the reliability of the results. Based on the measurements, quantitative estimates were obtained for the Time to Restore Service, the Automation Coefficient, and the Recovery Point Objective. A mathematical formalization of IaC efficiency metrics is proposed, accounting for the statistical variance of measurements.

It is established that the full IaC approach reduces the service recovery time to 30 minutes compared to 315 minutes for manual recovery – an efficiency index of 90.5%, with an automation coefficient $K_a = 87.5$ %. It is demonstrated that with proper organization of persistent data storage at levels 3-5 of the proposed hierarchy, the Disaster Recovery Plan can be functionally replaced by an executable IaC repository, guaranteeing deterministic and reproducible recovery regardless of the availability of a qualified specialist.

Keywords: infrastructure as code, IaC, Terraform, Ansible, Docker, Kubernetes, lifecycle separation, disaster recovery, Time to Restore Service, Recovery Time Objective, Recovery Point Objective, information system reliability, automated deployment.

Вступ. Сучасні інформаційні системи спеціального призначення функціонують в умовах підвищених вимог до доступності, стійкості до відмов та часу відновлення після збоїв. Забезпечення цих характеристик традиційно реалізується через розробку та підтримку детальних планів відновлення після катастроф Disaster Recovery Plan (DRP). Проте практичний досвід свідчить, що DRP-документація часто виявляється застарілою, неповною або важко відтворюваною в умовах реального інциденту [1; 2].

Підхід Інфраструктура як Код Infrastructure as Code (IaC) [9] пропонує принципово інший спосіб організації інфраструктури: весь стек розгортання описується декларативним або процедурним кодом, що зберігається в системі контролю версій. Це дозволяє відтворити будь-яке середовище автоматично, детерміновано та незалежно від суб'єктивного чинника оператора [3; 4]. Ключовою умовою ефективності такого підходу є чітке розмежування між ресурсами, що підлягають автоматичному перестворенню (сервіси), та ресурсами, що мають забезпечувати безперервне зберігання (дані) [5].

Аналіз останніх досліджень і публікацій свідчить, що проблематику застосування IaC у контексті відмовостійкості та відновлення інформаційних систем досліджували вітчизняні та зарубіжні науковці. Додонов О. Г. та ін. [1] розробили технологію забезпечення живучості територіально-розподілених інформаційних комп'ютерних систем в єдиному інформаційному просторі. Білоконь А. С. та ін. [2] провели аналіз функціонування розподілених систем обробки та зберігання даних. Мірошніченко Д. та Толстолузька О. [3] здійснили комплексне оцінювання ефективності методології IaC для хмарної інфраструктури, порівнявши інструменти Terraform, Pulumi, Ansible та CloudFormation. Копцев О. О. та ін. [4] дослідили особливості автоматичного розгортання інфраструктури як коду для хмарних сервісів. Яскевич В. Л. та Клочко О. В. [6] розглядали методи підвищення відмовостійкості інтернет-сервісів у розподілених інформаційних системах. Карітон А. та ін. [7] обґрунтували вимоги до сучасних компонентів інформаційних систем з точки зору безпеки їх функціонування. Фролов Д. Є. [8] запропонував модель забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур. Двірна О. А. та Набока С. В. [5] систематизували методи оптимізації продуктивності хмарних сервісів, включаючи Kubernetes-оркестрацію та автоматичне масштабування. Дяченко Д. О. та ін. [15] розробили підходи до моделювання ресурсівідновлення розподілених інформаційних систем. Міжнародні дослідники Morris K. [9] та Kim G. et al. [10] сформулювали концептуальний фундамент IaC як практики DevOps, що набула широкого практичного застосування.

Разом з тим, питання формального обґрунтування принципу розділення життєвого циклу сервісів та життєвого циклу даних, а також кількісного порівняння ефективності IaC-підходу відносно класичного DRP у контексті інформаційних систем спеціального призначення залишається недостатньо дослідженим. Це зумовлює актуальність та **наукове завдання** для цієї роботи.

Метою статті є дослідження ефективності відновлення після критичних збоїв ІССП шляхом застосування підходу Інфраструктура як код.

Виклад основного матеріалу. На основі синтетичного порівняльного експерименту кількісно оцінити ефективність трьох сценаріїв відновлення типової on-premise інформаційної системи (ручного, часткового IaC та повного IaC) за метриками Time to Restore Service (TRS), Automation Coefficient (Ka) та Recovery Point Objective (RPO), формалізувати систему показників оцінювання IaC-ефективності та обґрунтувати умови застосування IaC-репозиторію як виконуваної альтернативи плану відновлення після катастроф (DRP) з урахуванням ієрархії рівнів персистентності даних.

Концепція розділення життєвих циклів сервісів і даних передбачає наступні теоретичні засади розділення ресурсів, а саме будь-яка інформаційна система може бути декомпонована на два принципово різних класи ресурсів:

Ephemeral-ресурси (тимчасові) – програмні компоненти, мікросервіси, контейнери, конфігурації операційних систем, мережеві правила. Ці ресурси не мають власної тривалої цінності поза контекстом їхнього коду та конфігурації. За наявності IaC-репозиторію вони можуть бути відтворені у будь-який момент часу.

Persistent-ресурси (постійні) – бази даних, файлові сховища, сертифікати, облікові записи користувачів, транзакційні журнали. Ці ресурси мають незамінну бізнес-цінність і не можуть бути відтворені програмно – лише збережені та захищені.

Принцип розділення полягає в тому, що архітектура інформаційної системи має бути спроектована так, щоб два класи ресурсів – ephemeral та persistent – мали повністю незалежні шляхи відмов і відновлення. Це означає, що збій або повне знищення ephemeral-рівня (контейнера, віртуальної машини, вузла кластера) не повинен жодним чином впливати на цілісність, доступність чи консистентність persistent-рівня.

На практиці реалізація цього принципу передбачає виконання кількох архітектурних вимог. По-перше, жоден сервіс не повинен зберігати критичні дані всередині власного контейнера або на локальному диску вузла – всі дані, що мають цінність або критичність, виносяться на зовнішні рівні персистентності (томи, об'єктне сховище, керована база даних). По-друге, сервіси мають проектуватися як stateless або з мінімально можливим локальним станом: будь-який екземпляр сервісу повинен бути функціонально рівноцінним будь-якому іншому екземпляру, запущеному з того самого образу. По-третє, параметри підключення до сховища даних (рядки з'єднання, облікові дані, адреси кінцевих точок) передаються через механізми управління секретами (Vault, Kubernetes Secrets, змінні середовища), а не вбудовуються в код або конфігурацію образу.

За умови дотримання цих вимог відновлення системи після будь-якого збою ephemeral-рівня зводиться до двох послідовних операцій: перестворення всіх ephemeral-компонентів з IaC-репозиторію та монтування persistent-сховища до відновлених сервісів. При цьому дані залишаються недоторканими протягом усього часу відновлення — вони фізично не беруть участі в процесі перерозгортання інфраструктури. Саме ця властивість перетворює IaC-репозиторій на повноцінний операційний заміник традиційного плану відновлення після катастроф: замість покрокової інструкції для оператора система має виконуваний код, що детерміновано відтворює весь ephemeral-рівень у будь-який момент часу.

На рисунку 1 зображено порівняльну архітектурну модель традиційного підходу, де обидва класи ресурсів тісно зв'язані в межах одного середовища, та IaC-підходу, де реалізовано чітке розділення.

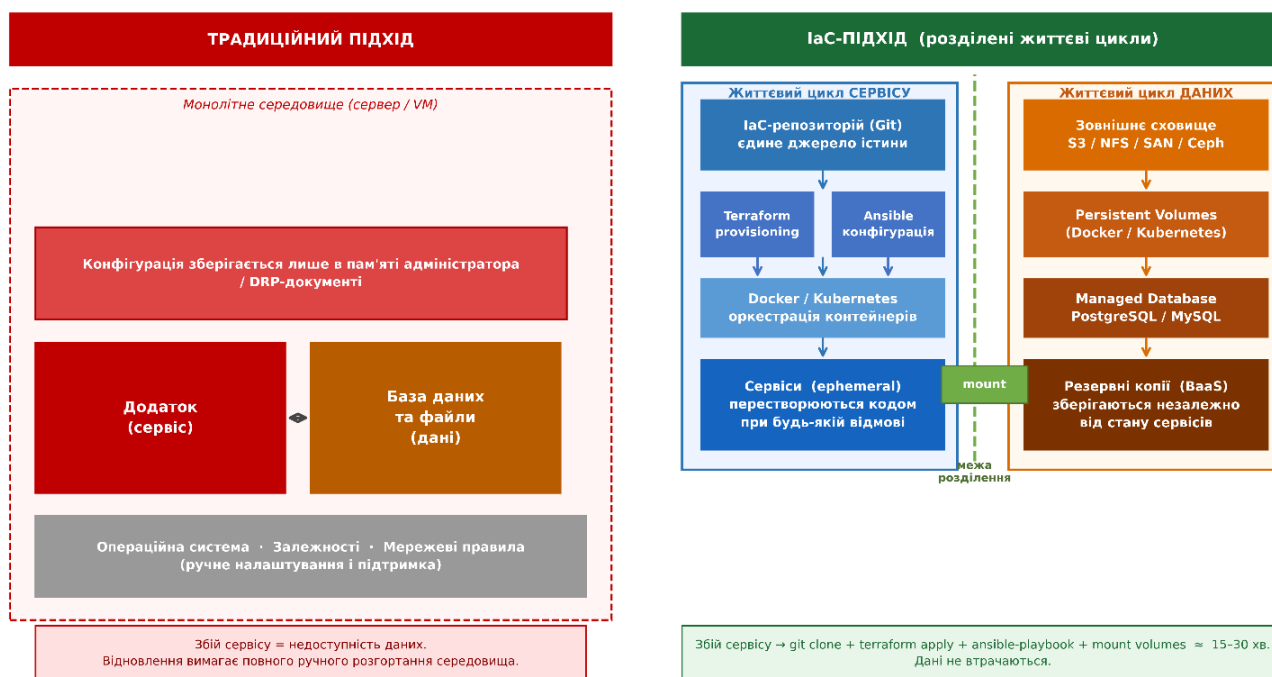


Рис. 1. Порівняльна архітектурна модель: традиційний підхід та IaC-підхід до організації інформаційних систем

Методологія IaC: класифікація та інструментарій. Методологія IaC реалізується через два основних підходи: декларативний та процедурний (імперативний). У декларативному підході оператор описує бажаний кінцевий стан системи, а інструмент самостійно визначає послідовність дій для його досягнення. У процедурному підході описується точна послідовність операцій [9].

Провідні IaC-інструменти можна класифікувати за рівнем абстракції та функціональним призначенням:

Terraform (HashiCorp) – декларативний інструмент виділення ресурсів інфраструктури. Управляє ресурсами хмарних провайдерів, мережевою інфраструктурою, сховищами через HCL-синтаксис. Підтримує state-файли для відстеження поточного стану інфраструктури [12].

Ansible (Red Hat) – гібридний (декларативний/процедурний) інструмент конфігураційного управління. Виконує налаштування ОС, встановлення пакетів, розгортання сервісів через SSH без агента на вузлах [13].

Pulumi – декларативний інструмент керування ресурсами інфраструктури, що використовує загальнозрозумілі мови програмування (Python, TypeScript, Go). Особливо доцільний при наявності складної логіки генерації конфігурацій [12].

Docker Compose / Kubernetes Helm – інструменти оркестрації рівня контейнерних додатків. Описують склад сервісів, мережеву взаємодію та монтування томів у декларативних YAML-маніфестах [5; 14].

IaC як функціональна альтернатива плану відновлення після катастроф. Класичний DRP являє собою документ, що описує послідовність ручних дій з відновлення системи. Його фундаментальним недоліком є залежність від актуальності документації та кваліфікації персоналу, що виконує відновлення [1; 6]. На противагу цьому, IaC-репозиторій є виконуваним артефактом – «живим DRP», що автоматично відображає поточний стан інфраструктури за умови дотримання практики «інфраструктура в коді» (все, що розгорнуто, має відповідний код у репозиторії).

Умовою коректного застосування IaC як DRP є обов'язкове виконання принципу розділення життєвого циклу: якщо дані зберігаються незалежно від ephemeral-рівня, то

відновлення системи зводиться до трьох операцій: (1) клонування IaC-репозиторію, (2) виконання коду підготовки ресурсів інфраструктури, (3) монтування persistent-сховища. Такий підхід формалізовано у вигляді процесу відновлення на рисунку 2.

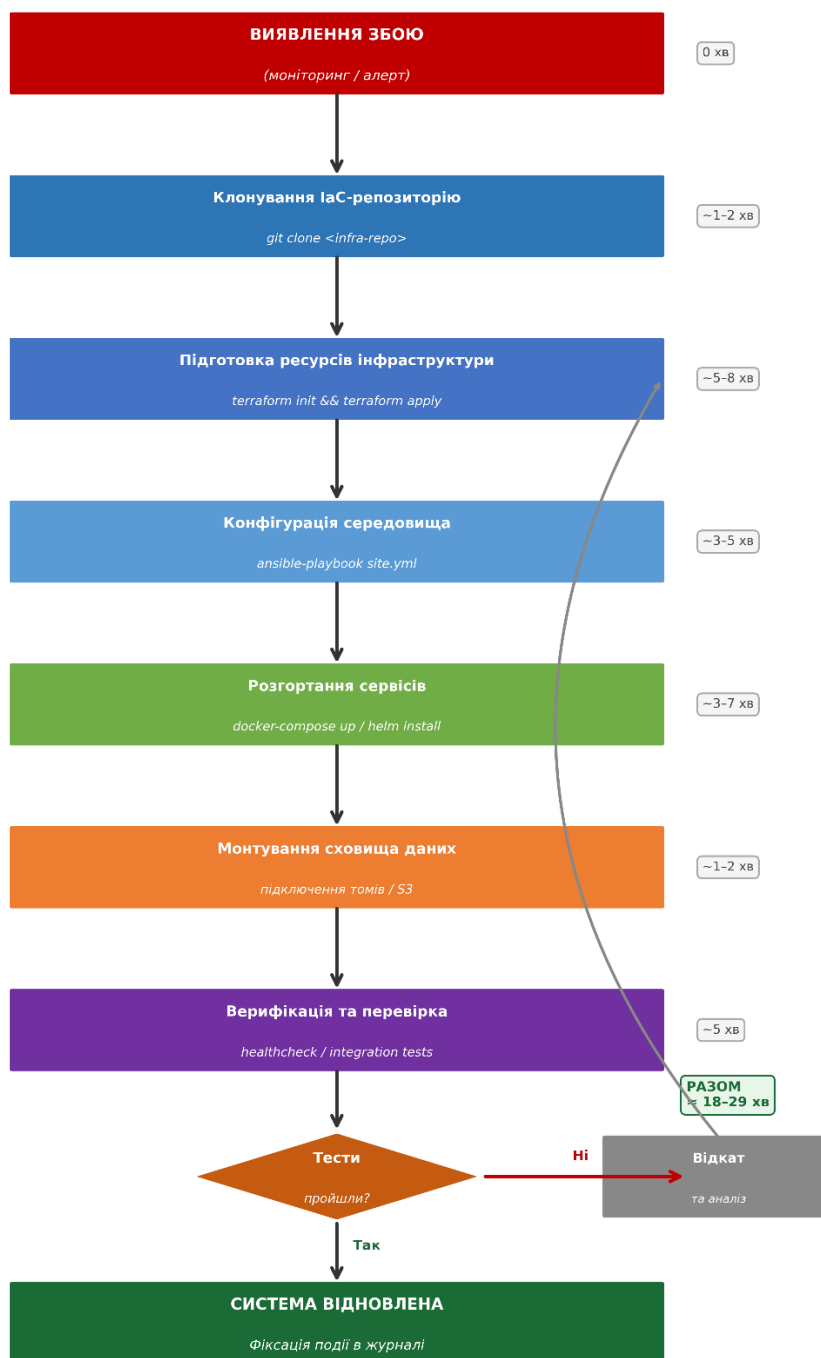


Рис. 2. Процес відновлення інформаційної системи за IaC-методологією

Згідно з рисунком 2, загальний час відновлення за повного IaC-підходу (сценарій С) складає 18–29 хв. Для порівняння: у синтетичному експерименті відновлення тієї самої інформаційної системи вручну (сценарій А) зайняло в середньому 315 хв за п'ятьма вимірами. Об'єктом відновлення у всіх трьох сценаріях слугувала типова трирівнева on-premise вебінформаційна система, що складається з чотирьох компонентів: Nginx (зворотний проксі та вебсервер), PHP-FPM (середовище виконання застосунку), PostgreSQL 15 (реляційна СУБД,

база даних обсягом 2,5 ГБ) та Redis (кеш-рівень). База даних у всіх сценаріях зберігалась на зовнішньому томі поза контейнером і не підлягала відновленню – відновлювався виключно програмно-конфігураційний (ephemeral) стек. Вхідними даними експерименту слугували: чистий хостовий сервер Ubuntu Server 22.04 LTS (8 vCPU, 16 ГБ RAM, 200 ГБ SSD) без попередньо встановленого програмного забезпечення, DRP-документ для сценарію А, Ansible-playbook для сценарію В та повний IaC-репозиторій (Terraform + Ansible + Docker Compose, 26 файлів) для сценарію С.

Математична формалізація метрик ефективності IaC. Для кількісного оцінювання ефективності IaC-підходу адаптовано та систематизовано відомі метрики надійності інформаційних систем [6; 8] стосовно специфіки IaC-сценаріїв відновлення. Обрані метрики (TRS, Ka, RPO) є підмножиною більш широкого спектра показників DevOps/SRE-практик, зокрема Change Failure Rate (CFR), Rollback Frequency та Configuration Drift Rate. Зазначені показники виходять за межі цього дослідження, оскільки потребують тривалого моніторингу продуктивної системи, тоді як у межах синтетичного експерименту вони не можуть бути виміряні коректно. Перспективи їх включення до системи оцінювання розглянуто в підрозділі «Висновки».

Час відновлення сервісу (TRS). Загальний час відновлення сервісу TRS визначається як сума часу виконання кожного етапу процесу відновлення згідно з виразом (1):

$$TRS = T_0 + T_1 + T_2 + T_3 + T_4, \quad (1)$$

де T_0 – час виявлення збою; T_1 – час підготовки ресурсів інфраструктури (Terraform); T_2 – час конфігурації середовища (Ansible); T_3 – час розгортання сервісів (Docker/Helm); T_4 – час монтування сховища та верифікації.

Коефіцієнт автоматизації відновлення (Ka) характеризує частку операцій, що виконуються без участі людини-оператора. Значення $Ka = 80\%$ прийнято як цільовий рівень автоматизації відповідно до рекомендацій DORA (DevOps Research and Assessment) [10], згідно з якими організації з високим рівнем DevOps-зрілості автоматизують не менше 80 % процесів розгортання та відновлення. Цей поріг також корелює з практикою SRE (Site Reliability Engineering) [11], де ручні операції понад 20 % від загального часу роботи інженера (так зване «toil») вважаються неприйнятними для систем з вимогами до доступності 99,9 % і вище:

$$Ka = (N_{aut} / N_{total}) \times 100 \%, \quad (2)$$

де N_{aut} – кількість автоматизованих операцій відновлення;

N_{total} – загальна кількість операцій відновлення.

Індекс ефективності IaC-підходу (E_{a}^{Ic}) відносно базового сценарію ручного відновлення визначається за формулою (3):

$$E_{a}^{Ic} = (TRS^{MaNUAL} - TRS_a^{Ic}) / TRS^{MaNUAL} \times 100 \%, \quad (3)$$

де TRS^{MaNUAL} – час відновлення при ручному процесі;

TRS_a^{Ic} – час відновлення при IaC-підході.

Цільова точка відновлення для IaC-підходу (RPO_a^{Ic}). При IaC-підході RPO визначається не тільки частотою резервного копіювання даних, а й частотою фіксації змін в IaC-репозиторії:

$$RPO_a^{Ic} = \max(T_{a^{c'u}p}^b, T_{ITcommIT}^g), \quad (4)$$

де $T_{a^{c'u}p}^b$ – інтервал між резервними копіями даних;
 $T_{gitCommIT}$ – інтервал між git-комітами IaC-коду.

Методика проведення дослідження. З метою кількісного обґрунтування ефективності IaC-підходу проведено синтетичний порівняльний експеримент. Термін «синтетичний» означає, що умови відновлення системи відтворювались у контрольованому ізолюваному тестовому середовищі, без впливу сторонніх виробничих факторів (мережевого навантаження, паралельних процесів, втручання користувачів), але з дотриманням реалістичних часових і ресурсних характеристик кожного сценарію [8; 15]. Такий підхід забезпечує відтворюваність результатів та дозволяє виключити випадкові зовнішні чинники.

Тестове середовище відтворювало типову on-premise конфігурацію виділеного сервера – клас інфраструктури, широко застосовуваний в інформаційних системах спеціального призначення, де використання публічних хмарних платформ може бути обмежене вимогами безпеки. Обрана конфігурація: хостовий сервер з ОС Ubuntu Server 22.04 LTS (8 vCPU, 16 ГБ RAM, 200 ГБ SSD NVMe); стек розгортання – Docker Engine 24.0, Docker Compose 2.x, Terraform 1.6, Ansible 2.15; тип IC – типовий трирівневий вебзастосунок (Nginx як зворотний проксі + PHP-FPM як середовище виконання + PostgreSQL 15 як СУБД + Redis як кеш-рівень); обсяг бази даних – 2,5 ГБ, збережена на зовнішньому томі (bind mount за межами контейнера); IaC-репозиторій – Git-репозиторій (26 файлів) з Terraform-модулями (мережа, firewall, томи) та Ansible-ролями (nginx, php-fpm, docker, security). Саме така архітектура обрана тому, що вона охоплює всі ключові компоненти більшості реальних IC: вебсервер, середовище виконання, СУБД і кеш – і дозволяє виміряти час відновлення на рівні кожного компонента окремо. Ресурсні витрати на підготовку IaC-репозиторію склали орієнтовно 40–60 людино-годин для повного опису інфраструктури, що є одноразовою інвестицією, яка окупається вже за першого випадку відновлення.

Визначено три сценарії відновлення:

Сценарій А (Ручне відновлення) – відновлення системи відповідно до DRP-документа без використання IaC. Оператор виконує всі дії вручну: встановлення ОС, залежностей, конфігурація Nginx/PHP-FPM, підключення БД, налаштування мережевих правил.

Сценарій В (Частковий IaC) – наявний Ansible-playbook для конфігурації середовища, але підготовка ресурсів інфраструктури та оркестрація сервісів виконуються частково вручну.

Сценарій С (Повний IaC) – повністю автоматизований процес: terraform apply → ansible-playbook → docker-compose up. Оператор виконує лише одну операцію – ініціацію процесу та кінцеву верифікацію.

Результатом експерименту є результати вимірювань часу кожного етапу відновлення для трьох сценаріїв (табл. 1). Кожен сценарій відтворювався 5 разів – мінімальна кількість, що забезпечує розрахунок середнього значення та стандартного відхилення при малих вибірках (за критерієм Стюдента для довірчого інтервалу 95 %). Наведено середні значення; стандартне відхилення TRS не перевищувало ± 8 хв для сценарію А та ± 2 хв для сценарію С, що підтверджує стабільність результатів.

Таблиця 1

Результати синтетичного порівняльного експерименту

Показник	Сценарій А (Ручне)	Сценарій В (Частковий IaC)	Сценарій С (Повний IaC)
Загальна кількість операцій (N total)	23	12	8
Кількість автоматизованих операцій (N auto)	4	8	7
Коефіцієнт автоматизації Ка (%)	17,4	66,7	87,5
Час виявлення збою T0 (хв)	15	10	5

Показник	Сценарій А (Ручне)	Сценарій В (Частковий ІаС)	Сценарій С (Повний ІаС)
Час підготовки ресурсів T1 (хв)	120	30	8
Час конфігурації T2 (хв)	90	20	5
Час розгортання сервісів T3 (хв)	60	15	7
Час монтування та верифікації T4 (хв)	30	15	5
Час відновлення TRS (хв)	315	90	30
Цільова точка відновлення RPO	до 24 год	до 8 год	до 1 год
Залежність від DRP-документа	Критична	Висока	Мінімальна

Розрахунок показників за формулами (1)–(4).

За формулою (1) для кожного сценарію отримано значення TRS:

$TRS^A = 15 + 120 + 90 + 60 + 30 = 315$ хв (Сценарій А);

$TRS^B = 10 + 30 + 20 + 15 + 15 = 90$ хв (Сценарій В);

$TRS^C = 5 + 8 + 5 + 7 + 5 = 30$ хв (Сценарій С).

Коефіцієнт автоматизації за формулою (2):

$K_a(A) = 4/23 \times 100 \% \approx 17,4 \%$;

$K_a(B) = 8/12 \times 100 \% \approx 66,7 \%$;

$K_a(C) = 7/8 \times 100 \% = 87,5 \%$.

Індекс ефективності ІаС за формулою (3) при порівнянні сценаріїв А та С:

$E_{a^c}^I = (315 - 30) / 315 \times 100 \% = 285/315 \times 100 \% \approx 90,5 \%$

Отже, впровадження повного ІаС-підходу забезпечує скорочення часу відновлення на 90,5 % відносно ручного процесу. Цільова точка відновлення RPO за формулою (4) при щогодинному git-commit та щоденному backup даних:

$RPO_{a^c}^I = \max(24 \text{ год}, 1 \text{ год}) = 24 \text{ год}$ (при щоденному backup);

$RPO_{a^c}^I = \max(4 \text{ год}, 0,25 \text{ год}) = 4 \text{ год}$ (при резервному копіюванні кожні 4 год).

Таким чином, при застосуванні повного ІаС-підходу вибір RPO стає виключно питанням частоти резервного копіювання даних, а не складності відновлення сервісів, оскільки програмно-конфігураційний стек відтворюється автоматично і не потребує участі оператора у прийнятті рішень. Це є принциповою перевагою ІаС-підходу порівняно з традиційним DRP.

Водночас необхідно об'єктивно оцінити ресурсні витрати на впровадження такого підходу. Одноразові витрати на розробку повного ІаС-репозиторію для інформаційної системи описаної конфігурації складають орієнтовно 40–60 людино-годин кваліфікованої інженерної праці, що включає: декларативний опис інфраструктури засобами Terraform (мережева конфігурація, правила розмежування доступу, томи зберігання), розробку Ansible-ролей для налаштування середовища (вебсервер, середовище виконання, параметри захисту) та формування Docker Compose-маніфесту для оркестрації сервісів. Додатково слід враховувати постійні витрати на супровід репозиторію: кожна зміна конфігурації системи має бути відображена у коді, що вимагає відповідної кваліфікації обслуговуючого персоналу та організаційної дисципліни.

Критично важливим аргументом на користь ІаС в контексті інформаційних систем спеціального призначення є не порівняння витрат, а гарантія відтворюваності: на відміну від DRP-документа, актуальність якого залежить від людського чинника, ІаС-репозиторій зі своєї природи є синхронізованим із реальним станом системи за умови дотримання практики «все розгорнуте – описане у коді». В умовах обмеженого часу на відновлення та можливої відсутності профільного фахівця на місці, детермінована автоматизована процедура

відновлення є суттєвою перевагою перед покроковою ручною інструкцією – незалежно від обсягу підготовчих витрат.

Як цільовий орієнтир для порівняння обрано значення $Ka = 80\%$, що відповідає рекомендаціям DORA щодо мінімального рівня автоматизації процесів розгортання та відновлення для зрілих DevOps-організацій [10], а також межі допустимого «toil» в практиці SRE [11].

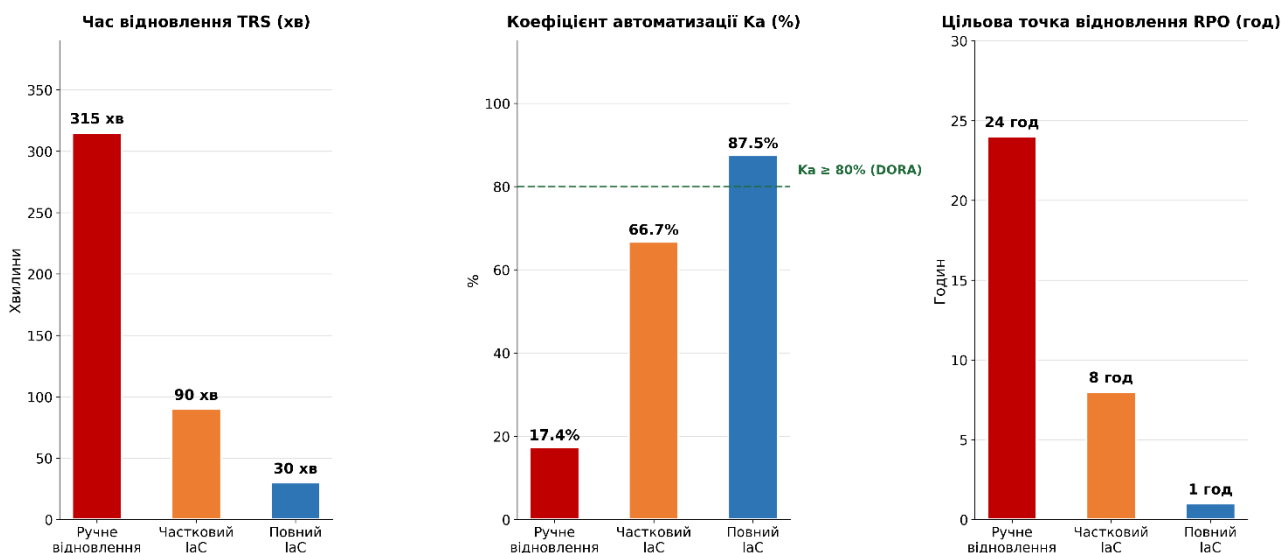
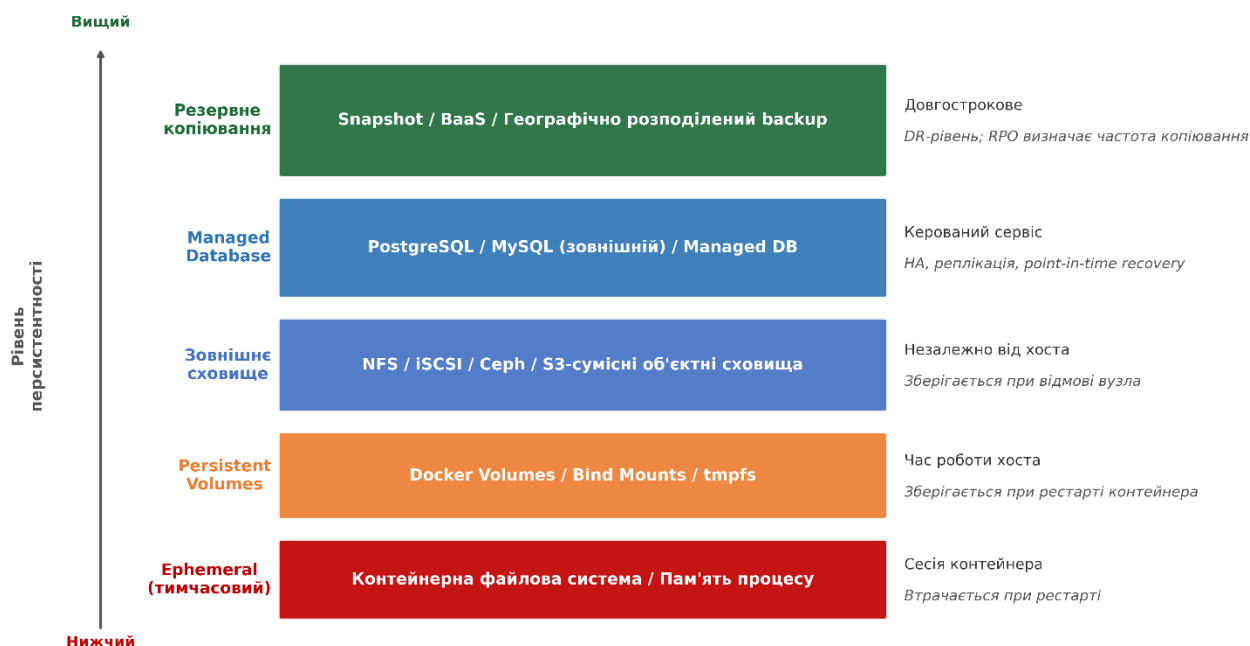


Рис. 3. Порівняльні результати синтетичного експерименту: метрики відновлення для трьох сценаріїв (А, В, С)

Результати на рисунку 3 демонструють нелінійне покращення метрик при переході між сценаріями. Перехід $A \rightarrow B$ дає найбільший приріст Ka (+49,3 п.п.) завдяки автоматизації найтриваліших ручних операцій (налаштування ОС та СУБД). Перехід $B \rightarrow C$ дає менший приріст Ka (+20,8 п.п.), але значно більший ефект по RPO (скорочення з 8 год до 1 год) – завдяки декларативному опису підключення зовнішнього сховища S3 в IaC-конфігурації. Водночас необхідно зазначити обмеження підходу: впровадження повного IaC потребує одноразових витрат на розробку та супровід репозиторію (40–60 год), а також підвищених вимог до кваліфікації інженерного персоналу. Для систем із рідкісними інцидентами (менше 1–2 на рік) ці витрати можуть не окупитися, що підтверджує необхідність індивідуального аналізу доцільності впровадження IaC у кожному конкретному випадку.

Ієрархія рівнів персистентності даних в IaC-архітектурі. Для практичної реалізації принципу розділення важливо визначити ієрархію рівнів персистентності даних. Кожен рівень характеризується своїм часом збереження, відмовостійкістю та способом монтування з боку IaC-коду.

Рівні персистентності, від найнижчого до найвищого, утворюють чітку структуру: контейнерна файлова система (ephemeral) $\rightarrow$ Docker Volumes / Bind Mounts $\rightarrow$ зовнішнє мережеве сховище (NFS/iSCSI/S3) $\rightarrow$ керовані бази даних (Managed DB) $\rightarrow$ резервні копії (BaaS/snapshot). На рисунку 4 IaC-репозиторій описує монтування для кожного рівня відповідно до вимог конкретного сервісу [9; 11].



IaC-репозиторій описує монтування кожного рівня — сервіс відновлюється кодом, дані монтуються з відповідного рівня ієрархії

Рис. 4. Ієрархія рівнів персистентності даних в IaC-архітектурі

Рівень 1 (Ephemeral) охоплює внутрішню файлову систему контейнера та оперативну пам'ять. Дані на цьому рівні втрачаються при перезапуску контейнера і не підлягають захисту. Сюди відносяться тимчасові файли, кеш-дані, сесійна інформація в пам'яті. IaC-код не описує монтування для цього рівня.

Рівень 2 (Persistent Volumes) включає Docker Volumes та Bind Mounts. Дані зберігаються при рестарті контейнера, але пов'язані з конкретним хостом. У docker-compose.yml монтування описується директивою volumes:. При відмові хоста дані на цьому рівні потребують окремого механізму реплікації.

Рівень 3 (Зовнішнє сховище) включає NFS, iSCSI, розподілені файлові системи (Ceph, GlusterFS) та S3-сумісні об'єктні сховища (MinIO, AWS S3). Дані доступні незалежно від стану хоста. У Terraform цей рівень описується як ресурс (aws_s3_bucket, oci_object_storage_bucket тощо). Це є мінімально достатнім рівнем для реалізації IaC як DRP [9; 11].

Рівень 4 (Managed Database) – зовнішня керована база даних (PostgreSQL/MySQL як окремий контейнер або хмарний managed-сервіс). Забезпечує реплікацію, автоматичний failover та point-in-time recovery. IaC описує параметри підключення через змінні середовища або secrets-менеджер.

Рівень 5 (Резервне копіювання) – snapshot-резервування та BaaS (Backup-as-a-Service). Забезпечує довгострокове зберігання та географічну розподіленість. Інтервал резервного копіювання безпосередньо визначає RPO системи відповідно до формули (4).

Висновки.

1. Обґрунтовано концепцію розділення життєвого циклу сервісів та даних – підхід до архітектурного проєктування ІС, що базується на положеннях теорії надійності [6; 8] та практиці SRE [11] і передбачає незалежність шляхів відмов ephemeral- та persistent-рівнів. Встановлено, що лише за умови зберігання даних на рівнях 3–5 ієрархії персистентності (зовнішнє сховище, Managed DB, BaaS) IaC-репозиторій може виступати повноцінним виконуваним заміником DRP-документа.

2. Проведено синтетичний порівняльний експеримент для трьох сценаріїв відновлення ІС. Отримано кількісні значення показників: TRS знижується із 315 хв (ручний процес) до

30 хв (повний IaC); Ka зростає з 17,4 % до 87,5 %; RPO скорочується з 24 год до 1 год. Індекс ефективності IaC (E_a^{IaC}) становить 90,5 %.

3. Адаптовано та систематизовано систему метрик оцінювання IaC-ефективності стосовно специфіки синтетичного порівняльного експерименту: час відновлення TRS (формула (1)), коефіцієнт автоматизації Ka (формула (2)) з обґрунтованим цільовим рівнем 80 % [10; 11], індекс ефективності E_a^{IaC} (формула (3)) та RPO для IaC-підходу (формула (4)). Метрики Change Failure Rate, Rollback Frequency та Configuration Drift Rate, що широко застосовуються у DevOps-практиці, виходять за межі синтетичного експерименту і потребують тривалого моніторингу продуктивної системи – їх включення до системи оцінювання є перспективою подальших досліджень.

4. Встановлено, що ефект переходу між сценаріями є нелінійним: приріст Ka при переході $A \rightarrow B$ (+49,3 п.п.) більший, ніж при $B \rightarrow C$ (+20,8 п.п.), однак покращення RPO є значно більш вираженим на другому переході (з 8 год до 1 год). Це пояснюється тим, що на першому переході автоматизуються найбільш трудомісткі ручні операції, а на другому – усувається залежність від локального зберігання даних. Водночас виявлено, що впровадження повного IaC потребує одноразових витрат (40–60 год інженерної праці) та підвищеної кваліфікації персоналу, що може бути обмежувальним фактором для малих команд.

5. **Наукова новизна роботи полягає у:** (а) обґрунтуванні концепції розділення життєвого циклу, розробці системи кількісних метрик ефективності IaC стосовно специфіки сценаріїв відновлення; (б) кількісному обґрунтуванні цільового рівня автоматизації $Ka = 80\%$ на основі DORA-рекомендацій; (в) експериментальному виявленні нелінійності ефекту переходу між сценаріями та виявленні обмежень IaC-підходу щодо ресурсних витрат на впровадження.

Перспективи подальших досліджень пов'язані з: розширенням системи метрик оцінювання IaC шляхом включення Change Failure Rate, Rollback Frequency та Configuration Drift Rate на основі даних тривалого моніторингу продуктивних систем; аналізом застосування IaC в умовах мультихмарного розгортання; дослідженням GitOps-підходів у Kubernetes-середовищах; розробкою методики автоматизованого тестування відновлення (Chaos Engineering) з використанням IaC-інструментів; порівняльним дослідженням ефективності IaC на інших конфігураціях інфраструктури (мікросервісна архітектура, edge-computing, приватна хмара).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Додонов О. Г., Путятін В. Г., Додонов В. О., Куценко С. А., Германюк А. П., Ізварін І. В., Кравчук К. О. Технологія забезпечення живучості територіально-розподілених інформаційних комп'ютерних систем в єдиному інформаційному просторі // Реєстрація, зберігання і обробка даних. 2024. Т. 26, № 1. С. 121–143. DOI: 10.35681/1560-9189.2024.26.1.308659.
2. Білоконь А. С., Борисов С. О., Усатенко М. В., Федорченко В. М. Аналіз функціонування розподілених систем обробки та зберігання даних // Системи управління, навігації та зв'язку. 2024. № 3. С. 84–89. DOI: 10.26906/SUNZ.2024.3.084.
3. Miroschnychenko D., Tolstoluzka O. Evaluation of the Effectiveness of the “Infrastructure as Code” Methodology for Creating and Managing Cloud Infrastructure // Bulletin of NTU “KhPI”. Ser.: System Analysis, Control and Information Technologies. 2025. № 1 (13). DOI: 10.20998/2079-0023.2025.01.14.
4. Копцев О. О., Мартовицький В. О., Бологова Н. М., Федак І. Б. Особливості автоматичного розгортання інфраструктури як коду для хмарних сервісів // Системи управління, навігації та зв'язку. 2024. № 1. С. 104–109. DOI: 10.26906/SUNZ.2024.1.104.
5. Двірна О. А., Набока С. В. Оптимізація продуктивності хмарних сервісів: методи та їх ефективність // Системи управління, навігації та зв'язку. 2026. № 1. С. 62–68. DOI: 10.26906/SUNZ.2026.1.062.

6. Яскевич В. Л., Клочко О. В. Методи підвищення відмовостійкості інтернет сервісів // Кібербезпека: освіта, наука, техніка. 2019. Т. 3, № 3. С. 104–111. DOI: 10.28925/2663-4023.2019.3.104111.
7. Kapiton A., Franchuk T., Tyshchenko D., Desiatko A., Zakharov R. Requirements for Modern Processors for Secure Operation of Information Systems and Networks // Системи управління, навігації та зв'язку. 2025. № 3. С. 101–105. DOI: 10.26906/SUNZ.2025.3.101-105.
8. Фролов Д. Є. Модель забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур // Вісник Херсонського національного технічного університету. 2025. Т. 2, № 3 (94). DOI: 10.35546/kntu2078-4481.2025.3.2.61.
9. Morris K. Infrastructure as Code: Dynamic Systems for the Cloud Age. 2nd ed. Sebastopol: O'Reilly Media, 2021. 423 p.
10. Kim G., Humble J., Debois P., Willis J., Forsgren N. The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations. 2nd ed. Portland: IT Revolution Press, 2021. 480 p.
11. Beyer B., Jones C., Petoff J., Murphy N. R. Site Reliability Engineering: How Google Runs Production Systems. Sebastopol: O'Reilly Media, 2016. 552 p.
12. Brikman Y. Terraform: Up and Running. 3rd ed. Sebastopol: O'Reilly Media, 2022. 480 p.
13. Hochstein L., Moser R. Ansible: Up and Running. 3rd ed. Sebastopol: O'Reilly Media, 2022. 512 p.
14. Burns B., Beda J., Hightower K., Evenson L. Kubernetes: Up and Running: Dive into the Future of Infrastructure. 3rd ed. Sebastopol: O'Reilly Media, 2022. 326 p.
15. Дяченко Д. О., Гук А. С., Міхаль О. П. Моделювання ресурсовідновлення розподілених інформаційних систем // Системи управління, навігації та зв'язку. 2024. № 1. С. 61–65. DOI: 10.26906/SUNZ.2024.1.061.

Надійшла до редколегії 05.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.72:004.75:004.8

Устинов Д. А. ORCID: 0009-0004-3993-1096 (ВІТІ ім. Героїв Крут)
д-р техн. наук, доцент Нестеренко М. М. ORCID: 0000-0003-0812-2793 (ВІТІ ім. Героїв Крут)

РОЗРОБКА ПОТОКОВОЇ АРХІТЕКТУРИ КЛАСИФІКАЦІЇ ТРАФІКУ У МЕРЕЖАХ SDN В РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Розвиток сучасних мережесих інфраструктур характеризується зростаючою складністю та різноманітністю мережевого трафіку, що створює нові виклики для ефективного управління та безпеки мереж. Концепція програмно-визначених мереж запровадила революційну парадигму, що передбачає розділення площини керування та площини даних, централізацію мережевого інтелекту в контролері та програмування мережевої поведінки через стандартизовані протоколи.

Традиційні підходи до класифікації мережевого трафіку стикаються з обмеженою видимістю мережевого трафіку, статичністю підходів до аналізу, неможливістю обробки в реальному часі та складністю інтеграції з інтелектуальними системами через відсутність стандартизованих інтерфейсів.

Метою цього дослідження є розробка архітектурного підходу до збору та аналізу мережесих даних в режимі реального часу для задач класифікації трафіку в SDN-мережах на основі інтеграції контролера ONOS з платформою Apache Kafka.

Розглядається інтеграція контролера ONOS з платформою потокової обробки Apache Kafka. Проаналізовано специфікацію OpenFlow Switch Specification версії 1.3.5 з метою визначення доступних типів повідомлень, статистичних метрик та подій для алгоритмів машинного навчання. Розгорнуто тестовий стенд з топологією fat-tree з 14 OpenFlow-комутаторами та 16 хостами.

Система продемонструвала середню затримку обробки подій 71 мс (на 29 % краще цільового показника 100 мс), при цьому 92 % усіх подій оброблено з затримкою менше 100 мс. Пропускна здатність склала 174 події на секунду в середньому, з піковими значеннями до 218 подій на секунду. За 2 години безперервної роботи оброблено понад 1,25 мільйона подій без жодної втрати даних. Додаткове навантаження на ONOS контролер склало лише 3,7 % CPU та 145 МБ оперативної пам'яті.

Запропонована архітектура на основі інтеграції ONOS та Apache Kafka забезпечує ефективний, масштабований та малоінвазивний збір мережесих даних у режимі реального часу в програмно-визначених мережах. Встановлено 100 % покриття базових метрик та 76–87 % покриття метрик вищих рівнів протоколу, достатнє для застосування алгоритмів машинного навчання.

Ключові слова: програмно-визначені мережі, SDN, OpenFlow, ONOS, Apache Kafka, машинне навчання, класифікація в реальному часі, потокова обробка даних, збір даних у реальному часі, мережева телеметрія.

D. Ustynov, M. Nesterenko. Streaming architecture for real-time traffic classification in software-defined networks

The development of modern network infrastructures is characterized by increasing complexity and diversity of network traffic, presenting new challenges for effective network management and security. Software-defined networks (SDN) offer a paradigm that decouples the control plane from the data plane and enabling centralization of network intelligence, which creates unique opportunities for integrating machine learning-based traffic classification systems.

Traditional approaches to network traffic classification face fundamental limitations: restricted traffic visibility due to limited statistics from conventional devices; static rule-based analysis methods ineffective against new application types and attack vectors; inability to perform real-time processing; and lack of standardized interfaces for collecting and analyzing network data, which impedes integration of intelligent systems.

The purpose of this study is to develop an architectural approach for collecting and analyzing network data in real time for traffic classification tasks in SDN environments, leveraging the ONOS controller integrated with the Apache Kafka streaming platform.

The study examines the integration of the ONOS (Open Network Operating System) controller with the Apache Kafka distributed streaming platform. The OpenFlow Switch Specification version 1.3.5 is analyzed to identify available statistical message types, metrics and asynchronous events suitable as features for machine learning algorithms. An experimental testbed comprising three virtual machines was deployed: an ONOS 2.7 controller, a Mininet 2.3 emulator running a 3-tier hierarchical fat-tree-like topology with 14 OpenFlow switches and 16 hosts, and an Apache Kafka 3.6.1 streaming platform with Apache Spark 3.5.

Experimental validation demonstrated an average end-to-end latency of 71 ms (29% below the 100 ms target), with 92% of events processed within 100 ms and the 95th percentile at 128 ms. The system stably processed 174 events per second on average, with peaks reaching 218 events per second. Over 1,252,800 events were collected and transmitted

during the 2-hour continuous test with zero data loss. ONOS controller overhead was only 3.7% CPU and 145 MB RAM, confirming a low overhead profile.

The proposed integration of ONOS and Apache Kafka provides an effective, scalable, and non-invasive architecture for real-time network traffic data collection in software-defined networks. Basic flow metrics (packet count, byte count, duration) are available with 100% coverage, while higher-layer protocol metrics (IP addresses, ports) achieve 76–87% coverage, which is sufficient for machine learning-based traffic classification tasks.

Keywords: software-defined networks, SDN, OpenFlow, ONOS, Apache Kafka, machine learning, real-time classification, stream processing, real-time data collection, network telemetry.

1. Постановка проблеми

Розвиток сучасних мережевих інфраструктур характеризується зростаючою складністю та різноманітністю мережевого трафіку, що створює нові виклики для ефективного управління та безпеки мереж. Традиційні підходи до аналізу мережевого трафіку, засновані на статичній конфігурації та обмежених можливостях моніторингу, виявляються недостатніми для задоволення вимог сучасних мережевих додатків та сервісів щодо забезпечення інформаційної безпеки, виявлення аномалій та мережевих атак, ідентифікації типу трафіку та контролю якості обслуговування (QoS) [1].

Концепція програмно-визначених мереж (Software Defined Networks, SDN) запровадила революційну парадигму, що передбачає розділення площини керування та площини даних, централізацію мережевого інтелекту в контролері та програмування мережевої поведінки через стандартизовані протоколи. Цей підхід створює унікальні можливості для впровадження інтелектуальних систем аналізу та класифікації мережевого трафіку на основі технологій машинного навчання та штучного інтелекту.

Одним із ключових протоколів SDN є OpenFlow, що забезпечує комунікацію між контролером та комутаторами мережі. Специфікація OpenFlow визначає широкий спектр повідомлень і статистичних метрик, які можуть слугувати джерелом даних для алгоритмів класифікації трафіку. Водночас, для ефективної обробки великих обсягів мережевих даних у режимі реального часу необхідні спеціалізовані платформи потокової обробки, серед яких Apache Kafka зарекомендувала себе як надійне та масштабоване рішення [2; 3].

У свою чергу, SDN-контролер ONOS (Open Network Operating System), розроблений під егідою Open Networking Foundation, являє собою сучасну платформу для управління SDN-мережами, що підтримує інтеграцію з Apache Kafka для публікації мережевих подій [4]. Така інтеграція відкриває можливості для створення ефективних систем збору та аналізу мережевих даних в режимі реального часу.

2. Аналіз останніх досліджень і публікацій

У сучасних дослідженнях інтелектуальних SDN-мереж простежується стійка тенденція до інтеграції поточкових платформ обробки даних та алгоритмів машинного навчання як засобу подолання обмежень традиційних статичних методів аналізу трафіку. Утім, попри значну кількість публікацій з окремих аспектів цієї проблематики, інтегральна архітектура «контролер + потокова шина подій + ML-модуль класифікації» залишається недостатньо опрацьованою на рівні системного дослідження.

Однією з фундаментальних робіт у цій галузі є дослідження D. Comer та A. Rastegarnia [5], в якому вперше проведено комплексну оцінку Apache Kafka та gRPC для дезагрегації площини управління SDN на базі контролера ONOS. Експериментальний стенд із десяти OpenFlow-комутаторів продемонстрував середній час відгуку 65 мс для Kafka проти 45 мс для gRPC. Ключовим внеском є демонстрація принципової життєздатності Kafka як транспортного шару для ONOS. Водночас фокус дослідження зосереджений на дезагрегації площини управління, а не на інтеграції з ML-конвеєром, тому питання застосовності цієї архітектури для задач класифікації трафіку в реальному часі залишається відкритим.

Найновішою роботою, дотичною до запропонованої тематики, є дослідження [6], в якому представлено трирівневу архітектуру з Kafka-конвеєрами для виявлення аномалій

у SDN-мережах розумних міст. Автори досягли точності 99 % з використанням Random Forest, Linear Regression та XGBoost на наборі даних InSDN. Ключовий внесок — демонстрація комбінації SDN-контролера з Kafka та ML-аналітикою на хмарно-граничному рівні. Однак робота орієнтована на специфічний сценарій smart cities, а кількісні характеристики наскрізної затримки та горизонтальної масштабованості систематично не оцінено.

У роботі А. О. Salau та М. М. Beyene [7] оцінено шість алгоритмів машинного навчання на SDN-стенді з контролером Ryu, де Decision Tree досягнув найвищої точності 99,81 % при класифікації DNS, Telnet, Ping та Voice трафіку з використанням 15 flow-based ознак. Робота демонструє високий потенціал класичних ML-алгоритмів для класифікації трафіку в SDN. Разом з тим, дослідження виконане в пакетному режимі обробки на контролері Ryu без потокової шини подій, що унеможливорює пряме перенесення результатів на сценарії реального часу. Додатковим суттєвим обмеженням є вибір контролера Ryu, активна розробка якого фактично припинилася понад десять років тому, що ставить під сумнів перспективи production-розгортань на цій платформі та обумовлює актуальність перенесення подібних експериментів на сучасні підтримувані контролери (ONOS, OpenDaylight).

Гібридні архітектури глибокого навчання представлено у роботі [8], де М. Abdallah, N. A. Le Khas, Н. Jahromi та А. D. Jurcut поєднали згорткові шари (CNN) для просторового виділення ознак з LSTM-блоком для моделювання темпоральних залежностей, досягнувши 96,32 % точності виявлення аномалій на наборі даних InSDN. Ключовий внесок – здатність моделі захоплювати просторово-часові патерни трафіку. Обмеженням підходу є висока обчислювальна складність моделі, що ускладнює її розгортання як інлайн-класифікатора у потоковому конвеєрі без дискретизації обчислень.

Еталонне дослідження J. Karimov та ін. [9] надає критичні порівняння продуктивності платформ потокової обробки Apache Storm, Spark та Flink на 20-вузловому кластері: Apache Flink стабільно демонструє найкращу продуктивність із пропускну здатністю 1,2 М/с та середньою затримкою 0,2 с проти показників Spark та Storm. Робота встановлює бенчмаркові орієнтири для вибору stream-платформи. Проте дослідження виконане в загальному контексті обробки поточкових даних поза специфікою SDN, тому особливості інтеграції з SDN-контролером (періодичність опитування, формат OpenFlow-статистики, обсяг повідомлень типу Packet-In) залишаються поза його межами.

Прикладом потокового конвеєра для конкретної задачі безпеки є дослідження N. V. Patil та ін. [10], в якому продемонстровано використання топіків Apache Kafka для препроцесингу мережевого трафіку зі Spark MLlib для класифікації семи типів DDoS-атак на наборі даних CICDDoS2019. Ключовим внеском є практичне підтвердження життєздатності зв'язки Kafka + Spark Streaming + ML для задач реального часу. Обмеженням підходу є відсутність інтеграції із SDN-контролером як джерелом подій: вхідні дані надходять із PCAP-файлів, а не з телеметрії OpenFlow-комутаторів, тому архітектура не валідована в умовах реальної SDN-мережі.

Виконаний аналіз свідчить про фрагментарний характер сучасних досліджень: одні роботи зосереджені на інтеграції Kafka з ONOS без ML-компонента [5], інші – на ML-класифікації без потокової шини [8], треті – на поточкових платформах поза контекстом SDN [10]. У більшості існуючих підходів відсутня кількісна оцінка наскрізної затримки в межах інтегрованого конвеєра «контролер → транспорт подій → класифікатор», а валідація горизонтальної масштабованості обмежується одиничними експериментами. Ця обставина обґрунтовує доцільність розробки інтегральної потокової архітектури, в якій контролер ONOS, шина повідомлень Apache Kafka та модуль машинного навчання утворюють єдиний конвеєр класифікації трафіку SDN з кількісно оціненими характеристиками затримки, пропускну здатності та масштабованості.

У контексті програмно-визначених мереж ці проблеми набувають особливої актуальності, оскільки централізована архітектура SDN не лише створює нові можливості, а й додає нові складнощі щодо управління мережею.

Наукове завдання полягає у розробці архітектурного підходу до побудови інтегрованого програмного середовища, що поєднує SDN-контролер, платформу потокової обробки даних і методи машинного навчання для забезпечення класифікації мережевого трафіку в режимі реального часу з низькою затримкою та можливістю горизонтального масштабування.

Метою дослідження є побудова та експериментальна валідація програмно-визначеної архітектури потокової класифікації мережевого трафіку в режимі реального часу, яка інтегрує контролер ONOS як джерело OpenFlow-статистики, Apache Kafka як транспортний шар подій та алгоритми машинного навчання як модуль класифікації, із кількісною оцінкою затримки, пропускну здатності, горизонтальної масштабованості та точності класифікації.

3. Виклад основного матеріалу

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Аналіз можливостей збору даних в SDN: дослідити специфікацію OpenFlow Switch Specification версії 1.3.5 для визначення доступних типів статистичних повідомлень, метрик та подій [11].

2. Проектування архітектури інтеграції: розробити архітектурне рішення для інтеграції контролера ONOS з платформою Apache Kafka [2; 4].

3. Ідентифікація ключових метрик: визначити набір метрик та ознак на рівні потоків, портів і пакетів, які є найбільш релевантними для конкретних задач аналізу трафіку, що розглядаються в дослідженні: бінарної класифікації нормального трафіку та DDoS-атак, виявлення аномалій поведінки потоків та ідентифікації типу прикладного трафіку.

4. Оцінка практичної реалізації: проаналізувати технічні аспекти впровадження запропонованого підходу та його сумісність з існуючими SDN-рішеннями.

В роботі пропонується інтеграційна архітектура збору даних з метою подальшої класифікації мультимедійного трафіку. Запропонована архітектура базується на інтеграції трьох ключових компонентів: SDN-контролера ONOS; платформи Apache Kafka та системи класифікації на основі машинного навчання (рис. 1).

ONOS Controller виступає центральним елементом управління SDN-мережею та забезпечує: управління топологією мережі за допомогою протоколу OpenFlow; збір статистичної інформації з комутаторів; генерацію мережевих подій при змінах стану мережі; публікацію подій до системи Kafka через вбудований Kafka Integration Application.

Apache Kafka слугує розподіленою платформою потокової обробки та забезпечує: надійну доставку повідомлень між компонентами системи; масштабовану архітектуру для обробки великих обсягів даних; буферизацію подій для забезпечення стійкості системи; підтримку множинних постачальників та споживачів даних (producers and consumers) для паралельної обробки.

Система класифікації на основі машинного навчання (data processing plane) реалізує: модель підписника на мережеві події з іменованих каналів повідомлень (topics) платформи Kafka; видобуток ознак для машинного навчання з поточкових даних; класифікацію трафіку в режимі реального часу; передачу результатів до SDN контролера через REST API.

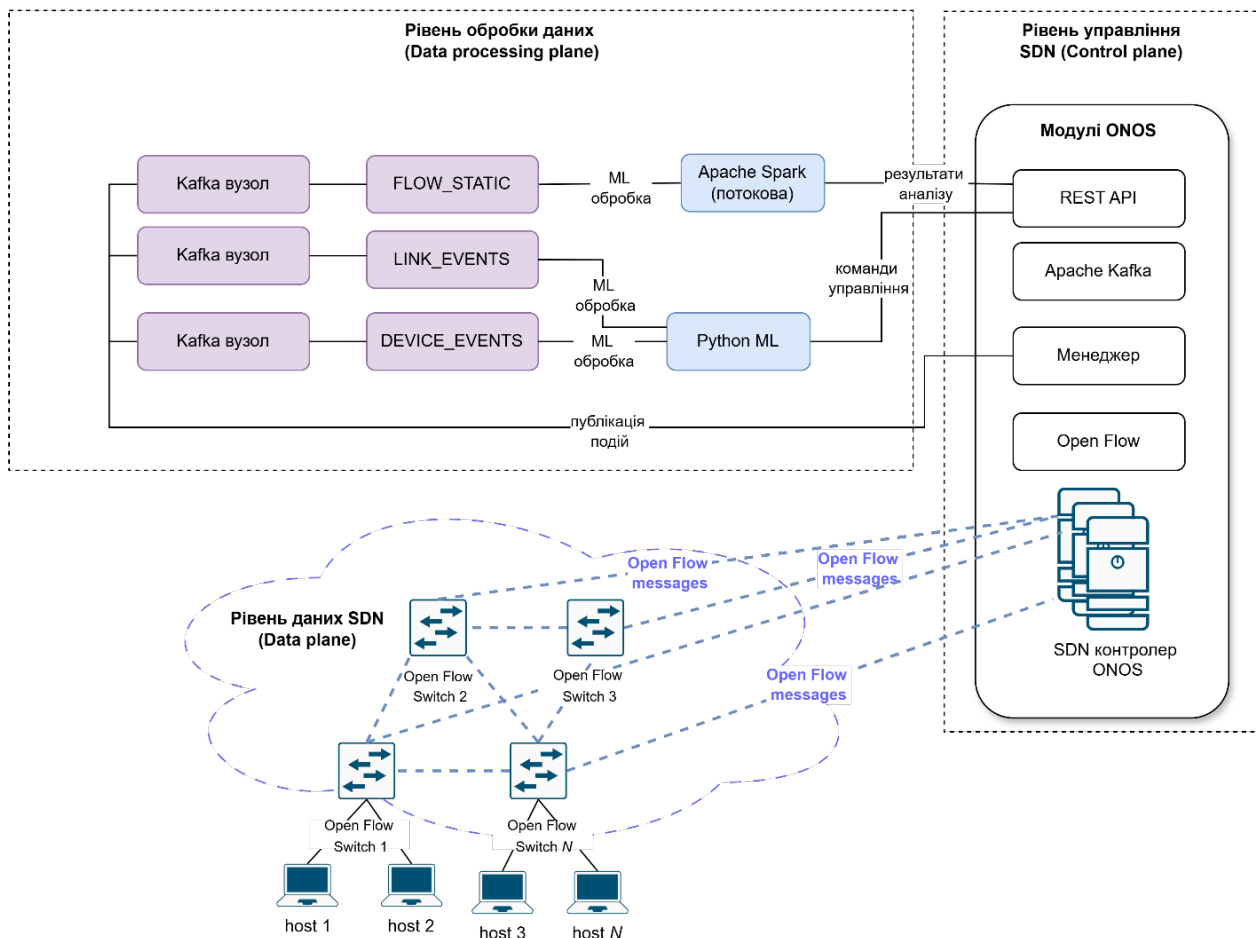


Рис. 1. Загальна архітектура системи збору, аналізу та класифікації мережних даних реального часу

На рисунку 2 приведена діаграма послідовності подій, що відбуваються при обробці трафіку, починаючи від надходження пакету в систему до прийняття рішення щодо класифікації і видачі команди управління. Відповідно до загальноприйнятого в літературі підходу [7; 8], наскрізна затримка (end-to-end latency) від моменту виникнення події в мережі до прийняття рішення класифікатором не має перевищувати 100 мс – саме цей поріг вважається критерієм обробки в режимі реального часу.

Для проведення подальшого дослідження та коректної інтерпретації результатів отриманих експериментів було здійснено класифікацію основних типів подій та метрик відповідно до OpenFlow Switch Specification версії 1.3.5.

Статистичні повідомлення (Multipart Messages) [11]:

статистика індивідуальних потоків, Individual Flow Statistics (packet_count – кількість пакетів, що відповідали правилу потоку; byte_count – загальний обсяг байтів оброблених пакетів; duration_sec/duration_nsec – час існування потоку; table_id – ідентифікатор таблиці потоків; priority – пріоритет правила потоку; idle_timeout/hard_timeout – параметри завершення потоку; match – поля заголовків для співставлення пакетів);

статистика портів, Port Statistics (rx_packets/tx_packets – кількість отриманих / переданих пакетів; rx_bytes/tx_bytes – обсяг отриманих/переданих байтів; rx_dropped/tx_dropped – кількість втрачених пакетів; rx_errors/tx_errors – кількість помилок передачі; rx_frame_err – помилки вирівнювання кадрів; rx_over_err – помилки переповнення буферу; collisions – кількість колізій);

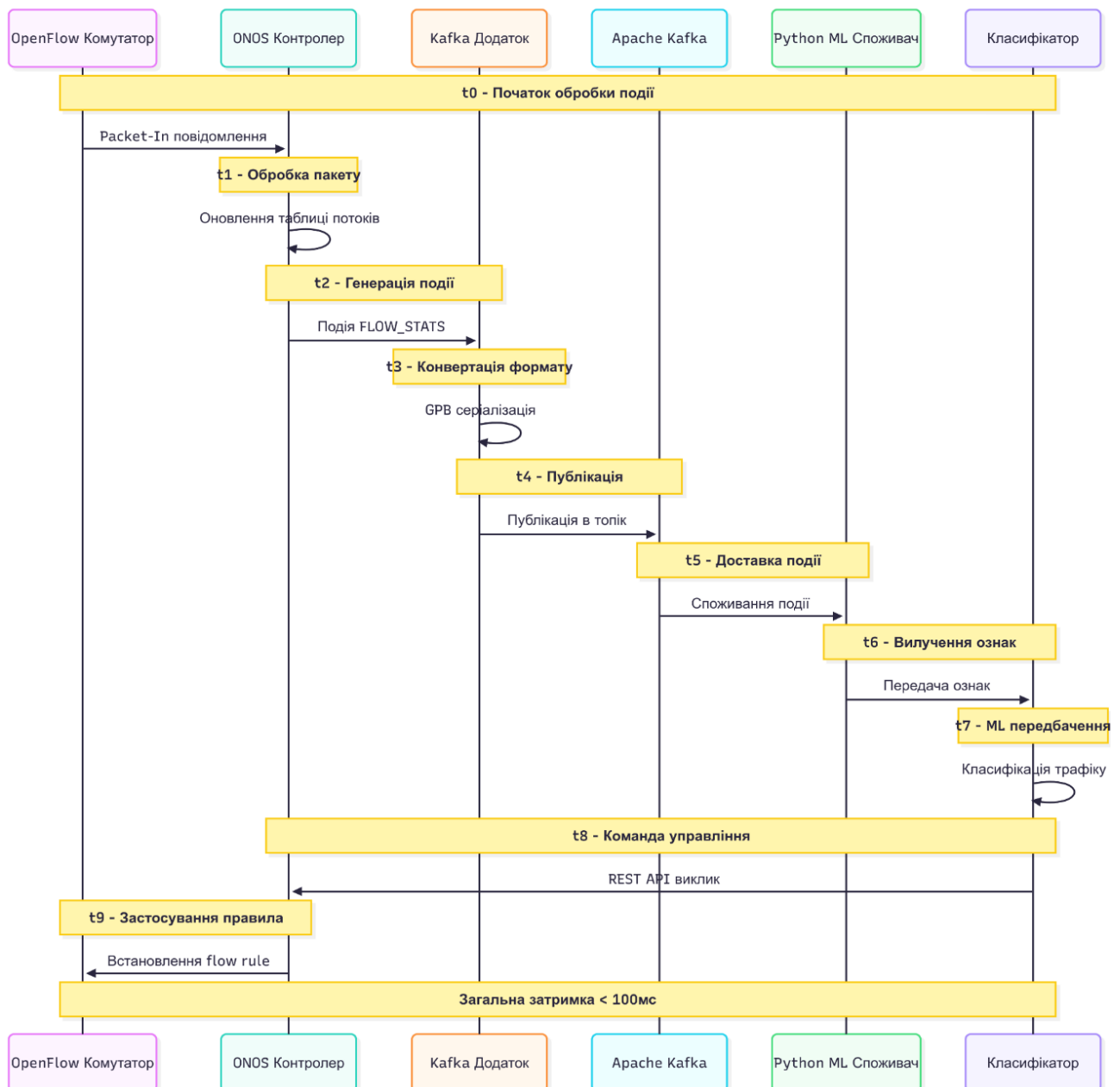


Рис. 2. Послідовність обробки мережевих подій для класифікації трафіку

агреговані статистики потоків, Aggregate Flow Statistics (packet_count – загальна кількість пакетів по всіх потоках; byte_count – загальний обсяг байтів по всіх потоках; flow_count – кількість активних потоків).

Повідомлення про події (Asynchronous Messages)

Packet-In повідомлення генеруються при надходженні пакетів, що не мають відповідного правила в таблиці потоків, та містять: buffer_id – ідентифікатор буферизованого пакету; total_len – повна довжина оригінального пакету; reason – причина надсилання до контролера; table_id – таблиця, що згенерувала подію; match – поля заголовків пакету; data – дані пакету.

Flow-Removed повідомлення інформують про видалення потоків та включають статистики видаленого потоку, причину видалення (timeout, delete) та час існування потоку. *Port-Status* повідомлення повідомляють про зміни стану портів, конфігураційні зміни портів, зміни фізичного стану лінків та параметри швидкості і дуплексності.

Поля співставлення (Match Fields) для класифікації

Специфікація OpenFlow визначає розширений набір полів для співставлення пакетів.

Поля Layer 2 (Ethernet): eth_dst/eth_src – MAC-адреси призначення та відправника; eth_type – тип Ethernet кадру.

Поля VLAN: vlan_vid – ідентифікатор VLAN; vlan_pcp – пріоритет VLAN.

Поля Layer 3 (IP): ipv4_src/ipv4_dst – IP-адреси відправника та призначення; ip_proto – номер IP-протоколу; ip_dscp – поле DSCP для QoS класифікації.

Поля Layer 4 (Transport): tcp_src/tcp_dst – порти джерела та призначення TCP; udp_src/udp_dst – порти джерела та призначення UDP; tcp_flags – TCP прапорці (SYN, ACK, FIN тощо).

Розширення ONOS для інтеграції з Kafka

ONOS забезпечує вбудовану інтеграцію з Apache Kafka через спеціальний додаток “Kafka Integration Application” [4], який: підписується на події ONOS через внутрішні Java API; перетворює формат даних до стандартного GPB (Google Protocol Buffers); публікує події до Kafka-топиків для подальшої обробки.

Поточна реалізація підтримує DEVICE події (підключення/відключення комутаторів, зміни конфігурації), LINK події (встановлення/розрив лінків, зміни топології). Архітектура дозволяє розширення для додаткових типів подій: FLOW_STATS події (оновлення статистик потоків в реальному часі), PORT_STATS події (статистики портів), PACKET_IN події (повідомлення про нові потоки).

Для підтвердження працездатності запропонованої архітектури було розгорнуто експериментальний стенд на базі трьох віртуальних машин, що емулюють типову конфігурацію SDN-інфраструктури з централізованим збором та обробкою даних (рис. 3.).

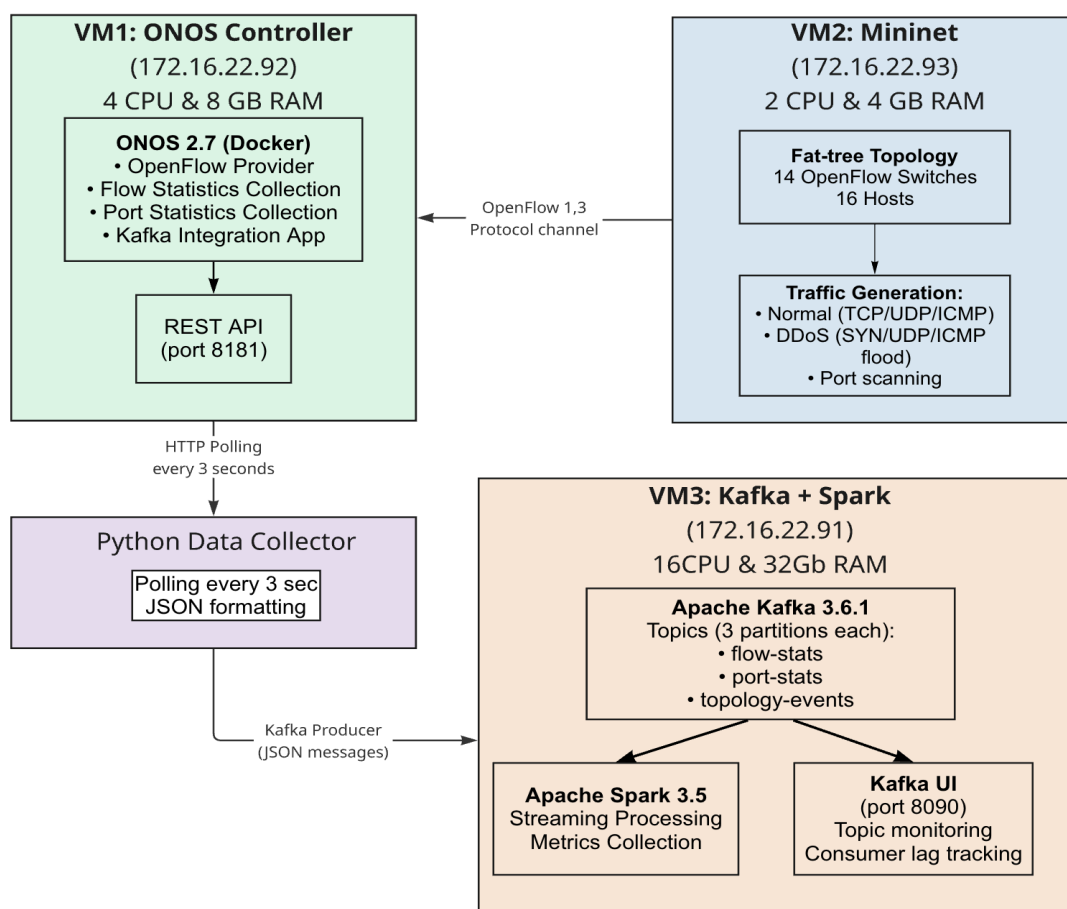


Рис. 3. Схема основних компонентів віртуального стенду для проведення експерименту

Перша віртуальна машина (VM1, IP: 172.16.22.92) виконувала роль SDN-контролера на базі ONOS версії 2.7, розгорнутого в Docker-контейнері (4 CPU, 8 ГБ RAM). Друга віртуальна машина (VM2, IP: 172.16.22.93) використовувалась для емуляції SDN-мережі засобами Mininet версії 2.3 (2 CPU, 4 ГБ RAM) з ієрархічною 3-рівневою топологією типу fat-tree з 14 OpenFlow-комутаторами та 16 хостами (див. рис. 3). Третя віртуальна машина (VM3, IP: 172.16.22.91) функціонувала як платформа для потокової обробки даних (16 CPU, 32 ГБ RAM) з Apache Kafka 3.6.1, Apache Zookeeper 3.8 та Apache Spark 3.5. В таблиці 1 наведено дані щодо конфігурації компонентів розгорнутого стенду та їх призначення.

Таблиця 1

Конфігурація компонентів тестового стенду

Компонент	Версія	Ресурси	IP-адреса	Роль в архітектурі
ONOS Controller	2.7	4 CPU, 8 ГБ RAM	172.16.22.92	Управління SDN, збір статистик
Mininet	2.3	2 CPU, 4 ГБ RAM	172.16.22.93	Емуляція мережі, генерація трафіку
Apache Kafka	3.6.1	8 CPU, 16 ГБ RAM	172.16.22.91	Потокова передача подій
Apache Zookeeper	3.8	2 CPU, 4 ГБ RAM	172.16.22.91	Координація Kafka-кластера
Apache Spark	3.5	6 CPU, 12 ГБ RAM	172.16.22.91	Обробка потоків даних

Процес збору даних здійснювався через Python-скрипт, який виконував періодичні опитування (polling) REST API контролера ONOS з інтервалом 3 секунди. Скрипт отримував статистичну інформацію про потоки (flow statistics), стан портів (port statistics) та події топології (topology events), після чого публікував ці дані до відповідних Kafka-топіків у форматі JSON. Для проведення дослідження та тестування мережі на віртуальній машині VM2 в середовищі Mininet була розгорнута SDN-мережа, яка складається із 14 OpenFlow комутаторів, топологія якої показана на рисунку 4.

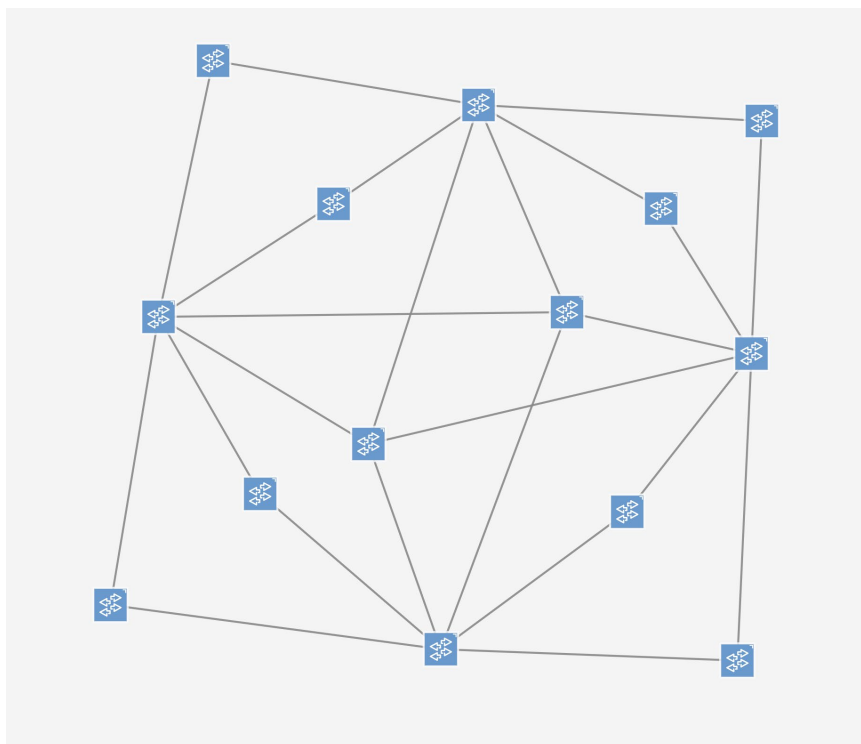


Рис. 4. Ієрархічна (гібридна) топологія SDN-мережі типу Fat-tree

У подальшому була проведена валідація розробленої інтеграційної архітектури завдяки виміру продуктивності конвеєра обробки даних. Основною метою валідації було підтвердження здатності запропонованої архітектури забезпечувати збір та передачу мережових подій у режимі, близькому до реального часу, без втрати інформації та з прийнятними показниками затримки.

Для вимірювання затримки end-to-end (від моменту генерації статистики в ONOS до її обробки в Spark consumer) було розроблено Python-скрипт збору даних та Spark-додаток. Скрипт додавав до кожного повідомлення мітку часу збору (collection_timestamp) з точністю до мілісекунди. Spark consumer обчислював різницю міток часу: ONOS REST API → Python collector → Kafka broker → Spark consumer.

У цілому, експеримент тривав 2 години безперервної роботи з активною генерацією мережового трафіку різних типів: нормального «легітимного» трафіку (60 % часу), атак типу DDoS (25 % часу) та сканування портів (15 % часу). Система обробляла в середньому 174 події на секунду, що відповідає 1 252 800 подіям за весь період тестування.

Розподіл затримок end-to-end показав наступні характеристики: середня затримка обробки подій – 71 мс; медіана затримки – 68 мс; 95-й перцентиль затримки – 128 мс; 99-й перцентиль затримки – 203 мс.

При чому максимальна затримка – 487 мс (поодинокий випадок при пікових навантаженнях). Результати випробувань зведено в таблиці 2.

Таблиця 2

Результати вимірювань продуктивності системи

Метрика	Отримане значення	Порогове значення	Статус
Середня затримка end-to-end	71 мс	< 100 мс	Досягнуто
Медіана затримки	68 мс	< 100 мс	Досягнуто
95-й перцентиль затримки	128 мс	< 200 мс	Досягнуто
99-й перцентиль затримки	203 мс	< 300 мс	Досягнуто
Події з затримкою < 100 мс	92 %	90 %	Досягнуто
Пропускна здатність	174 події/с	100 події/с	Досягнуто
Пікова пропускна здатність	218 події/с	150 події/с	Досягнуто
Overhead ONOS CPU	3,7 %	< 10 %	Досягнуто
Overhead ONOS RAM	145 МБ	< 500 МБ	Досягнуто
Втрата повідомлень	0 (0 %)	< 0,1 %	Досягнуто
Тривалість безперервної роботи	120 хв	60 хв	Досягнуто

Важливо зазначити, що 92 % усіх подій було оброблено з затримкою менше 100 мс, що підтверджує придатність архітектури для застосувань реального часу.

Аналіз складових загальної затримки показав наступний розподіл: опитування ONOS REST API – 8 мс (11 %); обробка в Python collector – 6 мс (8 %); передача до Kafka broker – 5 мс (7 %); зберігання в Kafka (буферизація) – 12 мс (17 %); отримання Spark consumer – 9 мс (13 %); обробка в Spark (десеріалізація JSON) – 15 мс (21 %); внутрішні операції Spark Streaming – 16 мс (23 %).

Моніторинг ресурсів показав, що запропонована архітектура характеризується низькими накладними витратами роботи конвеєра щодо SDN-контролера. Додаткове навантаження на

ONOS, спричинене періодичним опитуванням (polling) через REST API кожні 3 секунди, складало лише 3,7 % CPU та 145 МБ додаткової оперативної пам'яті.

Протягом всього тестування система забезпечила 100 % доставку подій – не було зафіксовано жодного випадку втрати повідомлень. Це підтверджено через механізм offset tracking у Kafka: кількість відправлених повідомлень producer-ом точно відповідала кількості отриманих повідомлень consumer-ом.

Розподіл за типами подій (табл. 3): Flow statistics (flow-stats) – 847 000 подій (67,6 %); Port statistics (port-stats) – 342 000 подій (27,3 %); Topology events (topology-events) – 63 800 подій (5,1 %).

Таблиця 3

Розподіл отриманих подій за типами

Тип події	Кількість подій	Відсоток	Розмір даних	Топік Kafka
Flow Statistics	847 000	67,6 %	182,3 МБ	flow-stats
Port Statistics	342 000	27,3 %	68,4 МБ	port-stats
Topology Events	63 800	5,1 %	12,8 МБ	topology-events
Всього	1 252 800	100 %	263,5 МБ	–

Далі представлені результати перевірки якості даних, зібраних з елементів SDN-мережі (рис. 4) через протокол OpenFlow (табл. 4). Тобто, які саме дані вдалося отримати з потоків трафіку і наскільки вони повні (як часто метрики зустрічаються у зібраних статистичних даних):

за характеристиками потоків flow statistics показав, що базові метрики (packet_count, byte_count, duration_sec/nsec, device_id, flow_id) мають 100 % покриття;

метрики різних протоколів мають змінне покриття: IP-протокол (IP_PROTO) – 87,3 %; TCP/UDP порти – 76,2 %; MAC-адреси – 100 %; IP-адреси – 87,3 %; VLAN ID – 23,4 %; TCP прапорці – 0% (не підтримується OpenFlow 1.3).

TCP-прапорці мають нульове покриття, оскільки їх підтримка як окремого поля співставлення була введена лише у специфікації OpenFlow.

Також були обчислені похідні метрики для більш точної класифікації потоків трафіка в подальшому.

Таблиця 4

Доступність метрик OpenFlow у зібраних даних

Категорія метрик	Метрика	Покриття	Джерело OpenFlow
Базові лічильники	Кількість пакетів	100 %	packet_count
	Кількість байтів	100 %	byte_count
	Тривалість потоку	100 %	duration_sec/nsec
Ідентифікатори	ID-пристрою	100 %	deviceId
	ID-потoku	100 %	id
Протоколи L2	MAC-адреси	100 %	match.ETH_SRC/DST
	VLAN ID	23,4 %	match.VLAN_VID
Протоколи L3	IP-адреси	87,3 %	match.IPV4_SRC/DST
	IP-протокол	87,3 %	match.IP_PROTO

Категорія метрик	Метрика	Покриття	Джерело OpenFlow
Протоколи L4	TCP/UDP порти	76,2 %	match.TCP_*/UDP_*
	TCP-прапорці	0 %	Не підтримується OF 1.3
Похідні метрики	Пакети/с	100 %	Обчислено
	Байти/с	100 %	Обчислено
	Середній розмір пакету	100 %	Обчислено

Отримані результати підтверджують, що запропонована архітектура забезпечує доступ до комплексної інформації про мережеві потоки на рівні, достатньому для подальшого застосування алгоритмів машинного навчання [7; 8]. Базові характеристики (кількість пакетів, байтів, тривалість) доступні для всіх потоків без винятку. Інформація про протоколи вищих рівнів доступна для переважної більшості потоків (76–87 %).

Висновки. У цій роботі пропонується інтеграційна архітектура на основі ONOS та Apache Kafka для класифікації трафіку в мережах SDN засобами машинного навчання, яка дозволяє здійснювати збір та аналіз мережевого трафіку в режимі реального часу.

Експериментальна валідація запропонованої архітектури на розгорнутому віртуальному стенді підтвердила можливість її технічної реалізації та відповідність вимогам до систем реального часу.

Під час тестування на сегменті мережі SDN з 14 OpenFlow-комутаторів розроблена система продемонструвала наступні ключові характеристики:

затримка обробки: середня затримка end-to-end склала 71 мс, що на 29 % краще цільового порогу в 100 мс. При цьому 92 % усіх подій було оброблено з затримкою менше 100 мс, а 95-й перцентиль затримки становив 128 мс;

продуктивність конвеєрної обробки мережевих подій: система стабільно обробляла 174 події на секунду в середньому, з піковими значеннями до 218 подій на секунду при інтенсивній генерації трафіку. Протягом експерименту було успішно зібрано та передано понад 1,25 мільйона подій без жодної втрати даних;

гарантована доставка даних: механізм буферизації на базі Apache Kafka забезпечив 100 % доставку повідомлень. Offset tracking підтвердив повну відповідність кількості відправлених та отриманих повідомлень;

мінімальні витрати ресурсів (low overhead): додаткове навантаження на ONOS контролер складало лише 3,7 % CPU та 145 МБ оперативної пам'яті, що є незначним для сучасних серверних платформ;

повнота даних (coverage): аналіз зібраних flow statistics показав 100 % покриття базових метрик та 76–87 % покриття метрик вищих рівнів, що є достатнім для застосування алгоритмів машинного навчання.

У результаті проведеного дослідження встановлено, що інтеграція контролера ONOS з платформою Apache Kafka створює ефективну архітектуру для збору та аналізу мережевих даних в режимі реального часу в програмно-визначених мережах. Аналіз специфікації OpenFlow Switch Specification версії 1.3.5 виявив широкий спектр статистичних метрик та типів подій, доступних для класифікації трафіку. Визначено три основні категорії даних: статистики потоків, статистики портів та асинхронні події (packet-in, flow-removed, port-status повідомлення).

Подальші дослідження доцільно зосередити на розробці специфічних алгоритмів машинного навчання для аналізу поточкових мережевих даних, оптимізації продуктивності системи збору даних та розширенні можливостей інтеграції ONOS-Kafka для додаткових типів мережевих подій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jammal M., Singh T., Shami A., Asal R., Li Y. Software defined networking: State of the art and research challenges // Computer Networks. 2014. Vol. 72. P. 74–98. DOI: 10.1016/j.comnet.2014.07.004.
2. Apache Software Foundation. Apache Kafka Documentation. URL: <https://kafka.apache.org/documentation/>.
3. Kreps J., Narkhede N., Rao J. Kafka: A Distributed Messaging System for Log Processing. Proceedings of the NetDB Workshop, 2011. P. 1–7.
4. ONOS Project Team. Open Network Operating System (ONOS) Architecture Guide. Linux Foundation, 2024.
5. Comer D., Rastegarnia A. Towards Disaggregating the SDN Control Plane. arXiv preprint arXiv:1902.00581v2, 2019. URL: <https://arxiv.org/abs/1902.00581>.
6. Karthick G., Mapp G., Crowcroft J. Toward Secure SDN Infrastructure in Smart Cities: Kafka-Enabled Machine Learning Framework for Anomaly Detection // MDPI Future Internet. 2025. Vol. 17. No. 9, article 415. DOI: 10.3390/fi17090415.
7. Salau A. O., Beyene M. M. Software defined networking based network traffic classification using machine learning techniques // Scientific Reports, 2024. Vol. 14, article 20065. DOI: 10.1038/s41598-024-70983-6.
8. Abdallah M., Le-Khac N. A., Jahromi H., Jurcut A. D. A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs. Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES '21), August 2021. Article No. 34. P. 1–7. DOI: 10.1145/3465481.3469190.
9. Karimov J., Rabl T., Katsifodimos A., Samarev R., Heiskanen H., Markl V. Benchmarking Distributed Stream Data Processing Systems. 2018 IEEE 34th International Conference on Data Engineering (ICDE), Paris, France, April 16–19, 2018. P. 1507–1518. DOI: 10.1109/ICDE.2018.00169.
10. Patil N. V., Krishna C. R., Kumar K. SSK-DDoS: Distributed Stream Processing Framework Based Classification System for DDoS Attacks // Cluster Computing. 2022. Vol. 25, No. 2. P. 1355–1372. DOI: 10.1007/s10586-022-03538-x.
11. Open Networking Foundation. OpenFlow Switch Specification Version 1.3.5. ONF TS-023. March 2015.

Надійшла до редколегії 20.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 621.3:623.4:629.07–044.4

д-р філософії Фесенко О. Д. ORCID: 0000-0002-2114-5327 (ВІТІ ім. Героїв Крут)

МАТЕМАТИЧНА МОДЕЛЬ ЕВОЛЮЦІЇ ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ НА ОСНОВІ ЕНТРОПІЇ, ДОВІРИ ТА ЦИФРОВИХ ДВІЙНИКІВ

У статті розглядається формалізація людино-машинного інтерфейсу як динамічної системи, яка динамічно переходить від стану емпіричної неузгодженості до більш впорядкованої та передбачуваної взаємодії в контурі «людина – робот – середовище». Запропоновано математичну модель яка через інтегральні характеристики ентропії, довіри, середньої зв'язності та ваги участі оператора описує процес взаємодії людино-машинного інтерфейсу. Такий підхід дозволяє перейти від інтуїтивного опису до формалізованого аналізу еволюції системи. Модель побудована у вигляді операторної структури, що поєднує проєкцію фізичного стану у простір цифрових двійників, генерацію та оцінювання сценаріїв, формування структури взаємодії та вибір керуючих дій з урахуванням обмежень безпеки. Особливу увагу приділено ролі невизначеностей середовища, які визначають рівень ентропії та істотно впливають на швидкість і характер переходу системи до узгодженого режиму.

Показано, що за умов, коли система накопичує інформацію швидше, ніж зростає рівень випадкових збурень, відбувається поступове зменшення ентропії та посилення зв'язків між її компонентами. Це природно призводить до зростання довіри між людиною та машиною. У свою чергу, довіра визначає, наскільки система може брати на себе частину функцій керування, зменшуючи навантаження на оператора. Для узагальненої оцінки ефективності додатково введено інтегральний індекс, що дозволяє кількісно порівнювати різні режими функціонування.

Практичну перевірку моделі виконано у середовищі Gazebo із використанням ансамблевого прогнозування та адаптивної матриці взаємодії. Отримані результати співпадають з теоретичними висновками та демонструють стабільну динаміку основних характеристик системи. Зокрема, у порівнянні з базовими підходами спостерігається зменшення ентропії на 25–40%, зростання довіри більше ніж дворазове, а також суттєве зниження навантаження на оператора.

Таким чином, отримані результати підтверджують, що перехід до структурованої взаємодії відбувається насамперед у просторі цифрових двійників і забезпечується замкненим контуром прогнозування, узгодження та прийняття рішень. Запропонований підхід може бути використаний як основа для розробки адаптивних людино-машинних інтерфейсів у робототехнічних системах, що працюють в умовах невизначеності.

Ключові слова: автономні платформи, адаптивне управління, людино-машинний інтерфейс, цифрові двійники, кібернетичний контур прогнозування, довіра людина – машина, ентропія прогнозу, роботизовані системи, miltech, Gazebo.

O. Fesenko. A mathematical model of the evolution of the human-machine interface based on entropy, trust, and digital twins.

The article considers the proposed formalization of the human-machine interface as a dynamic system that dynamically transitions from a state of empirical inconsistency to a more orderly and predictable interaction in the “human – robot – environment” loop. A mathematical model is proposed that describes the process of human-machine interface interaction through the integral characteristics of entropy, trust, average connectivity and operator participation weight. This approach allows us to move from an intuitive description to a formalized analysis of the evolution of the system. The model is built in the form of an operator structure that combines the projection of the physical state into the space of digital twins, the generation and evaluation of scenarios, the formation of the interaction structure and the selection of control actions taking into account safety constraints. Special attention is paid to the role of environmental uncertainties that determine the level of entropy and significantly affect the speed and nature of the system's transition to a consistent regime.

It is shown that under conditions when the system accumulates information faster than the level of random disturbances increases, there is a gradual decrease in entropy and a strengthening of connections between its components. This naturally leads to an increase in trust between man and machine. In turn, trust determines to what extent the system can take on part of the control functions, reducing the load on the operator. For a generalized assessment of efficiency, an integral index is additionally introduced, which allows quantitatively comparing different modes of operation.

Practical verification of the model was performed in the Gazebo environment using ensemble forecasting and an adaptive interaction matrix. The results obtained coincide with the theoretical conclusions and demonstrate stable dynamics of the main characteristics of the system. In particular, compared with the basic approaches, a decrease in

entropy by 25–40 %, an increase in trust by more than two times, as well as a significant decrease in the load on the operator are observed.

Thus, the obtained results confirm that the transition to structured interaction occurs primarily in the space of digital twins and is provided by a closed loop of prediction, coordination and decision-making. The proposed approach can be used as a basis for the development of adaptive human-machine interfaces in robotic systems operating under uncertainty.

Keywords: autonomous platforms, adaptive control, human-machine interface, digital twins, cybernetic prediction loop, human – machine trust, prediction entropy, environment, simulator, Gazebo, robotic systems, miltech.

1. Постановка проблеми

Сучасний етап розвитку робототехнічних систем характеризується переходом від простих схем дистанційного керування до складних людино-машинних інтерфейсів, у яких людина-робот утворюють єдиний функціональний контур взаємодії [1]. У таких системах ефективність визначається не лише точністю виконання команд, але й ступенем узгодженості між когнітивними діями оператора, станом технічної платформи та динамікою зовнішнього середовища. Саме тому людино-машинний інтерфейс доцільно розглядати не як статичний канал зв'язку, а як динамічну систему, що змінюється в процесі експлуатації, навчання та адаптації. На початкових етапах взаємодії людини-робота така система часто має ознаки неузгодженості, а саме сигнали керування є нестабільними, реакції технічної платформи не завжди відповідають очікуванням оператора, а рішення формуються під впливом великої кількості емпіричних й частково випадкових чинників. Умовно такий стан можна визначити як емпіричний хаос людино-машинної взаємодії. Для нього характерні підвищена ентропія, слабка зв'язність між елементами системи, нестійкість довіри та висока залежність від людського фактору. У міру накопичення досвіду, адаптації алгоритмів і формування стійких зворотних зв'язків система переходить до нового рівня структурованої взаємодії, де поведінка людини-робота стає більш узгодженою, передбачуваною та математично описуваною.

Зазначена проблема актуальна у військовій робототехніці, автономних транспортних системах, дистанційних операціях і тренажерних комплексах VR, де помилка у взаємодії людини та машини може спричинити не лише зниження ефективності, а також привести до критичних наслідків. У зв'язку з цим виникає потреба у формуванні математичної моделі, здатної описати еволюцію людино-машинного інтерфейсу від стану емпіричної неузгодженості до стану структурованої, довірчо-стабільної взаємодії. Така модель має не лише теоретичне значення, але й може стати основою проєктування адаптивних інтерфейсів, побудови нових підходів до керування системами типу «людина-робот».

2. Аналіз останніх досліджень та публікацій

Сучасні дослідження у сфері взаємодії людини і роботів в форматі людино-машинних інтерфейсів (ЛМІ) охоплюють широкий спектр підходів, зокрема системи спільного керування, адаптивну автономність, інтерфейси безпеки довіри та використання ШІ для підтримки прийняття рішень. Значна увага приділяється розподілу ролей між оператором і машиною для оптимізації когнітивного навантаження, а також формуванню довіри до автоматизованих систем [2; 3].

Важливим кроком у напрямі інтеграції цифрових двійників у людино-машинну взаємодію є робота Kuras та співавтори [4], у якій людино центричний цифровий двійник розглядається як засіб підтримки роботи людини й машини в форматі «Індустріальної революції 5.0». Автори узагальнюють технології та методи, що забезпечують побудову таких рішень, і підкреслюють необхідність переходу від суто виробничо-орієнтованих цифрових моделей до систем, у центрі яких перебуває людина. Але це дослідження має переважно оглядовий характер і не пропонує формалізації динамічної моделі, яка б описувала, як саме у часі еволюціонують узгодженість, невизначеність, довіра та розподіл ролей між людиною і машиною.

Не менш цікавим є дослідження довіри як центральної змінної ЛМІ. У систематичному огляді Firmino de Souza та співавторів [5] проаналізовано 34 публікації та показано, що довіра і надійність визначаються базовими передумовами безпеки й ефективної взаємодії людини з роботизованими системами. Разом із тим автори виявили серйозну методологічну проблему, що майже 30% розглянутих робіт не містять чіткого визначення довіри, що ускладнює порівняння результатів і формування узгодженого теоретичного підходу. Отже, навіть у сучасній літературі довіра часто розглядається як важливий, але концептуально неоднорідний параметр, який рідко включається до єдиної математичної схеми еволюції ЛМІ.

Питання часової динаміки довіри розкрито у праці Roesler та співавторів [6], де показано, що взаємодія з роботом супроводжується змінами ставлення до довіри залежно від досвіду, зокрема довіра суттєво знижується після збоїв або відмов. Водночас автори встановили, що зміни у ставленні до робота не обов'язково прямо переходять у поведінкову адаптацію оператора. Цей результат є важливим, оскільки підтверджує, що довіра не може розглядатися як ізольований психологічний елемент. Довіра має аналізуватись спільно зі структурою взаємодії, прогнозуванням та реальним механізмом делегування функцій. Недоліком зазначеної роботи є те, що вона зосереджена насамперед на експериментально-поведінковому аспекті і не поєднує динаміку довіри із цифровими двійниками, оцінкою ентропії, а виступає в ролі формального критерію переходу системи до структурованого режиму.

У роботі Chauhan та інші [7], представлено варіант подальшого розвитку напряму кількісного аналізу довіри, де для прогнозування рівня довіри до робота використано моделі машинного навчання та психофізіологічні показники, зібрані у VR-сценарії спільного виконання будівельного завдання. Автори показали, що електродермальна активність та температура шкіри можуть бути значущими предикторами довіри. Значення цього дослідження полягає у підтвердженні того, що довіра піддається не лише якісному опису, а й кількісному прогнозуванню в процесі взаємодії. Проте робота має обмеження за рахунок того, що довіра представлена як окрема цільова змінна прогнозування, а не елемент цілісної моделі самоорганізації ЛМІ, в якій одночасно враховуються невизначеність середовища, структурна зв'язність і зміна ролі оператора.

Найближчою до тематики даного дослідження є робота Li та ін. [8], у якій запропоновано структура взаємної довіри керування цифровими двійниками для взаємовідношень людина-робот. Сильною стороною роботи є інтеграція цифрових двійників людини та робота в єдину архітектуру взаємної довіри, що дозволяє перейти від однобічного трактування довіри людини до машини в напрямку більш збалансованого підходу. Однак в цій праці також основним акцентом є архітектура довіри системи та прикладні механізми взаємодії, тоді як формальна модель еволюції інтерфейсу від стану неузгодженості до структурованої взаємодії через інтегральні змінні невизначеності, довіри, зв'язності та участі оператора залишається нерозробленою.

Таким чином, наукова проблема полягає у відсутності узагальненої математичної моделі, що описує еволюцію ЛМІ як динамічний процес переходу від високої невизначеності та слабкої узгодженості до структурованої, довірчо-стабільної взаємодії, причому з одночасним урахуванням ентропії, цифрових двійників і адаптивного перерозподілу ролей між людиною та машиною.

Мета дослідження полягає у розробці математичної моделі еволюції людино-машинного інтерфейсу на основі ентропії, довіри та цифрових двійників.

3. Виклад основного матеріалу дослідження

3.1. Формалізація граничних станів. Для побудови математичної моделі еволюції ЛМІ насамперед необхідно формалізувати два граничні стани системи, емпіричний хаос та структуровану взаємодію. У межах даного дослідження вони розглядаються як два якісно різні режими функціонування контуру «людина-робот», між якими система може переходити в процесі адаптації, навчання та накопичення досвіду.

Під емпіричним хаосом розуміється початковий або деградований стан людино-машинної взаємодії, у якому рішення формуються переважно на основі часткових, неповних або слабо узгоджених емпіричних даних. Для такого стану характерні висока невизначеність, нестабільність реакцій, слабка передбачуваність поведінки системи та значна залежність від випадкових зовнішніх і внутрішніх факторів. У формальному сенсі стан емпіричного хаосу можна пов'язати з підвищеним рівнем ентропії керування, низьким ступенем довіри до автоматизованих рекомендацій, слабкою зв'язністю між підсистемами та високою вагою безпосереднього втручання людини.

Позначимо, ентропію поточного стану взаємодії через $H(t)$, інтегральний показник довіри через $\tau(t)$, середню узгодженість або зв'язність між функціональними представленнями людини й машини як $\bar{w}(t)$, а вагу участі оператора в контурі керування як $\lambda_h(t)$, то емпіричний хаос можна якісно описати умовами, $H(t) \rightarrow \max$; $\tau(t) \rightarrow \min$; $\bar{w}(t) \rightarrow \min$; $\lambda_h(t) \rightarrow \max$.

Отже, такий режим характеризується максимальною невизначеністю, мінімальною довірою, слабкою структурованістю та високою залежністю від оператора як єдиного джерела стабілізації. Натомість структурована взаємодія є станом людино-машинного інтерфейсу зі стійким, повторюваним і математично описуваним зв'язком між оператором, технічною системою та допоміжними алгоритмічними модулями такими як: дії оператора та реакції робота узгоджені, цифрові представлення адекватно відтворюють поведінку об'єктів, прогнозування зменшує невизначеність, а функція довіри набуває стабілізуючої ролі в контурі прийняття рішень.

За інтегральними характеристиками H , w , τ , λ_h структурована взаємодія відповідає конфігурації $H(t) \downarrow$, $\tau(t) \uparrow$, $w(t) \uparrow$, $\lambda_h(t) \downarrow$. Спадання ентропії означає зменшення невизначеності та підвищення передбачуваності взаємодії, зростання довіри визначає формування стійкого механізму делегування окремих функцій машині, збільшення зв'язності посилює узгодженість між елементами системи, а зменшення λ_h знижує потребу у постійному втручанні оператора.

Таким чином, розвиток ЛМІ слід інтерпретувати як перехід системи з області високої ентропії та низької узгодженості до області впорядкованої, довірчо-стабільної взаємодії. Принципово, що такий перехід не є миттєвим і не зводиться до одноразового налаштування параметрів, а становить безперервну динаміку самоорганізації, залежну від історії взаємодії, якості прогнозування, точності цифрових двійників, умов середовища та накопиченого досвіду системи. Отже, у проведеному дослідженні ЛМІ розглядається як динамічна система, ключовим предметом аналізу якої є не лише поточний стан, а й вектор подальшого розвитку (рис. 1). Зазначена логіка дає можливість перейти від загального опису ЛМІ до побудови математичної моделі, де хаос і структура постають не абстрактними характеристиками, а формалізованими фазами становлення взаємодії людини та робота

3.2. Простір станів і матриця взаємодії. На відміну від класичних підходів, де людина, машина та середовище розглядаються ізольовано або через спрощені зв'язки, пропонується описувати їх як єдину динамічну систему, структура якої визначається не лише станами компонентів, а також й характером їх взаємодії. Тоді доцільно провести формалізацію граничних станів людино-машинного інтерфейсу як емпіричного хаосу та структурованої взаємодії, з подальшою побудовою математичного опису системи у вигляді простору станів.

Загальний стан системи «людина–робот–середовище» задамо вектором стану $\mathbf{X}(t)$ (1):

$$\mathbf{X}(t) = \begin{bmatrix} x_h(t) \\ x_r(t) \\ x_e(t) \end{bmatrix}, \quad (1)$$

де $x_h(t)$ – описує когнітивно-поведінковий стан оператора такий як рішення, реакції, рівень навантаження, $x_r(t)$ – це технічний стан роботизованої платформи, а саме стан кінематики, сенсорні дані, внутрішні контролери, а $x_e(t)$ є станом зовнішнього середовища враховуючи перешкоди, динаміку об'єктів або інформаційні впливи. Така декомпозиція дозволяє враховувати як внутрішню динаміку підсистем, так і їх взаємний вплив.

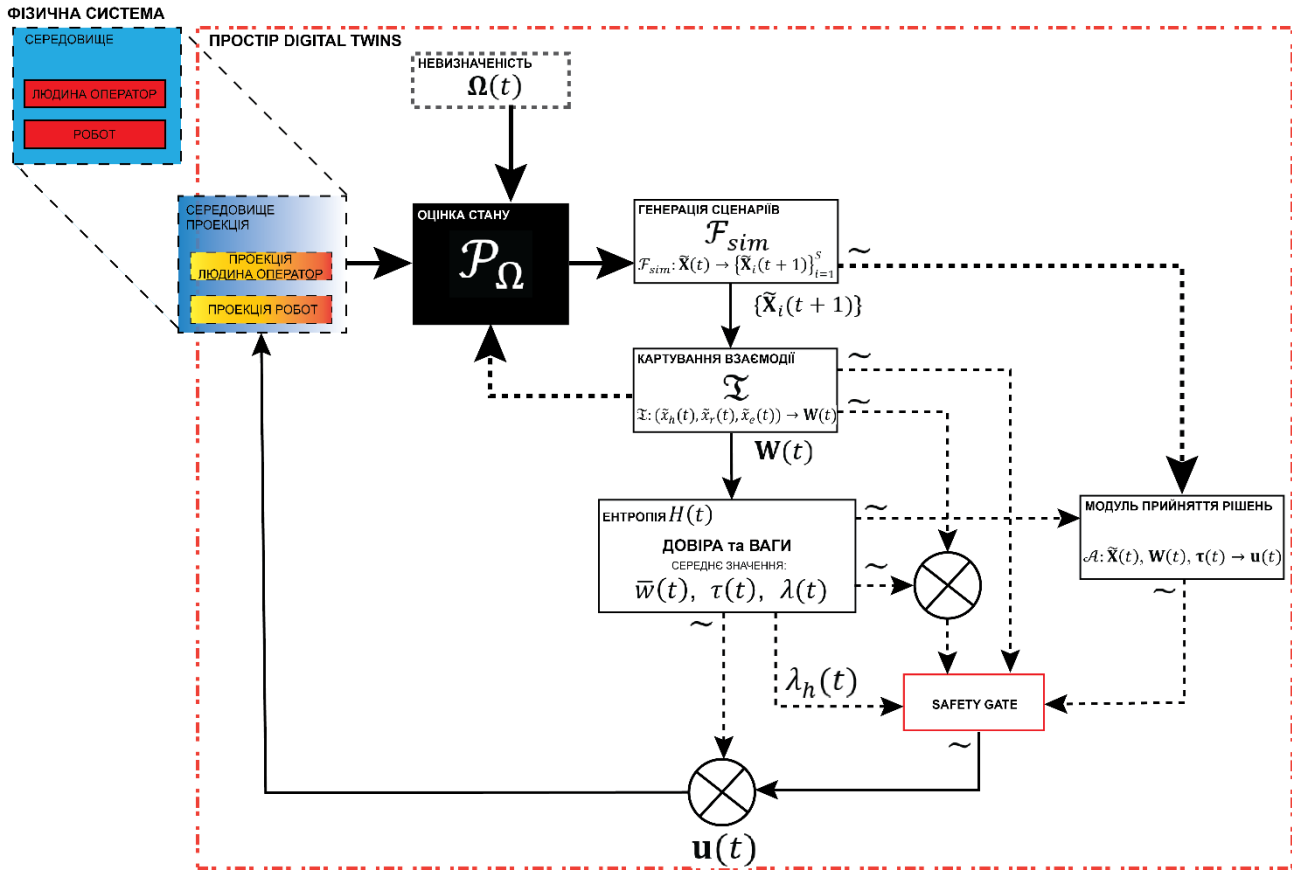


Рис. 1. Блок-схема моделі еволюції людино-машинного інтерфейсу

Ключовим елементом запропонованої моделі є матриця (2) взаємодії, яка відображає інтенсивність, напрям і узгодженість інформаційних та керуючих зв'язків між компонентами системи (2):

$$\mathbf{W}(t) = \begin{bmatrix} 0 & W_{hr}(t) & W_{he}(t) \\ W_{rh}(t) & 0 & W_{re}(t) \\ W_{eh}(t) & W_{er}(t) & 0 \end{bmatrix}, \quad (2)$$

Елементи матриці не є фіксованими, а змінюються у часі залежно від якості взаємодії, точності прогнозів і рівня довіри.

Динаміка системи описується узагальненим рівнянням переходу станів (3):

$$\mathbf{X}(t+1) = \mathcal{F}(\mathbf{X}(t), \mathbf{W}(t), \mathbf{u}(t), \mathbf{\Omega}(t)), \quad (3)$$

де $\mathbf{u}(t)$ – керуючі дії, сформовані оператором або автоматизованими модулями; $\mathbf{\Omega}(t)$ – сукупність невизначеностей, що включає шум сенсорів, затримки, інформаційні атаки та випадкові збурення середовища.

Для забезпечення повноти математичного опису уточнимо природу невизначеності середовища $\Omega(t)$ та визначимо її складові. Формально невизначеність представимо, як вектор, рівняння (4):

$$\Omega(t) = (\omega_s(t), \omega_c(t), \omega_e(t), \omega_a(t)), \quad (4)$$

де $\omega_s(t)$ – сенсорні невизначеності такі як шум вимірювань, похибки IMU, LiDAR, GNSS;
 $\omega_c(t)$ – комунікаційні збурення, а саме затримки, втрати пакетів, джамінг;
 $\omega_e(t)$ – динамічні зміни середовища. Наприклад рух перешкод або зміна умов середовища;
 $\omega_a(t)$ – активні впливи що спричиняють спотворення. Наприклад спуфінг, інформаційні атаки, дезінформація.

Кожна з цих складових може бути описана як стохастичний процес із відповідними розподілами, що дозволяє формалізувати рівень невизначеності в системі. Вплив $\Omega(t)$ проявляється у двох ключових аспектах. По-перше, він безпосередньо впливає на динаміку стану системи (3). По-друге, невизначеність розкриває форму розподілу сценаріїв $p_i(t)$, що використовується для обчислення ентропії $H(t)$. Таким чином, саме $\Omega(t)$ є *первинним джерелом* ентропії у моделі.

З точки зору еволюції системи, роль $\Omega(t)$ є двоякою. По-перше вона ускладнює процес узгодження та може спричиняти флуктуації у значеннях $H(t)$, $\bar{w}(t)$ та $\tau(t)$. Але наявність невизначеності також стимулює розвиток прогнозного контуру, що дозволяє системі навчатися, адаптуватися та переходити до більш структурованого стану.

Для подальшого аналізу доцільно ввести рівень інтенсивності невизначеності (5):

$$\|\Omega(t)\| = \sigma_s + \sigma_c + \sigma_e + \sigma_a, \quad (5)$$

який узагальнює вплив окремих компонентів. У залежності від цього, можна виділити різні режими функціонування системи. Прийmemo $L1$, як рівень з низькою невизначеністю, $L2$ рівень середньої $\Omega(t)$ і $L3$ коли $\Omega(t)$ висока. Таким чином, $\Omega(t)$ виступає ключовим фактором, що визначає складність середовища, рівень ентропії та швидкість переходу системи від емпіричного хаосу до структурованої взаємодії.

Важливо зазначити, що динаміка самої матриці зв'язків відіграє особливу роль, а саме відображає процес адаптації та навчання системи. У загальному вигляді вона може бути представлена як (6):

$$\mathbf{W}(t + 1) = \mathbf{W}(t) + \eta \cdot \Delta \mathbf{W}(t), \quad (6)$$

де η – коефіцієнт адаптації, а $\Delta \mathbf{W}(t)$ визначається мірою узгодженості між відповідними підсистемами. Інтуїтивно це означає, що зв'язки між компонентами посилюються у разі їх узгодженої поведінки та послаблюються у випадку розбіжностей. Таким чином, матриця $\mathbf{W}(t)$ еволюціонує разом із системою, відображаючи перехід від випадкових і слабких зв'язків до стійкої структурованої конфігурації. У межах такого представлення інтегральні характеристики системи, зокрема середня зв'язність $\bar{w}(t)$, довіра $\tau(t)$ та ентропія $H(t)$, можуть бути інтерпретовані як функції від станів і структури взаємодії. Зокрема, $\bar{w}(t)$ відображає загальний рівень узгодженості між компонентами системи, тоді як $\tau(t)$ характеризує ступінь довіри між людиною та машиною, що формується на основі якості взаємодії та рівня невизначеності.

Таким чином, запропоноване матричне представлення дозволяє розглядати ЛМІ як структурно-динамічну систему, у якій стан і взаємозв'язки еволюціонують спільно. У цьому контексті емпіричний хаос відповідає режиму, в якому матриця $\mathbf{W}(t)$ є слабо структурованою та близькою до випадкової, тоді як структурована взаємодія характеризується її збіжністю до стабільної конфігурації з вираженими та узгодженими зв'язками.

3.3. Інтегральні змінні моделі. Запропонований підхід створює основу для введення інтегральних характеристик, які узагальнюють стан взаємодії та дозволяють описати її еволюцію у компактній формі та побудувати динамічну модель переходу від хаосу до структури. На відміну від окремих компонентів вектору стану або елементів матриці взаємодії $\mathbf{W}(t)$, інтегральні змінні відображають глобальні властивості системи, такі як рівень невизначеності, ступінь узгодженості та баланс ролей між людиною і машиною.

Для забезпечення математичної коректності подальших теоретичних тверджень зафіксуємо припущення у межах яких функціонує запропонована модель й уникнення неоднозначності у трактуванні інтегральних змінних, уточнимо межі їх зміни та встановимо умови, за яких результати, щодо монотонності довіри і зменшення участі оператора, є коректними. Визначимо, що у подальшому вважаємо, що ентропія взаємодії $H(t)$, середня зв'язність $\bar{w}(t)$, функція довіри $\tau(t)$ та вага участі оператора $\lambda(t)$ є нормованими величинами, а саме (7):

$$(H(t), \bar{w}(t), \tau(t), \lambda(t)) \in [0,1]. \quad (7)$$

При цьому ентропія взаємодії $H(t)$, інтерпретується як міра невизначеності у процесі прийняття рішень та прогнозування станів системи [9]. Тобто в загальному вигляді $H(t)$ визначається як нормалізована ентропія ансамблю сценаріїв прогнозного контуру (8):

$$H(t) = -\frac{1}{\log S} \sum_{i=1}^S p_i(t) \log p_i(t), \quad (8)$$

де S – кількість сценаріїв ансамблю, $p_i(t)$ це ймовірність реалізації i -го сценарію в момент часу t , $\sum_{i=1}^S p_i(t) \log p_i(t) = 1$. За такого означення виконується умова $0 \leq H(t) \leq 1$. При цьому високе значення $H(t)$ відповідає стану емпіричного хаосу, коли система не має чіткої переваги між альтернативами, тоді як зменшення ентропії свідчить про формування структурованого та передбачуваного режиму взаємодії.

Елементи матриці взаємодії вважаються нормованими та задовольняють співвідношення (9):

$$W_{ij}(t) \in [0,1], \quad W_{ii}(t) = 0. \quad (9)$$

Активним зв'язком будемо вважати пару підсистем (i, j) , для якої вага взаємодії перевищує заданий поріг активності $\varepsilon_w \in (0,1)$, згідно з виразом (10):

$$(i, j) \in \mathcal{A}_t \Leftrightarrow W_{ij}(t) \geq \varepsilon_w. \quad (10)$$

Тоді середня зв'язність системи визначається як середнє значення ваг активних зв'язків згідно з виразом (11):

$$\bar{w}(t) = \frac{1}{|\mathcal{A}_t|} \sum_{(i,j) \in \mathcal{A}_t} W_{ij}(t), \quad (11)$$

де $\mathcal{A}_t$ – множина активних зв'язків у момент часу t , а $W_{ij}(t) \in [0,1]$ – вага взаємодії між i -ю та j -ю підсистемами. Звідки розуміємо, що $0 \leq \bar{w}(t) \leq 1$, що відображає загальний рівень узгодженості між людиною, роботом і середовищем. Низькі значення $\bar{w}(t)$ характерні для хаотичних режимів, тоді як зростання свідчить про формування стійких і узгоджених взаємодій.

Для формалізації процесу узгодження між підсистемами введемо міру узгодженості $c_{ij}(t) \in [0,1]$, яка може бути задана як комбінація подібності дій та точності прогнозування (12):

$$c_{ij}(t) = \alpha \operatorname{sim}(u_i(t), u_j(t)) + (1 - \alpha) \exp(-\beta e_{ij}(t)), \quad (12)$$

де $\operatorname{sim}(u_i(t), u_j(t)) \in [0,1]$ є нормованою мірою подібності або узгодженості дій, $e_{ij}(t) \geq 0$, це похибка прогнозування або розбіжність між очікуваним і фактичним станом, а $\alpha \in [0,1]$, $\beta > 0$. Таким чином, високі значення $c_{ij}(t)$ відповідають високій узгодженості між компонентами системи.

Еволюція ваг зв'язків задається правилом адаптивного оновлення (13):

$$W_{ij}(t+1) = \Pi_{[0,1]}^{\mathcal{P}_\Omega}((1-\eta)W_{ij}(t) + \eta c_{ij}(t)), \quad \eta \in (0,1], \quad (13)$$

де $\Pi_{[0,1]}^{\mathcal{P}_\Omega}$ – оператор проєкції на інтервал $[0,1]$. Таке означення гарантує збереження нормування ваг зв'язків у процесі еволюції.

Центральною змінною моделі виступає функція довіри $\tau(t)$, яка визначає ступінь делегування управління від людини до машини (14):

$$\tau(t) = \bar{w}(t) e^{-\gamma H(t)}, \quad \text{при } \gamma \geq 0, \quad (14)$$

де γ – параметр чутливості до невизначеності. За умов $\bar{w}(t) \in [0,1]$ та $H(t) \in [0,1]$, виконується співвідношення $0 \leq \tau(t) \leq 1$. Така форма відображає природну залежність, коли довіра зростає при підвищенні узгодженості та одночасному зменшенні ентропії. Вага участі оператора $\lambda_h(t)$ моделює рівень залученості людини в контурі керування, що визначається як спадна функція довіри (15):

$$\lambda(t) = \lambda_{\min} + (\lambda_{\max} - \lambda_{\min}) (1 - \tau(t)), \quad (15)$$

при умові $0 \leq \lambda_{\min} < \lambda_{\max} \leq 1$, отримуємо $\lambda(t) \in [\lambda_{\min}, \lambda_{\max}] \subseteq [0,1]$. Таким чином, при низькому рівні довіри система покладається на оператора, а при її зростанні відбувається поступове делегування функцій машині.

Сукупність введених змінних дозволяє описати стан людино-машинного інтерфейсу у вигляді узагальненого вектору $\mathbf{Z}(t)$ (16) який характеризує не окремі компоненти системи, а її інтегральну поведінку.

$$\mathbf{Z}(t) = (H(t), \bar{w}(t), \tau(t), \lambda_h(t)). \quad (16)$$

Еволюція $\mathbf{Z}(t)$ у часі відображає процес переходу від емпіричного хаосу до структурованої взаємодії. Важливо підкреслити, що зазначені змінні є взаємопов'язаними, а саме, зменшення ентропії призводить до зростання довіри, що, у свою чергу, впливає на

перерозподіл ролей між людиною та машиною і стимулює подальше підсилення зв'язків у матриці $\mathbf{W}(t)$.

Таким чином, система демонструє властивості самоорганізації, у якій локальні покращення узгодженості накопичуються та призводять до глобальної структуризації взаємодії. Таким чином впровадження інтегральних змінних створює необхідне підґрунтя для формування динамічної моделі еволюції, у якій буде формалізовано механізм переходу між режимами функціонування системи.

3.4. Динаміка переходу. Застосуємо інтегральні змінні для побудови динамічної моделі еволюції ЛМІ. Для цього опишемо перехід від емпіричного хаосу до структурованої взаємодії як функцію впливу узгодженої зміни ентропії, зв'язності, довіри й ролі оператора у часі під впливом механізмів прогнозування, навчання та зворотного зв'язку.

Еволюція системи, що задається дискретною динамікою станів має вигляд (17):

$$\mathbf{Z}(t + 1) = \mathcal{F}(\mathbf{Z}(t), \mathbf{W}(t), \mathbf{\Omega}(t)), \quad (17)$$

де $\mathbf{Z}(t)$ – вектор інтегральних змінних (13);

$\mathbf{W}(t)$ – матриця взаємодії (2);

$\mathbf{\Omega}(t)$ – невизначеності середовища (4).

Такий запис підкреслює, що еволюція не є лінійною і визначається взаємодією кількох факторів одночасно.

Опишемо зменшення ентропії як результат прогнозування та накопичення інформації формуюлю (18):

$$H(t + 1) = H(t) - \alpha \cdot \Delta I(t) + \xi H(t), \quad (18)$$

де $\Delta I(t)$ – приріст інформації за рахунок симуляції сценаріїв, досвіду або навчання; α – коефіцієнт ефективності навчання; $\xi H(t)$ – стохастичний вплив середовища. Таким чином, у відсутності сильних збурень ентропія має тенденцію до зменшення, що відображає процес упорядкування системи.

Динаміка зв'язності визначається узгодженістю дій між компонентами системи (19):

$$\bar{w}(t + 1) = \bar{w}(t) + \eta(C(t) - \bar{w}(t)), \quad (19)$$

де $C(t)$ – міра узгодженості;

η – швидкість адаптації.

Якщо система демонструє узгоджену поведінку, $\bar{w}(t)$ зростає, і навпаки.

Функція довіри $\tau(t)$, як було визначено раніше, залежить від ентропії та зв'язності (13). Тому її динаміка є похідною від змін у $H(t)$ та $\bar{w}(t)$, що узгоджується з сучасними підходами до посилення зв'язків зростання довіри у командах “людина–робот” [10], відіграючи ключову роль у стабілізації системи.

Вага участі оператора змінюється обернено до довіри (20):

$$\lambda_h(t + 1) = \min\{1, \zeta e - \rho \tau(t)\}, \quad (20)$$

що означає поступове зменшення необхідності втручання людини у міру підвищення узгодженості системи. Водночас у разі падіння довіри або зростання невизначеності відбувається зворотний процес повернення контролю до оператора.

Таким чином, динаміка системи має характер замкненого кібернетичного контуру де зменшення ентропії сприяє зростанню довіри, що підсилює зв'язність, яка, у свою чергу, покращує якість прогнозування й додатково зменшує ентропію. Цей позитивний зворотний зв'язок формує механізм самоорганізації системи. У той же час наявність стохастичних впливів $\Omega(t)$ та обмежень безпеки створює умови для відхилень від ідеальної траєкторії. У складних середовищах ці впливи можуть уповільнювати або тимчасово порушувати процес структуризації, що призводить до флуктуацій у $H(t)$, $\bar{w}(t)$ та $\tau(t)$. Проте за умови коректного налаштування параметрів системи середня тенденція до впорядкування зберігається.

Побудована динамічна модель описує еволюцію ЛМІ, як процес взаємопов'язаних змін ентропії, довіри, зв'язності та ролі оператора і дозволяє перейти до формалізації критерію, який визначає момент переходу системи від стану емпіричного хаосу до структурованої взаємодії. Такий критерій має базуватися на інтегральних змінних $H(t)$, $\bar{w}(t)$, $\tau(t)$ та $\lambda_h(t)$, що характеризують глобальний стан системи.

Визначимо стан структурованої взаємодії через виконання сукупності умов (21):

$$\begin{cases} H(t) \leq H^*; \\ \tau(t) \geq \tau^*; \\ \bar{w}(t) \geq w^*; \\ \lambda_h(t) \leq \lambda^*. \end{cases} \quad (21)$$

де H^* , τ^* , w^* , λ^* – граничні порогові значення, що задають допустимий рівень невизначеності, мінімально необхідну довіру, достатню узгодженість і максимальну частку участі оператора відповідно. Такий перехід до структурованого режиму інтерпретується як досягнення системою області станів, у якій ці умови виконуються одночасно.

3.5. Теоретичні твердження. Для формалізації процесу переходу ЛМІ від емпіричного хаосу до структурованої взаємодії розглянемо властивості інтегральних змінних системи, де ключову роль відіграють ентропія $H(t)$, середня зв'язність $\bar{w}(t)$ та функція довіри $\tau(t)$.

В зв'язку з цим визначимо і доведемо *твердження про монотонність довіри*.

Лема 1. *Про монотонне спадання ентропії.*

Нехай еволюція ентропії описується рівнянням (18), де у системі на кожному кроці прогнозний контур генерує приріст інформації $\Delta I(t) \geq 0$, а стохастичне збурення $\xi_H(t)$ є обмеженим у середньому. Тоді за умови, що приріст інформації перевищує рівень шуму або невизначеності середовища відповідає умові (22):

$$\alpha \mathbb{E}[\Delta I(t)] > \mathbb{E}[\xi_H(t)], \quad (22)$$

ентропія $H(t)$ не зростає у середньому, тобто (23):

$$\mathbb{E}[H(t+1)] \leq \mathbb{E}[H(t)]. \quad (23)$$

Доведення: Із рівняння (18) маємо (24):

$$\mathbb{E}[H(t+1)] = \mathbb{E}[H(t)] - \alpha \mathbb{E}[\Delta I(t)] + \mathbb{E}[\xi_H(t)]. \quad (24)$$

За умови, що (22), тобто $-\alpha \mathbb{E}[\Delta I(t)] + \mathbb{E}[\xi_H(t)] \leq 0$, отримаємо (23). Отже, за умови, що система отримує більше інформації, ніж втрачає через шум, доводить про те, що ентропія не зростає. *Лему доведено.*

Лема 2. *Про не спадання середньої зв'язності.*

Нехай середня зв'язність визначається як (13), де оновлення матриці взаємодії $\mathbf{W}(t)$ відбувається за правилом узгодженого підсилення зв'язків, а міра узгодженості $C(t)$ задовольняє умову $C_{ij}(t) \geq W_{ij}(t)$, $\forall (i, j) \in \mathcal{A}_t$ і перевищує поточне значення $\bar{w}(t)$ для $\eta > 0$. Тоді маємо (25):

$$\mathbb{E}[\bar{w}(t+1)] \geq \mathbb{E}[\bar{w}(t)]. \quad (25)$$

Доведення: З рівняння (13) маємо (26.1):

$$W_{ij}(t+1) = (1 - \eta)W_{ij}(t) + \eta c_{ij}(t), \eta \in (0,1]. \quad (26.1)$$

Тоді маємо (26.2):

$$\mathbb{E}[\bar{w}(t+1)] = \mathbb{E}[\bar{w}(t)] + \eta(\mathbb{E}[C(t)] - \mathbb{E}[\bar{w}(t)]). \quad (26.2)$$

Якщо $\mathbb{E}[C(t)] \geq \mathbb{E}[\bar{w}(t)]$, усереднення за всіма активними зв'язками дає (25) тобто приріст є невід'ємним. *Лему доведено.*

Лема 3. *Про монотонність експоненційного множника.*

Якщо ентропія $H(t)$ не зростає у середньому, то функція $e^{-\gamma H(t)}$, зростає при $\gamma \geq 0$.

Доведення: Функція $f(H) = e^{-\gamma H}$ при $\gamma \geq 0$ є монотонно спадною за H . Тому якщо $H(t+1) \leq H(t)$, (27):

$$e^{-\gamma H(t+1)} \geq e^{-\gamma H(t)}. \quad (27)$$

А враховуючи, що у середньому ця властивість зберігається – *лему доведено.*

Твердження про монотонність довіри.

Нехай у системі «людина–робот» функція довіри визначається як (28):

$$\tau(t) = \bar{w}(t) e^{-\gamma H(t)}, \quad \gamma > 0. \quad (28)$$

Якщо виконуються умови лем 1–3, тобто (29):

$$H(t+1) \leq H(t), \bar{w}(t+1) \geq \bar{w}(t), \quad (29)$$

Тоді функція довіри $\tau(t)$ не спадає (30):

$$\mathbb{E}[\tau(t+1)] \geq \mathbb{E}[\tau(t)]. \quad (30)$$

Доведення:

Згідно з лемою 1, ентропія $H(t)$ є зростаючою, а саме $\bar{w}(t+1) \geq \bar{w}(t)$ за лемою 3 означає, що множник $e^{-\gamma H(t)}$ не спадає, тому застосовуючи лему 2 розуміємо, що середня зв'язність $\bar{w}(t)$ також не спадає. Таким чином, обидва множники у виразі для $\tau(t)$ мають неспадну тенденцію, а отже їхній добуток також зростає (31):

$$\mathbb{E}[\tau(t+1)] = \mathbb{E}[\bar{w}(t+1)e^{-\gamma H(t+1)}] \geq \mathbb{E}[\bar{w}(t)e^{-\gamma H(t)}] = \mathbb{E}[\tau(t)]. \quad (31)$$

Твердження доведено.

Короларій про зменшення участі оператора.

Нехай вага участі оператора визначається як (32):

$$\lambda_h(t) = \min\{1, \zeta e^{-\rho\tau(t)}\}, \quad \rho > 0. \quad (32)$$

Тоді при виконанні умов основного твердження, що функція $\lambda_h(t)$ не спадаюча (33):

$$\mathbb{E}[\lambda_h(t+1)] \leq \mathbb{E}[\lambda_h(t)]. \quad (33)$$

Це означає, що зі зростанням довіри відбувається закономірне зменшення інтенсивності безпосереднього втручання оператора у контурі керування, що відповідає переходу системи до більш структурованого та частково автономного режиму функціонування.

Отримане твердження формалізує ключову властивість запропонованої моделі, що за умов ефективного зменшення невизначеності та підвищення узгодженості між компонентами системи довіра між людиною та машиною зростає природним чином. Це зростання не є випадковим, а виступає наслідком внутрішньої структури кібернетичного контуру взаємодії.

Важливо підкреслити, що монотонність довіри має місце зростати і може супроводжуватися локальними флуктуаціями, зумовленими стохастичними впливами середовища або порушенням умов узгодженості. У складних умовах функціонування система може тимчасово повертатися до менш структурованих станів, що відображає реалістичну поведінку людино-машинних систем.

На основі введених змінних та отриманого твердження перехід до структурованої взаємодії визначається досягненням порогового значення функції довіри $\tau(t) \geq \tau^*$, де τ^* – наперед заданий рівень, що відповідає стабільному узгодженому режиму. Додатково врахуємо обмеження на ентропію, зв'язність та участь оператора (34):

$$\begin{cases} H(t) \leq H^*; \\ \bar{w}(t) \geq w^*; \\ \lambda_h(t) \leq \lambda^*. \end{cases} \quad (34)$$

Таким чином, структурована взаємодія визначається як область станів, у якій система демонструє низьку невизначеність, високу узгодженість та раціональний розподіл ролей між людиною і машиною.

3.6. Інтерпретація через цифрові двійники. Отримана математична модель еволюції ЛМІ набуває повного змісту лише за умови явного введення механізмів відображення фізичної системи у цифровий простір та взаємодії між її компонентами. У цьому контексті ключову роль відіграють цифрові двійники, які розглядаються не як статичні копії, а як результат проєкції, що формується під впливом невизначеностей середовища [11; 12].

Кібернетичний контур прогнозування реалізує процес генерації та оцінювання множини можливих сценаріїв розвитку ситуації [13]. Для кожного сценарію здійснюється прогноз станів системи, обчислюються відповідні значення ризику, вартості та інших метрик, після чого формується розподіл ймовірностей $p_i(t)$. Саме на основі цього розподілу обчислюється ентропія $H(t)$, яка відображає рівень невизначеності у виборі дій. Зі зростанням точності прогнозування та накопиченням досвіду розподіл стає більш концентрованим, що призводить до зменшення ентропії.

Нехай $\mathbf{X}(t)$, є стан фізичної системи «людина–робот–середовище», а $\mathbf{\Omega}(t)$ вектор невизначеностей, що включає сенсорні, комунікаційні, динамічні та інформаційні збурення. Тоді оператор проєкції доцільно визначити як (35):

$$\mathcal{P}_{\Omega}: (\mathbf{X}(t), \mathbf{\Omega}(t)) \rightarrow \tilde{\mathbf{X}}(t), \quad (35)$$

де $\tilde{\mathbf{X}}(t)$ – стан цифрових двійників. Цей оператор узагальнює процеси сенсорного сприйняття, фільтрації та оцінювання стану, включаючи методи злиття даних, фільтр Калмана або нейромережеві підходи. Таким чином, цифровий двійник є оцінкою реального стану, що формується з урахуванням похибок сприйняття, обмеженої спостережності та впливу середовища з урахуванням невизначеностей $\mathbf{\Omega}(t)$.

У загальному вигляді це відображення можна представити як (36):

$$\tilde{\mathbf{X}}(t) = \mathcal{P}(\mathbf{X}(t)) + \varepsilon_{\Omega}(t), \quad (36)$$

де $\varepsilon_{\Omega}(t)$ – похибка проєкції, індукована невизначеностями $\mathbf{\Omega}(t)$. Зростання інтенсивності невизначеностей призводить до збільшення цієї похибки, що безпосередньо впливає на якість цифрового двійника.

З урахуванням окремих компонентів системи можна записати як (37):

$$\tilde{\mathbf{X}}(t) = \begin{bmatrix} \tilde{x}_h(t) \\ \tilde{x}_r(t) \\ \tilde{x}_e(t) \end{bmatrix} = \begin{bmatrix} \mathcal{P}_h(x_h(t), \Omega_h(t)) \\ \mathcal{P}_r(x_r(t), \Omega_r(t)) \\ \mathcal{P}_e(x_e(t), \Omega_e(t)) \end{bmatrix}. \quad (37)$$

де $\tilde{x}_h(t)$ – цифровий двійник оператора;

$\tilde{x}_r(t)$ – цифровий двійник роботизованої платформи;

$\tilde{x}_e(t)$ – цифровий двійник середовища.

Подальша еволюція відбувається у просторі цифрових двійників через оператор прогнозування (38):

$$\mathcal{F}_{sim}: \tilde{\mathbf{X}}(t) \rightarrow \{\tilde{\mathbf{X}}_i(t+1)\}_{i=1}^S, \quad (38)$$

де формується ансамбль сценаріїв розвитку системи. Саме цей ансамбль визначає розподіл ймовірностей $p_i(t)$, і таким чином, ентропія є властивістю не фізичного простору, а функцією цифрового представлення системи простору прогнозованих станів цифрових двійників і прямо залежить від якості оператора $\mathcal{P}_{\Omega}$.

Ключовим елементом запропонованої моделі є оператор взаємодії (39) який формує матрицю зв'язків на основі узгодженості між цифровими двійниками (39):

$$\mathfrak{I}: (\tilde{x}_h(t), \tilde{x}_r(t), \tilde{x}_e(t)) \rightarrow \mathbf{W}(t). \quad (39)$$

Зокрема, елементи матриці можуть бути визначені як функції кореляції, узгодженості або помилки прогнозу (40):

$$W_{ij}(t) \sim \text{sim}(\tilde{x}_i(t), \tilde{x}_j(t)), \quad (40)$$

де $\text{sim}(\cdot)$ – функція подібності або узгодженості, що враховує кореляцію, похибку прогнозу або ступінь відповідності дій. Таким чином, матриця $\mathbf{W}(t)$ є результатом взаємодії саме у просторі цифрових двійників, а не безпосередньо у фізичному просторі.

На основі отриманої матриці зв'язків $\mathbf{W}(t)$ та розподілу сценаріїв $H(t)$, формується функція довіри (14), яка визначає баланс між автоматизованим управлінням і участю оператора. У цьому контексті довіра є інтегральною характеристикою відповідності між прогнозованими та фактичними станами системи. Формування зворотного керуючого впливу на фізичну систему здійснюється через оператор прийняття рішень (41):

$$\mathcal{A}: \tilde{\mathbf{X}}(t), \mathbf{W}(t), \boldsymbol{\tau}(t) \rightarrow \mathbf{u}(t), \quad (41)$$

що формує керуючу дію з урахуванням результатів прогнозування, рівня довіри та функціональні обмеження.

Важливим елементом архітектури є блок безпеки SafetyGate [14, 15], який виконує функцію обмеження простору допустимих дій. Незалежно від рівня довіри чи прогнозованих виграшів, жодна дія не може бути реалізована у фізичному контурі без проходження перевірки безпеки [16]. Це забезпечує стабільність системи навіть у випадках тимчасових збоїв у прогнозованому контурі або деградації довіри. Повний контур функціонування системи може бути представлений як композиція операторів (42):

$$(\mathbf{X}(t), \boldsymbol{\Omega}(t)) \xrightarrow{\mathcal{P}_{\Omega}} \tilde{\mathbf{X}}(t) \xrightarrow{\mathcal{F}_{\text{sim}}} \{\tilde{\mathbf{X}}_i(t+1)\} \xrightarrow{\mathcal{T}} \mathbf{W}(t) \xrightarrow{\boldsymbol{\tau}} \mathbf{u}(t) \rightarrow \mathbf{X}(t+1). \quad (42)$$

У такому поданні невизначеність середовища $\boldsymbol{\Omega}(t)$ не лише впливає на фізичну динаміку системи, а також виконує формування структури взаємодії, визначаючи якість проєкції, структуру прогнозу та рівень ентропії. Таким чином, запропонована математична модель знаходить природну реалізацію у вигляді кібернетичної архітектури, де цифрові двійники забезпечують моделювання поведінки, прогнозний контур впливає на зменшення невизначеності, а адаптивна матриця зв'язків, на накопичення узгодженості. В такому вигляді вони виступають фундаментальним фактором, який визначає швидкість і характер зменшення невизначеності, зростання узгодженості та формування довіри, що забезпечує перехід системи від емпіричного хаосу до структурованої взаємодії.

Отже отримана інтерпретація забезпечує повну узгодженість між математичною моделлю, архітектурою системи та механізмами її реалізації, створюючи безпосередній міст між теоретичною моделлю та її практичною реалізацією, що відкриває можливість для експериментальної перевірки у симуляційному середовищі.

4. Практичні результати та обговорення

Реалізація запропонованої моделі еволюції ЛМІ побудована з урахуванням процесу структуризації взаємодії, відбувається у симуляційному просторі цифрових двійників, тоді як фізичний контур виконує роль джерела даних і об'єкта керування. Відповідно до цього архітектура симуляційного середовища організована як багаторівнева система, що відтворює операторну структуру $\mathcal{P}_{\Omega}$, $\mathcal{F}_{\text{sim}}$, $\mathcal{T}$ та $\mathcal{A}$. Як базове симуляційне середовище використано ROS2/ Gazebo, яке забезпечує фізично коректне моделювання динаміки роботизованих систем, сенсорних даних та взаємодії з середовищем. Симуляція інтегрована з обчислювальним контуром, що реалізує цифрові двійники та алгоритми прогнозування, що дозволяє відокремити фізичний рівень від рівня прийняття рішень [17]. Функціональна блок-схема інтеграції математичної моделі людино-машинного інтерфейсу з симуляційним середовищем Gazebo через стек ROS 2 зображено на рисунку 2.

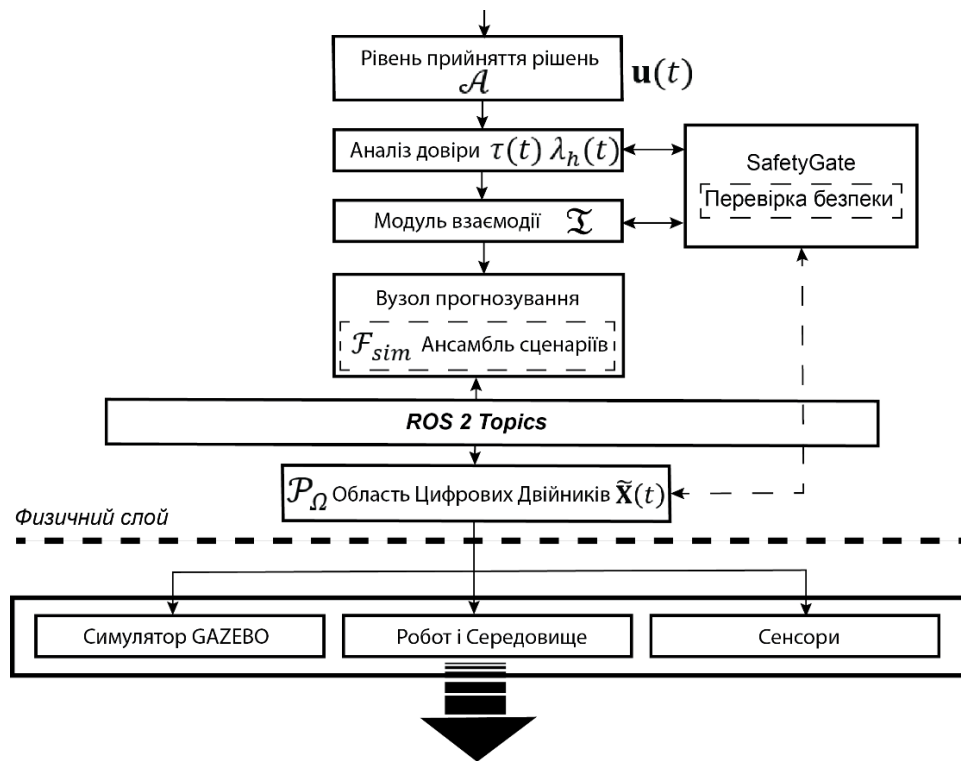


Рис. 2. Функціональна блок-схема інтеграції математичної моделі людино-машинного інтерфейсу з симуляційним середовищем Gazebo через стек ROS 2

Архітектура системи включає три базових рівні, а саме – фізичний, рівень проєкції та цифровий рівень. Фізичний рівень представлений моделями оператора, роботизованої платформи та середовища, які генерують стан $\mathbf{X}(t)$ і піддаються впливу невизначеностей $\Omega(t)$. Рівень проєкції реалізує оператор $\mathcal{P}_\Omega$, який виконує перетворення фізичного стану у цифровий простір, враховуючи шуми сенсорів, затримки та часткову спостережуваність. У результаті формується стан цифрових двійників $\tilde{\mathbf{X}}(t)$, що виступає основою для подальшого аналізу. Цифровий рівень є центральним елементом архітектури та реалізує процеси прогнозування, оцінювання та прийняття рішень. Ентропія $H(t)$ обчислюється на основі розподілу ймовірностей сценаріїв, сформованих у прогнозному контурі. Для цього використовується ансамбль траєкторій, що дозволяє оцінити невизначеність у виборі дій. Середня зв'язність $\bar{w}(t)$ визначається як агрегована характеристика матриці $\mathbf{W}(t)$, після чого обчислюється функція довіри $\tau(t)$, яка визначає баланс між автономністю системи та участю оператора.

Для забезпечення відтворюваності результатів і коректної оцінки ефективності запропонованої архітектури було сформовано формалізований протокол симуляційних експериментів, що охоплює параметри середовища, гіперпараметри моделі, план запусків та методи обробки результатів. Симуляційне середовище організовано у дискретному часі з кроком 100 мс, що відповідає типовим вимогам до систем реального часу в робототехнічних застосуваннях. Планувальне вікно становить 1 с (10 кроків), що дозволяє узгодити горизонт прогнозування з динамікою середовища. Базовий горизонт прогнозу в межах оператора $\mathcal{F}_{sim}$ встановлено на рівні 7 кроків (0,7 с), при цьому для аналізу чутливості використовуються варіанти 3 та 11 кроків, що дозволяє оцінити вплив глибини прогнозування на стабільність системи. Формування ансамблю сценаріїв здійснюється з розміром $S = 64$, що є компромісом між точністю оцінки ентропії та обчислювальною складністю. Для дослідження стійкості результатів додатково розглядаються варіанти $S = 32$ та $S = 128$. Кожен сценарій генерується з урахуванням випадкових реалізацій невизначеностей $\Omega(t)$, що включають сенсорні шуми, комунікаційні затримки, втрати даних, а також динамічні зміни середовища. Невизначеності

середовища встановлюють параметри через три рівні складності, де $L1$ низька невизначеність, $L2$ середня, $L3$ висока. Для рівня $L1$ характерні малі дисперсії сенсорних шумів і стабільні комунікації; $L2$ передбачає помірні флуктуації та часткові втрати даних; $L3$ моделює складні умови з високим рівнем шуму, затримками, можливими спотвореннями сигналів та динамічними перешкодами. Таким чином, рівні $L1$ – $L3$ відповідають різним значенням інтенсивності $\|\Omega(t)\|$ і дозволяють дослідити поведінку системи в широкому діапазоні умов. Гіперпараметри моделі обрано таким чином, щоб забезпечити баланс між адаптивністю та стабільністю системи. Зокрема, функція довіри задається як $\tau(t) = \bar{w}(t)e^{-\gamma H(t)}$, $\gamma = 0,5$, коефіцієнт адаптації зв'язків $\eta = 0,05$, параметри підсилення узгодженості $\kappa = 1,0$ та штрафу ризику $\lambda = 0,5$. Функціонал вибору дії має вигляд $J = \mathbb{E}[\text{Risk}] + \mu H + \nu \text{Cost} - \chi \tau$, де $\mu = 0,2$, $\nu = 0,1$, $\chi = 0,3$. Вага участі оператора визначається як $\lambda_h(t) = \min\{1, \zeta e - \rho \tau(t)\}$, $\zeta = 1,0$, $\rho = 1,0$. Матриця взаємодії $\mathbf{W}(t)$ ініціалізується як повнозв'язна без діагональних елементів зі стартовим значенням $W_{ij} = 0,2$, а її регуляризація здійснюється через $L2$ -норму $\|\mathbf{W}\|_2^F$ з коефіцієнтом 10^{-3} , що запобігає перенасиченню зв'язків.

План експериментів включає три типи сценаріїв оборона, атака та евакуація у поєднанні з трьома рівнями невизначеності ($L1$ – $L3$), що формує 9 базових конфігурацій. Для кожної конфігурації проводиться 20 незалежних запусків із різними початковими умовами, що забезпечує статистичну достовірність результатів. Тривалість кожного епізоду становить 300с симуляційного часу або 3000 крокам.

Додатково виконуються абляційні експерименти, спрямовані на оцінку внеску окремих компонентів моделі: а) без адаптації матриці $\mathbf{W}$; б) без урахування ентропії у функціоналі; с) без компоненти довіри; д) з фіксованою участю оператора. Для кожного варіанту виконується по 10 запусків на конфігурацію.

Для порівняння використовуються дві базові архітектури. A – класичний людино-машинний інтерфейс без цифрових двійників і прогнозного контуру й B – система з використанням штучного інтелекту, але без механізму прогнозування та адаптивної матриці взаємодії. Це дозволяє оцінити внесок кожного з ключових елементів запропонованої моделі.

Збір даних здійснюється на кожному кроці симуляції та включає значення $H(t)$, $\bar{w}(t)$, $\tau(t)$, $\lambda_h(t)$, обрані дії, показники ризику та вартості, а також результати перевірки SafetyGate. Обробка результатів виконується з використанням медіанних оцінок та 95 % довірчих інтервалів. Для оцінки ризику додатково використовується метрика $\text{CVaR}@0,9$, що характеризує поведінку системи у найгірших 10 % випадків.

Критеріями оцінки ефективності є монотонне зменшення ентропії $H(t)$ у середньому, зростання довіри $\tau(t)$, що відповідає сучасній тенденції до формалізованої оцінки довіри у ЛІМІ [18; 19] за рахунок зменшення ризику та CVaR порівняно з базовими підходами, а також зростання частки безпечних дій без перевищення допустимого рівня затримок.

Таким чином, сформований протокол експериментів забезпечує всебічну перевірку запропонованої моделі в умовах різної складності середовища та дозволяє об'єктивно оцінити її ефективність.

На рисунку 3 представлено динаміку ентропії $H(t)$, довіри $\tau(t)$, середньої зв'язності $\bar{w}(t)$ та ваги участі оператора $\lambda_h(t)$ у процесі симуляції. Отримані результати демонструють чітко виражену залежність поведінки системи від рівня невизначеності середовища.

Ентропія $H(t)$ у всіх випадках має тенденцію до зменшення, що підтверджує ефективність прогнозного контуру $\mathcal{F}_{\text{sim}}$ та оператора проєкції $\mathcal{P}_{\Omega}$. Для рівня $L1$ спадання є швидким і майже монотонним, що свідчить про високу якість цифрового відображення та стабільність середовища. У випадку $L2$ спостерігається більш плавна динаміка зі слабкими флуктуаціями, тоді як для $L3$ характерне повільніше зменшення ентропії з вираженими коливаннями, що відображає вплив високої інтенсивності $\Omega(t)$ на точність проєкції.

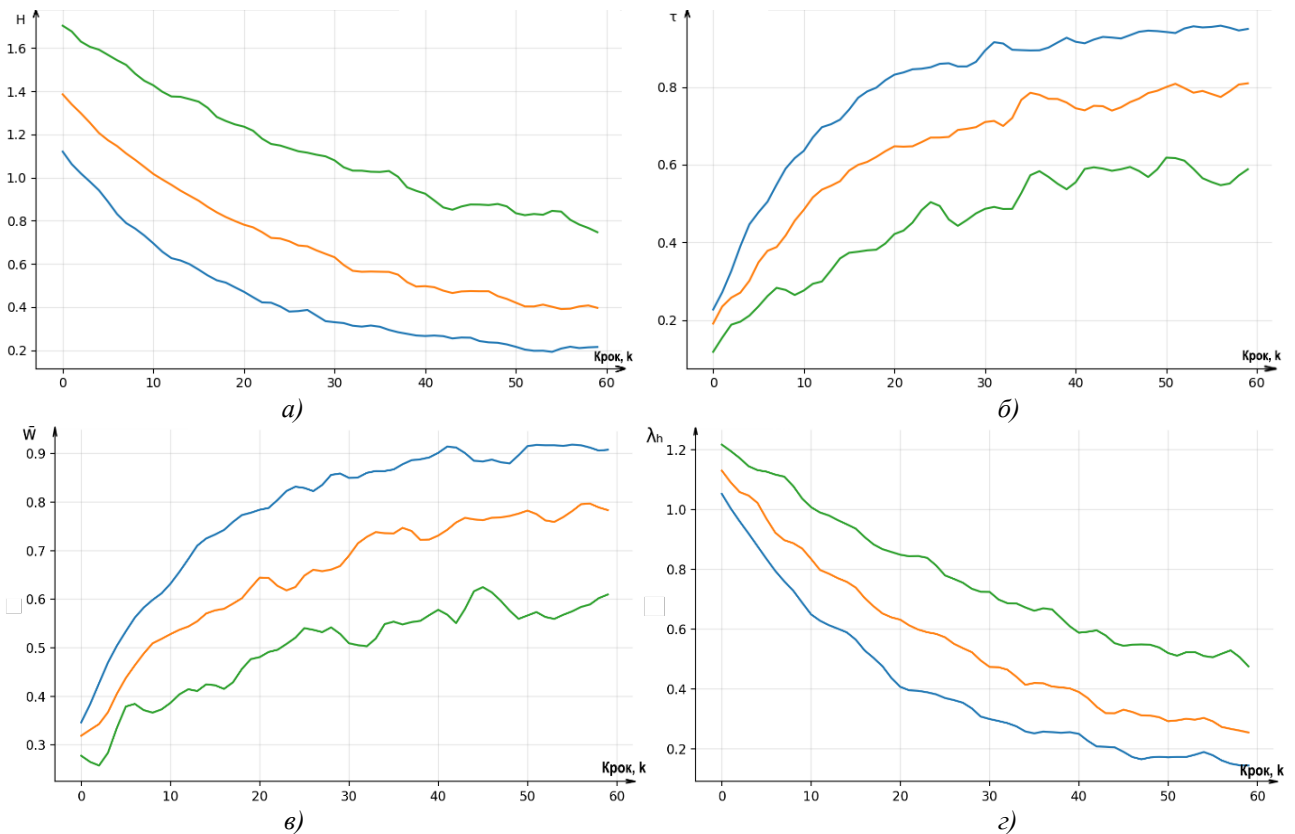


Рис. 3. Динаміка показників ентропії, коефіцієнта довіри, середньої зв'язності та ваги участі оператора за різних рівнів невизначеності середовища (— $L1$, — $L2$, — $L3$):
 а) ентропія прогнозування $H(t)$; б) функція довіри $\tau(t)$;
 в) середньої зв'язності $\bar{w}(t)$; г) ваги участі оператора $\lambda_h(t)$

Функція довіри $\tau(t)$ демонструє протилежну динаміку, а саме зростання у процесі симуляції. У середовищі $L1$ довіра швидко досягає високих значень, що відповідає стабільному узгодженню між цифровими двійниками. У $L2$ зростання є більш поступовим, а у $L3$ довіра формується значно повільніше і залишається обмеженою, що узгоджується з теоретичною залежністю $\tau(t) = \bar{w}(t)e^{-\gamma H(t)}$.

Середня зв'язність $\bar{w}(t)$ зростає в усіх випадках, що підтверджує ефективність оператора взаємодії $\mathcal{Z}$. Для $L1$ зростання є швидким і стабільним, що відображає формування стійкої структури взаємодії у просторі цифрових двійників. У $L2$ спостерігається помірний темп зростання, тоді як у $L3$ процес є повільнішим і супроводжується флуктуаціями, що свідчить про складність досягнення узгодженості в умовах високої невизначеності.

Вага участі оператора $\lambda_h(t)$ зменшується обернено до зростання довіри, що повністю узгоджується з отриманим аналітичним результатом. У середовищі $L1$ оператор швидко «розвантажується», тоді як у $L2$ цей процес відбувається поступово. У випадку $L3$ значення $\lambda_h(t)$ залишається відносно високим протягом усього експерименту, що вказує на необхідність збереження активної участі людини у складних умовах.

На рисунку 4 наведено порівняння стабілізованих значень інтегральних змінних для трьох архітектур, А класичний людино–машинний інтерфейс, В система з АІ без прогнозного контуру та запропонована модель. Результати показують суттєву перевагу запропонованого підходу у всіх сценаріях. Для архітектури А ентропія залишається високою, що свідчить про відсутність механізму зменшення невизначеності. Довіра τ у цьому випадку є низькою, а вага участі оператора λ_h – максимальною, що відповідає ручному режиму управління. У випадку

В спостерігається покращення показників, однак відсутність прогностного контуру та адаптивної матриці взаємодії обмежує рівень структуризації.

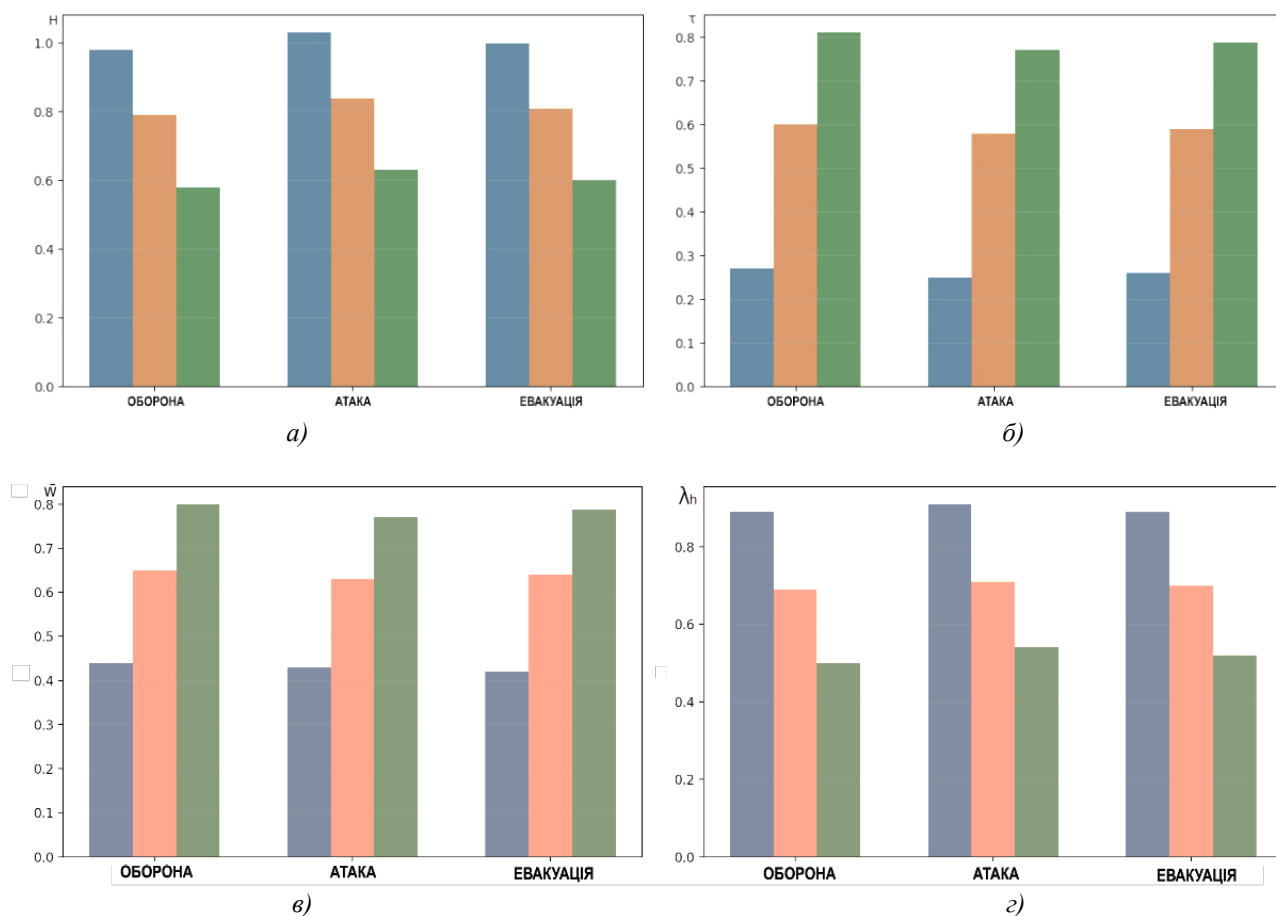


Рис. 4. Порівняння стабілізованих значень ентропії, довіри, середньої зв'язності та ваги участі оператора для архітектур **A**, **B** та **Запропонована** у Gazebo-сценаріях Оборона, Атака та Евакуація:

а) стабілізація ентропії $H(t)$;

б) стабілізація довіри $\tau(t)$;

в) стабілізація зв'язності $\bar{w}(t)$;

г) стабілізація оператора $\lambda_h(t)$

Запропонована архітектура демонструє найкращі результати: мінімальні значення ентропії, максимальну довіру та найбільшу середню зв'язність. При цьому вага участі оператора зменшується майже вдвічі порівняно з A, що свідчить про ефективний перехід до режиму спільного або автономного управління.

Таблиця 1

Порівняння інтегральних показників

Сценарій	Архітектура	$H \downarrow$	$\tau \uparrow$	$\bar{w} \uparrow$	$\lambda_h \downarrow$
Оборона	A	0,98	0,27	0,44	0,89
	B	0,79	0,60	0,65	0,69
	Proposed	0,58	0,81	0,80	0,50
Атака	A	1,03	0,25	0,43	0,91
	B	0,84	0,58	0,63	0,71
	Proposed	0,63	0,77	0,77	0,54
Евакуація	A	1,00	0,26	0,42	0,90
	B	0,81	0,59	0,64	0,70
	Proposed	0,60	0,79	0,78	0,52

Таблиця 2

Показники покращення (%) Відносно А

Сценарій	$\Delta H \downarrow$	$\Delta \tau \uparrow$	$\Delta \bar{w} \uparrow$	$\Delta \lambda_h \downarrow$
Оборона	-40,8 %	+200 %	+81,8 %	-43,8 %
Атака	-38,8 %	+208 %	+79,1 %	-40,7 %
Евакуація	-40,0 %	+204 %	+85,7 %	-42,2 %

Показники покращення (%) Відносно В

Сценарій	$\Delta H \downarrow$	$\Delta \tau \uparrow$	$\Delta \bar{w} \uparrow$	$\Delta \lambda_h \downarrow$
Оборона	-26,6 %	+35 %	+23,1 %	-27,5 %
Атака	-25,0 %	+32,8 %	+22,2 %	-23,9 %
Евакуація	-25,9 %	+33,9 %	+21,9 %	-25,7 %

Кількісний аналіз показує, що запропонована архітектура забезпечує зменшення ентропії на 25–40 % та підвищення довіри більш ніж у 2 рази порівняно з класичним підходом. При цьому середня зв'язність зростає на 20–85 %, а навантаження на оператора зменшується приблизно на 25–45 %, що підтверджує ефективність механізму адаптивного розподілу ролей.

Таким чином, результати симуляції підтверджують ключову гіпотезу дослідження: структуризація взаємодії відбувається у просторі цифрових двійників і забезпечується поєднанням оператора проєкції $\mathcal{P}_\Omega$, прогностного контуру $\mathcal{F}_{\text{sim}}$ та адаптивної матриці взаємодії $\mathbf{W}(t)$. Запропонована архітектура забезпечує стійке зменшення невизначеності, зростання довіри та оптимізацію ролі оператора навіть у складних умовах функціонування.

5. Висновки та напрями подальших досліджень

У роботі запропоновано математичну модель еволюції людино-машинного інтерфейсу, що описує перехід від стану емпіричного хаосу до структурованої взаємодії в системі «людина–робот». Ключовою особливістю підходу є представлення процесу взаємодії у просторі цифрових двійників, сформованому оператором проєкції $\mathcal{P}_\Omega$, що враховує вплив невизначеностей середовища.

Практична реалізація моделі у середовищі Gazebo підтвердила її ефективність. Отримані результати демонструють узгоджену динаміку інтегральних змінних для різних рівнів невизначеності середовища та підтверджують здатність системи адаптуватися до змін умов функціонування. Порівняння з базовими підходами показало суттєве зменшення ентропії, зростання довіри та зниження навантаження на оператора.

Наукова новизна роботи полягає у формалізації людино-машинного інтерфейсу як динамічної системи, у якій ентропія виступає інтегральною мірою невизначеності та впорядкованості розвитку взаємодії [9]. Запропонована модель, на відміну від існуючих, одночасно інтегрує: по-перше, ентропію як міру невизначеності; по-друге, довіру як інтегральний показник структурованості взаємодії; по-третє, середню зв'язність як характеристику узгодженості компонентів системи; по-четверте, вагу участі оператора як показник перерозподілу ролей у контурі керування.

Зазначений підхід передбачає введення простору цифрових двійників людини, роботизованої платформи та середовища, де формується розподіл сценаріїв, обчислюється ентропія та визначається матриця взаємодії. Сформульовано критерій переходу системи до структурованої взаємодії на основі порогових значень ентропії, довіри, зв'язності та участі оператора, що формує підґрунтя для симуляційної верифікації та подальшого проєктування адаптивних людино-машинних інтерфейсів. Встановлено аналітичний зв'язок між ентропією, довірою та структурованістю системи, а також введено інтегральний індекс ефективності як універсальний критерій оцінки систем людино-машинної взаємодії, для якого сформульовано умови забезпечення зростання довіри та інтегральної ефективності.

Практичне значення роботи полягає у можливості застосування запропонованої моделі для побудови адаптивних систем управління роботизованими комплексами в умовах

невизначеності. Архітектура, реалізована засобами середовища Gazebo, може застосовуватися як основа для розробки систем спільного управління, автономних роботів та кіберфізичних систем із високим рівнем адаптивності.

Незважаючи на отримані результати, запропонована модель має низку обмежень. Ефективність моделі залежить від якості оператора проєкції, що визначає точність цифрового двійника; за умов високого рівня невизначеності або обмежених спостережень похибки проєкції можуть суттєво впливати на подальші етапи обробки. Обчислювальна складність прогнозного контуру залишається значною, що обмежує застосування моделі у системах із жорсткими вимогами до реального часу без додаткових оптимізацій. Окремим обмеженням є чутливість до вибору гіперпараметрів, що потребує процедур адаптивного налаштування або навчання.

Перспективи подальших досліджень пов'язані з розвитком окремих компонентів моделі та її розширенням. Також доцільним є вдосконалення оператора проєкції на основі байєсівських та глибинних методів оцінювання стану, що дозволить зменшити вплив невизначеностей середовища. Іншим важливим напрямом є оптимізація прогнозного контуру шляхом застосування методів зменшення розмірності сценарного простору або адаптивного формування ансамблю. Окрему увагу слід приділити розширенню моделі на мультиагентні системи, де взаємодія відбувається не лише між людиною та роботом, але й між кількома автономними агентами; за такої постановки матриця взаємодії набуває складнішої структури, а процес формування довіри стає багатовимірним. Перспективним є також дослідження інтеграції запропонованого підходу з методами навчання з підкріпленням та великими мовними моделями, що дозволить реалізувати складніші когнітивні механізми прийняття рішень у системах людино-машинної взаємодії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. O'Neill T., McNeese N., Barron A., Schelble B. Human–Autonomy Teaming: A Review and Analysis of the Empirical Literature // *Human Factors*. 2022. № 64 (5). P. 904–938. DOI: 10.1177/0018720820960865.
2. Lee J. D., See K. A. Trust in Automation: Designing for Appropriate Reliance // *Human Factors*. 2004. № 46 (1). P. 50–80. DOI: 10.1518/hfes.46.1.50_30392.
3. Hancock P. A., Billings D. R., Schaefer K. E., Chen J. Y. C., de Visser E. J., Parasuraman R. A Meta-Analysis of Factors Affecting Trust in Human–Robot Interaction // *Human Factors*. 2011. № 53 (5). P. 517–527. DOI: 10.1177/0018720811417254.
4. Krupas M., Kajati E., Liu C., Zolotova I. Towards a Human–Centric Digital Twin for Human–Machine Collaboration: A Review on Enabling Technologies and Methods // *MDPI. Sensors*. 2024. URL: <https://doi.org/10.3390/s24072232>.
5. Firmino de Souza D., Sousa S., Kristjuhan–Ling K., Dunajeva O., Roosileht R., Pentel A., Möttus M., Can Özdemir M., Gratšjova Ž. Trust and Trustworthiness from Human–Centered Perspective in Human – Robot Interaction (HRI) – A Systematic Literature Review // *MDPI. Electronics*. 2025. № 14 (8). P. 1557. URL: <https://doi.org/10.3390/electronics14081557>.
6. Roesler E., Vollmann M., Manzey D., Onnasch L. The dynamics of human-robot trust attitude and behavior — Exploring the effects of anthropomorphism and type of failure // *Computers in Human Behavior*. 2024. V. 150. P. 108008. URL: <https://doi.org/10.1016/j.chb.2023.108008>.
7. Chauhan H., Jang Y., Jeong I. Predicting human trust in human-robot collaborations using machine learning and psychophysiological responses // *Advanced Engineering Informatics*. 2024. V. 62. Part B. P. 102720. URL: <https://doi.org/10.1016/j.aei.2024.102720>.
8. Li J., Zhu E., Lin W., Yang S. X., Yang S. A novel digital twins-driven mutual trust framework for human-robot collaborations // *Journal of Manufacturing Systems*. 2025. V. 80. P. 948–962, URL: <https://doi.org/10.1016/j.jmsy.2025.04.009>.

9. Valavanis K. P. The Entropy Based Approach to Modeling and Evaluating Autonomy and Intelligence of Robotic Systems. *Journal of Intelligent & Robotic Systems*, 2018. DOI: 10.1007/s10846-018-0905-6.
10. de Visser E. J., Peeters M. M. M., Jung M. F. et al. Towards a Theory of Longitudinal Trust Calibration in Human-Robot Teams // *International Journal of Social Robotics*. 2020. № 12 (2). P. 459–478. DOI: 10.1007/s12369-019-00596-x.
11. Ramasubramanian A. K., Mathew R., Kelly M., Hargaden V., Papakostas N. Digital Twin for Human-Robot Collaboration in Manufacturing: Review and Outlook // *Applied Sciences*. 2022. № 12 (10). P. 4811. DOI: 10.3390/app12104811.
12. Coronado E., Ueshiba T., Ramirez-Alpizar I. G. A Path to Industry 5.0 Digital Twins for Human-Robot Collaboration by Bridging NEP+ and ROS // *Robotics*. 2024. № 13 (2). P. 28. DOI: 10.3390/robotics13020028.
13. Chen J. Y. C., Lakhmani S. G., Stowers K., Selkowitz A. R., Wright J. L., Barnes M. Situation Awareness-Based Agent Transparency and Human-Autonomy Teaming Effectiveness // *Theoretical Issues in Ergonomics Science*. 2018. № 19 (3). P. 259–282. DOI: 10.1080/1463922X.2017.1315750.
14. Бернацький А. П., Коваленко О. О. Адаптивне керування бойовим середовищем на основі просторово – часової ентропії // *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2025. № 7. С. 5–19. DOI: 10.58254/viti.7.2025.01.05.
15. Бернацький А. П., Радзівілов Г. Д., Фесенко О. Д. Метод адаптивного керування бойовим середовищем з кібернетичним контуром прогнозування // *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2025. № 8. С. 5–23. DOI: 10.58254/viti.8.2025.01.05.
16. Li W., Hu Y., Zhou Y., Pham D. T. Safe human-robot collaboration for industrial settings: a survey // *Journal of Intelligent Manufacturing*. 2024. № 35 (5). DOI: 10.1007/s10845-023-02159-4.
17. Mengacci R. et al. An Open-Source ROS-Gazebo Toolbox for Simulating Robots With Compliant Actuators // *Frontiers in Robotics and AI*. 2021. 8:713083. DOI: 10.3389/frobt.2021.713083.
18. Campagna G., Rehm M. A Systematic Review of Trust Assessments in Human-Robot Interaction // *ACM Transactions on Human-Robot Interaction*. 2025. № 14 (2). Article 30. DOI: 10.1145/3706123.
19. Krausman A. et al. Trust Measurement in Human–Autonomy Teams: Development of a Conceptual Toolkit // *ACM Transactions on Human-Robot Interaction*. 2022. № 11 (3). Article 33. DOI: 10.1145/3530874.

Надійшла до редколегії 27.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.853+004.056.5

д-р філософії, доцент Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Легкобит В. С. ORCID: 0000-0002-9118-4188 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ДВОРІВНЕВОЇ ОРГАНІЗАЦІЇ ЗНАНЬ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ КІБЕРЗАХИСТУ НА ОНТОЛОГІЧНІЙ ОСНОВІ

У контексті підвищення ефективності управління знаннями в інтелектуальних системах кіберзахисту (ІСК) вирішується завдання організації знань на основі онтології кіберзагроз із використанням таксономій MITRE ATT&CK, MITRE CAPEC та наборів даних від European Repository of Cyber Incidents (EuRepoC). Актуальність зазначеного обумовлена необхідністю оперативної інтеграції зростаючих обсягів отриманих даних про кібератаки з наявним семантичним ядром ІСК. До того ж, існуючі підходи до уніфікації та формалізації гетерогенних даних у домені кіберзахисту не забезпечують оперативної та контрольованої інтеграції нових знань у семантичне ядро повноцінного формування єдиного когерентного, семантично-інтероперабельного простору знань, натомість зосереджені виключно на поверхневій консолідації онтологічних ресурсів окремих постачальників, що супроводжується обмеженою гнучкістю масштабування та високим рівнем абстракції, який ускладнює відображення причинно-наслідкових зв'язків між елементами кіберзагроз. У зв'язку з цим, розроблено модель дворівневої організації знань в ІСК на онтологічній основі. Суть запропонованої моделі полягає у формалізації процесу контрольованої інтеграції динамічних потоків фрагментованих даних з домену кіберзахисту через процедуру контекстної узгодженості між динамічним і статичним рівнями на основі розрахунку комплексного показника готовності кандидатів у знання. Оцінка ефективності застосування запропонованої моделі проводилася шляхом автоматизованого послідовного надходження 36 824 векторів даних з 4 наборів даних (MITRE та EuRepoC). В результаті до онтології було додано 23 830 нових сутностей з середнім показником їх готовності до формалізації 0,76 та загальним показником узгодженості онтології на рівні 99 %, що свідчить про збереження здатності онтології підтримувати формування логічних висновків в межах поточного контексту при істотному збагаченні фактологічного змісту.

Ключові слова: дані, знання, організація знань, управління знаннями, онтології, кібератаки, кіберзахист, контекстна узгодженість, підтримка прийняття рішень.

V. Fesokha, V. Lehkobyт. A two-level model of knowledge organization in ontology-based cybersecurity systems

In the context of improving the effectiveness of knowledge management in intelligent cyber defense systems (ICDS), the task at hand is to organize knowledge based on a cyber-threat ontology using the MITRE ATT&CK and MITRE CAPEC taxonomies, as well as datasets from the European Repository of Cyber Incidents (EuRepoC). The relevance of this is driven by the need for rapid integration of the growing volumes of cyberattack data into the existing semantic core of the ICDS. Moreover, existing approaches to the unification and formalization of heterogeneous data in the cybersecurity domain do not ensure the rapid and controlled integration of new knowledge into the semantic core for the full-fledged formation of a single coherent, semantically interoperable knowledge space; but instead focus exclusively on the superficial consolidation of ontological resources from individual vendors, accompanied by limited scalability and a high level of abstraction, which complicates the representation of cause-and-effect relationships between elements of cyber threats. In this regard, a model of a two-level ontology-based knowledge organization in ICDS has been developed. The essence of the proposed model lies in formalizing the process of controlled integration of dynamic streams of fragmented data from the cyber defense domain through a procedure of contextual consistency between the dynamic and static levels based on the calculation of a comprehensive knowledge candidate readiness index. The effectiveness of the proposed model was evaluated through the automated sequential input of 36,824 data vectors from 4 datasets (MITRE and EuRepoC). As a result, 23,830 new entities were added to the ontology with an average formalization readiness index of 0.76 and an overall ontology consistency index of 99%, indicating that the ontology retains its ability to support the formation of logical inferences within the current context while significantly enriching its factual content.

Keywords: data, knowledge, knowledge organization, knowledge management, ontologies, cyberattacks, cybersecurity, contextual consistency, decision support.

Вступ. У сучасних умовах стрімкої еволюції способів реалізації кіберзагроз ІСК функціонують в середовищі високої інформаційної ентропії та безперервного надходження нових даних, де традиційні стратегії акумуляції та систематизації досвіду вичерпують свою ефективність. Протягом тривалого часу домінуючим підходом до інтеграції розрізнених даних у домені кіберзахисту був пошук ефективного способу створення універсальної онтології, яка

об'єднала б фізичні, когнітивні та соціальні аспекти кіберпростору [1]. Однак такий підхід часто призводить до теоретичного колапсу та категоріальних помилок, виявляючись надто жорстким для динамічних загроз.

У зв'язку з цим особливої актуальності набуває не лише побудова моделей знань в домені кіберзахисту, а й організація процесів їх формування, оновлення та використання в умовах безперервного надходження даних.

Постановка завдання в загальному вигляді. Організація знань в сучасних ІСК є одним із ключових етапів життєвого циклу управління знаннями, оскільки саме ступінь узгодженості елементів моделі знань забезпечує чітку категоризацію, швидкий пошук і доступ, полегшує інтеграцію, а також сприяє однозначному розумінню та ефективному використанню збережених знань. У контексті зазначеного залишається невирішеним завдання досягнення компромісу між здатністю до своєчасного регулярного оновлення моделі знань ІСК та забезпеченням якості і достовірності знань у процесі прийняття рішень, а також збереженням цілісності та консистентності знань під час їх оновлення, масштабування або трансформації структури моделі знань [2]. Зазначене обумовлює необхідність підвищення адаптивності моделей знань ІСК на онтологічній основі до безперервного надходження гетерогенних даних кіберрозвідки (Cyber Threat Intelligence, CTI) з урахуванням вимог до їхньої якості та достовірності у процесі інтеграції.

Аналіз попередніх досліджень та публікацій [3–14] вказує на необхідність розробки онтологій, що враховують різні аспекти організації та представлення знань у домені кіберзахисту, зокрема важливість інтеграції гетерогенних даних для покращення ситуаційної обізнаності та ефективність застосування когнітивних технологій та технологій штучного інтелекту/машинного навчання порівняно з експертами для вилучення ключових атрибутів предметної області з метою формування комплексного уявлення про поточний ландшафт кіберзагроз.

На сьогодні існує ряд загальнодоступних онтологій (CRATELO, STUCCO, UCO, MALOnt, WAVED Ontology) [3–7], які формують семантичну основу не лише для побудови enterprise CTI/Security Operations Center рішень, а й для проведення наукових досліджень за такими напрямками:

- підвищення рівня кіберситуаційної обізнаності [3–14] – формування цілісного, контекстуального розуміння поточного стану інформаційного середовища, активів, кіберзагроз та вразливостей з метою своєчасного виявлення, оцінювання та прогнозування кіберінцидентів;

- уніфікації гетерогенних даних і забезпечення узгодженого семантичного контексту [3–5; 7; 8; 12; 14] – узгодження, інтеграція та стандартизація даних, отриманих із різномірних джерел (баз вразливостей, мережевої телеметрії, системи виявлення вторгнень, звітних даних антивірусних систем тощо) у єдиному семантичному просторі з метою створення спільної моделі знань, у межах якої різні типи інформації матимуть єдине визначення, зв'язки та властивості;

- автоматизація вилучення та інтеграція знань [5; 9–11; 14] – автоматичне виявлення, формалізація та об'єднання релевантних фрагментів знань із різних джерел у єдину семантичну модель без участі або з мінімальним втручанням експертів;

- інтеграція принципів організації знань (Knowledge Organization) з технологічними перевагами представлення знань (Knowledge Representation) [3; 4; 7; 12] – поєднання методів систематизації знань, орієнтованих на класифікацію, таксономію та впорядкування понять із формальними технологіями їх подання, що забезпечують машинну обробку, логічне виведення та інтероперабельність;

– підвищення якості моделювання невизначеності [10; 11; 13; 14] – вдосконалення здатності онтологічних систем враховувати неповноту, неоднозначність або відсутність знань про події, об'єкти та зв'язки у сфері кіберзахисту.

Наведений огляд основних напрямків наукових досліджень щодо формалізації знань на онтологічній основі свідчить про значні досягнення у забезпеченні семантичного базису для уніфікації гетерогенних джерел даних для підвищення кіберситуаційної обізнаності. Водночас їх застосування у реальних умовах функціонування інформаційно-комунікаційних систем обмежено відсутністю ефективного механізму узгодження між динамічними потоками даних про кібератаки та статичною онтологічною моделлю знань. Так, у сучасних системах кіберзахисту інтеграція нових знань, як правило, відбувається лише після їх повної верифікації, що призводить до затримок у представленні актуального стану способів реалізації кіберзагроз. З іншого боку, використання сирих або частково оброблених даних без належного семантичного узгодження з існуючою моделлю знань породжує суперечності, знижує якість знань та ускладнює прийняття рішень. До того ж, наразі в галузі кіберзахисту не існує єдиної універсальної онтології, тоді як декілька загальновизнаних моделей знань, стандартів структурованого обміну даними та таксономій використовуються де-факто як онтологічні основи для організації знань у різних піддоменах.

Таким чином, виникає об'єктивне протиріччя між необхідністю оперативного використання динамічних даних з домену кіберзахисту та необхідністю забезпечення їх семантичної узгодженості при інтеграції в онтологічну модель знань.

У зв'язку з цим **метою статті** є розробка моделі організації знань для формалізації поетапної інтеграції даних у онтологію із контролем їх узгодженості в умовах інтенсивного поточкового надходження кіберрозвідданих, зберігаючи при цьому повноту доступної для інтерпретації експертом інформації.

Викладення основного матеріалу. Фактичні обмеження метаонтологічних підходів до представлення ландшафту кіберзагроз, зокрема таких як UCO та STUCCO [3; 7], ускладнюють не лише консолідацію гетерогенних даних, представлених у межах спеціалізованих моделей (CAPEC, CVE, CWE, MITRE ATT&CK, STIX) [6; 8], а й забезпечення належного рівня їх семантичної узгодженості та контрольованої інтеграції в єдину модель знань. Основною причиною цього є їх орієнтація на централізовану інтеграцію, що супроводжується обмеженою гнучкістю масштабування та високим рівнем абстракції, який ускладнює відображення причинно-наслідкових зв'язків між елементами кіберзагроз.

У зв'язку з цим доцільним є застосування федеративного підходу, що сформувався в межах розвитку Semantic Web та концепції Ontology alignment [15; 16] і передбачає збереження автономності окремих онтологій при їх узгодженні через систему семантичних відповідностей. Такий підхід забезпечує можливість встановлення коректних відповідностей між концептуально різнорідними сутностями, що надає можливість формувати узгоджений, семантично інтероперабельний простір знань без необхідності повного злиття моделей. На відміну від метаонтологічних реалізацій [3; 7], запропонована модель в кінцевому результаті орієнтована не лише на інтеграцію даних, а й на підтримку аналітичного представлення динаміки способів реалізації кіберзагроз, зокрема через явне врахування взаємозв'язків між кібератаками, вразливостями, цифровими артефактами та механізмами реагування, що є особливо важливим для прийняття рішень в умовах неповноти (фрагментації) інформації.

Архітектура запропонованої моделі передбачає наявність двох рівнів (статичного та динамічного), а також процедури контекстної узгодженості між ними, яка забезпечує прийняття рішень щодо формалізації даних про кібератаки, накопичених на динамічному рівні, як елементів статичної моделі знань (рис. 1).

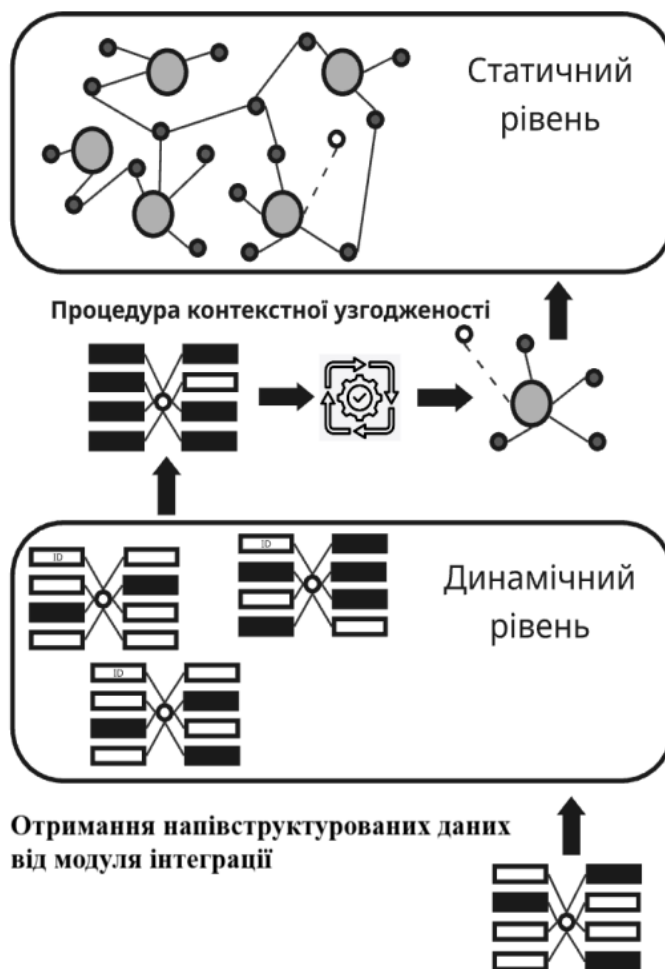


Рис. 1. Узагальнена графічна інтерпретація моделі

Статичний рівень моделі організації знань – федеративна онтологія, що описує домен кіберзахисту, де визначено основні сутності (кампанії, кібератаки, техніки, події тощо), процеси та зв'язки між ними, які у поєднанні формують достатньо повний цикл зловмисної активності у кіберпросторі. Кожному класу статичного рівня відведено специфічну роль у логіко-структурній конфігурації домену, тоді як семантичні зв'язки між ними задають чіткі правила взаємодії, що дає змогу логічно обробляти дані, робити висновки та поєднувати інформацію з різних джерел кіберрозвідки (OpenCTI, OSINT, Dark Web, IoC feeds, CERT, STIX/TAXII тощо). Зазначена онтологія охоплює повний цикл OODA (Observe-Orient-Decide-Act) [17] та побудована на основі підходу, орієнтованого на порушника [18]. На рисунку 2 представлено концептуальну схему статичного рівня моделі організації знань в домені кіберзахисту на онтологічній основі.

Vulnerability Context – експлуатацію вразливостей, *Detection* – спостережувані артефакти та індикатори, *Victim Context* – характеристики цільових об'єктів, а *Defense* – механізми протидії. Зазначена модульна організація узгоджується з підходами побудови кібербезпекових графів знань, у яких сутності та їх відношення структуруються відповідно до функціональних аспектів домену [19]. В таблиці 1 наведено класи онтології за функціональними групами [3; 5–7; 9; 19].

Таблиця 1

Опис класів онтології статичного рівня

Найменування класу	Науково-прикладне обґрунтування
Threat Actor	Центр атрибуції ініціатора цілеспрямованого деструктивного впливу на об'єкти критичної інформаційної інфраструктури
Campaign	Описує стратегічний контекст зловмисної активності через агрегацію відомостей про реалізацію кібератак, спрямованих проти конкретних цілей для досягнення певної мети
Attack Pattern	Абстракція множини технік, що реалізують спільний логічний механізм експлуатації вразливостей системи
Technique	Операційно-процедурна одиниця, яка формалізує конкретні технічні методи реалізації зловмисної активності і слугує точкою конвергенції між її стратегічним плануванням та технічними артефактами
Tactic	Концептуальний елемент ланцюга подій, що структурує життєвий цикл кібератаки
Malware	Програмне забезпечення, спеціально розроблене або модифіковане для порушення конфіденційності, цілісності чи доступності інформаційно-комунікаційних систем
Tool	Формалізує програмні утиліти, комерційні засоби або легітимне програмне забезпечення подвійного призначення, які використовуються зловмисником для підтримки кампаній, але не обов'язково є шкідливими за функціональним призначенням
Infrastructure	Репрезентує матеріально-технічну та технологічну основу забезпечення операційної спроможності проводити кібератаки. З точки зору детекції, інфраструктура є джерелом цифрових артефактів
Observable	Визначає атомарну одиницю цифрової реальності, емпіричний факт, що є продуктом виконання технічних процедур в межах інформаційної інфраструктури
Indicator	Певний набір закономірностей, що формалізує логіку детекції та інтерпретації окремого емпіричного факту як свідчення зловмисної активності
Weakness	Репрезентує фундаментальний рівень абстракції першопричин технічного ризику, які за певних умов можуть призвести до появи вразливостей
Vulnerability	Формалізує сукупність дефектів конкретного програмно-апаратного забезпечення, яка визначає схильність системи до потенційного деструктивного впливу
Exploit	Формалізує активний інструментальний компонент, що використовує вразливості для реалізації деструктивного впливу
Victim Context	Формалізує об'єкти шкідливого впливу та забезпечує стратегічний рівень аналізу загроз через ідентифікацію цілей зловмисника з урахуванням специфічних ризиків для окремих галузей та геополітичної обстановки
Course Of Action	Репрезентує рекомендаційний компонент онтології, спрямований на нейтралізацію загроз та мінімізацію потенційних збитків
Reference	Виконує роль позаієрархічної сутності, що забезпечує епістемологічну цілісність та фактологічну підтримку верифікації знань про кіберзагрози.

Динамічний рівень є операційним каркасом онтології статичного рівня та визначає спосіб перетворення отриманих сирих даних з домену кіберзахисту у формалізовані знання. Так, вхідна інформація про кібератаки в якості кандидатів у формалізовані знання представляється у вигляді множини іменованих підграфів $\{G_1, G_2, \dots, G_n\}$, структура яких узгоджена з класами та відношеннями статичного рівня запропонованої моделі. При цьому підграфи можуть містити неповні, суперечливі або слабоструктуровані дані, що потребують подальшої обробки. Кожен іменований підграф G_i інтерпретується як кандидат на екземпляр відповідного класу онтології та включає фактологічне ядро (сукупність предикатів, що описують сутність та її зв'язки) і метадані (відомості про джерело даних, хронологічні анотації, рівень довіри) з метою подальшого аналізу походження інформації, оцінки її персистентності та забезпечення можливості ретроспективного відстеження змін.

Інтеграція підграфів до статичного рівня здійснюється через комплексну оцінку якості:

- *на рівні предикатів* – перевірка коректності, несуперечливості та семантичної валідності окремих фактів (табл. 2) [20–23];
- *на рівні підграфа* – оцінка структурної цілісності, узгодженості зв'язків та повноти опису (табл. 3) [20–23].

Таблиця 2

Показники якості даних про кібератаки на рівні окремих предикатів

Найменування	Позначення	Практичний сенс	Одиниця виміру	Референтні значення
Надійність	r_s	Апріорна оцінка джерела даних, що базується на минулому досвіді	Коефіцієнт (0,0–1,0)	[0,8–1,0] – висока; [0,5–0,7] – середня; < 0,5 – сумнівне джерело
Вірогідність	p_v	Внутрішній статус факту, визначає міру, до якої дані вважаються істинними	Коефіцієнт (0,0–1,0)	[0,9–1,0] – перевірено аналітиком; [0,7–0,9] – технічний факт; [0,5–0,7] – припущення системи
Впевненість	c_p	Апостеріорна оцінка значення предикату, що обчислюється на основі довіри до джерела та міри істинності даних	Коефіцієнт (0,0–1,0)	[0,8–1,0] – висока; [0,5–0,7] – середня; < 0,5 – сумнівний факт
Кардинальність	a_p	Потужність множини унікальних джерел, які надали різні значення предикату	Ціле число	1 – однозначність; > 1 – наявність семантичного конфлікту
Рівень короборації	k_p	Потужність множини унікальних джерел, які надали ідентичні значення предикату	Ціле число	1 – гіпотеза; > 1 – шлях до консенсусу

Таблиця 3

Показники якості даних про кібератаки на рівні іменованого підграфа

Найменування	Позначення	Одиниця виміру	Як враховує рівень предикатів
Точність семантичної класифікації	A_G	Коефіцієнт (0,0–1,0)	Міра відповідності між значеннями полів вхідного фрагмента даних та формальними обмеженнями предикатів (семантичною сигнатурою) обраного класу онтології статичного рівня
Агрегована впевненість	$Conf_G$	Коефіцієнт (0,0–1,0)	Середньозважене значення впевненості всіх предикатів підграфа
Структурна повнота	$Compl_G$	Коефіцієнт (0,0–1,0)	Відношення фактично заповнених значеннями предикатів до обов'язкового набору предикатів, передбаченого семантичною сигнатурою класу

Найменування	Позначення	Одиниця виміру	Як враховує рівень предикатів
Логічна узгодженість	$Cons_G$	Коефіцієнт (0,0–1,0)	Агрегує показники кардинальності кожного предикату та визначає ступінь потенційного впливу на семантичну цілісність наявної моделі знань
Темпоральна релевантність	T_G	Коефіцієнт (0,0–1,0)	Відображає результат впливу часу на цінність накопичених фактів на рівні предикатів

Для кожного іменованого підграфа G_i передбачено використання унікального ідентифікатора $TYPE_{ID}$, що забезпечує уникнення дублювання даних про кібератаки. Ідентифікатор генерується на основі детермінованого відбору та канонізації значень стабільних предикатів семантичної сигнатури відповідного класу онтології, їх уніфікованої серіалізації та обчислення криптографічної хеш-функції [24].

Семантична сигнатура – це структурована специфікація об'єктних і функціональних властивостей певного класу, яка визначає ступінь відповідності фрагмента вхідних даних екземпляру цього класу. У межах запропонованого підходу кожна семантична сигнатура поділяється на обов'язкові, рекомендовані та опціональні предикати відповідних класів онтології статичного рівня шляхом застосування системи ваг, що надає можливість гнучко оцінювати критичність кожної прогалини в майбутніх знаннях. Наприклад, відсутність значень обов'язкових предикатів не лише знижує показник повноти, а й безпосередньо впливає на агреговану впевненість всього іменованого підграфа. Це гарантує, що навіть технічно бездоганні, але позбавлені контексту фрагментовані дані залишатимуться на динамічному рівні в статусі кандидата.

З метою уникнення впливу на описану модель знань потенційно небажаних проявів інтеграції шкідливих даних (отруєння, дезінформація, маніпуляції контекстом та семантичне спотворення) запропоновано введення багатоетапної процедури контекстної узгодженості між статичним та динамічним рівнями.

Процедура контекстної узгодженості.

Етап 1. Семантична обробка отриманих даних.

На вхід динамічного рівня надходить фрагмент напівструктурованих даних СТІ d_{in} , який визначається наступним аналітичним виразом (1):

$$d_{in} = \{ \{ \langle key_j, v_j \rangle \} \in P_{in}, r_s, p_v, t_{first}, M_{orig} \}, \quad (1)$$

де P_{in} – множина синтаксично коректних нормалізованих відомостей СТІ, в яких кожна пара $\langle key_j, v_j \rangle$ еквівалентна окремому предикату для S_{class} (2) – семантичної сигнатури певного класу онтології статичного рівня:

$$S_{class} = \langle N_{class}, \{ \langle key_i, w_i \rangle \} \rangle, \quad (2)$$

де N_{class} – найменування класу онтології статичного рівня; key_i – найменування предиката; w_i – ваговий коефіцієнт.

Для кожного класу онтології статичного рівня семантична сигнатура визначає набір предикатів з ваговими коефіцієнтами (обов'язкові $w_i = [0,8-1,0]$, рекомендовані $w_i = [0,6-0,8]$ та опціональні $w_i = [0,1-0,6]$), які використовуються для вибору конкретної сигнатури відносно фрагменту вхідних даних. Сукупність предикатів з найвищими ваговими коефіцієнтами ($w_i \geq 0,9$) формують семантичний якор v_{anchor} , на підставі якого можливо з високою ймовірністю визначити, на основі якої семантичної сигнатури на динамічному рівні необхідно створити іменований підграф G_i . Обраний набір діапазонів вагових коефіцієнтів для обов'язкових, рекомендованих та опціональних предикатів, а також порогове значення $\geq 0,9$ для семантичного якоря не є визначеним у міжнародних стандартах або нормативних

документах. Однак вони узгоджується з широко розповсюдженими підходами до застосування вагових коефіцієнтів в онтологічних і семантичних системах [25; 26], а також зі стандартними конвенційними рівнями надійності у статистичних дослідженнях [27].

1.2. Ініціалізація іменованого підграфа.

Після реалізації семантичної класифікації вхідних даних відбувається генерація унікального ідентифікатора на основі найменування класу онтології статичного рівня та значень стабільних предикатів цього класу (3) [24]:

$$TYPE_{ID} = H \left(f_{can}(N_{class}) \parallel f_{can}(v_{anchor}) \right), \quad (3)$$

де H – хеш функція; v_{anchor} – значення семантичного якоря визначеної семантичної сигнатури; f_{can} – функція канонізації, представлена виразом (4):

$$x' = f_{can}(x) = f_{lowcase} \left(f_{trim}(f_{clean}(x)) \right). \quad (4)$$

Такий підхід дає змогу уникнути міжкласових колізій шляхом створення різних просторів імен для різних сутностей, зменшити час пошуку існуючих підграфів на динамічному рівні та забезпечити незмінність ідентифікатора при інкрементальному нарощуванні фактології кандидатів у знання.

Після генерації $TYPE_{ID}$ здійснюється запит до сховища унікальних ідентифікаторів з метою виявлення еквівалентів серед існуючих кандидатів у знання на динамічному рівні. Якщо $TYPE_{ID_{in}} \in \{TYPE_{ID_{exist}}\}$, то на динамічному рівні створюється структура, описана виразом (5):

$$G_{new} = \langle TYPE_{ID}, S_{class}, V_G, P \rangle, \quad (5)$$

де V_G – множина інтегральних показників кандидата у знання, які розраховуються на момент ініціалізації, та визначаються виразом (6); P – фактологічне ядро, що складається з векторів окремих предикатів та має вигляд (7):

$$V_G = \{A_G, Conf_G, Compl_G, Cons_G, T_G\}. \quad (6)$$

$$P = \bigcup_{p \in P_{in}} \{key_p : \langle v_p, V_p, M_p \rangle\}, \quad (7)$$

де key_p – найменування предиката; v_p – значення предиката; M_p – множина метаданих походження значення цього предиката; V_p – вектор показників якості даних рівня предикатів, що має вигляд (8):

$$V_p = \langle r_s, p_v, c_p, t_{first}, t_{last}, a_p, k_p \rangle, \quad (8)$$

де оцінка впевненості в істинності факту розраховується за формулою згідно з [28]: $c_p = r_s \times p_v$, а показники a_p та k_p отримують початкові значення, що дорівнюють одиниці.

Етап 2. Збагачення іменованого підграфа та обробка семантичних конфліктів.

2.1. Підтвердження отриманих даних про кіберінцидент.

У випадку коли $TYPE_{ID_{in}} \in \{TYPE_{ID_{exist}}\}$, можливі декілька сценаріїв розвитку подій. Якщо для знайденого еквівалентного кандидата у знання значення v_p окремого предиката

key_p співпадають між собою, тоді відбувається інкрементальне підсилення існуючого факту. Для кожного предикату p значення якого збіглося, відбувається оновлення вектора V_p , а саме:

- змінюється значення інкрементального лічильника унікальних підтверджень k_p на одиницю, за умови відмінності метаданих походження фактів;
- t_{first} – залишається незмінним;
- t_{last} – оновлюється до часу надходження поточного фрагмента;
- Δt – скидається, що веде до зростання релевантності;
- оцінка впевненості в істинності значення предикату обчислюється як імовірнісна сума попереднього значення та внеску від нового джерела (9) [29]:

$$c_p = 1 - (1 - c_{p, old}) \times (1 - (r_{s, new} \times p_{v, new})); \quad (9)$$

- a_p – залишається незмінною ($a_p = 1$), оскільки конфлікту не виявлено.

Оновлення одного або кількох предикатів за даним сценарієм запускає ланцюгову реакцію перерахунку всього вектора V_G :

- A_G – не змінюється, оскільки семантична класифікація підтверджується і підстави сумніватись в цьому відсутні;
- $Conf_G$ – завдяки збільшенню c_p оновленого предикату загальна довіра до об'єкта підвищується;
- $Compl_G$ – не змінюється, оскільки нові значення предикатів не додавались;
- $Cons_G \rightarrow 1$ – підтвердження існуючого значення без появи альтернатив зміцнює логічну цілісність;
- T_G – темпоральна релевантність підвищується завдяки оновленню показника t_{last} .

Таким чином, після підтвердження вже існуючих фактів підграф набуває вигляду (10):

$$G_{updated} = \langle TYPE_{ID}, S_{class}, V_G(Conf_G \uparrow, T_G \uparrow), P\{key_p : \langle v_p, V_p \uparrow \rangle\} \rangle. \quad (10)$$

2.2. Збагачення іменованого підграфа новими фактами про кіберінцидент.

Якщо для знайденого еквівалентного кандидата у знання G_i структура фактологічного ядра P або значення окремих предикатів v_p відрізняються від тих, що вже зберігаються, то відбувається або розширення фасетної структури підграфа або вирішення семантичного конфлікту. Розширення відбувається через включення нового вектора предикату (11):

$$P = P_{exist} \bigcup_{p \in P_{in}} \{key_{p, new} : \langle v_{p, new}, V_{p, new}, M_{p, new} \rangle\}, \quad (11)$$

де вектор $V_{p, new}$ отримує початкові значення, аналогічно до процедури формування нового підграфа. Додавання нового значення предиката суттєво змінює V_G кандидата у знання, особливо в контексті його повноти:

- A_G – перевіряється, якщо $key_{p, new} \in S_{class}$, то A_G залишається високим, в іншому випадку знижується;
- $Conf_G$ – змінюється, якщо значення c_p для нового факту вище за середнє значення всього підграфа, то загальна довіра підвищується, в іншому випадку – знижується;
- $Compl_G$ – зростає, це головний наслідок збагачення фактології;
- $Cons_G$ – залишається стабільною через відсутність семантичних конфліктів;
- T_G – оновлюється, оскільки новий факт стає причиною підвищення релевантності всього підграфа.

Таким чином, у результаті збагачення кандидата у знання новими фактами підграф набуває вигляду (12):

$$G_{enriched} = \langle TYPE_{ID}, S_{class}, V_G(Compl_G \uparrow T_G \uparrow), P \cup \{p_{new}\} \rangle. \quad (12)$$

2.3. Обробка суперечливих даних про кіберінцидент.

Виникнення семантичного конфлікту відбувається, коли для одного й того самого предиката в межах певної семантичної сигнатури $v_{p,new} \neq v_p$. Фактологічне ядро підграфа перетворюється в множину альтернативних значень, що включає унітарні та конфліктні вектори предикатів, забезпечуючи тим самим висококонкурентне середовище та набуває вигляду (13):

$$P = \{key_p : \{\langle v_{p1}, V_{p1}, M_{p1} \rangle, \langle v_{p2}, V_{p2}, M_{p2} \rangle, \dots, \langle v_{pn}, V_{pn}, M_{pn} \rangle\}\}. \quad (13)$$

Для кожного значення предиката v_{pn} розраховуються та встановлюються початкові значення показників якості даних V_{pn} , а також для всіх альтернатив key_p оновлюється значення a_p до числа, що дорівнює кількості альтернатив. Семантичний конфлікт суттєво знижує значення показника готовності, оскільки знижуються значення основних показників рівня підграфа $Cons_G$ та A_G , які безпосередньо впливають на узгодженість кандидата у знання G_i з наявною моделлю знань. Наявність суперечливих значень ключових предикатів ставить під сумнів точність семантичної класифікації S_{class} та суттєво знижує агреговану впевненість всього підграфа. Таким чином, після надходження альтернативних значень предикатів, що викликало виникнення локального семантичного конфлікту підграф має наступний вигляд (14):

$$G_{conflict} = \langle TYPE_{ID}, S_{class}, V_G(Cons_G \downarrow, A_G \downarrow), P \{key_p : \{\langle v_{p1}, V_{p1}, M_{p1} \rangle, \langle v_{p2}, V_{p2}, M_{p2} \rangle, \dots, \langle v_{pn}, V_{pn}, M_{pn} \rangle\}\} \rangle. \quad (14)$$

У цьому випадку виникнення навіть одного локального конфлікту унеможливає перехід кандидата G_i на рівень знань. Реалізація сценарію 2.1 відносно одного з конкуруючих значень предиката іменованого підграфа G_i сприятиме підвищенню показників якості даних рівня предикатів V_p та призведе до його остаточного домінування над іншими значеннями та перерахунку показників якості даних всього вектора V_G . У випадку перебування кандидата G_i на динамічному рівні протягом тривалого часу передбачається реалізація підходу “Людина в циклі” [30], коли експерт оцінює контекст конфліктної ситуації та приймає рішення щодо її усунення.

Етап 3. Прийняття рішення про підвищення кандидата G_i до рівня знання.

3.1. Оцінка готовності даних до набуття статусу формалізованих знань.

Процедура контекстної узгодженості отриманих вхідних даних з домену кіберзахисту з існуючою моделлю знань визначається як нелінійний ітеративний алгоритм обробки вхідних даних, покликаний оцінити ступінь семантичного резонансу на вході динамічного рівня, знизити рівень ентропії кандидатів у знання та ініціювати процедуру їх формалізації як повноцінних екземплярів відповідних класів онтології на підставі обчислення агрегованого показника готовності R_G (15):

$$R_G = (A_G \times Cons_G) \times (\alpha Compl_G + \beta Conf_G + \gamma T_G). \quad (15)$$

Оскільки не існує універсальних коефіцієнтів важливості показників якості даних, ваги α, β, γ у запропонованій моделі вводяться як контекстно-залежні коефіцієнти, що відображають вплив відповідних показників на прийняття рішень у конкретній ситуації. У цьому випадку $\alpha = 0,2, \beta = 0,5, \gamma = 0,3$, у зв'язку з тим, що сумнівне походження ідеально наповнених фрагментів даних може свідчити про факт дезінформації або наміру отруєння моделі, що не надає достатньої інформаційної цінності.

Для оцінки релевантності кіберрозвідданих T_G найбільш доцільним є сигмоїдальне згасання, оскільки для більшості загроз вони залишаються критично важливими протягом обмеженого проміжку часу, після чого їхня цінність стрімко падає, коли ІСК адаптуються під кібератаку або зловмисники змінюють її вектор [11]. Це дослідження показує, що широко вживана експоненціальна крива Еббінгауза часто поступається сигмоїдальній та інверсній функціям у моделюванні реальних процесів втрати актуальності. Розрахунок темпоральної релевантності на основі сигмоїдального згасання з урахуванням хронологічних метаданих рівня предикатів зводиться до наступного аналітичного виразу (16) [11]:

$$T_G = \frac{1}{1 + e^{-k(\min(\Delta t) - \tau)}}, \quad (16)$$

де $\Delta t = t_{now} - t_{last}$ – час з моменту останнього оновлення значення предикату; τ – горизонт актуальності спостереження, визначає момент коли актуальність починає різко спадати; k – коефіцієнт крутизни спаду, визначає, наскільки швидко факт втрачає релевантність за межами горизонту актуальності спостереження.

Розрахунок агрегованої впевненості $Conf_G$ здійснюється відносно наявної фактології без врахування відсутніх значень предикатів семантичної сигнатури (17) [31]:

$$Conf_G = \frac{\sum (\frac{\max(c_{pi})}{a_{pi}} \times w_i)}{\sum w_i}. \quad (17)$$

Структурна повнота $Compl_G$ відображає ступінь наповнення іменованого підграфа G_i доступною фактологією відносно еталонного набору даних, передбаченого семантичною сигнатурою S_{class} (18) [32]:

$$Compl_G = \frac{\sum n_{filled}}{\sum n_{ss}}, \quad (18)$$

де n_{filled} – кількість заповнених значеннями предикатів іменованого підграфа G_i ; n_{ss} – кількість предикатів, які передбачені семантичною сигнатурою S_{class} .

Наявність суперечливих значень у ключових полях ставить під сумнів точність семантичної класифікації S_{class} , тому розрахунок значення загального показника узгодженості $Cons_G$ здійснюється з урахуванням показників кардинальності доступних значень предикатів іменованого підграфа (19) [33]:

$$Cons_G = \frac{n_{ss}}{n_{filled}} \times \sum_{i=1}^{n_{filled}} \frac{1}{a_{pi}}. \quad (19)$$

Точність семантичної класифікації A_G відіграє важливу роль у розрахунку загального показника готовності R_G , оскільки саме від неї залежить наскільки високими будуть показники

повноти, впевненості та узгодженості. Логіка розрахунку ґрунтується на принципі ймовірнісного об'єднання незалежних свідчень, що є апроксимацією часткового випадку теорії Демпстера – Шафера [34], та має вигляд (20):

$$A_G = 1 - \prod_{i \in v_{anchor}} (1 - w_i). \quad (20)$$

Таким чином, узгоджені свідчення взаємно підсилюють одне одного, тоді як суперечливі зменшують точність класифікації через нормалізацію, що забезпечує інтуїтивно коректне агрегування незалежних джерел інформації в умовах неповноти та конфліктності даних.

Кожного разу, коли до іменованого підграфа G_i на динамічному рівні застосовується один із сценаріїв підтвердження або розширення наявної фактології, вирішення семантичних конфліктів, агрегований показник його готовності R_G до набуття статусу формалізованих знань перераховується та порівнюється із пороговим значенням. Позитивний результат порівняння ініціює процес формалізації фактологічного ядра P кандидата у знання G_i у відповідний набір RDF-триплетів (базова одиниця представлення знань у моделі Resource Description Framework) екземпляра відповідного класу онтології статичного рівня, що інтерпретується як перехід між її поточним та потенційно більш контекстуально насиченим станами. Формально модель організації знань описується наступним аналітичним виразом (21):

$$L_{stat}(j+1) = L_{stat}(j) \cup \{G_i \in L_{dyn}(j) : R_G(G_i) \geq \theta\}, \quad (21)$$

де L_{stat} – множина формалізованих знань до моменту набуття кандидатом у знання значення показника готовності $\theta_{min} \geq 0,7$; L_{dyn} – множина кандидатів у формалізовані знання; G_j – іменований підграф, що репрезентує сукупність відомостей про кіберінцидент.

Враховуючи відсутність у міжнародних стандартах фіксованих числових значень порогів щодо якості даних, зокрема в [20], у яких значення визначаються контекстно як мінімальний рівень, достатній для практичного використання знань у процесах прийняття рішень. Порогове значення $\theta_{min} = 0,7$ обрано як емпіричний компроміс між вимогами до релевантності, впевненості, логічної узгодженості та повноти знань та відповідає загальноприйнятій практиці в інтелектуальному аналізі даних, де рівень 0,7 інтерпретується як межа переходу від слабких до операційно придатних оцінок знань [27].

Для забезпечення перевірки того, чи зберігається логічна узгодженість під час масштабування онтології статичного рівня передбачається поєднання двох механізмів онтологічного виведення (HermiT та Pellet) [35; 36]. Завдяки оптимізації детермінованих кроків виведення HermiT надає можливість перевірки цілісності всієї онтології, забезпечуючи виявлення порушення функціональних властивостей або циклічних визначень. Однак продуктивність HermiT має свою ціну, механізми інтерпретації виявлених розбіжностей часто менш деталізовані, що може ускладнити діагностику при інтеграції нових знань. Тому для вирішення виявлених конфліктів на локальному рівні передбачено застосування логічного висновувача Pellet, який безпосередньо вказує на конкретну множину аксіом, що призвели до нього, що призводить до зменшення часу обробки семантичних колізій. Таким чином, перевірка нового стану моделі знань $L_{stat}(j+1)$ реалізується як дворівневий процес, у якому HermiT та Pellet підтверджують логічну узгодженість, розраховану на основі (19).

Результати дослідження

Для оцінки ефективності запропонованої моделі було обрано набори даних [37–40]. Онтологічну основу для накопичення формалізованих знань реалізовано відповідно до концептуальної схеми, зазначеної на рисунку 2.

Критерії оцінки ефективності запропонованої моделі включали середні значення показників готовності R_G , узгодженості $Cons_G$, повноти $Compl_G$, агрегованої впевненості $Conf_G$ та темпоральної релевантності T_G для іменованих підграфів $\{G_1, G_2, \dots, G_n\}$, які були обрані для подальшої формалізації як екземпляри відповідних класів.

Суть експерименту полягала у реалізації контрольованої інтеграції динамічних потоків фрагментованих даних з [37–40] через процедуру контекстної узгодженості між динамічним і статичним рівнями на основі розрахунку комплексного показника готовності R_G кандидатів у знання G_i з подальшим визначенням ступеня впливу потенційного елемента моделі знань на здатність онтології підтримувати формування логічних висновків в межах поточного контексту.

Результати проведеного експерименту:

- загальна кількість ітерацій процедури контекстної узгодженості – 36 824;
- загальна кількість ініційованих сценарії підтвердження наявної фактології – 1 985;
- загальна кількість ініційованих сценарії розширення наявної фактології – 1 693;
- загальна кількість локальних конфліктів – 436;
- загальна кількість доданих до онтології нових сутностей – 23 830;
- загальна кількість кандидатів у формалізовані знання, які залишились у просторі динамічного рівня – 8 880;
- середнє значення показника готовності доданих до онтології нових сутностей – 0,76;
- середнє значення показника повноти доданих до онтології нових сутностей – 0,32;
- середнє значення показника впевненості доданих до онтології нових сутностей – 0,82;
- середнє значення показника узгодженості доданих до онтології нових сутностей – 0,99;
- середнє значення показника релевантності доданих до онтології нових сутностей – 0,99.

Варто зазначити, що перевірка логічної узгодженості онтології в результаті істотного збагачення її фактологічного змісту під час експерименту (засобами HermiT) показала відсутність порушень функціональних властивостей та циклічних визначень, тоді як засобами Pallet було виявлено незначну кількість локальних конфліктів. Аналіз діагностичних даних про виявлені конфлікти показав, що вони виникли внаслідок розбіжності у термінології опису певних аспектів кіберінцидентів у наборах MITRE та EuRepoC. Враховуючи ступінь гетерогенності вхідних даних, запропонована модель демонструє достатньо високий показник ефективності відбору кандидатів у формалізовані знання, що свідчить про її значний потенціал для сучасних ІСК.

На рисунку 3 представлено побудовану онтологію кіберзагроз після збагачення її фактологічного змісту у вигляді графа. З метою уникнення візуальної надмірності кількість екземплярів відповідних класів суттєво обмежена.

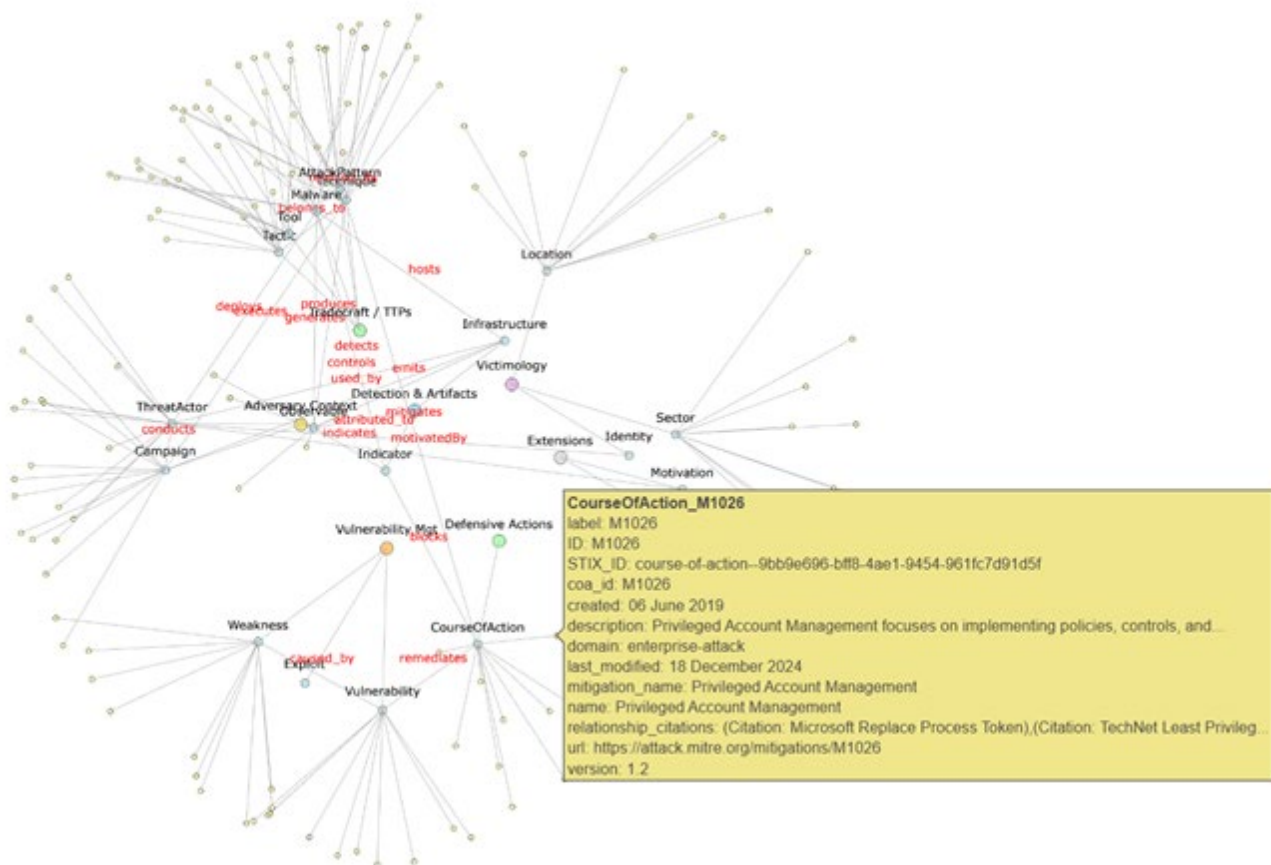


Рис. 3. Онтологія кіберзагроз після збагачення її фактологічного змісту у вигляді графа

Висновки та перспективи подальших досліджень. У статті запропоновано модель дворівневої організації знань в ІСК на онтологічній основі. На відміну від існуючих підходів, які переважно зосереджені на поверхневій консолідації онтологічних ресурсів окремих постачальників, запропонований підхід спрямований на формалізацію процесу контрольованої інтеграції динамічних потоків фрагментованих даних з домену кіберзахисту через процедуру контекстної узгодженості між динамічним і статичним рівнями на основі розрахунку комплексного показника готовності кандидатів у знання. Розроблено федеративну онтологію, структура якої узгоджується з підходами побудови кібербезпекових графів знань, у яких сутності та їхні відношення описані відповідно до функціональних аспектів домену. Реалізовано процедуру контекстної узгодженості як нелінійний ітеративний алгоритм обробки вхідних даних, покликаний оцінити ступінь семантичного резонансу на вході динамічного рівня, знизити рівень ентропії кандидатів у знання та ініціювати процедуру їх формалізації як повноцінних екземплярів відповідних класів онтології.

Результати дослідження показали, що незважаючи на істотне збагачення фактологічного змісту 23 830 новими сутностями з середнім показником їх готовності 0,76, показник узгодженості онтології залишився на рівні 99 %, з урахуванням виникнення незначної кількості локальних конфліктів. Отримані результати свідчать про ефективність запропонованого підходу щодо забезпечення семантичної та концептуальної цілісності онтології при безперервному надходженні гетерогенних даних кіберрозвідки з урахуванням вимог до їхньої якості та достовірності у процесі інтеграції.

Перспективним напрямком подальших досліджень є розробка моделі контекстно-орієнтованої інтеграції знань з елементами самонавчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Refereed Proceedings Papers. KM Conference 2025 (Knowledge Management, Cybersecurity, Learning, Information Technology). Siena, Italy, 2025. URL: https://www.iiakm.org/conference/proceedings/KM2025_RefereedProceedingsPapers.pdf.
2. Фесьоха В. В., Легкобит В. С., Чернявський Р. Г., Романенко С. О. Аналіз підходів до реалізації життєвого циклу управління знаннями в інтелектуальних системах кіберзахисту // Вісник Вінницького політехнічного інституту. 2025. № 4 (181). С. 95–107. URL: <https://doi.org/10.31649/1997-9266-2025-181-4-95-107>.
3. Syed Z., Padia A., Mathews M. L., Finin T., Joshi A. UCO: A Unified Cybersecurity Ontology. Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security. 2016. URL: https://ebiquity.umbc.edu/_file_directory_/papers/781.pdf.
4. Oltramari A., Cranor L. F., Walls R. J., McDaniel P. Building an ontology of cyber security // CEUR Workshop Proceedings. 2014. № 1304. P. 54–61. URL: https://ceur-ws.org/Vol-1304/STIDS2014_T08_OltramariEtAl.pdf.
5. Christian R., Dutta S., Park Y., Rastogi N. An Ontology-driven Knowledge Graph for Android Malware. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. 2021. P. 2435–2437. URL: <https://doi.org/10.1145/3460120.3485353>.
6. Akbar A., Rahman F., Singhal A., Khan L., Thuriasingham B. The Design and Application of a Unified Ontology for Cyber Security. Information Systems Security. 2023. P. 1–15. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=956387.
7. Obrst L., Chase P., Markeloff R. Developing an Ontology of the Cyber Security Domain // CEUR Workshop Proceedings. 2012. № 966. P. 49–56. URL: https://ceur-ws.org/Vol-966/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf.
8. Zhou J., Song X., Li Y., Gao Y., Zhang X. Building Real-Time Ontology Based on Adaptive Filter for Multi-Domain Knowledge Organization // IEEE Access. 2021. № 9. P. 66486–66497. URL: <https://doi.org/10.1109/ACCESS.2021.3076833>.
9. Satyapanich T., Ferraro F., Finin T. CASIE: Extracting Cybersecurity Event Information from Text. Proceedings of the AAAI Conference on Artificial Intelligence. 2020. № 34 (5). C. 8749–8757. URL: <https://doi.org/10.1609/aaai.v34i05.6401>.
10. Giunchiglia F., Bagchi M., Das S. From Knowledge Organization to Knowledge Representation and Back. 2024. URL: <https://doi.org/10.48550/arXiv.2401.11753>.
11. Sha A., Gu Z., Nunes B.P., Gu Z. Is there a better way to forget? Modelling memory decay in deep knowledge tracing. Knowledge-Based Systems. 2026. Vol. 332. P. 114884. URL: <https://doi.org/10.1016/j.knosys.2025.114884>.
12. Valero-Jorquera J. M., López Martínez A., Sánchez-Sánchez P.M., Navarro-Martínez D. Unlocking the Potential of Knowledge Graphs: A Cyber Defense Ontology for a Knowledge Representation and Reasoning System // Proceedings of the ACM Web Conference (WWW) / The Web Conf. 2024. URL: <https://doi.org/10.1145/3664476.3670916>.
13. Jin B., Kim E., Lee H., Bertino E., Kim D., Kim H. Sharing cyber threat intelligence: Does it really help? Proceedings of the 31st Network and Distributed System Security Symposium (NDSS 2024), San Diego, CA, USA, 2024. URL: <https://doi.org/10.14722/ndss.2024.24228>.
14. Gu Z., Lanti D., Corcoglioniti F., Montali M., Poggi A., Maccani M., Calvanese D., Xiao G. Ontology-based data federation and query optimization // Knowledge-Based Systems. 2025. Vol. 329 (Part A). P. 1–26. URL: <https://doi.org/10.1016/j.knosys.2025.114216>.
15. Wimmer H., Yoon V., Rada R. Applying Semantic Web Technologies to Ontology Alignment // International Journal of Intelligent Information Technologies. 2012. Vol. 8, no. 1. P. 1–9. URL: <https://doi.org/10.4018/JIIT.2012010101>.
16. Codescu M., Kuksa E., Kutz O., Mossakowski T., Neuhaus F. Ontohub: A semantic repository for heterogeneous ontologies. 2016. URL: <https://doi.org/10.48550/arXiv.1612.05028>.
17. OODA Loops // Iterum. URL: <https://iterum.co.uk/ooda-loops>.
18. Staves A., Gouglidis A., Hutchison D. An Analysis of Adversary-Centric Security Testing within Information and Operational Technology Environments // Digital Threats: Research and Practice. 2023. Vol. 4, no. 1. Article 14. P. 1–29. URL: <https://doi.org/10.1145/3569958>.
19. Sikos L. F. Cybersecurity knowledge graphs // Knowledge and Information Systems. 2023. Vol. 65, no. 3. P. 3511–3531. URL: <https://doi.org/10.1007/s10115-023-01860-3>.

20. ISO/IEC 25012: Data Quality model // ISO/IEC 25000 Standards Portal. URL: <https://iso25000.com/index.php/en/iso-25000-standards/iso-25012>.
21. DAMA-DMBOK®2 Revised Edition – FAQs // DAMA International. URL: <https://dama.org/dama-dmbok2-revised-edition-faqs>.
22. W3C Data Quality Vocabulary (DQV). Web Content – Data on the Web Best Practices: Data Quality Vocabulary // World Wide Web Consortium (W3C), 2016. URL: <https://www.w3.org/TR/vocab-dqv>.
23. NIST Cybersecurity Framework (CSF) // National Institute of Standards and Technology (NIST). URL: <https://www.nist.gov/cyberframework>.
24. The CBOR, dCBOR, and Gordian Envelope Book: Introduction. URL: <https://cborbook.com/introduction/cover.html>.
25. Atencia M., Borgida A., Euzenat J., Ghidini C., Serafini L. A Formal Semantics for Weighted Ontology Mappings. The Semantic Web – ISWC 2012 // Lecture Notes in Computer Science. 2012. № 7649. P. 17–33. URL: <https://disi.unitn.it/~p2p/RelatedWork/Matching/atencia2012c.pdf>.
26. Keikha M. M., Nematbakhsh M. A., Tork Ladani B. Structural Weights in Ontology Matching // International Journal of Web & Semantic Technology (IJWesT). 2013. № 4. P. 41–58. URL: <https://doi.org/10.48550/arXiv.1311.3800>.
27. Izah S.C., Sylva L., Hait M. Cronbach's Alpha: A Cornerstone in Ensuring Reliability and Validity in Environmental Health Assessment // ES Energy & Environment. 2023. Vol. 23. Article 1057. URL: <https://dx.doi.org/10.30919/ese1057>.
28. JDP 2-00 (4th Edition): Intelligence, Counter-intelligence and Security Support to Joint Operations. United Kingdom Ministry of Defence (MOD). 2023. URL: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.
29. Csenki A. Independent events in elementary probability theory // International Journal of Mathematical Education in Science and Technology. 2011. № 42 (6). P. 685–691. URL: <https://doi.org/10.1080/0020739X.2011.562313>.
30. Keet C. M., Grütter R. Toward a systematic conflict resolution framework for ontologies // Journal of Biomedical Semantics. 2021. № 12 (1). P. 15. URL: <https://doi.org/10.1186/s13326-021-00246-0>.
31. Tchakounté F., Faissal A., Atemkeng M., Ntyam A. A Reliable Weighting Scheme for the Aggregation of Crowd Intelligence to Detect Fake News // Information. 2020. № 11 (6). P. 319. URL: <https://doi.org/10.3390/info11060319>.
32. Ehrlinger L., Wöß W. A Survey of Data Quality Measurement and Monitoring Tools // Frontiers in Big Data. 2022. № 5. P. 850611. URL: <https://doi.org/10.3389/fdata.2022.850611>.
33. Bisewski K., Hashorva E., Shevchenko G. The harmonic mean formula for random processes // International Journal of Computer Mathematics. 2022. № 99 (4). P. 591–603. URL: <https://doi.org/10.1080/07362994.2022.2055574>.
34. Mercier D., Lefevre E. Introduction to Dempster-Shafer Theory of Belief Functions // Tutorial PFIA 2022. 2022. URL: https://davidmercier.fr/talks/2022_PFIA_BFintro.pdf.
35. Glimm B., Horrocks I., Motik B., Stoilos G., Wang Z. HermiT: An OWL 2 Reasoner // Journal of Automated Reasoning. 2014. Vol. 53. P. 245–269. URL: <https://doi.org/10.1007/s10817-014-9305-1>.
36. Sirin E., Parsia B., Cuenca Grau B., Kalyanpur A., Katz Y. Pellet: A practical OWL-DL reasoner // Journal of Web Semantics. 2007. № 5 (2). P. 51–53. URL: <https://doi.org/10.1016/j.websem.2007.03.004>.
37. MITRE. Enterprise ATT&CK Framework. Версія 18.1. 2026. URL: <https://attack.mitre.org/docs/attack-excel-files/v18.1/enterprise-attack/enterprise-attack-v18.1.xlsx>.
38. MITRE. Common Attack Pattern Enumeration and Classification (CAPEC). Версія 3.9. 2026. URL: https://capec.mitre.org/data/archive/capec_v3.9.zip.
39. EuRepoC. Global Dataset of Cyber Incidents. Версія 1.3.2. 2025. URL: <https://doi.org/10.5281/zenodo.14965395>.
40. EuRepoC. Global Dataset of Cyber Incidents. Версія 1.2. 2024. URL: <https://doi.org/10.5281/zenodo.11108195>.

Надійшла до редколегії 07.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 004.056.5

д-р філософії, доцент Фесьоха Н. О. ORCID: 0000-0002-9797-5589 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)
д-р філософії Нестеров О. М. ORCID: 0000-0001-5092-6205 (ВІТІ ім. Героїв Крут)

БАГАТОКРИТЕРІАЛЬНА МЕТОДИКА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІОТ-ПРИСТРОЇВ НА ОСНОВІ СИНТЕЗУ МЕТОДІВ АНР ТА TOPSIS

Стрімке зростання кількості підключених пристроїв Інтернету речей формує нові виклики у сфері кібербезпеки: відсутність уніфікованого інструментарію кількісного оцінювання захищеності ІоТ-пристроїв ускладнює прийняття обґрунтованих рішень під час їх проєктування, закупівлі, інтеграції та аудиту. У статті запропоновано теоретико-методичні засади багатокритеріальної методики оцінювання рівня захищеності ІоТ-пристроїв, що ґрунтується на гібридному синтезі методу аналітичного ієрархічного процесу та методу ранжування альтернатив за схожістю до ідеального рішення. Методика охоплює п'ять послідовних етапів: формування ієрархічної системи критеріїв безпеки на підставі вимог міжнародних стандартів ETSI EN 303 645 v3.1.3 та NIST IR 8425; попарне порівняння критеріїв за шкалою Сааті з перевіркою узгодженості суджень ($CR \leq 0,10$); нормалізацію матриці оцінок пристроїв; розрахунок зваженої нормалізованої матриці та інтегрального індексу захищеності методом TOPSIS; формування шкали інтерпретації результатів і рекомендацій. Система критеріїв включає сім вимірюваних показників, об'єднаних у чотири функціональні групи: автентифікація, захищена комунікація, управління оновленнями та захист даних. Кожен критерій прив'язано до конкретної вимоги стандарту ETSI EN 303 645 та NIST IR 8425, що забезпечує нормативну обґрунтованість методики. Повний математичний апарат методу – від формування матриці попарних порівнянь і розрахунку вектора пріоритетів до обчислення евклідових відстаней і коефіцієнта відносної близькості – викладено у вигляді покрокового алгоритму з відповідними формулами. Запропонована методика є практичним інструментом для задач безпекового аудиту, проєктування захищених ІоТ-систем та підтримки прийняття рішень при виборі ІоТ-пристроїв.

Ключові слова: Інтернет речей, безпека ІоТ, багатокритеріальне оцінювання, MCDM, АНР, TOPSIS, аналітичний ієрархічний процес, критерії захищеності, ETSI EN 303 645, NIST IR 8425, кібербезпека.

N. Fesokha, O. Symonenko, O. Nesterov. Multi-criteria method for evaluating IoT device security based on the integration of AHP and TOPSIS methods

The rapid growth in the number of connected Internet of Things devices creates new challenges in the field of cybersecurity: the lack of a unified quantitative assessment framework for IoT device security complicates informed decision-making during their design, procurement, integration, and auditing. This paper proposes the theoretical and methodological foundations of a multi-criteria approach for evaluating the security level of IoT devices based on a hybrid integration of the Analytic Hierarchy Process and the Technique for Order Preference by Similarity to Ideal Solution.

The proposed methodology consists of five sequential stages: (1) formation of a hierarchical system of security criteria based on the requirements of international standards ETSI EN 303 645 v3.1.3 and NIST IR 8425; (2) pairwise comparison of criteria using the Saaty scale with consistency verification ($R \leq 0.10$); (3) normalization of the device evaluation matrix; (4) construction of the weighted normalized matrix and calculation of the integrated security index using TOPSIS; and (5) development of an interpretation scale with corresponding recommendations.

The system of criteria includes seven measurable indicators grouped into four functional categories: authentication, secure communication, update management, and data protection. Each criterion is explicitly mapped to specific requirements of ETSI EN 303 645 and NIST IR 8425, ensuring the regulatory relevance of the methodology.

The complete mathematical framework – from pairwise comparison matrix construction and priority vector calculation to Euclidean distance computation and closeness coefficient estimation – is presented as a step-by-step algorithm with corresponding formulas. The proposed methodology serves as a practical tool for security auditing, secure IoT system design, and formalized decision support in the field of IoT cybersecurity.

Keywords: Internet of Things; IoT security; multi-criteria decision-making, MCDM, AHP, TOPSIS, analytic hierarchy process, security criteria, ETSI EN 303 645, NIST IR 8425, cybersecurity.

Постановка проблеми. Поняття “Інтернет речей” (Internet of Things, IoT), введене в науковий обіг Кевіном Ештоном у 1999 році, сьогодні описує глобальну екосистему фізичних об'єктів, оснащених датчиками, вбудованими обчислювальними модулями та засобами бездротової комунікації. За прогнозами аналітиків IoT Analytics, до 2030 року

загальна кількість підключених IoT-пристроїв у світі перевищить 29 мільярдів одиниць [1]. Такий масштаб розгортань формує принципово нову поверхню кіберзагроз: кожен підключений пристрій є потенційним вектором проникнення до корпоративних і домашніх мереж, джерелом витоку персональних даних або вузлом ботнет-інфраструктури.

Проблематика захищеності IoT визнана пріоритетною у міжнародній нормативній базі. У 2020 році Європейський інститут телекомунікаційних стандартів (ETSI) опублікував стандарт EN 303 645 “Кібербезпека для споживчих IoT-пристроїв”, оновлений у вересні 2024 року до версії 3.1.3 [2]. Паралельно у 2022 році Національний інститут стандартів і технологій США (NIST) опублікував NIST IR 8425 – профіль базових вимог кіберзахисту для споживчих IoT-продуктів [3]. На рівні Європейського Союзу з 2024 року набув чинності Акт про кіберстійкість (Cyber Resilience Act), що закріпив обов'язкові вимоги безпеки для підключених пристроїв на ринку ЄС [8]. Перераховані документи визначають вимоги до безпеки IoT-пристроїв, однак не містять уніфікованого кількісного інструментарію для порівняльного оцінювання конкретних пристроїв на відповідність цим вимогам.

Незважаючи на наявність міжнародних стандартів і нормативних вимог до безпеки IoT-пристроїв, на сьогодні відсутній уніфікований кількісний інструментарій, що дозволяє здійснювати їх порівняльне оцінювання за рівнем кіберзахищеності. Це ускладнює обґрунтований вибір пристроїв під час їх закупівлі, знижує об'єктивність результатів аудиту безпеки та обмежує застосування формалізованих методів прийняття рішень у сфері IoT. Таким чином, актуальною науковою проблемою є розроблення підходу до кількісного оцінювання рівня захищеності IoT-пристроїв.

Аналіз останніх досліджень та публікацій. Методи багатокритеріального прийняття рішень (MCDM) є апробованим математичним апаратом для вирішення задач комплексного оцінювання за множиною конкуруючих критеріїв. Гібридний підхід АНП-TOPSIS, що поєднує метод аналітичного ієрархічного процесу [9] і метод ранжування за схожістю до ідеального рішення [10], широко застосовується в задачах оцінювання безпеки інформаційних систем, вибору постачальників та управління ризиками [5–7]. Застосування цього апарату до задачі оцінювання захищеності IoT-пристроїв є науково обґрунтованим і перспективним напрямом дослідження.

Проблематика оцінювання захищеності IoT-систем досліджується у кількох взаємопов'язаних науково-прикладних напрямках, що охоплюють класифікацію вразливостей і загроз, розробку захисних архітектур, стандартизацію вимог безпеки та методи кількісного аналізу захищеності.

У сучасній науковій літературі виокремлюються три основних підходи до оцінювання захищеності IoT-пристроїв.

Перший підхід – якісний аудит на основі контрольних списків (checklist-based approach). Цей підхід базується на зіставленні характеристик пристрою з переліком вимог стандарту. Стандарт ETSI EN 303 645 v3.1.3 містить 33 обов'язкові та 35 рекомендованих вимог, згрупованих у 13 тематичних категорій [2]. OWASP IoT Security Testing Guide (версія 1.0, 2024) пропонує деталізований перелік тест-кейсів для практичного тестування на проникнення IoT-пристроїв [12]. Перевагою підходу є простота реалізації та прямий зв'язок з нормативними вимогами. Ключовим недоліком є відсутність агрегованого кількісного результату, що унеможливорює порівняльний аналіз кількох пристроїв та обмежує застосовність підходу до задач ранжування альтернатив.

Другий підхід – ризик-орієнтовані моделі. У роботі [4] запропоновано таксономію ризиків безпеки в IoT-середовищах, де виокремлено шість ключових складових ризику: апаратне забезпечення, мережева інфраструктура, операційні системи, програмне забезпечення, дані та людський фактор. Дослідники підкреслюють, що традиційні мережецентричні моделі безпеки є недостатніми для гетерогенних IoT-розгортань і пропонують перехід до активоцентричних підходів, де кожен фізичний пристрій

розглядається як самостійна одиниця оцінювання ризику. Хоча цей підхід враховує ширший спектр векторів загроз, результати оцінювання часто залишаються якісними, що ускладнює об'єктивне порівняння пристроїв.

Третій підхід – методи багатокритеріального прийняття рішень (MCDM). Систематичний огляд [6] засвідчує, що методи AHP, TOPSIS, SAW, VIKOR і COPRAS активно застосовуються в IoT-контексті для задач вибору та оцінювання. Зокрема, у роботі [5] запропоновано фреймворк ISA (Identified Security Attributes) для оцінювання безпеки пристроїв Інтернету медичних речей (IoMT), де AHP використовується для визначення вагових коефіцієнтів критеріїв безпеки, а TOPSIS – для ранжування альтернативних рішень. Авторами доведено, що двофазний підхід AHP-TOPSIS забезпечує вищу об'єктивність та відтворюваність оцінки порівняно з монокритеріальними підходами. У роботі [7] аналогічний підхід застосовано до оцінювання медичних IoT-пристроїв із використанням нечіткого AHP для моделювання лінгвістичної невизначеності в судженнях експертів.

Аналіз наукових праць дозволяє ідентифікувати кілька ключових прогалин у наявних дослідженнях. По-перше, більшість підходів MCDM орієнтована на вузькоспеціалізовані застосування (медичні пристрої, промислові системи) і не є узагальнено застосовними до широкого класу споживчих IoT-пристроїв. По-друге, наявні підходи, як правило, не прив'язані до актуальних міжнародних стандартів безпеки IoT (ETSI EN 303 645, NIST IR 8425), що обмежує їхню нормативну релевантність. По-третє, у жодній з розглянутих праць не запропоновано інтегровану шкалу інтерпретації значень індексу захищеності з рекомендованими діями для кожного рівня.

Наукове завдання полягає у розробленні та формалізації універсального кількісного підходу до оцінювання рівня захищеності IoT-пристроїв на основі інтеграції методів багатокритеріального прийняття рішень, який забезпечує одночасне врахування пріоритетності критеріїв безпеки, їхньої нормативної відповідності міжнародним стандартам та можливість об'єктивного порівняльного ранжування альтернатив.

Запропонована у цій статті методика дозволить усунути зазначені прогалини через розробку узагальненого, нормативно обґрунтованого підходу для широкого класу споживчих IoT-пристроїв із повним математичним апаратом та шкалою інтерпретації результатів.

Метою дослідження є розробка багатокритеріальної методики оцінювання захищеності IoT-пристроїв на основі синтезу методів AHP та TOPSIS, узгодженої з вимогами стандартів ETSI EN 303 645 v3.1.3 та NIST IR 8425, що дозволяє отримати кількісний відтворюваний рейтинг захищеності будь-якого споживчого IoT-пристрою.

Виклад основного матеріалу дослідження. Запропонована методика оцінювання захищеності IoT-пристроїв є п'ятиетапною ітеративною процедурою, що поєднує нормативно-орієнтований підхід до формування критеріїв та математично обґрунтований апарат MCDM для агрегованого оцінювання. Загальну архітектуру методики зображено у вигляді блок-схеми (рис. 1).

Методику побудовано з дотриманням таких принципів:

нормативна обґрунтованість – кожен критерій прив'язано до конкретної вимоги визнаного міжнародного стандарту;

вимірюваність – усі критерії оцінюються за чітко визначеною числовою шкалою;

відтворюваність – повний математичний апарат забезпечує можливість незалежного відтворення результатів;

масштабованість – методика застосовна до будь-якої кількості пристроїв і може бути розширена додатковими критеріями.

Вхідними даними методики є оцінки пристроїв за кожним із визначених критеріїв, отримані шляхом тестування на проникнення (penetration testing), аналізу технічної документації виробника або незалежного експертного оцінювання за шкалою від 1 до 5. Вихідними даними є ранжований список пристроїв за значенням інтегрального індексу

захищеності $CI \in [0; 1]$ та рекомендації щодо підвищення захищеності для кожного пристрою на основі шкали (табл. 6).

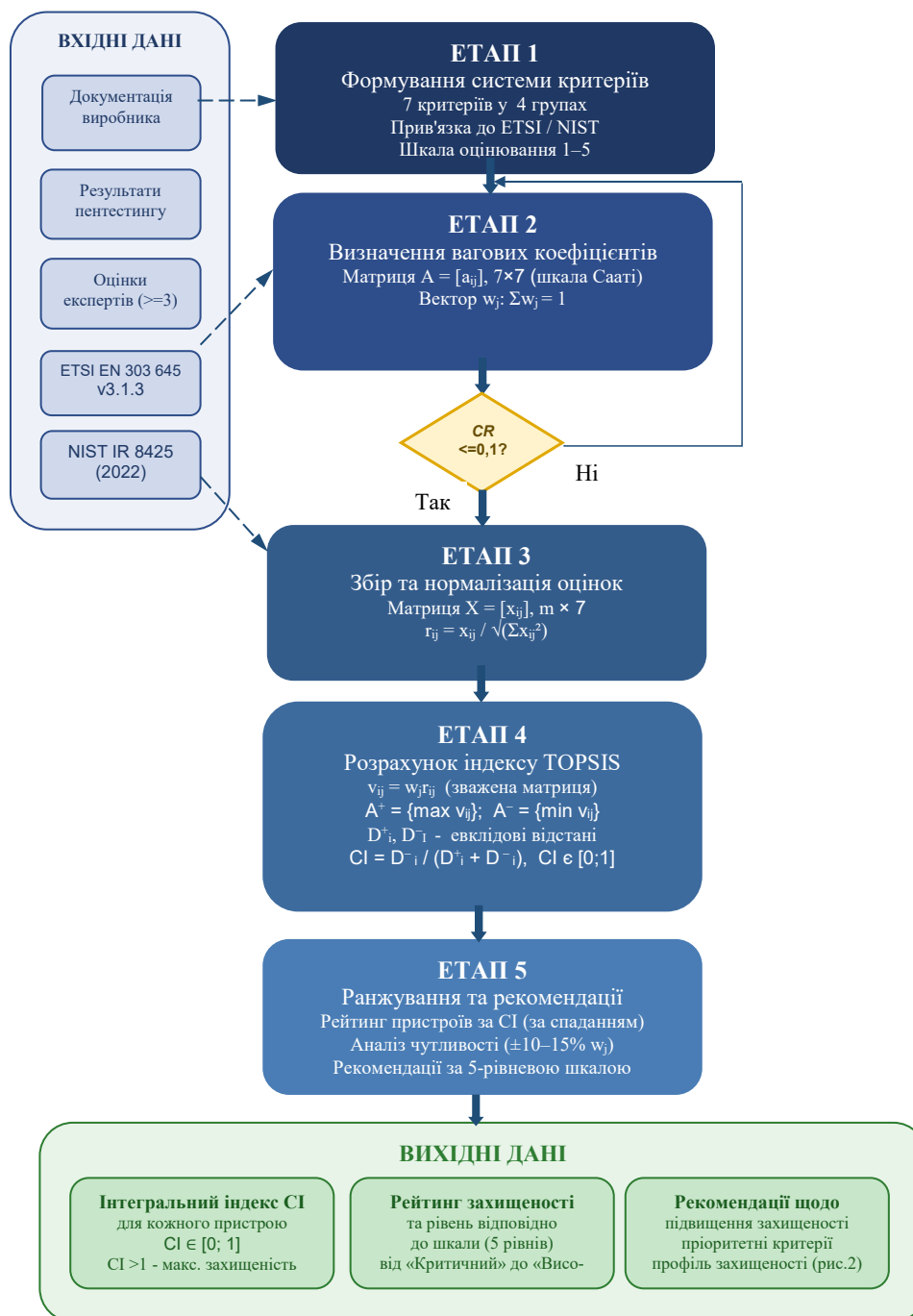


Рис. 1. Загальна архітектура п'ятиетапної методики оцінювання захищеності IoT-пристроїв

Система критеріїв є фундаментом всієї методики, оскільки від повноти та вимірюваності критеріїв безпосередньо залежить якість кінцевого результату. Критерії формуються на основі двох ключових міжнародних стандартів: ETSI EN 303 645 v3.1.3 та NIST IR 8425. ETSI EN 303 645, розроблений Комітетом технічних стандартів ETSI TC CYBER, є найбільш широко використовуваним міжнародним стандартом у сфері кібербезпеки споживчих IoT-пристроїв

та є технічною основою для регуляторних вимог Cyber Resilience Act ЄС [8]. NIST IR 8425 визначає базовий профіль вимог кіберзахисту для споживчих IoT-продуктів на ринку США.

У результаті систематичного аналізу вимог обох стандартів та виявлення їх перетину сформовано систему з семи критеріїв, об'єднаних у чотири функціональні групи (табл. 1). Кожен критерій відповідає таким вимогам до його включення в систему: об'єктивна вимірюваність за шкалою 1–5; наявність відповідної прямої вимоги у стандарті ETSI EN 303 645 або NIST IR 8425; суттєвий вплив на загальний рівень захищеності пристрою.

Таблиця 1

Система критеріїв оцінювання захищеності IoT-пристроїв

№ з/п	Код	Назва критерію	Відповідна вимога стандарту	Група	Шкала
1	K ₁	Захист від несанкціонованого доступу (МФА, управління сесіями)	ETSI EN 303 645, Вимога 5.1; NIST IR 8425, §3.1	Автентифікація	1–5
2	K ₂	Унікальність та складність облікових даних за замовчуванням	ETSI EN 303 645, Вимога 5.1-1; NIST IR 8425, §3.2	Автентифікація	1–5
3	K ₃	Шифрування каналів передачі даних (TLS 1.2/1.3, DTLS 1.2)	ETSI EN 303 645, Вимога 5.5; NIST IR 8425, §3.5	Комунікація	1–5
4	K ₄	Захищений механізм оновлення прошивки (цифровий підпис, rollback)	ETSI EN 303 645, Вимога 5.3; NIST IR 8425, §3.4	Оновлення	1–5
5	K ₅	Мінімізація поверхні атаки (відключені невикористані інтерфейси)	ETSI EN 303 645, Вимога 5.6; NIST IR 8425, §3.6	Архітектура	1–5
6	K ₆	Забезпечення конфіденційності та цілісності персональних даних	ETSI EN 303 645, Вимога 5.12; NIST IR 8425, §3.7	Захист даних	1–5
7	K ₇	Наявність задокументованої політики розкриття вразливостей (VDP)	ETSI EN 303 645, Вимога 5.2; NIST IR 8425, §3.9	Управління	1–5

Шкала оцінювання критеріїв: 5 – повна відповідність вимогам стандарту; 4 – відповідність із незначними недоліками; 3 – часткова відповідність; 2 – суттєві відхилення від вимог; 1 – повна невідповідність або відсутність механізму. До оцінювання рекомендується залучати сертифікованих фахівців у сфері кібербезпеки (Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP)).

Метод аналітичного ієрархічного процесу (АНП), розроблений Томасом Сааті у 1980 році [9], є одним із найбільш теоретично обґрунтованих і практично апробованих методів визначення відносних пріоритетів критеріїв у задачах MCDM. Метод здійснює декомпозицію складної задачі вибору на ієрархію підзадач і синтезує часткові судження в загальний вектор пріоритетів через систему попарних порівнянь.

Порівняння критеріїв між собою здійснюється за дев'ятибальною шкалою Сааті (табл. 2), яка дозволяє перетворити якісні судження експертів про відносну важливість критеріїв на числові значення.

Таблиця 2

Шкала попарних порівнянь Сааті для методу АНП

Значення a _{ij}	Вербальна оцінка	Пояснення
1	Рівнозначність	Обидва критерії однаково важливі для захищеності пристрою
3	Помірна перевага	Один критерій дещо важливіший; досвід підтверджує незначну перевагу

Значення a_{ij}	Вербальна оцінка	Пояснення
5	Суттєва перевага	Один критерій явно важливіший; перевага підтверджена практично
7	Значна перевага	Один критерій набагато важливіший; домінування добре доведене
9	Абсолютна перевага	Максимально можлива перевага одного критерію над іншим
2, 4, 6, 8	Проміжні значення	Компромісні судження між суміжними рівнями шкали

Повний алгоритм методу АНР у запропонованій методиці складається з шести кроків (табл. 3).

Таблиця 3

Покроковий алгоритм методу АНР для визначення вагових коефіцієнтів критеріїв

Крок	Операція	Математичний вираз / опис
1	Формування матриці попарних порівнянь	$A = [a_{ij}], n \times n; a_{ij} = \frac{1}{a_{ji}}; a_{ii} = 1.$ Елемент a_{ij} – відносна важливість критерію i над j за шкалою Сааті
2	Нормалізація матриці	$r_{ij} = \frac{a_{ij}}{\sum_i a_{ij}}$ (нормалізація по стовпцях)
3	Обчислення вектора пріоритетів	$w_j = \left(\frac{1}{n}\right) \sum_i r_{ij}$ (середнє по рядках нормалізованої матриці)
4	Розрахунок λ_{max}	$\lambda_{max} = \left(\frac{1}{n}\right) \sum_j \left[\frac{(A_w)_j}{w_j} \right]$, де A_w добуток матриці A на вектор w
5	Індекс узгодженості	$CI = \frac{\lambda_{max} - n}{n - 1}$
6	Коефіцієнт узгодженості	$CR = CI/R_n$ – умова прийнятності: $CR \leq 0,10$

Значення випадкового індексу RI , що використовується у формулі коефіцієнта узгодженості CR , залежить від розмірності матриці n та наведено у таблиці 4 [9].

Таблиця 4

Значення випадкового індексу RI за Сааті (для матриць різного розміру n)

n	1	2	3	4	5	6	7	8	9	10
R_n	0,00	0,00	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

Для застосування запропонованої методики ($n = 7$ критеріїв) використовується значення $R_7 = 1,32$. Якщо $CR > 0,10$, необхідно переглянути матрицю попарних порівнянь, виявити суперечливі судження та скоригувати їх. Рекомендується залучати до процедури порівняння від трьох до семи незалежних експертів у галузі безпеки IoT, а остаточну матрицю формувати як геометричне середнє індивідуальних матриць кожного експерта.

Вектор пріоритетів $w = (w_1, w_2, \dots, w_7)$, де $\sum w_j = 1$, є числовим відображенням відносної важливості кожного критерію безпеки в загальній оцінці захищеності пристрою. Критерій з найбільшим значенням w_j справляє найбільший вплив на підсумковий рейтинг TOPSIS. Вектор ваг встановлюється одноразово для методики та залишається незмінним протягом усього циклу оцінювання однотипних пристроїв. При суттєвій зміні нормативного контексту (наприклад, при виході нової версії стандарту ETSI EN 303 645) рекомендується повторна процедура АНР.

Матриця оцінок $X = [x_{ij}]$ розміром $m \times n$, де m – кількість досліджуваних пристроїв, $n = 7$ – кількість критеріїв, формується на основі зібраних оцінок. Нормалізація матриці необхідна для забезпечення порівняльності значень різних критеріїв та усунення впливу одиниць вимірювання. У методі TOPSIS застосовується векторна нормалізація (1):

$$r_{ij} = x_{ij} / \sqrt{\sum_i x_{ij}^2}, i = 1 \dots m, j = 1 \dots n, \quad (1)$$

де r_{ij} – нормалізована оцінка альтернативи (пристрою) i за критерієм j . Нормалізована матриця $R = [r_{ij}]$ має ту саму розмірність, що і вихідна матриця X , але всі значення є безрозмірними і задовольняють умові: $\sum_i r_{ij}^2 = 1$ для кожного j .

Метод TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) запропонований Хвангом та Юном у 1981 році [10]. Концептуальна основа методу полягає у тому, що найкраща альтернатива одночасно максимально наближена до ідеального позитивного рішення (еталон максимальної захищеності) та максимально віддалена від ідеального негативного рішення (еталон мінімальної захищеності). Повний алгоритм TOPSIS наведено у таблиці 5.

Таблиця 5

Покроковий алгоритм методу TOPSIS для ранжування IoT-пристроїв за захищеністю

Крок	Операція	Математичний вираз
1	Векторна нормалізація матриці рішень	$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_i x_{ij}^2}}$, де x_{ij} – оцінка альтернативи i за критерієм j
2	Зважена нормалізована матриця	$v_{ij} = w_j r_{ij}$, де w_j – вагові коефіцієнти (АНР)
3	Ідеальне позитивне рішення	$A^+ = \{v_j^+\} = \{\max(v_{ij})\}, j = 1 \dots n$ (максимум по кожному критерію)
4	Ідеальне негативне рішення	$A^- = \{v_j^-\} = \{\min(v_{ij})\}, j = 1 \dots n$ (мінімум по кожному критерію)
5	Відстань до A^+ (евклідова)	$D_i^+ = \sqrt{\sum_j (v_{ij} - v_j^+)^2}$
6	Відстань до A^- (евклідова)	$D_i^- = \sqrt{\sum_j (v_{ij} - v_j^-)^2}$
7	Інтегральний індекс захищеності	$CI = \frac{D_i^-}{(D_i^+ + D_i^-)}; CI \in [0, 1]$
8	Ранжування альтернатив	Альтернативи ранжуються за спаданням CI ; $CI \rightarrow 1$ означає максимальну захищеність

Ідеальне позитивне рішення A^+ відповідає гіпотетичному пристрою з максимальними зваженими оцінками за всіма критеріями; A^- – з мінімальними. Інтегральний індекс $CI = \frac{D_i^-}{(D_i^+ + D_i^-)}$ відображає відносну наближеність пристрою до еталона: $CI = 1$ – максимальна захищеність; $CI = 0$ – мінімальна.

Радарна діаграма на рисунку 2 ілюструє принцип побудови профілю захищеності пристрою: кожна вісь відповідає одному критерію $K_1 - K_7$; площа полігону візуалізує загальний рівень захищеності та дозволяє наочно ідентифікувати “слабкі місця” – критерії, за якими значення суттєво відхиляються від ідеального еталона.

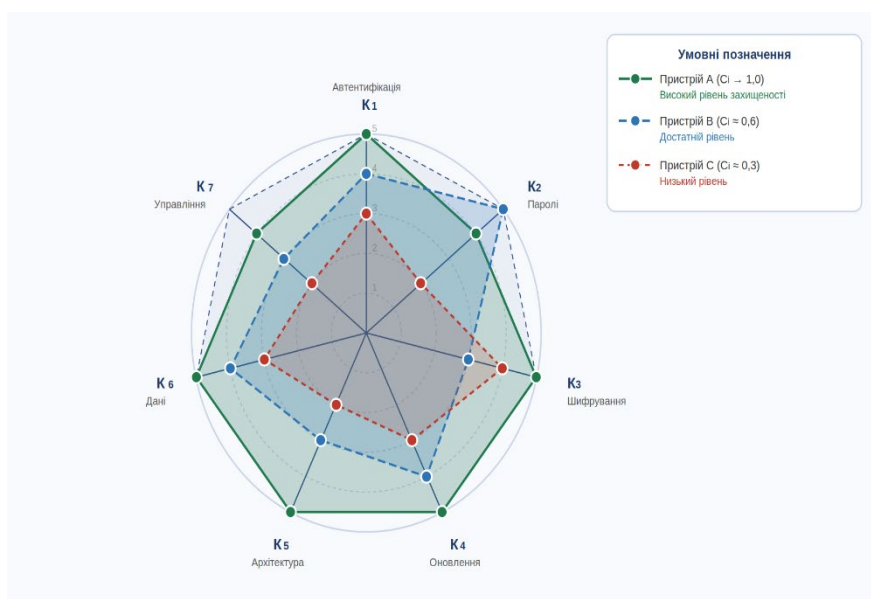


Рис. 2. Ілюстрація профілю захищеності IoT-пристроїв у вигляді радарної діаграми (К₁ – К₇)

Для практичного застосування результатів методики розроблено п'ятирівневу шкалу інтерпретації значень інтегрального індексу захищеності СІ з рекомендованими заходами для кожного рівня (табл. 6). Межі рівнів встановлено рівномірно в діапазоні [0; 1] з виділенням п'яти зон, що відповідають практично значущим рівням захищеності від критичного до високого.

Таблиця 6

Шкала інтерпретації значень інтегрального індексу захищеності СІ та рекомендовані заходи

Діапазон СІ	Рівень захищеності	Рекомендовані дії
0,80–1,00	Високий	Пристрій відповідає більшості вимог ETSI EN 303 645. Рекомендується моніторинг та планове оновлення
0,60–0,79	Достатній	Наявні окремі вразливості. Необхідне усунення виявлених недоліків протягом 3–6 місяців
0,40–0,59	Задовільний	Суттєві прогалини у безпеці. Потрібні термінові заходи з підвищення захищеності
0,20–0,39	Низький	Критичні вразливості. Рекомендується обмежити використання або замінити пристрій
0,00–0,19	Критичний	Пристрій не відповідає базовим вимогам безпеки. Необхідне негайне виведення з експлуатації

Для перевірки практичної придатності запропонованої методики проведено її апробацію на прикладі трьох умовних споживчих IoT-пристроїв: розумної камери відеоспостереження А₁, розумної IP-розетки А₂ та фітнес-браслета А₃. Вибір саме таких типів пристроїв зумовлений їхньою широкою поширеністю у побутовому сегменті та відмінностями у функціональному призначенні, архітектурі та профілі загроз (табл. 7).

Таблиця 7

Матриця вихідних оцінок трьох IoT-пристроїв за критеріями захищеності

Пристрій	К ₁	К ₂	К ₃	К ₄	К ₅	К ₆	К ₇
А ₁ – розумна камера відеоспостереження	5	4	5	4	3	4	3
А ₂ – розумна IP-розетка	3	2	3	2	4	3	2
А ₃ – фітнес-браслет	4	3	4	3	4	5	4

Для демонстрації роботи методики було сформовано матрицю вихідних оцінок трьох умовних IoT-пристроїв за сімома критеріями захищеності K_1 – K_7 . Значення оцінок було задано за п'ятибальною шкалою, де 1 відповідає повній невідповідності вимогам безпеки, а 5 – повній відповідності.

Пристрій A_1 (розумна камера відеоспостереження) характеризується високим рівнем захищеності каналів зв'язку та механізмів автентифікації, однак має певні обмеження щодо мінімізації поверхні атаки та документованої політики розкриття вразливостей. Пристрій A_2 (розумна IP-розетка) демонструє нижчі оцінки за більшістю критеріїв, зокрема щодо захисту облікових даних та безпечного оновлення прошивки. Пристрій A_3 (фітнес-браслет) займає проміжне положення, поєднуючи достатньо високий рівень захисту даних із помірними характеристиками в частині автентифікації та оновлень.

На першому етапі для системи критеріїв K_1 – K_7 методом АНР було визначено вагові коефіцієнти, що відображають відносну важливість кожного критерію у загальній оцінці захищеності. Для цього сформовано матрицю попарних порівнянь критеріїв за шкалою Сааті, на основі якої обчислено вектор пріоритетів $w = (w_1, \dots, w_7)$. Узгодженість експертних суджень перевірено шляхом обчислення коефіцієнта узгодженості CR . Оскільки $CR \leq 0,10$, матрицю визнано прийнятною для подальшого використання.

На другому етапі було сформовано матрицю оцінок пристроїв $X = [x_{ij}]$, де кожний елемент x_{ij} відображав оцінку i -го пристрою за j -м критерієм за шкалою від 1 до 5. Оцінювання було виконано на основі експертно заданих демонстраційних значень. Після цього до матриці X було застосовано процедуру TOPSIS: виконано нормалізацію, побудовано зважену нормалізовану матрицю, визначено позитивне і негативне ідеальні рішення, обчислено евклідові відстані до них та інтегральний індекс захищеності CI для кожного пристрою.

Отримані значення CI дали змогу здійснити ранжування альтернатив за рівнем захищеності та віднести кожен пристрій до одного з інтерпретаційних рівнів, наведених у таблиці 6. Крім того, аналіз зважених нормалізованих оцінок дав змогу виявити критерії, які найбільше вплинули на підсумковий результат і, відповідно, визначити пріоритетні напрями підвищення захищеності конкретного пристрою.

Наведена апробація демонструє, що серед розглянутих підходів запропонована методика АНР-TOPSIS найбільш повно забезпечує всі шість функціональних властивостей.

Таблиця 8

Вагові коефіцієнти критеріїв захищеності, визначені методом АНР

Критерій	Позначення	Вага w_j
Захист від несанкціонованого доступу	K_1	0,22
Унікальність та складність облікових даних	K_2	0,16
Шифрування каналів передачі даних	K_3	0,18
Захищений механізм оновлення прошивки	K_4	0,17
Мінімізація поверхні атаки	K_5	0,09
Захист персональних даних	K_6	0,12
Політика розкриття вразливостей	K_7	0,06
Сума		1,00

За результатами застосування методу АНР було отримано вектор вагових коефіцієнтів критеріїв $w = (0,22; 0,16; 0,18; 0,17; 0,09; 0,12; 0,06)$ (табл. 8). Найбільшу вагу отримали критерії, пов'язані з автентифікацією, захистом каналів зв'язку та безпечним оновленням, оскільки саме вони найбільшою мірою визначають стійкість IoT-пристрою до типових кіберзагроз. Меншу вагу було надано критеріям мінімізації поверхні атаки та наявності

політики розкриття вразливостей, які, хоча й є важливими, мають більш опосередкований вплив на безпосередній рівень технічної захищеності пристрою.

Після визначення вагових коефіцієнтів критеріїв було реалізовано процедуру оцінювання альтернатив методом TOPSIS. На основі матриці вихідних оцінок виконано векторну нормалізацію за кожним критерієм, після чого отримані значення було помножено на відповідні вагові коефіцієнти w_j . У результаті було сформовано зважену нормалізовану матрицю $V = [v_{ij}]$, яка стала основою для визначення ідеального позитивного та ідеального негативного рішень.

Таблиця 9

Нормалізована матриця оцінок IoT-пристроїв

Пристрій	K ₁	K ₂	K ₃	K ₄	K ₅	K ₆	K ₇
A ₁	0,707	0,743	0,707	0,743	0,469	0,566	0,557
A ₂	0,424	0,371	0,424	0,371	0,625	0,424	0,371
A ₃	0,566	0,557	0,566	0,557	0,625	0,707	0,743

Після визначення вагових коефіцієнтів критеріїв було реалізовано процедуру оцінювання альтернатив методом TOPSIS. На основі нормалізованої матриці (табл. 9) виконано формування зваженої нормалізованої матриці шляхом множення кожного елемента на відповідний ваговий коефіцієнт w_j (табл. 10).

Таблиця 10

Зважена нормалізована матриця оцінок IoT-пристроїв

Пристрій	K ₁	K ₂	K ₃	K ₄	K ₅	K ₆	K ₇
A ₁	0,156	0,119	0,127	0,126	0,042	0,068	0,033
A ₂	0,093	0,059	0,076	0,063	0,056	0,051	0,022
A ₃	0,124	0,089	0,102	0,095	0,056	0,085	0,045

Далі за кожним критерієм визначено компоненти ідеального позитивного рішення A^+ та ідеального негативного рішення A^- . Оскільки всі критерії у запропонованій методиці є критеріями вигоди, до складу A^+ включено максимальні значення зваженої нормалізованої матриці, а до складу A^- – мінімальні (табл. 11).

Таблиця 11

Ідеальне позитивне та ідеальне негативне рішення

Рішення	K ₁	K ₂	K ₃	K ₄	K ₅	K ₆	K ₇
A ⁺	0,156	0,119	0,127	0,126	0,056	0,085	0,045
A ⁻	0,093	0,059	0,076	0,063	0,042	0,051	0,022

На наступному кроці обчислено евклідові відстані кожної альтернативи до позитивного і негативного ідеальних рішень, а також інтегральний індекс захищеності CI. Чим більше значення CI, тим ближчою є альтернатива до ідеального рішення і тим вищим є її рівень захищеності (табл. 12).

Таблиця 12

Результати розрахунку інтегрального індексу захищеності методом TOPSIS

Пристрій	D _i ⁺	D _i ⁻	CI	Ранг	Рівень захищеності
A ₁ – розумна камера відеоспостереження	0,025	0,120	0,829	1	Високий
A ₂ – розумна IP-розетка	0,125	0,014	0,101	3	Критичний
A ₃ – фітнес-браслет	0,059	0,073	0,553	2	Задовільний

За результатами розрахунків найвище значення інтегрального індексу захищеності отримав пристрій A_1 – розумна камера відеоспостереження ($C_1 = 0,829$), що відповідає високому рівню захищеності. Це пояснюється високими оцінками за найбільш вагомими критеріями, зокрема захистом від несанкціонованого доступу, шифруванням каналів передачі даних та захищеним оновленням прошивки. Друге місце посів пристрій A_3 – фітнес-браслет ($C_3 = 0,553$), який належить до задовільного рівня захищеності. Незважаючи на високі показники за критерієм захисту даних, загальний результат цього пристрою знижується через помірні оцінки за критеріями автентифікації та оновлення. Найнижчий результат продемонстрував пристрій A_2 – розумна IP-розетка ($C_2 = 0,101$), що відповідає критичному рівню захищеності. Основними причинами такого результату є низькі оцінки за критеріями унікальності облікових даних, захищеного оновлення прошивки та політики розкриття вразливостей.

З метою підвищення достовірності отриманих результатів та перевірки масштабованості запропонованої методики було сформовано розширену вибірку з десяти споживчих IoT-пристроїв, що охоплюють різні класи застосувань: системи відеоспостереження, мережеве обладнання, носимі пристрої, елементи розумного дому та побутову техніку.

До набору альтернатив увійшли такі пристрої: A_1 – розумна камера відеоспостереження, A_2 – розумна IP-розетка, A_3 – фітнес-браслет, A_4 – розумний замок, A_5 – Smart TV, A_6 – розумна лампа, A_7 – Wi-Fi роутер, A_8 – розумний термостат, A_9 – голосовий асистент, A_{10} – розумний холодильник.

Оцінювання пристроїв здійснювалося за тією самою системою критеріїв K_1 – K_7 та шкалою 1–5, що забезпечує повну порівнянність результатів із попередньою апробацією. Вагові коефіцієнти критеріїв залишено незмінними, що дозволяє зберегти узгодженість моделі та коректність інтерпретації отриманих результатів.

Таблиця 13

Матриця оцінок 10 IoT-пристроїв за критеріями захищеності

Пристрій	K_1	K_2	K_3	K_4	K_5	K_6	K_7
A_1	5	4	5	4	3	4	3
A_2	3	2	3	2	4	3	2
A_3	4	3	4	3	4	5	4
A_4	5	4	4	4	3	4	3
A_5	4	3	4	3	3	4	2
A_6	2	2	3	2	3	2	1
A_7	5	5	5	4	4	4	4
A_8	4	3	4	4	3	4	3
A_9	3	3	4	3	3	3	2
A_{10}	3	2	3	3	2	3	2

Оцінки, наведені у таблиці 13, сформовано на основі узагальненого експертного аналізу функціональних можливостей пристроїв, типових реалізацій механізмів безпеки та відкритих результатів досліджень у сфері IoT-безпеки. Значення відображають узагальнений рівень відповідності пристроїв вимогам стандартів ETSI EN 303 645 та NIST IR 8425.

Таблиця 14

Результати оцінювання захищеності 10 IoT-пристроїв методом TOPSIS

Пристрій	CI	Ранг	Рівень захищеності
A_7 (роутер)	0,89	1	Високий
A_1 (камера)	0,83	2	Високий
A_4 (замок)	0,78	3	Достатній

Пристрій	CI	Ранг	Рівень захищеності
A_8 (термостат)	0,72	4	Достатній
A_3 (браслет)	0,66	5	Достатній
A_5 (TV)	0,58	6	Задовільний
A_9 (асистент)	0,51	7	Задовільний
A_{10} (холодильник)	0,39	8	Низький
A_2 (розетка)	0,21	9	Низький
A_6 (лампа)	0,08	10	Критичний

Отримані результати (табл. 14) демонструють чітку диференціацію IoT-пристроїв за рівнем захищеності. Найвище значення інтегрального індексу отримав Wi-Fi роутер (A_7), що пояснюється наявністю розвинених механізмів автентифікації, підтримкою сучасних криптографічних протоколів і регулярними оновленнями програмного забезпечення.

Високі позиції також займають камера відеоспостереження (A_1) та розумний замок (A_4), що характеризуються достатнім рівнем захисту каналів передачі даних і контролю доступу. Натомість пристрої нижчого цінового сегмента, зокрема розумна лампа (A_6) та IP-розетка (A_2), демонструють найнижчі значення індексу захищеності, що пов'язано з обмеженою реалізацією базових механізмів безпеки, відсутністю регулярних оновлень та слабкою політикою управління обліковими даними.

Аналіз результатів підтверджує, що найбільший вплив на підсумкове ранжування мають критерії, пов'язані з автентифікацією, шифруванням каналів зв'язку та механізмами оновлення програмного забезпечення, що узгоджується з отриманими ваговими коефіцієнтами методу АНР. Менш вагомі критерії відіграють допоміжну роль, формуючи комплексний профіль захищеності пристрою.

Отримані результати підтверджують практичну придатність методики забезпечувати обґрунтоване кількісне ранжування пристроїв, що може бути використано для підтримки прийняття рішень у задачах вибору IoT-обладнання, проведення безпекового аудиту та формування рекомендацій щодо підвищення рівня захищеності. Крім того, узгодженість результатів із попередньою апробацією підтверджує стабільність моделі та коректність застосування гібридного підходу АНР-TOPSIS.

Крім визначення загального рейтингу, методика передбачає аналіз внеску окремих критеріїв у підсумковий результат. Для ідентифікації “слабких місць” пристрою рекомендується побудова профілю захищеності – таблиці або радарної діаграми, що відображає зважені нормалізовані оцінки v_{ij} пристрою за кожним критерієм порівняно з відповідними значеннями A^+ та A^- . Критерії, за якими значення v_{ij} найбільш суттєво відхиляються від v_j^+ , є першочерговими об'єктами для заходів з підвищення захищеності.

Для забезпечення надійності результатів рекомендується також проводити аналіз чутливості: по чергово варіювати вагові коефіцієнти w_j у діапазоні $\pm 10\text{--}15\%$ від базових значень та перевіряти стійкість отриманого ранжування. Якщо ранжування пристроїв не змінюється при жодному з тестових сценаріїв, результати вважаються стійкими і придатними для прийняття рішень.

Для оцінювання переваг та обмежень запропонованої методики здійснено її порівняння з трьома найбільш поширеними підходами до оцінювання захищеності IoT-пристроїв (табл. 15):

якісний аудит на основі контрольних списків відповідно до ETSI EN 303 645;

ризик-матриця;

Common Vulnerability Scoring System (CVSS) – стандартизована методика кількісної оцінки вразливостей.

Таблиця 15

Порівняльний аналіз запропонованої методики АНР-TOPSIS з існуючими підходами

Характеристика	Checklist (ETSI EN 303 645)	Ризик-матриця	CVSS-оцінка	АНР-TOPSIS (запропонована)
Кількісний агрегований індекс	–	–	Частково	✓
Прив'язка до ETSI EN 303 645	✓	–	–	✓
Порівняльне ранжування пристроїв	–	–	–	✓
Врахування пріоритетності критеріїв	–	Частково	–	✓
Аналіз чутливості	–	–	–	✓
Відтворюваність результатів	✓	Частково	✓	✓

Як видно з таблиці 15, запропонована методика АНР-TOPSIS є єдиним підходом, що одночасно забезпечує всі шість розглянутих функціональних властивостей. Якісний checklist-підхід на основі ETSI EN 303 645 задовольняє вимогу нормативної прив'язки та відтворюваності, але не дозволяє отримати кількісний агрегований індекс і порівнювати пристрої між собою. Ризик-матриця враховує пріоритетність загроз лише частково і не пов'язана безпосередньо зі стандартом ETSI EN 303 645. CVSS забезпечує кількісну оцінку окремих вразливостей, але не призначений для оцінювання загального рівня захищеності пристрою.

Водночас, запропонована методика має певні обмеження. По-перше, якість вхідних оцінок пристроїв залежить від кваліфікації оцінювачів та повноти доступної технічної документації. По-друге, процедура попарного порівняння АНР є відносно трудомісткою при великій кількості критеріїв (понад 9), хоча для запропонованої системи з 7 критеріїв це не є суттєвим обмеженням. Перспективним напрямом розширення методики є застосування нечіткого АНР (Fuzzy АНР) для моделювання лінгвістичної невизначеності в судженнях експертів [7].

Таким чином, проведена розширена апробація підтверджує, що запропонована методика є масштабованою та придатною для оцінювання захищеності широкого класу IoT-пристроїв. На відміну від демонстраційного прикладу з обмеженою кількістю альтернатив, розширена вибірка дозволяє більш повно відобразити варіативність рівнів захищеності в реальних умовах та виявити стійкі закономірності впливу окремих критеріїв на підсумковий результат.

Наукова новизна дослідження полягає в розробці методики оцінювання захищеності IoT-пристроїв, що одночасно:

ґрунтується на актуальних міжнародних стандартах ETSI EN 303 645 v3.1.3 та NIST IR 8425;

застосовує математично обґрунтований апарат гібридного MCDM АНР-TOPSIS;

є придатною для широкого класу споживчих IoT-пристроїв;

містить шкалу інтерпретації результатів із практичними рекомендаціями.

Практична цінність методики полягає в її застосовності для: обґрунтованої закупівлі IoT-обладнання у корпоративному та державному секторах; проведення незалежного аудиту захищеності IoT-систем; проєктування нових IoT-рішень із врахуванням вимог безпеки на ранніх етапах.

Перспективи подальших досліджень: розширення системи критеріїв до повного охоплення вимог ETSI EN 303 645; застосування нечіткого АНР (Fuzzy АНР) для моделювання лінгвістичної невизначеності; розробка програмного інструменту автоматизації розрахунків; адаптація методики для промислових IoT-систем відповідно до стандарту ISA/IEC 62443.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. State of IoT – Spring 2023. Berlin: IoT Analytics GmbH, 2023. URL: <https://iot-analytics.com/number-connected-iot-devices>.
2. ETSI EN 303 645 V3.1.3 (2024-09). Cybersecurity for Consumer Internet of Things: Baseline Requirements. Sophia Antipolis: European Telecommunications Standards Institute, 2024. 72 p.
3. Fagan M., Megas K., Scarfone K., Smith M. IoT Core Baseline for Consumer IoT Products. NIST IR 8425. Gaithersburg: National Institute of Standards and Technology, 2022. DOI: <https://doi.org/10.6028/NIST.IR.8425>.
4. Al-Dhaqm A. et al. Security risk assessment in IoT environments: A taxonomy and survey // Computers & Security. 2025. Vol. 153. Article 104197. DOI: <https://doi.org/10.1016/j.cose.2025.104197>.
5. Khan H. U., Ali Y., Khan F. A. A features-based privacy preserving assessment model for authentication of internet of medical things (IoMT) devices in healthcare // Mathematics. 2023. Vol. 11, No. 5. P. 1197. DOI: <https://doi.org/10.3390/math11051197>.
6. Radulescu C. Z., Radulescu M. A. Hybrid group multi-criteria approach based on SAW, TOPSIS, VIKOR, and COPRAS methods for complex IoT selection problems // Electronics. 2024. Vol. 13, No. 4. P. 789. DOI: <https://doi.org/10.3390/electronics13040789>.
7. Ksibi S., Jaidi F., Bouhoula A. User-centric fuzzy AHP-based method for medical devices security assessment. In: Proceedings of the 15th International Conference on Security of Information and Networks (SIN). Sousse: IEEE, 2022. DOI: <https://doi.org/10.1109/SIN56466.2022.9970520>.
8. Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) // Official Journal of the European Union. 2024. L 2024/2847.
9. Saaty T. L. The analytic hierarchy process: planning, priority setting, resource allocation. New York: McGraw-Hill, 1980. 287 p.
10. Hwang C.-L., Yoon K. Multiple attribute decision making: methods and applications // Lecture Notes in Economics and Mathematical Systems. Vol. 186. Berlin: Springer, 1981. 259 p. DOI: <https://doi.org/10.1007/978-3-642-48318-9>.
11. Cîmpean D. A. et al. Security assessment of an Internet of Things device. In: Good practices and new perspectives in information systems and technologies. WorldCIST 2024 // Lecture Notes in Networks and Systems. Vol. 989. Cham: Springer, 2024. P. 261–272. DOI: https://doi.org/10.1007/978-3-031-60227-6_26.
12. OWASP IoT Security Testing Guide. Release 1.0. March 2024. URL: <https://owasp.org/blog/2024/03/01/iot-security-testing-guide>.
13. Sahoo S. K., Goswami S. S. A comprehensive review of multiple criteria decision-making (MCDM) methods: advancements, applications, and future directions // Decision Making: Advances. 2023. Vol. 1, No. 1. P. 25–48. DOI: <https://doi.org/10.31181/dma1120235>.
14. Alharbi A. et al. Selection of data analytic techniques by using fuzzy AHP TOPSIS from a healthcare perspective // BMC Medical Informatics and Decision Making. 2024. Vol. 24, No. 1. P. 240. DOI: <https://doi.org/10.1186/s12911-024-02651-8>.

Надійшла до редколегії 26.03.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

МЕТОД ПРІОРИТЕЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ ТЕХНОЛОГІЧНИХ СИСТЕМ ПРОМИСЛОВИХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЛЯ ПРОТИДІЇ ДЕСТРУКТИВНИМ КІБЕРАТАКАМ В УМОВАХ ОБМЕЖЕНИХ РЕСУРСІВ

У статті вирішується завдання забезпечення функціонування технологічних систем промислових об'єктів критичної інфраструктури в умовах обмежених ресурсів та постійно зростаючих кіберзагроз.

Під впливом поточних воєнних і соціально-економічних факторів ресурсне забезпечення промислових об'єктів критичної інфраструктури має тенденцію до скорочення та обмеження, що зумовлює необхідність оптимізації розподілу наявних ресурсів для реалізації заходів кібербезпеки, особливо по відношенню до такого критично важливого компоненту, як технологічна система.

Дослідження спрямоване на визначення ролі і місця запропонованого методу, його поетапного опису з відображенням чіткого й злагодженого алгоритму пріоритезації заходів кібербезпеки технологічних систем промислових об'єктів критичної інфраструктури для протидії деструктивним кібератакам в умовах обмежених ресурсів.

Описані підходи спираються на основи теорії управління ресурсами й елементи операційних досліджень, зокрема задачі розподілу, пріоритезації та оптимізації обмежених ресурсів. Разом з тим, метод дозволяє приймати управлінські рішення щодо кібербезпеки технологічних систем в умовах невизначеності. В якості математичного апарату для виконання одного з ключових підетапів методу, який дозволяє здійснити моделювання потенційних деструктивних кібератак на активи технологічної системи, запропоновано використати імітаційно-аналітичне структурне моделювання із застосуванням кольорових сіток Петрі. Для вирішення завдань окремих підетапів методу, що зумовлюють прийняття рішень в умовах невизначеності, обрано PERT-підхід.

Практична цінність використання методу полягає у можливості його застосування для підтримки прийняття управлінських рішень під час формування Плану реалізації заходів кібербезпеки для протидії деструктивним кібератакам на технологічні системи промислових об'єктів критичної інфраструктури на рік.

Таким чином, метод враховує низку реальних практичних факторів, які є необхідними елементами для визначення найбільш ресурсооптимальних і ефективних заходів кібербезпеки для протидії деструктивним кібератакам на технологічну систему промислового об'єкта критичної інфраструктури в умовах обмежених ресурсів та враховує обґрунтування прийнятих рішень з їхнім відповідним документальним оформленням.

Ключові слова: кібербезпека, метод пріоритезації заходів кібербезпеки, промислові об'єкти критичної інфраструктури, технологічна система, ресурсна обмеженість, управління ресурсами.

A. Khaver. Method for prioritizing cybersecurity measures in technological systems of industrial critical infrastructure facilities to counter destructive cyberattacks under resource constraints

This paper addresses the problem of ensuring the reliable functioning of technological systems of industrial critical infrastructure facilities under conditions of limited resources and continuously increasing cyber threats. Under the influence of ongoing military and socio-economic factors, the resource provision of industrial critical infrastructure facilities tends to decrease, which necessitates the optimization of available resource allocation for the implementation of cybersecurity measures, particularly with respect to such a critically important component as the technological system.

The study is aimed at defining the role and place of the proposed method, as well as providing its step-by-step description through a coherent and structured algorithm for prioritizing cybersecurity measures in technological systems of industrial critical infrastructure facilities to counter destructive cyberattacks under resource constraints.

The proposed approaches are based on the principles of resource management theory and elements of operations research (in particular, problems of allocation, prioritization, and optimization of limited resources). In addition, the method enables informed managerial decision-making in the field of cybersecurity of technological systems under conditions of uncertainty. As a mathematical tool for one of the key sub-stages of the method, which allows modeling potential destructive cyberattacks on technological system assets, simulation-analytical structural modeling using Colored Petri Nets is employed. To address tasks of individual sub-stages associated with decision-making under uncertainty, the PERT approach is applied.

The practical value of the method lies in its applicability for supporting managerial decision-making during the development of cybersecurity implementation plans aimed at countering destructive cyberattacks on technological systems of industrial critical infrastructure facilities over a planning period.

Thus, the method takes into account a set of real-world practical factors that are essential for identifying the most resource-efficient and effective cybersecurity measures to counter destructive cyberattacks on technological systems of

industrial critical infrastructure under resource constraints, while also ensuring the justification and proper documentation of the decisions made.

Keywords: *cybersecurity, cybersecurity measures prioritization method, industrial critical infrastructure, technological system, resource constraints, resource management.*

Постановка завдання.

Ефективне та раціональне впровадження заходів кібербезпеки у технологічних системах промислових об'єктів критичної інфраструктури є ключовою передумовою забезпечення їхнього належного рівня кіберстійкості. Особливої актуальності це питання набуває в умовах обмеженості ресурсів, зокрема часових, людських та фінансових.

Стан ресурсної обмеженості стає характерною ознакою функціонування таких об'єктів в Україні, що зумовлено сукупністю факторів, серед яких: економічні обмеження, дефіцит кваліфікованого персоналу, постійне розширення та ускладнення ландшафту кіберзагроз, зростання кількості кібератак, а також необхідність оперативного реагування на кіберінциденти.

У зв'язку з цим виникає необхідність забезпечення оптимального використання наявних ресурсів із метою підтримання сталого функціонування технологічного процесу промислового об'єкта критичної інфраструктури та підвищення рівня кіберстійкості його активів. Це, у свою чергу, спрямовано на мінімізацію ризику реалізації деструктивних кібератак, здатних спричинити найбільш критичні наслідки. Для вирішення зазначеної проблеми автором пропонується відповідний метод пріоритезації заходів кібербезпеки.

Аналіз літератури.

Враховуючи аналіз актуальних публікацій на платформі “Web of Science” та “Google Scholar”, питаннями дослідження методів управління ресурсами та пріоритезації заходів здебільшого займаються іноземні науковці. Вони пропонують різні підходи та алгоритми, які не завжди безпосередньо мають відношення до галузі кібербезпеки або промислових об'єктів критичної інфраструктури, проте їхній досвід можна враховувати й у цьому контексті. Зокрема, алгоритм пріоритезації для розподілу керування в системах із пріоритетами задач, що базується на рекурсивному перетині допустимих областей, запропонували автори [1]. Крім того, альтернативні підходи наведено у дослідженні [2], де автори зосереджуються на пріоритезації та розподілі ресурсів у складних програмах із великою кількістю проєктів на основі портфельного об'єднання. Питання розподілу фінансового ресурсу на забезпечення різних сегментів кібербезпеки (комплаєнс, інструменти та технології, навчання та проактивний кіберзахист) банківських установ при обмеженому фінансуванні підіймається у дослідженні [3]. Автори джерела [3] притримуються ризик-орієнтованого принципу при розподілі коштів на відповідні сегменти кібербезпеки, спираючись на їхню критичність для загальної кіберстійкості системи. Зазначену класичну концепцію використано у дослідженні автора та доповнено у запропонованому методі. Проактивному прогнозуванню кібератак на об'єкти критичної інфраструктури присвячено дослідження [4], у якому мотиваційний фактор суб'єкта кіберзагрози розглядається як ключова детермінанта вибору типу атаки. Зазначене положення підтримується в контексті нижчезапропонованого методу, де мотиваційна складова інтегрується у процес оцінювання та аналізу потенційних сценаріїв кібератак, що крім того враховують їхню ресурсооптимальність і як ключові тези входять до одного з підетапів методу.

На відміну від джерела [5], де пріоритезація заходів кіберзахисту здійснюється на основі потенційних наслідків та якісної оцінки загроз і вразливостей, у запропонованому методі додатково враховується ступінь обмеженості ресурсів на промислових об'єктах критичної інфраструктури (ПОКІ), ресурсовитратність реалізації кібератак з боку суб'єкта кіберзагрози, ефективність та пріоритетність реалізації заходів, що дозволяє більш обґрунтовано визначати пріоритети кібербезпеки в умовах обмежених ресурсів.

Таким чином, жодна із опрацьованих публікацій не пропонувала комплексного підходу для вирішення поставленого завдання, який би включав запропонований автором комплекс взаємодоповнюючих підходів. Проте окремі концепції було використано автором з метою підтвердження своїх припущень або для якісного доповнення методу.

Мета дослідження. Формалізований опис призначення, цільового спрямування, ролі, місця та змісту запропонованого методу пріоритезації заходів кібербезпеки технологічних систем промислових об'єктів критичної інфраструктури для протидії деструктивним кібератакам в умовах обмежених ресурсів.

Основними завданнями дослідження є:

- визначення призначення, цільового спрямування та функціональної ролі запропонованого методу;
- з'ясування місця методу в ієрархічній системі управління кібербезпекою промислового об'єкта критичної інфраструктури;
- викладення змісту методу відповідно до етапності його практичного застосування.

Основна частина.

1. Запропонований автором метод призначений для пріоритезації заходів кібербезпеки технологічних систем промислових об'єктів критичної інфраструктури (ТС ПОКІ) з метою протидії деструктивним кібератакам в умовах обмежених ресурсів. Цільове спрямування методу полягає у забезпеченні досягнення необхідного рівня кіберстійкості ТС ПОКІ шляхом раціонального розподілу наявних ресурсів та визначення пріоритетності реалізації заходів кібербезпеки з урахуванням необхідних факторів, зокрема найбільш вагомого – реальних кіберзагроз.

Метод призначений для застосування щодо ТС ПОКІ, оскільки його цільовим спрямуванням є забезпечення кіберстійкості технологічного процесу. Водночас концептуально метод є придатним для застосування і до традиційних комунікаційних систем, що функціонують на об'єктах критичної інфраструктури, однак у такому випадку потребує адаптації з урахуванням специфіки їх функціонування та відсутності технологічних процесів, характерних для промислових систем.

Метод може бути застосований до промислових об'єктів критичної інфраструктури (ПОКІ) I–IV категорій критичності [6]. Для об'єктів I–II категорій, в окремих випадках, доцільною є автоматизація окремих підетапів методу (в частині підетапу 3.1).

Викладені в методі підходи придатні до застосування як в умовах достатнього рівня ресурсного забезпечення для реалізації заходів кібербезпеки ТС ПОКІ проти деструктивних кібератак – тоді він дозволяє визначити доцільність і пріоритетність реалізації таких заходів, так і в умовах обмеженості ресурсів – тоді він дозволяє визначити активи і заходи, які потребують першочергової уваги для збереження необхідного рівня кіберстійкості ТС ПОКІ.

Функціонально метод виконує роль інструменту підтримки прийняття управлінських рішень для уповноваженої особи з кібербезпеки (Chief Information Security Officer, CISO) у процесі формування Плану реалізації заходів кібербезпеки для протидії деструктивним кібератакам на ТС ПОКІ, враховуючи рівень ресурсного обмеження.

Можна сказати, що метод пріоритезації заходів кібербезпеки ТС ПОКІ – це сукупність взаємопов'язаних алгоритму, процедур та моделей, спрямованих на формалізоване визначення пріоритетності заходів кібербезпеки шляхом комплексного врахування рівня критичності активів ТС ПОКІ, цільових пріоритетів підвищення їхньої кіберстійкості, оцінки та прогнозування коливань ресурсного забезпечення впродовж планового періоду, визначення рівня обмеженості ресурсів, вибору відповідного управлінського режиму, а також аналізу потенційних деструктивних кібератак і обчислення їхнього загального ресурсного шляху з метою забезпечення необхідного рівня кіберстійкості технологічних систем в умовах обмеженості ресурсів.

2. Місце методу у ієрархічній системі управління кібербезпекою ПОКІ зображено на рисунку 1, що структурно являє собою п'ятирівневу пірамідальну модель, яка наочно зображує черговість застосування основних загальноприйнятих етапів для забезпечення кібербезпеки, кіберстійкості та адаптивності ТС ПОКІ, що і є кінцевою метою (рівень 5).

Проаналізуємо рівні, зображені на вищезазначеній моделі більш детально.

Рівень 1 є початковим етапом формування основ кібербезпеки сучасних українських ТС ПОКІ. На практиці його реалізація здійснюється через розробку та впровадження комплексу організаційно-нормативних документів, передбачених серією нормативних документів із технічного захисту інформації України (НД ТЗІ), а також через застосування профілів безпеки.



Рис. 1. Концептуальна пірамідальна модель ієрархічної системи управління кібербезпекою ПОКІ з урахуванням запропонованого методу

НД ТЗІ регламентують: формування концепції кіберзагроз, побудову моделі порушника, визначення потенційних каналів несанкціонованого доступу, а також встановлення вимог до організації заходів кібербезпеки, що в сукупності формує нормативну основу для створення комплексної системи захисту інформації в автоматизованих системах відповідного класу. Згідно з вимогами НД ТЗІ та з урахуванням класу критичності ПОКІ, автоматизовані системи управління технологічними процесами, такі як Basic Process Control System (BPCS) та Safety Instrumented System (SIS), за результатами обстеження та класифікації у більшості випадків відносяться до класу АС-2 (клас АС визначається залежно від потенційних наслідків втрати доступності, конфіденційності або цілісності даних, тому для конкретного об'єкта можуть застосовуватися інші класи). Це зумовлює необхідність впровадження комплексної системи захисту інформації відповідно до встановлених нормативних вимог.

З 2025 року в Україні набрав чинності Порядок розробки профілів безпеки, затверджений Кабінетом Міністрів України. Профілі безпеки дозволяють чітко визначити, які вимоги з кібербезпеки має бути реалізовано в системі, залежно від типу інформації, яку вона обробляє: відкрита, конфіденційна, службова тощо. Профілі безпеки поділяються на: базовий, галузевий, цільовий. На практиці профілі безпеки використовуються разом із НД ТЗІ, що дозволяє адаптувати правила та механізми технічного захисту інформації під конкретні типи систем та притаманні їм ризики.

Таким чином рівень 1 формує концептуально-нормативне підґрунтя всієї кібербезпеки ТС ПОКІ.

Рівень 2 є наступним етапом загальноприйнятої архітектури кібербезпеки ТС ПОКІ та відповідає міжнародним стандартам у галузі оцінювання та управління кіберризиками для ТС ПОКІ. До таких стандартів належать ISO 31000, ISO/IEC 31010 та ISO/IEC 27005,

які формують методологічну основу процесів ідентифікації, аналізу та оцінювання кіберризиків [7]. Зазначені стандарти дозволяють здійснювати систематизований аналіз сценаріїв кібервпливу та їхніх наслідків, однак не передбачають кількісного обґрунтування пріоритетності заходів кібербезпеки з урахуванням обмежених ресурсів і специфіки реалізації деструктивних кібератак у технологічних системах (що враховано в одному з етапів методу).

Отже, рівень 2 створює системну методологічну основу для управління кіберризиками ТС ПОКІ, однак не забезпечує формалізованого механізму оптимізації розподілу захисних ресурсів, що обумовлює необхідність розроблення та впровадження відповідного методу.

Рівень 3 передбачає застосування запропонованого автором методу пріоритезації заходів кібербезпеки для протидії деструктивним кібератакам в умовах обмежених ресурсів. Саме на цьому етапі, маючи вихідні дані, сформовані на першому та другому рівнях, але до початку технічної реалізації заходів кіберзахисту, доцільно застосовувати запропонований метод. Висновки, отримані в процесі його реалізації, дозволяють обґрунтовано прийняти найбільш ефективні управлінські рішення та визначити пріоритетність реалізації заходів кібербезпеки.

Отже, рівень 3 виступає інструментальним етапом моделі, який забезпечує формалізовану оптимізацію розподілу обмежених ресурсів кібербезпеки з урахуванням пріоритетності кіберзагроз.

Рівень 4 передбачає реалізацію практичних заходів кіберзахисту ТС ПОКІ через технічну складову з урахуванням результатів методу. На цьому рівні здійснюється впровадження технічних і організаційних заходів кібербезпеки для визначених підсистем [8]. Реалізація зазначених заходів здійснюється відповідно до положень галузевих стандартів кібербезпеки промислових систем, зокрема серії ІЕС 62443, а також із використанням рекомендаційних документів NIST, таких як NIST SP 800-82 та NIST SP 1800-10, які застосовуються як практичні керівництва з впровадження заходів кіберзахисту [9].

Таким чином, рівень 4 забезпечує практичну імплементацію управлінських рішень, сформованих на попередніх рівнях, та трансформує результати методу у конкретні технічні й організаційні механізми підвищення кіберстійкості ТС ПОКІ.

3. Метод логічно вписується в систему багаторівневого планування кібербезпеки на ПОКІ (рис. 2). На верхньому рівні ієрархії розташована Концепція кібербезпеки ПОКІ (далі – Концепція), яка визначає стратегічні цілі та орієнтири розвитку системи кібербезпеки на довгострокову перспективу. Заходи відповідно до Концепції конкретизуються у щорічному Плані реалізації заходів кібербезпеки для ПОКІ (в контексті цього дослідження План реалізації заходів кібербезпеки для протидії деструктивним кібератакам на ТС ПОКІ, далі – План), що є документом короткострокового планування (на 1 рік) і розглядається надалі як окремий документ. У свою чергу, План містить перелік заходів кібербезпеки за кожним активом ТС ПОКІ, розподілених за пріоритетністю їх реалізації (першочергові, планові та довгострокові), та призначений для практичного використання відповідними підрозділами кібербезпеки впродовж запланованого періоду.

Результати застосування методу оформлюються у вигляді інформаційних матеріалів, які додаються до Плану та використовуються для обґрунтування прийнятих управлінських рішень.

Для забезпечення адаптивності такого методу передбачено його (або окремих його етапів) повторне застосування впродовж року у разі: форс-мажорних обставин, які значно вплинули або можуть вплинути на систему кібербезпеки ТС ПОКІ, різкої зміни ландшафту кіберзагроз (виникнення нових небезпечних кіберзагроз), непередбачуваної зміни динаміки наявного ресурсного забезпечення на реалізацію заходів кібербезпеки ТС ПОКІ (збільшення або зменшення передбаченого людського, часового або фінансового ресурсу).

У процесі планування заходів щодо забезпечення кібербезпеки ТС ПОКІ на майбутній рік та при використанні методу важливо враховувати результати діяльності за поточний рік,

що дозволяють оцінити наявні ресурси та динаміку їхніх змін з урахуванням попереднього досвіду (накопиченої статистики).

Метод складається з чотирьох основних етапів: підготовчий, операційний, аналітичний та заключний. Виконання кожного з попередніх етапів забезпечує результат, необхідний для виконання наступного.



Рис. 2. Структурно-логічна схема багаторівневого планування кібербезпеки ПОКІ з урахуванням запропонованого методу

Розглянемо етапи методу більш детально.

1. Підготовчий етап методу складається з:

1.1. Оцінки критичності активів і поточного рівня кіберстійкості ТС ПОКІ (окремо за кожним активом ТС ПОКІ з 1-го по 3-й рівень моделі Purdue) [10].

Оцінка критичності активів ТС ПОКІ здійснюється з урахуванням методичних рекомендацій, наведених у додатках до методу, та базується на принципах ризик-орієнтованого управління, зокрема ідеях, закладених у ІЕС 62443, ІЕС 61511 та ISO 20815, де критичність визначається через наслідки відмови або компрометації системи. Рекомендації з оцінки рівня критичності активів методу ґрунтуються на багатокритеріальному аналізі з ваговими коефіцієнтами, що дозволяє кількісно оцінити рівень критичності активів за сукупністю факторів (безпека людей, каскадність, єдина точка відмови та інші релевантні фактори) та ранжувати їх для пріоритетного розподілу ресурсів кібербезпеки [11].

Оцінка поточного рівня кіберстійкості активів здійснюється з урахуванням методичних рекомендацій, наведених у додатках до методу, шляхом присвоєння їм кількісного значення за визначеними критеріями: кіберстійкість фізичної та логічної архітектури; повнота забезпечення та коректність конфігурації апаратного/програмного забезпечення та його кіберстійкість; повнота функціонування процесів моніторингу і логування; коректність політики розмежування доступу; ефективність політики усунення вразливостей; ризик перехоплення ланцюжка поставок; ступінь резервування та потенціал відновлення (як єдиний показник), кожен з яких оцінюється в інтервалі [0; 1].

Оцінка критичності та поточного рівня кіберстійкості активів ТС ПОКІ проводиться на підставі наказу (розпорядження) керівника ПОКІ щодо реалізації заходів кібербезпеки на майбутній рік. У зазначеному документі, зокрема, визначається склад експертної комісії та встановлюються строки проведення оцінювання. Склад експертної комісії попередньо визначається CISO та має становити не менше трьох профільних фахівців різного профілю функціональних обов'язків.

Якщо впродовж попереднього року не було функціональних змін у фізично-логічній архітектурі активів ТС ПОКІ, їхня критичність може визначатися на основі результатів оцінювання за попередній рік.

Визначені експерти надають CISO відомості щодо результатів оцінювання критичності активів та їхнього поточного стану кіберстійкості у вигляді Актів оцінки критичності та поточного стану кіберстійкості відповідно, в яких в обов'язковому порядку міститься перелік активів, які підлягали оцінці та їх складових підсистем із зазначенням ступеню їхньої критичності, перелік критеріїв, оцінка та її обґрунтування, а також як підсумок – узагальнені відомості щодо оцінювання кожного активу з використанням статистичної медіани або медіани Кеммелі (як робастної оцінки, що зменшує вплив крайніх значень експертних оцінок). Отримані вагові коефіцієнти підлягають нормалізації таким чином, щоб їх сума дорівнювала одиниці ($\sum w_i = 1$), що забезпечує коректність застосування адитивної моделі згортки критеріїв та порівнюваність результатів оцінювання.

На підставі отриманих експертних оцінок щодо поточного стану кіберстійкості активів CISO за допомогою формули зваженої суми нормованих критеріїв розраховується поточний рівень кіберстійкості ТС ПОКІ (загальний для ТС ПОКІ і окремий за кожним активом/підсистемою активу), який відповідно до еталонної таблиці може класифікуватися як: низька кіберстійкість; середня кіберстійкість; задовільна кіберстійкість; висока кіберстійкість; дуже висока кіберстійкість, та оформлюється у вигляді документа “Відомість оцінки поточного рівня кіберстійкості ТС ПОКІ та її активів”.

1.2. Формування цільових пріоритетів щодо підвищення рівня кіберстійкості за кожним з активів ТС ПОКІ на плановий період.

Цей підетап здійснюється за контролю CISO з урахуванням вихідних даних підетапу 1.1 (оцінки рівня критичності та поточного рівня кіберстійкості активів ТС ПОКІ), а також пропозицій керівників відповідних напрямків (підрозділів) кібербезпеки ТС ПОКІ. CISO розподіляє усі активи та їхні інформаційні підсистеми за рівнем критичності для функціонування технологічного процесу. Визначення цільових пріоритетів полягає у встановленні CISO, які активи та їхні підсистеми потребують підвищення рівня кіберстійкості впродовж планового періоду і в якому обсязі (наприклад, у одного з критичних активів ТС ПОКІ поточний рівень кіберстійкості “середній”, а ціллю є досягнення рівня кіберстійкості не нижче “високого”). Визначені цільові пріоритети мають супроводжуватися оцінкою необхідних ресурсів для їх реалізації та не передбачати надлишкових заходів (лише оптимальні з точки зору ресурсовитрат варіанти заходів). Кінцевим результатом цього підетапу є формування документа – Матриці цільових пріоритетів щодо підвищення рівня кіберстійкості активів ТС ПОКІ.

У контексті протидії впливу деструктивних кібератак на кіберстійкість ТС ПОКІ до активів із підвищеним пріоритетом, як правило, належить інформаційна підсистема SIS. Ще одним важливим критерієм є пріоритетність у підвищенні рівня кіберстійкості активів 2-1 рівнів моделі Purdue, враховуючи, що ці рівні становлять ядро технологічного процесу. Разом із тим, цільові пріоритети мають формуватися так, щоб критичні активи та їхні підсистеми досягали рівня кіберстійкості не нижче “високого” в умовах обмеженості ресурсів. За умови достатності ресурсів цільовим є “дуже високий рівень кіберстійкості”.

При формуванні цільових пріоритетів важливим для врахування з боку CISO залишається той факт, що впродовж року показники ресурсу все ще можуть коливатися.

Оскільки рівень коливання ресурсних показників перебуває в умовах невизначеності, доцільно застосувати PERT-підхід та розглянути три можливі сценарії коливання такого ресурсу (песимістичний, найбільш ймовірний та оптимістичний). Для подальшого планування цільових пріоритетів та розрахунку обмеженості ресурсу підетапу 1.3 за основу рекомендується обрати ресурсні показники песимістичного сценарію, оскільки він відповідає принципам консервативного планування.

1.3. Розрахунок можливих коливань ресурсного забезпечення впродовж планового періоду.

Зазначений підетап передбачає врахування можливих коливань наявного ресурсного забезпечення для забезпечення кібербезпеки ТС ПОКІ впродовж планового періоду завдяки використанню PERT-підходу із розглядом трьох сценаріїв: оптимістичного, найбільш ймовірного та песимістичного. Для кожного виду ресурсу (часового, людського, фінансового) визначаються відповідні значення ресурсного забезпечення за кожним зі сценаріїв.

З урахуванням необхідності забезпечення стійкості планування в умовах невизначеності та обмеженості ресурсів, для подальших розрахунків і формування цільових пріоритетів за основу приймаються показники песимістичного сценарію (показники двох інших сценаріїв враховуються як потенційний резерв ресурсного забезпечення).

Оцінка наявних ресурсів і динаміки їх змін з урахуванням попереднього періоду (накопиченої статистики), а також аналітичні прогнози на майбутній період дозволяють визначити раціональні межі варіації ресурсних показників між сценаріями.

Такий підхід дозволяє гарантувати реалізацію заходів кібербезпеки навіть у несприятливих умовах, а у разі покращення ресурсного забезпечення – забезпечує наявність резерву для додаткового підвищення рівня кіберстійкості пріоритетним активам. Таким чином, вибір базових значень ресурсного забезпечення для подальших розрахунків формалізується наступним співвідношенням, зазначеним у формулі (1):

$$R_i^{plan} = R_i^{pes}, \quad (1)$$

де R_i^{plan} – планове значення i -го ресурсу, що використовується для подальших розрахунків;

R_i^{pes} – значення i -го ресурсу за песимістичним сценарієм;

$i \in \{t, l, f\}$, де t – часовий ресурс; l – людський ресурс; f – фінансовий ресурс.

Результати цього підетапу використовуються як вхідні дані для подальших розрахунків обмеженості ресурсів на операційному етапі (підетап 2.1) й окремо не оформлюються у вигляді самостійного документа.

2. Операційний етап методу складається з:

2.1. Розрахунку обмеженості ресурсів для реалізації заходів кібербезпеки, визначених у межах цільових пріоритетів, для кожного активу ТС ПОКІ на плановий період.

Для розрахунку обмеженості ресурсів як планові значення наявних ресурсів використовуються кількісні показники часових, людських і фінансових ресурсів відповідно до песимістичного сценарію, а також кількісні показники необхідних ресурсів для реалізації цільових пріоритетів щодо підвищення рівня кіберстійкості за кожним з активів ТС ПОКІ на плановий період (результати підетапу 1.2).

Обмеженість ресурсу розраховується за кожним з його видів (часовим, людським і фінансовим, формули (2)–(10)), що в подальшому (з урахуванням низки нижчеописаних факторів), дозволить приймати зважені рішення щодо застосування кожного з них у процесі пріоритетизації заходів кібербезпеки ТС ПОКІ. Загальний принцип розрахунку обмеженості ресурсів відповідає формулі (2):

$$K_R = \frac{R_{req}}{R_{avail}}, \quad (2)$$

де K_R – коефіцієнт обмеженості ресурсу;
 R_{req} – необхідний ресурс;
 R_{avail} – доступний ресурс.
 При цьому:
 $K_R < 1$ – ресурс достатній;
 $K_R = 1$ – ресурс граничний;
 $K_R > 1$ – дефіцит ресурсу.

Формула розрахунку часового ресурсу реалізації заходу залежить від характеру організації робіт. У разі послідовного виконання робіт часовий ресурс визначається як сума тривалостей усіх робіт, необхідних для виконання відповідного заходу, згідно з формулою (3). Якщо окремі роботи можуть виконуватися паралельно, часовий ресурс реалізації заходу визначається за тривалістю критичного шляху, тобто найдовшого ланцюга взаємозалежних робіт, згідно з формулами (3), (4).

$$T_i = \sum_{j=1}^{m_i} t_{ij}, \quad (3)$$

де T_i – часовий ресурс реалізації i -го заходу;
 t_{ij} – тривалість j -ї роботи в межах заходу;
 m_i – кількість робіт.

$$T_i = \max_{p \in P_i} (\sum_{j \in p} t_{ij}), \quad (4)$$

де T_i – часовий ресурс реалізації i -го заходу;
 P_i – множина всіх можливих шляхів виконання робіт у межах i -го заходу;
 p – окремий шлях із множини P_i ;
 t_{ij} – тривалість j -ї роботи, що входить до шляху p .

Рівень обмеженості часового ресурсу обчислюється за формулою (5):

$$K_T = \frac{T_{req}}{T_{avail}}, \quad (5)$$

де K_T – коефіцієнт обмеженості часового ресурсу;
 T_{req} – необхідний часовий ресурс;
 T_{avail} – доступний часовий ресурс.

Для розрахунку обмеженості людського ресурсу необхідно обчислити загальну витрату певної ролі для реалізації заходів цільового планування відповідно до формули (6):

$$L_r = \sum_{i=1}^n h_{ir}, \quad (6)$$

де L_r – загальна трудомісткість ролі;
 h_{ir} – людино-години ролі r для заходу i .

Необхідна кількість фахівців конкретної ролі розраховується за формулою (7) (округлення результату здійснюється у більшу сторону):

$$N_r = \frac{L_r}{H_{year}}, \quad (7)$$

де N_r – необхідна кількість фахівців ролі r ;
 L_r – трудомісткість робіт для ролі r ;
 H_{year} – ефективний річний фонд робочого часу одного фахівця.

Обмеженість людського ресурсу розраховується згідно з формулою (8), при цьому передбачається, що кожен фахівець виконує роботи в межах однієї ролі без урахування багатофункціонального навантаження):

$$K_L = \frac{N_{req}}{N_{avail}}, \quad (8)$$

де K_L – коефіцієнт обмеженості людського ресурсу;
 N_{reg} – необхідна кількість фахівців відповідної ролі, визначена за формулою (7);
 N_{avail} – доступна кількість фахівців відповідної ролі, визначена з урахуванням песимістичного сценарію.

Необхідні фінансові ресурси рекомендується розраховувати за формулою (9):

$$F_{reg} = F_{sal} + F_{outsors} + F_{soft} + F_{equip} + F_{educ}, \quad (9)$$

де F_{reg} – загальний обсяг необхідного фінансового ресурсу;
 F_{sal} – витрати за оплату праці працівників;
 $F_{outsors}$ – витрати на аутсорсингові послуги;
 F_{soft} – витрати на придбання або оновлення необхідного програмного забезпечення;
 F_{equip} – витрати на придбання або модернізацію обладнання;
 F_{educ} – витрати на навчання та підвищення кваліфікації персоналу.

Обмеженість фінансового ресурсу розраховується за формулою (10):

$$K_F = \frac{F_{reg}}{F_{avail}}, \quad (10)$$

де F_{reg} – загальний обсяг необхідного фінансового ресурсу;
 F_{avail} – загальний обсяг доступного фінансового ресурсу.

Таким чином, результатом цього підетапу є визначення рівня обмеженості за кожним видом ресурсу, а також формування документа “Відомість оцінки обмеженості ресурсів для реалізації стратегічних цільових пріоритетів кібербезпеки активів ТС ПОКІ”.

2.2. Вибору управлінського режиму щодо збереження або підвищення рівня кіберстійкості.

Вибір управлінського режиму здійснюється на основі значень коефіцієнтів обмеженості ресурсів K_T , K_L , K_F , отриманих на підетапі 2.1.

За результатами аналізу практичних кейсів, на підприємствах критичної інфраструктури дефіцит одного ресурсу (часового, людського або фінансового) до 30–40 % дозволяє підтримувати основні операційні процеси (узагальнення практики експлуатації ТС ПОКІ). Тому в подальшому дослідженні враховуємо, що критичним порогом обмеженості ресурсу вважається 40 % (якщо ресурсна обмеженість нижча 40 % хоча б за одним з видів ресурсу впродовж тривалого часу (до пів року) ТС ПОКІ з високою долею ймовірності вразлива до деструктивних кібератак).

Загалом можна сформулювати таке твердження, що на цьому етапі методу вважається, що при дефіциті одного з ресурсів, який не перевищує 40 %, можлива його часткова компенсація завдяки іншим видам ресурсів (часового, людського та фінансового) за умови адаптації управлінського режиму та корекції цільових пріоритетів. Такий підхід відповідає

нормативному (при незначних обмеженнях, до 20 %) та адаптивному (при обмеженнях понад 20 %) управлінським режимам. Вартий уваги і той факт, що у разі нормативного управлінського режиму серед цільових пріоритетів заходів із підвищення кіберстійкості залишаються всі активи 3-1 рівнів моделі Purdue (так як вони становлять основу технологічного процесу) [7]. У разі ж адаптивного управлінського режиму серед заходів із підвищення кіберстійкості залишаються всі активи 2-1 рівнів моделі Purdue та ключові активи 3-го рівня моделі Purdue (критичні міжрівневі вузли 3-го рівня, що мають найбільший вплив на безпеку та безперервність виробництва).

Якщо обмеженість виникає одразу за двома видами ресурсу та не перевищує 40 % за кожним з них, то можливо забезпечити підвищення рівня кіберстійкості лише для активів 2-1 рівня моделі Purdue (для 3-го рівня моделі Purdue – збереження поточного рівня кіберстійкості). Такий підхід відповідає селективному (якщо обмеження не значні < 20 %) та обмежувальному управлінським режимам (якщо обмеження значні > 20 %). Аналіз показує, що найбільш критичною комбінацією подвійної ресурсної обмеженості для ТС ПОКІ є одночасний дефіцит людського та часового ресурсів, оскільки така ситуація безпосередньо унеможливорює практичну реалізацію заходів кібербезпеки незалежно від рівня фінансового забезпечення. На відміну від фінансового дефіциту, який може бути компенсований управлінськими рішеннями, кадрово-часові обмеження мають високий рівень інерційності та істотно впливають на безперервність технологічного процесу.

Якщо існує обмеженість за трьома видами ресурсу, підвищення кіберстійкості значно ускладнюється і переходить в режим “збереження поточного рівня кіберстійкості”. Такий підхід відповідає обмежувальному (якщо обмеження не значні < 20 % за кожним видом ресурсу) та кризовому (якщо обмеження значні > 20 % за кожним видом ресурсу) управлінським режимам. Якщо зберігається обмежувальний підхід, то кіберстійкість підвищується лише для критичних активів 2-1 рівня моделі Purdue. У разі переходу на кризовий управлінський режим, головним завданням стає збереження поточного рівня кіберстійкості активів 2-1 рівня моделі Purdue [12].

Результатом етапу 2.2 є визначення вектору подальшого стратегічного руху та відбір активів ТС ПОКІ (залежно від управлінського режиму, який обрано), для яких в подальшому буде здійснюватися розрахунок загального ресурсного шляху деструктивної кібератаки в рамках аналітичного етапу методу.

Таким чином, вибір управлінського режиму безпосередньо впливає на подальшу пріоритезацію заходів кібербезпеки, оскільки визначає область аналізу та дозволяє сфокусуватися на активах відповідних рівнів моделі Purdue, для яких реалізація таких заходів є першочерговою за наявного обсягу ресурсів.

Кінцевим результатом цього підетапу є формування “Матриці вибору управлінського режиму та відбору активів ТС ПОКІ”, яка встановлює відповідність між рівнем ресурсної обмеженості, обраним управлінським режимом і переліком активів, що підлягають подальшому аналізу.

2.3. Визначення структури розподілу ресурсів між пріоритетними активами ТС ПОКІ.

Після вибору управлінського режиму здійснюється розподіл наявного обсягу ресурсів між його відповідними пріоритетними групами активів ТС ПОКІ. При цьому, незалежно від обраного управлінського режиму необхідно виділяти щонайменше мінімально необхідну кількість ресурсів на кібербезпеку активів вищих рівнів моделі Purdue (3-го рівня моделі), навіть в умовах дефіциту ресурсів (за виключенням кризового управлінського режиму). Вищезазначене обумовлено функціональними характеристиками 3-го рівня моделі, а саме – забезпеченням міжрівневої взаємодії, диспетчеризацією, збором технологічних даних та підтримкою безперервності виробництва. У зв'язку з цим, управлінський режим визначає не лише перелік активів, що підлягають подальшому ранжуванню за рівнем критичності, але й встановлює пропорції розподілу ресурсів між відповідними групами активів.

Для формалізації розподілу ресурсів виділяються три групи активів:

Група А: активи 1–2 рівнів моделі;

Група В: критичні активи 3 рівня моделі;

Група С: інші активи 3 рівня моделі (допоміжні системи управління та моніторингу).

Рекомендована автором відповідність між управлінським режимом і структурою розподілу ресурсів між групами активів наведена у таблиці 1. Нищенаведені значення отримані в межах запропонованого методу та відображають авторське бачення раціонального розподілу ресурсів залежно від управлінського режиму з урахуванням критичності активів, що належать до окремих груп.

Таблиця 1

Рекомендований відсотковий розподіл ресурсів між групами активів
в межах обраного управлінського режиму

Назва управлінського режиму	Рекомендований розподіл за кожним з видів ресурсів		
	Група А	Група В	Група С
Нормативний	50 %–60 %	25 %–30 %	15 %–20 %
Адаптивний	60 %–70 %	20 %–25 %	10 %–15 %
Селективний	70 %–80 %	15 %–20 %	5 %–10 %
Обмежувальний	80 %–85 %	10 %–15 %	0 %–5 %
Кризовий	85 %–90 %	10 %–15 %	0 %

Розподіл ресурсів між групами активів здійснюється у вигляді визначення часток ресурсів для кожної групи активів у межах встановлених діапазонів залежно від обраного управлінського режиму. Зазначені у Таблиці 1 відсоткові частки мають інтервальний характер і визначають орієнтовну структуру спрямування ресурсів.

Враховуючи рекомендований ресурсний розподіл згідно з таблицею 1, за участі CISO формується попередній відсотковий розподіл ресурсів між активами ТС ПОКІ (таблиця 2):

Таблиця 2

Попередній відсотковий розподіл ресурсів між активами ТС ПОКІ

Назва управлінського режиму	Група А (60 %)						Група В (25 %)						Група С (15 %)					
Адаптивний	BPCS (поточний рівень кіберстійкості “високий”); SIS (поточний рівень кіберстійкості “високий”)						Manufacturing Execution System (поточний рівень кіберстійкості “середня кіберстійкість”); Historian (поточний рівень кіберстійкості “задовільна кіберстійкість”)						Система управління якістю (QMS) (поточний рівень кіберстійкості “задовільна кіберстійкість”); Система планування та диспетчеризації виробництва (APS / Scheduling) (поточний рівень кіберстійкості “середня кіберстійкість”)					
	T	L	F				T	L	F				T	L	F			
	30 %	30 %	35 %	25 %	25 %	35 %	10 %	15 %	5 %	20 %	10 %	15 %	10 %	5 %	10 %	5 %	11 %	4 %

Розподілені значення відповідно до таблиці 2 мають відносний характер і визначають структуру розподілу ресурсів у межах відповідної групи активів. Такий підхід забезпечує попереднє узгодження спрямування ресурсів перед етапом їх подальшого перерозподілу між заходами кібербезпеки в межах кожного активу. При цьому для розподілу ресурсів у межах окремого активу (підсистем активу) провідну роль відіграють його поточний та цільовий рівні кіберстійкості (визначається в рамках формування цільових пріоритетів, підпункт 1.2 Підготовчого етапу).

Конкретні значення часток часового, людського та фінансового ресурсів у межах зазначених діапазонів уточнюються CISO за результатами аналітичного етапу методу.

Кінцевим документом цього підетапу є відпрацювання Матриці попереднього розподілу ресурсів між активами ТС ПОКІ.

3. Аналітичний етап включає:

3.1. Обчислення загального ресурсного шляху потенційних деструктивних кібератак за кожним активом ТС ПОКІ.

З метою виявлення потенційно вразливих вузлів та/або ділянок (підсистем) технологічної системи, а також можливих способів реалізації деструктивного кібервпливу на технологічний процес з боку суб'єктів кіберзагрози, застосовується імітаційно-аналітичне структурне моделювання з використанням кольорових сіток Петрі [13; 14]. Зазначений підхід дозволяє здійснити формалізований опис можливих векторів і тактик реалізації кібератак та виконати обчислення загального ресурсного шляху потенційних деструктивних кібератак для кожного активу ТС ПОКІ.

Загальний ресурсний шлях деструктивної кібератаки — це інтегральний кількісний показник, який відображає сумарні витрати ресурсів (часових, людських і фінансових), необхідних суб'єкту кіберзагрози для повної реалізації обраного сценарію (тактики) кібератаки на технологічну систему, з урахуванням усіх етапів її виконання та невизначеності умов.

До виконання завдань з обчислення доцільно залучати фахівців напрямку Cyber Threat Intelligence або аналогічного за функціональним призначенням, із урахуванням повного вичерпного переліку актуальних векторів і тактик кіберзагроз.

За результатами моделювання визначаються та оцінюються потенційні вектори реалізації деструктивних кібератак для кожного активу з метою подальшого використання в процесі пріоритезації заходів кібербезпеки в умовах обмежених ресурсів.

Отримані результати використовуються для:

уточнення розподілу ресурсів між групами активів ТС ПОКІ;

обґрунтування порядку пріоритетності реалізації заходів кібербезпеки з урахуванням обраного управлінського режиму;

віднесення заходів кібербезпеки до відповідних класів пріоритетності: першочергової (оперативної) реалізації; планової реалізації; довгострокової реалізації [15].

Результати цього етапу оформлюються у вигляді Імітаційно-аналітичних моделей загального ресурсного шляху потенційних деструктивних кібератак на активи ТС ПОКІ. А результати таких моделей у вигляді ранжування тактик і технік потенційних деструктивних кібератак оформлюються у вигляді Відомості оцінювання загального ресурсного шляху деструктивних кібератак (за активами ТС ПОКІ).

3.2. Розрахунок відносного показника ефективності та пріоритетності заходів кібербезпеки.

У контексті цього дослідження захід кібербезпеки ми можемо вважати ефективним, якщо він суттєво підвищує рівень кіберстійкості активу/підсистеми активу і одночасно при цьому не вимагає надмірних ресурсовитрат. Захід вважається пріоритетнішим у тому випадку, якщо його реалізація забезпечує більший приріст рівня кіберстійкості активу/підсистеми активу на одиницю витраченого ресурсу порівняно з альтернативними заходами.

З метою обґрунтування пріоритетності заходів кібербезпеки в умовах обмежених ресурсів на цьому етапі методу здійснюється оцінювання відносної ефективності кожного заходу щодо окремого активу/підсистеми активу згідно з обраним управлінським режимом, а також формування інтегрального показника його пріоритетності.

Для кожного заходу кібербезпеки і відносний показник ефективності визначається за формулою (11):

$$E_i = \frac{\Delta S_i}{aT_i + bL_i + cF_i}, \quad (11)$$

де ΔS_i – очікуване нарощення рівня кіберстійкості активу, внаслідок впровадження заходу;
 T_i – часові витрати;
 L_i – людські ресурси;
 F_i – фінансові ресурси;
 a, b, c – вагові коефіцієнти ресурсів, причому $a + b + c = 1$.

Для подальших розрахунків і оцінки показника ефективності заходу кожен розглянемо з позиції безпекової потреби у захисті та ресурсно-управлінської доцільності.

Безпекова потреба у заході обчислюється за формулою (12):

$$N_i = a_1 K_i + a_2 (1 - S_i) + a_3 (1 - G_i), \quad (12)$$

де K_i – нормована критичність активу;
 S_i – нормований поточний рівень кіберстійкості;
 G_i – нормований показник загального ресурсного шляху кібератаки;
 a_1, a_2, a_3 – вагові коефіцієнти ($a_1 + a_2 + a_3 = 1$).

Такий показник, як G_i пропонується унормувати до інтервалу $[0;1]$ через максимальне значення за формулою (13):

$$G_i = \frac{G_i}{\max_j G_j}. \quad (13)$$

Оскільки абсолютне максимальне значення загального ресурсного шляху кібератаки апіорі невідоме, нормування показника G_i здійснюється відносно максимального значення, отриманого в межах активів, які розглядаються, або сценаріїв кібератак.

Ресурсно-управлінська доцільність обчислюється згідно з формулою (14):

$$D_i = b_1 (1 - O_i) + b_2 E_i, \quad (14)$$

де O_i – нормований показник обмеженості ресурсів;
 E_i – нормований показник ефективності заходу;
 b_1, b_2 – вагові коефіцієнти ($b_1 + b_2 = 1$).

При цьому показник обмеженості ресурсів визначається як зважена сума обмеженості часових, людських і фінансових ресурсів згідно з формулою (15):

$$O_i = w_t O_t + w_l O_l + w_f O_f. \quad (15)$$

Кінцевий інтегральний показник пріоритетності заходу обчислюється за формулою (16):

$$P_i = \lambda N_i + (1 - \lambda) D_i, \quad (16)$$

де P_i – інтегральний показник пріоритетності заходу;

$\lambda \in [0;1]$ – коефіцієнт балансу між безпековою потребою та ресурсною доцільністю.

Отримані значення P_i використовуються для ранжування заходів кібербезпеки та їх віднесення до класів пріоритетності в межах кожного активу/підсистеми активу управлінського режиму та відносяться до першочергової (оперативної), планової або довгострокової реалізації.

Наведемо приклад розрахунку відносного показника ефективності та пріоритетності заходів кібербезпеки активів інформаційної підсистеми ВРCS на умовних числових значеннях. Для прикладу використаємо такий захід кібербезпеки як сегментація мережі ВРCS.

Першочергово обчислимо відносний показник ефективності заходу кібербезпеки для ВРCS. Експертно присвоємо значення для змінних $\Delta Si = 0,30$; $T_i, L_i, F_i \geq 0$. Врахуємо, що існує обмеженість фінансового ресурсу на реалізацію зазначеного заходу. Припустимо, що існує потреба у 120 тисячах гривень на реалізацію сегментації, а доступно 100 тисяч гривень. Тоді відносний показник обмеженості фінансового ресурсу обчислюватиметься за формулою (17):

$$F_i = \frac{120}{100} = 1,2. \quad (17)$$

Врахуємо, що відповідно до формули (11) $T_i = 0,40$; $L_i = 0,50$; $F_i = 1,2$; $\alpha = 0,4$; $b = 0,3$; $c = 0,3$. Таким чином, відносний показник ефективності згідно з формулою (18) дорівнює:

$$E_i = \frac{0,30}{0,67} = 0,448; E_i \approx 0,45. \quad (18)$$

Наступним кроком розрахуємо безпекову доцільність сегментування мережі згідно з формулою (12).

Задамо значення для $K_i = 0,80$; $S_i = 0,40$; а показник G_i розрахуємо через максимальне значення загального ресурсного шляху деструктивної кібератаки для конкретного активу/підсистеми активу згідно з формулою (13): $G_i = 0,70$. Значення вагових коефіцієнтів $a_1 = 0,4$; $a_2 = 0,3$; $a_3 = 0,3$. Таким чином, безпекова доцільність згідно з формулою (19) дорівнює:

$$N_i = 0,32 + 0,18 + 0,09 = 0,59. \quad (19)$$

Наступним кроком розрахуємо ресурсно-управлінську доцільність реалізації заходу кібербезпеки згідно з формулою (14). Для цього спочатку обчислимо значення показника O_i згідно з уточнюючою формулою (15). Показник обмеженості ресурсів визначається як зважена сума обмеженості часових, людських і фінансових ресурсів. Для прикладу: $O_i = 0,4 \times 0,40 + 0,3 \times 0,60 + 0,3 \times 0,50 = 0,49$.

За умови, що відносний показник ефективності заходу $E_i = 0,45$, при вагових коефіцієнтах $b_1 = 0,5$; $b_2 = 0,5$ ресурсно-управлінська доцільність заходу відповідно до формули (20) дорівнює:

$$D_i = 0,5(1 - 0,49) + 0,5 \times 0,76 = 0,635. \quad (20)$$

Отже, $D_i \approx 0,64$, що відповідно до рекомендованої шкали (таблиця 3) свідчить про доцільність реалізації сегментації мережі ВРС з точки зору співвідношення ресурсно-управлінської доцільності.

Таблиця 3

Шкала оцінювання ресурсно-управлінської доцільності заходів кібербезпеки

Кількісне значення показника D_i	Інтерпретація	Рекомендоване рішення відповідно до ступеню пріоритезації заходу
0,76–1	Висока доцільність реалізації заходу	Реалізувати першочергово
0,50–0,75	Помірна доцільність	Реалізувати планово
0,25–0,49	Низька пріоритетність	Віднести до довгострокової реалізації
0–0,24	Недоцільність реалізації у разі обмеженості ресурсів	Не реалізовувати у разі обмеженості ресурсів

Інтегральний показник пріоритетності заходу визначається як зважена комбінація безпекової потреби та ресурсно-управлінської доцільності. Для вищезазначеного прикладу розрахунків, за умови, що $N_i = 0,59$; $D_i = 0,64$, а коефіцієнт балансу $\lambda = 0,6$ (показує збільшений пріоритет безпекової складової) згідно з формулою (16) та відповідно до розрахунків формули (21) отримуємо:

$$P_i = 0,6 \times 0,59 + 0,4 \times 0,64 = 0,61. \quad (21)$$

$\lambda \in [0;1]$, де при $\lambda \rightarrow 1$ пріоритезація заходів визначається переважно безпековою потребою, тоді як при $\lambda \rightarrow 0$ – ресурсною доцільністю. Це дозволяє використовувати метод як в умовах обмеженості ресурсів, так і в умовах планового управління.

Визначимо остаточну пріоритетність заходу кібербезпеки згідно зі шкалою оцінювання (таблиця 4).

Таблиця 4

Шкала оцінювання пріоритетності реалізації заходу кібербезпеки в умовах обмежених ресурсів

Кількісне значення показника P_i	Значення пріоритету
0,75–1	Високий (першочергова реалізація)
0,50–0,74	Середній (планова реалізація)
0,25–0,49	Низький (довгострокова реалізація)
< 0,25	Не пріоритетний

Таким чином, захід сегментації мережі для активу інформаційної підсистеми ВРС за отриманим значенням інтегрального показника пріоритетності $P_i = 0,61$ належить до категорії заходів планової реалізації. При цьому враховується наявність дефіциту фінансового ресурсу на рівні 20 %, що знижує його ресурсно-управлінську доцільність, однак не виключає доцільності впровадження цього заходу кібербезпеки.

Результати підетапу оформлюються у Матрицю інтегральних показників ефективності та пріоритетності заходів кібербезпеки для активів ТС ПОКІ.

3.3. Розподіл часток ресурсів у межах груп активів управлінського режиму.

За результатами аналітичного етапу методу, зокрема обчислення загального ресурсного шляху потенційних деструктивних кібератак та розрахунку відносних показників ефективності і пріоритетності заходів кібербезпеки, забезпечується можливість більш обґрунтованого розподілу обмежених ресурсів між групами активів технологічної системи (підпункт 2.3 в продовження таблиці 2). Результатом цього етапу є визначення розподілу всіх трьох видів ресурсів (часового, людського і фінансового) в рамках управлінського режиму між заходами кібербезпеки груп активів (та їх підсистем) та відпрацювання Матриці уточненого розподілу ресурсів між заходами кібербезпеки для активів ТС ПОКІ.

Заключний етап методу включає:

4.1. Ранжування заходів кібербезпеки за кожним активом ТС ПОКІ за черговістю їх реалізації відповідно до визначеної пріоритетності.

Цей підетап передбачає віднесення заходів кібербезпеки до пріоритетності їх реалізації: першочергової реалізації; планової реалізації; довгострокової реалізації та в рамках обраного управлінського режиму згідно з підходом, описаним у підпункті 3.2. Результатом виконання підетапу є складання Реєстру пріоритетності та черговості реалізації заходів кібербезпеки для активів ТС ПОКІ.

4.2. Формування Плану реалізації заходів кібербезпеки ТС ПОКІ.

Підетап є завершальною частиною методу та полягає у формуванні остаточної версії Плану реалізації заходів кібербезпеки ТС ПОКІ з урахуванням обмеженості ресурсів, який містить ранжований перелік заходів, розподіл ресурсів та відповідні додатки, що обґрунтовують прийняті управлінські рішення. Перелік рекомендованих додатків згідно з черговістю виконання етапів/підпунктів методу відображено у таблиці 5.

Таблиця 5

Перелік рекомендованих додатків згідно з черговістю виконання етапів/підетапів методу

Підпункт етапу методу	Назва додатку до Плану
1.1	Акти оцінки критичності та поточного стану кіберстійкості активів ТС ПОКІ
	Відомість оцінки поточного рівня кіберстійкості ТС ПОКІ та її активів
1.2	Матриця цільових пріоритетів щодо підвищення рівня кіберстійкості активів ТС ПОКІ
2.1	Відомість оцінки обмеженості ресурсів для реалізації цільових пріоритетів кібербезпеки активів ТС ПОКІ
2.2	Матриця вибору управлінського режиму та відбору активів ТС ПОКІ
2.3	Матриця попереднього розподілу ресурсів між активами ТС ПОКІ
3.1	Імітаційно-аналітичні моделі загального ресурсного шляху потенційних деструктивних кібератак на активи ТС ПОКІ
	Відомість оцінювання загального ресурсного шляху деструктивних кібератак
3.2	Матриця оцінки ефективності та пріоритетності заходів кібербезпеки для активів ТС ПОКІ
3.3	Матриця інтегрованого розподілу ресурсів між заходами кібербезпеки для активів ТС ПОКІ
4.1	Реєстр пріоритетності та черговості реалізації заходів кібербезпеки для активів ТС ПОКІ

Висновки. Таким чином, з аналізу змісту описаного методу встановлено, що пріоритезація заходів кібербезпеки для протидії деструктивним кібератакам в умовах обмежених ресурсів здійснюється з урахуванням таких головних критеріїв:

- рівня критичності активів ТС ПОКІ;
- рівня цільових пріоритетів щодо підвищення кіберстійкості активів ТС ПОКІ;
- найбільш ймовірних коливань рівня ресурсного забезпечення впродовж планового періоду;
- рівня обмеженості ресурсів;

загального ресурсного шляху потенційних деструктивних кібератак проти активів ТС ПОКІ.

Зазначені фактори інтегруються в узагальнений показник пріоритезації заходів кібербезпеки I , який можна описати формулою (22):

$$I = \sum_{i=1}^5 w_i \times K_i. \quad (22)$$

На відміну від класичних підходів до управління ресурсами (cost-benefit аналіз, risk-based підходи, АНР, optimization-моделі), запропонований метод поєднує оцінку внутрішніх параметрів системи з урахуванням поведінки суб'єкта кіберзагрози, що реалізується через використання імітаційно-аналітичного моделювання з використанням кольорових сіток Петрі. Це забезпечує перехід від статичної до сценарно-орієнтованої та адаптивної пріоритезації заходів кібербезпеки.

Таким чином, запропонований метод підвищує ефективність управління кібербезпекою ТС ПОКІ та забезпечує можливість обґрунтованого розподілу обмежених ресурсів з урахуванням актуального ландшафту кіберзагроз.

Майбутні шляхи досліджень.

Перспективними напрямками подальших досліджень є розвиток запропонованого методу у частині підвищення рівня його автоматизації та експериментальної верифікації. Зокрема, доцільним є розроблення програмних засобів, спрямованих на автоматизацію окремих підетапів методу, передусім підетапу обчислення загального ресурсного шляху потенційних деструктивних кібератак на основі імітаційно-аналітичного моделювання з використанням кольорових сіток Петрі. Автоматизація цього процесу може бути реалізована із застосуванням спеціалізованих середовищ моделювання (зокрема, “CPN Tools”) у поєднанні з програмними засобами обробки даних (наприклад, з використанням мови програмування Python).

Окрім цього, перспективним є проведення експериментальної апробації методу на реальних або наближених до реальних ТС ПОКІ, зокрема об'єктах енергетичної галузі (наприклад, теплових електростанціях). Така апробація дозволить оцінити ефективність методу, його чутливість до змін ресурсного забезпечення та релевантність отриманих управлінських рішень порівняно з існуючими підходами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Novais I., Marinatto M., Lizarralde F., Peixoto A. J. Hard Prioritization Control Allocation: Dealing With the Priority Inversion Phenomenon. URL: <https://ieeexplore.ieee.org/document/11038928>.
2. Miller C., Sage A. P. Application of a methodology for evaluation prioritization and resource allocation to energy conservation program planning. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0045790681900203?via%3Dihub>.
3. Mohammad Amir Hossain, Md. Adil Raza, Taqi Yaseer Rahman. Resource allocation and budgetary constraints for cybersecurity projects in small to medium sized banks. URL: <http://dx.doi.org/10.2139/ssrn.5207138>.
4. Rodrigo Román-Castro, Adel Alqudhaibi, Majed Albarrak, Abdulmohsan Aloheel, Sandeep Jagtap, Konstantinos Salonitis. Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. URL: <https://doi.org/10.3390/s23094539>.
5. SANDIA REPORT Methodology for Prioritizing Cyber vulnerable Critical Infrastructure Equipment and Mitigation Strategies. URL: <https://doi.org/10.2172/1028958>.
6. Про критичну інфраструктуру: Закон України від 18.11.2021 № 1909-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
7. Paté-Cornell M.-E. L., Kuypers M., Smith M., Keller P. Cyber risk management for critical infrastructure: A risk analysis model and three case studies // Risk Analysis. 2020. № 38 (2). URL: <https://doi.org/10.1111/risa.12844>.

8. Eric D. Knapp. Industrial Network Security Securing Critical Infrastructure Networks For Smart Grid Scada and other Industrial Control Systems 1st Edition. URL: <https://www.slideshare.net/slideshow/industrial-network-security-securing-critical-infrastructure-networks-for-smart-grid-scada-and-other-industrial-control-systems-1st-edition-eric-d-knapp/279202298#3>.
9. Ackerman Pascal. Industrial Cybersecurity Second Edition. 2021. 800 p.
10. What is the Purdue Model? URL: https://www.pera.net/Pera/Wha_PERA_Ref_Model.html?utm_source=chatgpt.com.
11. Хавер А. В. Метод ранжування критичності технологічних підсистем для визначення пріоритетності їх кіберзахисту на промислових об'єктах критичної інфраструктури // Всеукраїнська науково-практична конференція “Актуальні проблеми кібербезпеки”: тези доповідей, 2025 р. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf.
12. Савченко В. А., Хавер А. В. Метод розрахунку кіберстійкості 2-1 рівнів моделі Purdue проти спеціалізованого технологічного троянського програмного забезпечення // Системи і технології зв'язку, інформатизації та кібербезпеки. 2025. № 7. URL: <https://doi.org/10.58254/viti.7.2025.14.147>.
13. Harvey M. Wagner. Principles of Operations Research. URL: <https://ia801701.us.archive.org/33/items/in.ernet.dli.2015.132568/2015.132568.Principles-Of-Operations-Research-Second-Edition.pdf>.
14. An Introduction to the Theoretical Aspects of Coloured Petri Nets. URL: https://tidsskrift.dk/daimipb/article/view/6949?utm_source=chatgpt.com.
15. Хавер А. В. Метод обчислення загального ресурсного шляху деструктивних кібератак на промислові об'єкти критичної інфраструктури // Кібербезпека: освіта, наука, техніка. 2025. Том 3, № 31. URL: <https://doi.org/10.28925/2663-4023.2025.31.1064>.

Надійшла до редколегії 06.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

УДК 681.35

канд. техн. наук, доцент Хусаїнов П. В. ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Штаненко С. С. ORCID: 0000-0001-9776-4653 (ВІТІ ім. Героїв Крут)
Чурилова І. С. ORCID: 0009-0007-6195-9265 (ВІТІ ім. Героїв Крут)

ПРОБЛЕМА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В РЕАЛЬНОМУ МАСШТАБІ ЧАСУ

Кібернетичний підхід до розгляду систем управління базується на визначенні в їхньому складі технічного комплексу управління, каналів прямого (зворотного) зв'язку, пристрою зв'язку з об'єктом. Проходження інформації керуючого впливу на об'єкт управління та інформації про його стан утворюють цикл управління. Управління багатокомпонентним об'єктом управління здійснюється при посередництві множини пристроїв зв'язку з об'єктом та відповідної кількості циклів управління. Непрацездатність і/або неправильна робота технічних засобів циклів управління призводить до втрати (зменшення) якості управління.

Одним із видів цільового призначення об'єктів критичної інфраструктури є управління технологічними процесами в реальному масштабі часу. Використання мережі Інтернет для утворення каналів прямого (зворотного) зв'язку обумовлює загрозу інциденту безпеки критичної інфраструктури у формі кібератаки. Фахівець із реагування на кіберінциденти повинен здійснювати своєчасне виявлення та аналіз, стримування, усунення кібератаки, а також відновлювати штатне функціонування системи управління технологічними процесами у реальному масштабі часу. Наразі існуючий науковий апарат не відповідає вимогам практики, що складає наукову проблему.

До розгляду пропонується пристосування методології підтримки прийняття рішень оперативного персоналу систем управління технологічними процесами реального часу. Новизною викладеного підходу є відокремлення ситуацій непрацездатності та неправильної роботи технічних засобів, викликаних відмовою від наслідків кібератаки. Визначено фактори для оцінки тривалості часового відрізка від виявлення перших ознак до прояву цілі кібератаки.

Ключові слова: система управління технологічними процесами реального часу, реагування на інциденти.

P. Khusainov, S. Shtanenko, I. Churilova. The problem real time-based incident response in industrial control system

The cybernetic approach to the analysis of control systems is based on the components comprising the system: the control hardware, forward (and reverse) communication channels, and the interface with the controlled object. The flow of control information to the controlled object and information about its status constitute the control cycle. Control of a multi-component system is carried out through a set of communication devices connected to the system and a corresponding number of control cycles. Failure and/or malfunction of the technical components of control loops leads to a loss (or reduction) in control quality.

One of the primary functions of critical infrastructure facilities is the real-time management of technological processes. The use of the Internet to establish direct (two-way) communication channels poses a risk of unauthorized interference in the form of a cyberattack. A cyber incident response specialist must promptly detect, analyze, contain, and mitigate cyberattacks, as well as restore the normal operation of the process control system in real time. Currently, the existing scientific framework does not meet practical requirements, which poses a scientific challenge.

This paper proposes an adaptation of a decision-support methodology for operational personnel of real-time process control systems. What is novel about this approach is the distinction between situations of system failure and malfunctions of technical equipment caused by the consequences of a cyberattack. Factors have been identified to assess the duration of the time interval from the detection of the first signs to the full manifestation of a cyberattack.

Keywords: real time-based industrial control system, incident response.

Постановка проблеми (у загальному вигляді). Об'єкти критичної інфраструктури — об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Зокрема, на об'єкти критичної інфраструктури покладається забезпечення виконання за функцій та/або послуг управління технологічними процесами у сфері енергозабезпечення, водопостачання, водовідведення, фармацевтики, хімічної промисловості, виготовлення вакцин, транспорту, цивільного захисту і т. д. Сукупність параметрів штатного режиму функціонування критичної інфраструктури

відповідно до проєктного цільового призначення визначається їхнім оператором. Будь-яке порушення безперервності, стійкості, штатного режиму функціонування критичної інфраструктури чи окремого її об'єкта, реагування на яке потребує залучення додаткових сил і ресурсів, уособлює поняття “кризова ситуація”. Розглядаються два широкі класи причин (факторів) виникнення порушень штатного режиму функціонування об'єкта критичної інфраструктури. До першого класу належать причини (фактори), які обумовлюють події ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), які становлять загрозу безпеці об'єкта критичної інфраструктури, його системі управління технологічними процесами, до другого класу — всі можливі форми несанкціонованого втручання в його безпечне функціонування [1].

Об'єкти критичної інфраструктури відносяться до класу цілеспрямованих систем. Їхньою основною системною властивістю є здійснення управління — послідовна зміна станів об'єкта управління (об'єкта критичної інфраструктури) для досягнення (наближення до) цілі (одержання очікуваного результату) на визначеному часовому інтервалі функціонування. Процес управління має циклічний характер. Цикл управління є повторюваною послідовністю етапів вироблення, доведення, виконання та оцінювання результату керуючого впливу органом управління (об'єкта критичної інфраструктури) за методом програмного, оптимального управління чи авторегулювання. Зв'язність компонентів, здатних приймати, зберігати, перероблювати та передавати інформацію (керуючий вплив, опис стану об'єкта управління) уособлює справедливість застосування кібернетичного аспекту системного підходу для дослідження об'єктів критичної інфраструктури. Тракт передавання (перетворення) інформації в циклі управління ідеалізованої кібернетичної системи складається з таких функціональних компонентів: програмно-апаратний комплекс (органу управління); тракти каналів прямого (зворотного) зв'язку та пристрою зв'язку з об'єктом управління. За умови сталості (непошкодженості) об'єкта управління непрацездатність і/або неправильна робота функціональних компонентів такого об'єкта не дозволяє забезпечити сам принцип цілеспрямованості кібернетичної системи через неможливість забезпечити своєчасність надходження достовірної інформації про стан об'єкта управління, правильне вироблення та своєчасне доведення керуючого впливу і т. д. [2–4].

Втрата (тимчасове переривання) і/або недостовірність результатів передавання (перетворення) інформації хоча б в одному з множини трактів циклів управління, передбачених технічними умовами для об'єкта критичної інфраструктури, є фактичним проявом кризової ситуації через їхню непрацездатність (неправильну роботу). Ненавмисні причини такої ситуації через відмову програмно-апаратних засобів розглядаються у контексті теорії надійності, технічної діагностики, а негативний вплив відмов може бути нівельований (зменшений) на основі відповідного методичного апарату. Ознаки, аналогічні відмовам, характерні і прояву тактики *Impact* в кіберінцидентах, що обумовлені акціями *Advanced Persistence Threat*. Оперативне (кризове) реагування на кіберінциденти/кібератаки є прерогативою команди реагування на комп'ютерні надзвичайні події [5–11].

Аналіз останніх публікацій. Для одержання більш повної інформації необхідно звернутися до положень щодо організаційно-технічної моделі кіберзахисту [12]; ролі, завдань, функцій та відповідальності *Computer Security Incident Response Team (CSIRT)* під егідою *The Forum of Incident Response and Security Teams (FIRST)* [13; 14]; організації процесу реагування на кіберінциденти/кібератаки [15]; компетенції та результатів навчання професійного стандарту “Фахівець з реагування на інциденти кібербезпеки” [16].

Формулювання мети статті. Обґрунтування дослідження наукової проблеми, яка полягає в існуванні протиріччя між практичною необхідністю здійснювати оперативне (кризове) реагування на кіберінциденти несанкціонованого втручання в систему управління технологічними процесами реального часу (об'єкта критичної інфраструктури) у формі кібератак та відсутністю відповідного науково-методичного базису. До розгляду пропонується

пристосування методології підтримки прийняття рішень оперативного персоналу систем управління технологічними процесами реального часу у контексті кібернетичного підходу та нівелювання (усунення, зменшення) впливу невизначеності. Новизною викладеного підходу є відокремлення ситуацій непрацездатності та неправильної роботи програмно-апаратних засобів через відмову або внаслідок кібератаки.

Виклад основного матеріалу. Участь фахівця-оператора в управлінні технологічними процесами об'єкта критичної інфраструктури обумовлена необхідністю контролю та усунення (зменшення) за необхідністю відхилення фактичного результату керуючого впливу (стану об'єкта управління) від очікуваного, що не може бути здійснено автоматично програмно-апаратним комплексом органу управління (рис. 1). Непридатність працездатного програмно-апаратного комплексу (об'єкта управління) своєчасно виробляти правильні керуючі впливи у контексті забезпечення виконання ітерацій циклів управління на всьому часовому інтервалі функціонування об'єкта критичної інфраструктури будемо розглядати як явище “кризова ситуація компрометації тракту управління”. Словосполучення “компрометація тракту управління” пропонується розглядати у контексті понятійного апарату словосполучення “компрометація системи” [17]. У такій інтерпретації “тракт управління” є системою послідовно зв'язаних програмно-апаратних засобів, призначених для передавання (перетворення) інформації у циклі управління, структура якої автоматично утворюється і залишається сталою протягом часового інтервалу мінімум однієї ітерації проходження циклу управління. За умови сталості (непошкодженості) об'єкта управління причинами кризової ситуації компрометації тракту управління може бути:

несвоєчасність надходження (тимчасове припинення, перевищення граничного часу очікування) інформації керуючого впливу від програмно-апаратного комплексу (органу управління) до пристрою зв'язку з об'єктом через непрацездатність і/або неправильну роботу програмно-апаратних засобів тракту каналу прямого зв'язку;

несвоєчасність надходження (тимчасове припинення, перевищення граничного часу очікування) інформації про стан об'єкта управління від пристрою зв'язку з об'єктом до програмно-апаратного комплексу (органу управління) через непрацездатність і/або неправильну роботу програмно-апаратних засобів тракту каналу зворотного зв'язку;

невиконання керуючого впливу і/або неохочення інформації про стан об'єкта управління через непрацездатність і/або неправильну роботу програмно-апаратного засобу пристрою зв'язку з об'єктом, приймача і/або ефектора, та, відповідно, рецептора і/або передавача у його складі.

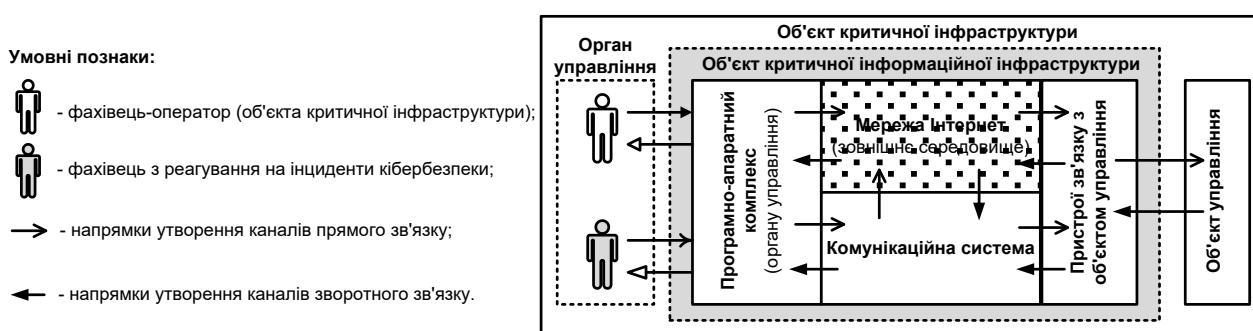


Рис. 1. Функціональна структура об'єкта критичної інфраструктури

Події, які призводять до непрацездатності і/або неправильної роботи програмно-апаратного засобу внаслідок зазвичай складної комбінації випадкових об'єктивних, суб'єктивних факторів (явищ) експлуатаційного, технологічного та організаційного характеру, прийнято асоціювати з поняттям “відмова” [6–9]. Прояв відмов як несприятливих

подій ненавмисного характеру уособлює першу складову поняття “інцидент безпеки критичної інфраструктури”. Друга складова поняття охоплює події несанкціонованого втручання (в функціонування об'єкта критичної інфраструктури). З'єднання комунікаційної системи з мережею Інтернет уособлює логічність розгляду для об'єкта критичної інформаційної інфраструктури (об'єкта критичної інфраструктури) множини форм несанкціонованого втручання у формі кібератаки, кіберпростору як середовища їх здійснення, роль та місце участі фахівця з реагування на інциденти кібербезпеки [12–16].

Сукупність програмно-апаратних засобів, які забезпечують функцію (функціональне призначення) передавання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів, утворюють такі функціональні компоненти (рис. 2):

канал прямого зв'язку для інформації керуючого впливу від програмно-апаратного комплексу (органу управління) в пристрій зв'язку з об'єктом управління;

канал зворотного зв'язку для інформації про стан об'єкта управління від пристрою зв'язку з об'єктом управління у програмно-апаратний комплекс (органу управління).

Пристрій зв'язку з об'єктом управління є програмно-апаратним засобом, який здійснює для перетворення інформації керуючого впливу з каналу прямого зв'язку у форму значень фізичних величин ефекторів впливу на об'єкт управління та інформації про стан об'єкта управління від рецепторів об'єкта управління у форму для каналу зворотного зв'язку.

Множина каналів прямого (зворотного) зв'язку, пристроїв зв'язку з об'єктом управління об'єкта критичної інфраструктури визначається технічним завданням (умовами, проєктом) відповідно до проєктного цільового призначення. Тракт каналу прямого (зворотного) зв'язку є системою послідовно зв'язаних програмно-апаратних засобів, призначених для передавання інформації через канал прямого (зворотного) зв'язку у кіберпросторі об'єкта критичної інформаційної інфраструктури, структура якої автоматично утворюється і залишається сталою протягом часового інтервалу мінімум однієї ітерації проходження циклу управління. Під поняттям “ітерація циклу управління” розглядається неперервне виконання послідовності операцій передавання (перетворення) інформації керуючого впливу від органу управління в об'єкт управління через тракт каналу прямого зв'язку, одержання і доставка інформації про стан об'єкта управління в орган управління через тракт каналу зворотного зв'язку.

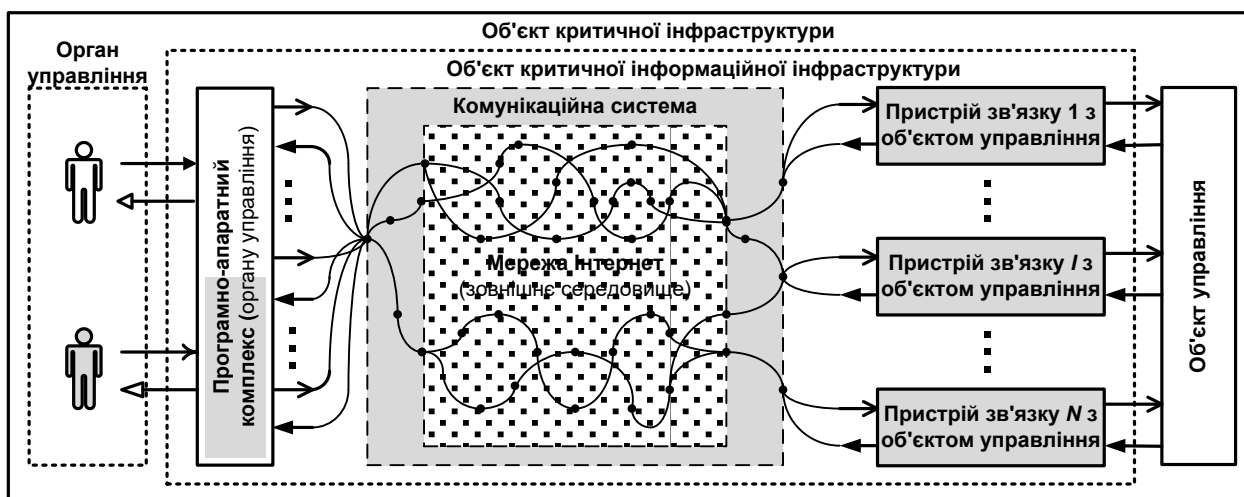


Рис. 2. Функціональні складові діяльності фахівця з реагування на інциденти кібербезпеки

Програмно-апаратний комплекс (органу управління) забезпечує виконання сукупності функцій для вироблення керуючих впливів в циклах управління об'єкта критичної інфраструктури на підставі інформації про стан об'єкта управління. Керуючий вплив є результатом його вибору з множини альтернативних варіантів (альтернатив). Порядок

створення множини альтернатив та вибору однієї з них визначається: методом управління (програмне, оптимальне, авторегулювання); особливостями цільової функції; характером функції оцінки корисності результату керуючого впливу (дослідження операцій, експертне оцінювання, імітаційне моделювання); невідповідністю одержуваної з каналу зворотного зв'язку інформації та реальним станом об'єкта управління. Мінімальна (допустима) невідповідність інформації дозволяє виробляти рішення автоматично на основі відповідних програмних алгоритмів керування, при перевищенні допустимого розходження – автоматизовано, за участю фахівця-оператора (об'єкта критичної інфраструктури).

За умови сталості (непошкодженості) об'єкта управління участь фахівця-оператора (об'єкта критичної інфраструктури) обумовлена явищем невизначеності (неповноти, недостовірності, неточності, обмеженості) та необхідністю його нівелювання (усунення, зменшення) при виборі керуючого впливу. Невизначеність є наслідком прояву одиничних, але, зазвичай, комплексних комбінацій обставин (причин, факторів) на етапах проєктування, розробки, впровадження та експлуатації системи управління технологічними процесами реального часу (об'єкта інформаційної інфраструктури), що передбачає обробку інформації в реальному масштабі часу або у темпі обслуговування технологічних процесів.

Можливість нівелювання (усунення, зменшення) впливу невизначеності базується на застосуванні апробованого науково-методичного апарату для адекватної оцінки, прогнозування та зменшення інтенсивності прояву відповідних обставин (причин, факторів). За характерною природою виникнення, приналежністю етапам життєвого циклу систем об'єкта критичної інформаційної інфраструктури та наявністю адекватного науково-методичного апарату можна відокремити когнітивно-помилкову, відмово-залежну та деструктивно-спрямовану підмножину обставин (причин, факторів) невизначеності.

Когнітивно-помилкова невизначеність. Когнітивна діяльність особи, яка приймає рішення (ОПР), розглядається як багаторівнева сукупність взаємозв'язаних процесів психофізичного, психологічного, гносеологічного та програмного характеру. Основні форми розумової діяльності: емпіричне, аксіоматичне, діалектичне. Емпіричне мислення базується на узагальненні попереднього досвіду, аксіоматичне – на застосуванні початкових знань про правила вирішення задачі. Діалектичне мислення є вищою формою психічних процесів людини, забезпечує позитивний прояв багатоваріантності, адаптації, самоорганізації, вибір рішення в умовах як повної, так і неповної інформації. Людина в ролі ОПР виступає складовим елементом ергатичної системи з функціями приймача, ретранслятора і перетворювача інформації, може здійснювати вибір рішення, контроль роботи об'єкта, вироблювати та виконувати команди.

Прямий чи опосередкований вплив на результат когнітивної діяльності ОПР мають психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формується) залежно від конкретних суспільно-історичних умов: світогляд (система поглядів на суспільство та природу явищ); інтереси (спрямованість на певні предмети та явища); здібності (індивідуальні особливості – умови успішного виконання якої-небудь однієї або кількох видів діяльності); темперамент; характер; увага (спрямованість свідомості на певний предмет або діяльність: стійкість, перемикавання, кількість та розподіл інформаційних одиниць).

При виборі рішення ОПР керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб'єктивними уявленнями, судженнями, емоціями. Людина має багатоканальне сприйняття, раціональне використання інформації, здатність до навчання, але і може здійснювати помилкові дії через малу пропускну спроможність, обмежену швидкість, втомлюваність, недостатність кваліфікації та досвіду. Основним підходом до нівелювання (усунення, зменшення) прояву когнітивно-помилкової невизначеності при виборі керуючого впливу фахівцем-оператором (об'єкта критичної інфраструктури) є органічне впровадження в його діяльність функцій інформаційної

підтримки прийняття рішень на базі програмно-апаратного комплексу (органу управління). Науково-методичний апарат інформаційної підтримки рішень оперативного персоналу технічних систем у реальному масштабі часу був розроблений та апробований під керівництвом професора Герасимова Б. М. під час проведення багатьох дисертаційних досліджень представниками цієї наукової школи [2; 3; 18].

Відмово-залежна невизначеність. Відмова – випадкова подія, яка полягає у втраті технічним об'єктом (система, компонент, елемент, пристрій, засіб) як самостійної одиниці з погляду надійності, здатності виконувати потрібну функцію. Під поняттям “функція” розглядається властивість такого технічного об'єкта відповідно до вимог нормативної та (чи) конструкторської (проектної) документації (на етапі розробки вимог, проєктування, виробництва, використання і ремонту об'єкта). Надійність – властивість об'єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах. В якості випадкових подій (обставин, причин), що можуть призвести до відмови, розглядаються:

недосконалість, порушення встановлених правил, норм проєктування та конструювання (конструкційна відмова);

невідповідність виготовлення проєкту нормам виробництва (виробнича відмова);

поступові зміни значень одного чи декількох параметрів (поступова відмова);

відмова чи несправність іншого технічного об'єкта (залежна відмова);

проєкт, виробництво, правила експлуатації, документація (систематична відмова);

перевищення навантаження (відмова через перевантаження);

неправильне чи необережне поводження (відмова через неправильне поводження);

неміцність без перевищення навантаження (відмова через неміцність);

процеси деградації при дотриманні усіх встановлених правил, норм проєктування, виготовлення та експлуатації (деградовна відмова);

непередбачуване стихійне лихо (відмова внаслідок стихійного лиха).

Неповнота (недостовірність, неточність, обмеженість) інформації про закони розподілу ймовірності випадкових подій виникнення відмов розглядається як відмово-залежна невизначеність. Прояв відмово-залежної невизначеності при виборі керуючого впливу фахівцем-оператором (об'єкта критичної інфраструктури) полягає у його залежності від своєчасного і правильного передавання (перетворення) інформації у трактах управління від відмов програмно-апаратних засобів трактів прямого (зворотного) зв'язку, пристроїв зв'язку з об'єктом. Раніше було зазначено, що непрацездатність і/або неправильна робота через відмови програмно-апаратних засобів передавання (перетворення) інформації хоча в одному з множини трактів управління повинна розглядатися як кризова ситуація компрометації тракту управління (об'єкта критичної інфраструктури).

Основним підходом до нівелювання (усунення, зменшення) прояву відмово-залежної невизначеності полягає у застосуванні резервування, оптимального управління запасними елементами, термінами експлуатації, технічного діагностування та обслуговування на основі апіорного аналізу надійності системи управління технологічними процесами (об'єкта інформаційної інфраструктури). Апіорний аналіз надійності полягає в обґрунтуванні вибору одного з можливих варіантів проєктування (створення) технічного об'єкта за умови наявності повної інформації про закони розподілу ймовірності випадкових подій виникнення відмов, що на практиці, зазвичай, повністю невідома для всіх програмно-апаратних засобів технічного об'єкта. Науково-методичний апарат нівелювання (усунення, зменшення) “апіорної невизначеності” в задачах теорії надійності був розроблений та апробований під керівництвом професора Креденцера Б. П. під час проведення багатьох дисертаційних досліджень представниками цієї наукової школи [6–9].

Деструктивно-спрямована невизначеність. Зазвичай, об'єкт управління є різновидом штучної системи, яка складається з множини структурних елементів, які мають фізичне

розташування у межах окремих територіально-технологічних майданчиків об'єкта критичної інфраструктури. Створення та експлуатація власної комунікаційної системи (об'єкта критичної інфраструктури) для утворення трактів каналів прямого (зворотного) зв'язку має високу вартість при значній кількості територіально-технологічних майданчиків, їх розташування на значній географічній відстані, складності побудови ліній комунікації і т. д. Тому, використання мережі Інтернет як універсального комунікаційного середовища між територіально-технологічних майданчиками (об'єкта критичної інфраструктури) полягає у їх комунікації через програмно-апаратні засоби автономних систем локальних провайдерів послуг Інтернету (*Internet Service Providers*).

Така організація трактів каналів прямого (зворотного) зв'язку (об'єкта критичної інфраструктури) зазвичай є найкращим варіантом зменшення відповідних експлуатаційних витрат, але має негативний аспект, який полягає у необхідності врахування можливості несанкціонованого втручання у формі кібератак [19–22]. Кібератака на об'єкт критичної інфраструктури – спрямовані (навмисні) дії в кіберпросторі, які здійснюються суб'єктом кібератаки (на об'єкт критичної інфраструктури) за допомогою засобів електронних комунікацій з метою (ціль) примушення (нав'язування) до прояву кризової ситуації.

Взагалі, поняття “ціль” уособлює очікуваний (ідеалізований, уявний) результат психологічної діяльності людини на певному інтервалі часу. Формулювання цілі виникає як певний стимул змінити поточну ситуацію у потрібному напрямку з урахуванням набутого досвіду. Лінійно-впорядкована послідовність дій, спрямована на досягнення цілі з деякої фіксованої початкової ситуації, називається траєкторією діяльності. Траєкторія діяльності є сукупністю структурованих казуальних відношень (причинно-наслідкові зв'язки, ланцюги зв'язків) просування до головної цілі через проміжні (часткові, тактичні). Ланцюжок зі структурованої послідовності типових дій (процедур), в якому кожна чергова дія створює умови для здійснення наступної, називається казуальним сценарієм. Поняття “сценарій” означає формалізований опис стереотипних знань у формі стандартної послідовності взаємозв'язаних фактів типової ситуації предметної області, послідовності дій або процедур досягнення цілей. Стереотипні знання – опис предметної області у формі послідовності фактів, який дозволяє передбачати та відновлювати пропущені факти.

Ціль кібератаки на об'єкт критичної інфраструктури уособлює очікуваний (ідеалізований, уявний) результат психологічної діяльності суб'єкта кібератаки (на об'єкт критичної інфраструктури) за визначений час для її досягнення (здійснення кібератаки). Введення поняття “суб'єкт кібератаки” здійснено для підкреслювання визначальної ролі антропогенної (людської) природи здійснення спрямованих (навмисних) дій у кіберпросторі з метою (ціль) примушення (нав'язування) до прояву кризової ситуації (об'єкта критичної інфраструктури) у формі проходження (виконання) відомої структурованої послідовності типових дій (процедур) казуального сценарію кібератаки. Отже, казуальний сценарій кібератаки визначає траєкторію діяльності суб'єкта кібератаки, яка спрямована на досягнення цілі кібератаки.

Примушення (нав'язування) до прояву кризової ситуації (ціль кібератаки на об'єкт критичної інфраструктури) може здійснюватися шляхом порушення штатного функціонування системи управління технологічними процесами (об'єкта критичної інформаційної інфраструктури), що полягає в одержанні хоча б одного успішного результату застосування технічних способів (*techniques*) на етапі досягнення тактичної цілі (*tactic*) *Impact* у такій формі (рис. 3):

відмова обслуговування (тимчасове припинення) пристрою зв'язку з об'єктом і/або ефектору в його складі (*Denial of Control*);



Рис. 3. Граф відношень між етапами досягнення тактичних цілей (*tactics*) казуального сценарію кібератаки на об'єкт критичної інфраструктури

відмова обслуговування (тимчасове припинення) пристрою зв'язку з об'єктом і/або рецептору в його складі (*Denial of View*);

недоступність пристрою зв'язку з об'єктом (*Loss of Availability*);

непрацездатність тракту каналу прямого зв'язку (*Loss of Control*);

непрацездатність тракту каналу зворотного зв'язку (*Loss of View*);

нав'язування хибної інформації керуючого впливу (*Manipulation of Control*);

нав'язування хибної інформації про стан об'єкта управління (*Manipulation of View*);

непрацездатність і/або неправильна робота функцій (процедур) безпеки технологічних процесів від несанкціонованого втручання (*Loss of Protection*);

непрацездатність і/або неправильна робота функцій (процедур) обробки аварійних ситуацій технологічних процесів (*Loss of Safety*);

порушення конфіденційності (витік) інформації керуючого впливу і/або про стан об'єкта управління (*Theft of Operation Information*);

довготривале та приховане нав'язування інформації керуючого впливу і/або про стан об'єкта управління для фізичного руйнування технологічних процесів (*Damage of Property*);

довготривале та приховане нав'язування інформації керуючого впливу і/або про стан об'єкта управління для зменшення продуктивності, якості, корисного ефекту технологічних процесів (*Loss of Productivity and Revenue*).

Досягнення цілі кібератаки на об'єкт критичної інфраструктури шляхом одержання хоча б одного успішного застосування технічних способів на етапі досягнення тактичної цілі *Impact* базується на якісному відпрацюванні етапів досягнення тактичних цілей та стадій:

Reconnaissance – збирання (узагальнення, аналіз) інформації про об'єкт критичної інформаційної інфраструктури (об'єкта критичної інфраструктури) для вироблення (уточнення) можливих казуальних сценаріїв для одержання успішного результату на етапі досягнення тактичної цілі *Gaining Access*;

Resource Development – підготовка (розробка) засобів для виконання казуальних сценаріїв одержання успішного результату на етапі досягнення тактичної цілі *Gaining Access*;

Gaining Access – стадія набуття повноважень авторизованого користувача в операційному середовищі хоча б одного з множини програмно-апаратних засобів функціональних компонентів системи управління технологічними процесами для виконання можливих казуальних сценаріїв для одержання успішного результату на етапі досягнення тактичної цілі *Action On Objects*;

Action On Objects – стадія багатоітераційного виконання казуальних сценаріїв для забезпечення можливості одержання успішного результату на етапі досягнення тактичної цілі *Impact*.

Орієнтовані дуги (див. рис. 3, а–в) ілюструють необхідність повернення до попередніх етапів (стадій) при неякісному результаті досягнення тактичних цілей відповідно до *Reconnaissance*, *Resource Development*, *Action On Objects*:

відсутність повної інформації для підготовки (розробки) засобів для виконання казуальних сценаріїв, у тому числі разом із виробленням іншого (більш перспективного) казуального сценарію одержання успішного результату на етапі досягнення тактичної цілі *Gaining Access* (див. рис. 3, а);

неможливість набуття повноважень авторизованого користувача в операційному середовищі хоча б одного з множини програмно-апаратних засобів функціональних

компонентів системи управління технологічними процесами, що обумовлює необхідність удосконалення (доброби) засобів для виконання казуальних сценаріїв одержання успішного результату стадії *Gaining Access* (див. рис. 3, б);

недостатність виконання дій *Action On Objects* для одержання хоча б одного успішного результату застосування технічних способів на етапі досягнення тактичної цілі *Impact*, у тому числі разом із виробленням іншого казуального сценарію одержання успішного результату стадії *Action On Objects* (див. рис. 3, в):

Persistence (забезпечення постійності повноважень *Initial Access*);

Privilege Escalation (розширення/зміна повноважень *Initial Access*);

Defense Evasion (запобігання виявлення несанкціонованого використання авторизованих повноважень *Initial Access* та *Privilege Escalation*);

Credential Access (одержання облікових та автентифікаційних даних для легітимного набуття повноважень поза контекстом тактичних цілей *Initial Access* та *Privilege Escalation*);

Discovery (одержання відомостей про внутрішню структуру та компоненти системи);

Lateral Movement (набуття авторизованих повноважень в операційному середовищі іншого програмно-апаратного засобу за результатами *Discovery*, але поза *Initial Access*);

Collection (акумуляування інформації системи для підготовки її подальшого витоку);

Command and Control (утворення прихованого каналу управління компонентом системи з повноваженнями авторизованого користувача);

Exfiltration (здійснення витоку інформації з циклів управління);

Inhibit Response Function (блокування процедур реагування на небезпечні стани технологічного процесу);

Impair Process Control (модифікація процедур реагування на небезпечні стани технологічного процесу та обробки інформації).

Прояв деструктивно-спрямованої невизначеності при виборі керуючого впливу фахівцем-оператором (об'єкта критичної інфраструктури) полягає у принциповій неповноті (недостовірності, неточності, обмеженості) інформації про успішний результат спрямованої (навмисної) реалізації суб'єктом кібератаки деструктивних технічних способів *Manipulation of Control, Manipulation of View, Loss of Protection, Loss of Safety, Damage of Property, Loss of Productivity and Revenue* на етапі досягнення тактичної цілі *Impact*, початок яких був раніше моменту спостереження та мав приховані ознаки акції *Advanced Persistent Threat*. Деструктивно-спрямована невизначеність уособлює складну комбінацію випадкових подій, обумовлених антропогенною (людською) сутністю суб'єкта кібератаки (на об'єкт критичної інфраструктури), для яких зазвичай невідома або принципово не може бути визначена функція розподілу ймовірностей, зокрема:

вибір певного варіанту з множини можливих казуальних сценаріїв траєкторії діяльності суб'єкта кібератаки (рис. 4) при застосуванні технічних способів (*techniques*) на етапах досягнення тактичних цілей:

– *Initial Access, Execution* стадії *Gaining Access*;

– *Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Inhibit Response Function, Impair Process Control* багатоітераційного проходження стадії *Action On Objects*;

– *Execution* стадії *Action On Objects*;

комбінування мотивації, кваліфікації та ресурсних обмежень суб'єкта кібератаки;

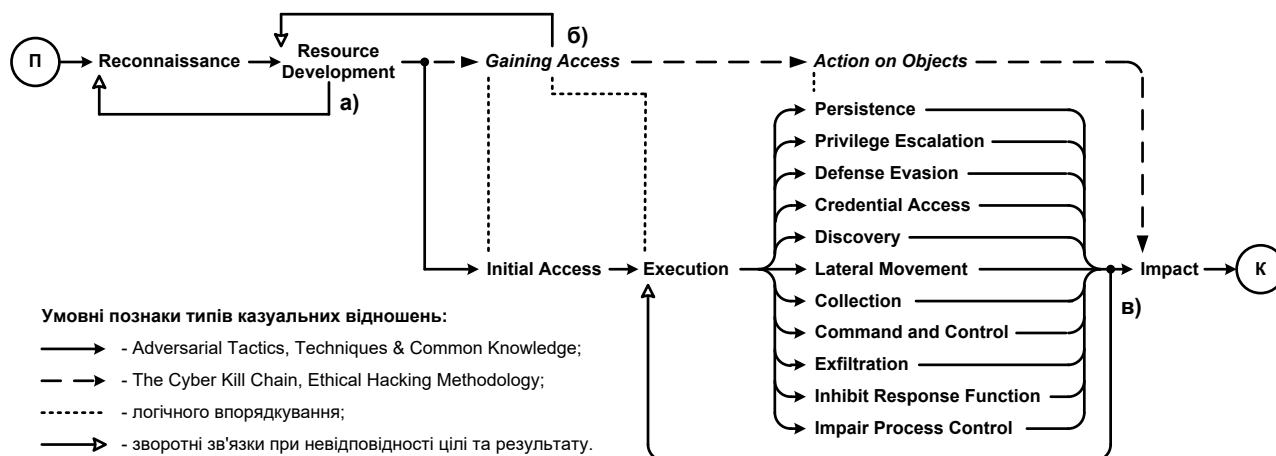


Рис. 4. Граф відношень формування можливих варіантів казуальних сценаріїв траєкторії діяльності суб'єкта кібератаки на об'єкт критичної інфраструктури

спроможність групового суб'єкта кібератаки забезпечити паралельність, координацію, обмін інформацією при виконанні незалежних операцій на множині можливих казуальних сценаріїв та технічних способів на етапах досягнення тактичних цілей та стадій;

наявність співпраці з інсайдером і/або інсайдерської інформації;

час початку суб'єктом кібератаки етапу досягнення тактичної цілі *Reconnaissance* та якість (повнота інформації) результатів його виконання;

час початку суб'єктом кібератаки стадії *Gaining Access*;

відрізок часу від початку суб'єктом кібератаки стадії *Gaining Access* до виявлення ознак її успішного результату;

відрізок часу від початку стадії *Gaining Access* до успішного результату етапу досягнення тактичної цілі *Impact*;

можливість розробки суб'єктом кібератаки на етапі досягнення тактичної цілі *Resource Development* новітніх засобів (з невідомими ознаками виявлення) для застосування технічних способів (*techniques*) на стадіях *Gaining Access* та *Action On Objects*.

Для з'ясування ролі орієнтованих дуг (див. рис. 4, а–в) необхідно звернутися до відповідних пояснень на граф відношень між етапами досягнення тактичних цілей (*tactics*) казуального сценарію кібератаки на об'єкт критичної інфраструктури (див. рис. 3, а–в). Успішний результат хоча б одного технічних способів на етапах досягнення тактичної цілі *Initial Access* та *Execution* утворюють комплекс умов для активації виконання шкідливого програмного засобу суб'єкта кібератаки в операційному середовищі деякого програмно-апаратного засобу системи управління технологічними процесами об'єкта критичної інфраструктури з повноваженнями авторизованого користувача.

Нівелювання (усунення, зменшення) прояву деструктивно-спрямованої невизначеності при виборі керуючого впливу фахівцем-оператором (об'єкта критичної інфраструктури) полягає у забезпеченні своєчасного та правильного оперативного (кризового) реагування на кіберінциденти. Реагування на кіберінциденти – структурована сукупність дій, спрямованих на підготовку до кіберінцидентів, їх виявлення та аналіз, мінімізацію шкоди від кіберінциденту та запобігання їх повторенню у майбутньому [5; 12; 17].

Раніше було доведено, що основна семантична відмінність поняття “кіберінцидент” від поняття “інцидент безпеки критичної інфраструктури” полягає в актуалізації розгляду для об'єктів критичної інфраструктури значної множини відомих казуальних сценаріїв здійснення несанкціонованого втручання у формі кібератак. За умови сталості (непошкодженості) об'єкта управління, програмно-апаратних засобів системи управління технологічними процесами в реальному масштабі часу (об'єкта критичної інформаційної інфраструктури) порушення

штатного функціонування об'єкта критичної інфраструктури здійснюється шляхом компрометації (хоча б одного, підмножини, всіх елементів) множини трактів управління технічними способами (*techniques*) досягнення тактичної цілі *Impact*. Своєчасне виявлення та аналіз фахівцем з реагування на інциденти кібербезпеки кіберінцидентів типу “кризова ситуація компрометації тракту управління”, вироблення множини автоматичних/автоматизованих сценаріїв виконання завдань стримування, усунення та відновлення штатного функціонування уособлює сутність практичних потреб.

Висновки. Усунення протиріччя між потребами практики та відсутністю необхідного теоретичного базису (наукова проблема) полягає у розробці науково-методичного апарату інформаційної підтримки вибору рішень фахівцем із реагування на інциденти кібербезпеки при виявленні, усуненні, стримуванні кіберінцидентів типу “кризова ситуація компрометації тракту управління” систем управління технологічними процесами в реальному масштабі часу, а також відновленні штатного функціонування об'єкта критичної інфраструктури.

В якості *найближчої перспективи* оприлюднення результатів дослідження наукової проблеми планується модель оцінки тривалості виконання казуального сценарію кібератаки на систему управління технологічними процесами в реальному масштабі часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX // Офіційний вісник України. 2021. № 98. С. 23. Ст. 6341.
2. Герасимов Б. М., Камишин В. В. Організаційна ергономіка: методи і алгоритми дослідження та проектування. К.: Інфосистем, 2009. 212 с.
3. Герасимов Б. М., Локажук В. М., Оксіюк О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень: навч. посіб. К.: Вид-во Європ. ун-ту, 2007. 335 с.
4. Хусаїнов П. В., Штаненко С. С. Обґрунтування інформаційної підтримки фахівця з реагування на інциденти кібербезпеки об'єкта критичної інфраструктури // Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. К.: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2025. № 8. С. 269–280. DOI: 10.58254/viti.8.2025.21.269.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. С. 42. Ст. 403.
6. ДСТУ 2860-94 Надійність техніки. Терміни та визначення. [Чинний від 1995-01-01]. URL: https://dbn.co.ua/load/normativy/dstu/dstu_2860_94/1-1-0-1099.
7. Основи теорії надійності та експлуатації радіоелектронних систем: навч. посіб. / В. І. Васишин, С. В. Женжера, О. В. Чечуй, А. П. Глушко. Х.: ХНУПС, 2018. – 208 с.
8. ДСТУ 2389-94 Технічне діагностування та контроль технічного стану. Терміни та визначення. [Чинний від 1995-01-01]. URL: <https://dbn.co.ua/load/normativy/dstu/1-1-0-1094>.
9. Фізичні основи теорії надійності: підруч. / М. К. Жердев, С. В. Ленков, Б. П. Креденцер та ін.; за ред. М. К. Жердева. К.: Видавничо-поліграфічний центр “Київський університет”, 2008. 215 с.
10. Adversarial Tactics, Techniques & Common Knowledge. URL: <https://attack.mitre.org>.
11. Хусаїнов П. В., Терещенко Т. П., Черешенко В. Б. Формування альтернативних стратегій тестування на проникнення Server-Side Web Application із врахуванням зменшення невизначеності // Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. К.: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2025. № 8. С. 257–268. DOI: 10.58254/viti.8.2025.20.257.
12. Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова КМУ від 29.12.2021 № 426 // Офіційний вісник України. 2022. № 4. С. 247. Ст. 219.
13. Computer Security Incident Response Team Services Framework, Service Role and Competencies. URL: <https://www.first.org/standards/frameworks/>.
14. The Modern Security Operations Center: The People, Process, and Technology for Operating SOC Services Joseph Muniz, Aamir Lakhani, Omar Santos, Moses Frost ISBN-10: 0135619858, ISBN-13: 978-0135619858 Addison-Wesley Professional.

15. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова КМУ від 04.04.2023 № 299 // Офіційний вісник України. 2023. № 39. С. 54. Ст. 2061.
16. Професійний стандарт “Фахівець з реагування на інциденти кібербезпеки”, затв. наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38. URL: https://register.nqa.gov.ua/uploads/0/571-fahivec_z_reaguvanna_na_incidenti_kiberbezpeki_v_2.pdf.
17. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570. URL: <https://zakon.rada.gov.ua/rada/show/v0570519-23#Text>.
18. Хусаїнов П. В. Система інформаційної підтримки адміністратора безпеки: структура, задачі, оцінка ефективності // Збірник наукових праць ВІТІ НТУУ “КПІ”. Вип. 3. К.: ВІТІ НТУУ “КПІ”, 2007. С. 146–155.
19. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX // Офіційний вісник України. 2021. № 6. С. 10. Ст. 306.
20. The Unified Kill Chain. URL: <https://www.unifiedkillchain.com>.
21. Certified Ethical Hacker. URL: <https://cert.eccouncil.org/certified-ethical-hacker.html>.
22. Хусаїнов П. В., Черниш Ю. О., Терещенко Т. П. Зменшення невизначеності оцінки часу компрометації Server-Side Web Application об'єкта критичної інфраструктури // Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. К.: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2025. № 7. С. 232–242. DOI: 10.58254/viti.7.2025.21.232.

Надійшла до редколегії 08.04.2026.

Схвалена до друку 22.05.2026.

Дата публікації 29.05.2026.

АВТОРИ НОМЕРА

1. **Андрієнко Оксана Володимирівна** – науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
2. **Антонюк Ярослав Михайлович** – старший науковий співробітник Інституту інформаційних технологій та систем Національної академії наук України, м. Київ, Україна.
3. **Бараннік Дмитро Володимирович** – доктор філософії, викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
4. **Бараннік Валерій Володимирович** – доктор філософії, викладач Харківського національного університету імені В. Н. Каразіна, м. Харків, Україна.
5. **Беляков Роберт Олегович** – доктор технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
6. **Бернацький Андрій Петрович** – доктор філософії, старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
7. **Бовда Едуард Миколайович** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
8. **Бондаренко Дмитро Михайлович** – начальник центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, м. Київ, Україна.
9. **Вороной Олександр Васильович** – науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
10. **Грінков Володимир Олександрович** – кандидат технічних наук, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
11. **Грінкова Галина Васиївна** – старший науковий співробітник Науково-дослідного інституту воєнної розвідки, м. Київ, Україна.
12. **Гудима Віктор Павлович** – кандидат технічних наук, доцент кафедри технічного забезпечення Національного університету оборони України, м. Київ, Україна.
13. **Данилюк Ігор Андрійович** – кандидат технічних наук, доцент, головний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
14. **Драглюк Олексій Вікторович** – начальник управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.
15. **Єрохін Віктор Федорович** – доктор технічних наук, професор, головний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
16. **Живило Євген Олександрович** – кандидат наук з державного управління, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем Національного університету «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна.
17. **Зарубенко Артур Олександрович** – доктор філософії, начальник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
18. **Зінченко Михайло Олександрович** – начальник науково-дослідного управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
19. **Клименко Віктор Михайлович** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

20. **Коваленко Ілля Григорович** – кандидат технічних наук, начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

21. **Коваленко Олексій Олександрович** – начальник Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

22. **Ковальчук Олег Олександрович** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

23. **Кокошинський Віталій Валерійович** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

24. **Кондрусь Андрій Володимирович** – заступник начальника кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

25. **Корольов Андрій Павлович** – кандидат технічних наук, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

26. **Крамарчук Владислав Вікторович** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

27. **Кузавков Василь Вікторович** – доктор технічних наук, професор, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

28. **Куцаєв Володимир Вікторович** – молодший науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

29. **Кучма Юрій Володимирович** – кандидат технічних наук, доцент, завідувач кафедри комп'ютерних наук ТОВ ПВНЗ «Університет сучасних технологій», м. Київ, Україна.

30. **Ланко Антон Вікторович** – начальник факультету інформаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

31. **Лапа Володимир Іванович** – викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

32. **Легкобит Володимир Сергійович** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

33. **Липський Олександр Анатолійович** – кандидат технічних наук, доцент, головний науковий співробітник Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, м. Київ, Україна.

34. **Масесов Микола Олександрович** – кандидат технічних наук, старший науковий співробітник, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

35. **Мазулевський Олег Євгенович** – кандидат технічних наук, начальник управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

36. **Мацаєнко Андрій Миколайович** – кандидат технічних наук, старший викладач кафедри електроніки та схемотехніки Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

37. **Металіди Олександр Геннадійович** – ад'юнкт науково-методичного центру Національного університету оборони України, м. Київ, Україна.

38. **Мочалюк Володимир Віталійович** – начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

39. **Нестеренко Микола Миколайович** – доктор технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

40. **Нестеров Олександр Миколайович** – доктор філософії, начальник кафедри бойового застосування підрозділів зв'язку Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

41. **Носков Олексій Олексійович** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

42. **Островський Анатолій Олексійович** – доцент кафедри технічного забезпечення Національного університету оборони України, м. Київ, Україна.

43. **Паламарчук Наталія Анатоліївна** – провідний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

44. **Паламарчук Світлана Анатоліївна** – начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

45. **Пантась Іван Олегович** – старший викладач кафедри комунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

46. **Пантась Сергій Олегович** – старший викладач кафедри комунікаційних систем та мереж Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

47. **Панченко Ігор В'ячеславович** – кандидат технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

48. **Пилипчук Ігор Юрійович** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

49. **Плахтій Максим Олександрович** – кандидат економічних наук, професор кафедри комп'ютерних наук, ТОВ ПВНЗ «Університет сучасних технологій», м. Київ, Україна.

50. **Побережець Тетяна Василівна** – науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

51. **Погребняк Сергій Васильович** – доктор філософії, старший викладач, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

52. **Поліновський Вячеслав Васильович** – кандидат технічних наук, доцент, професор кафедри комп'ютерних наук ТОВ ПВНЗ «Університет сучасних технологій», м. Київ, Україна.

53. **Радзівілов Григорій Данилович** – кандидат технічних наук, професор, заступник начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут з наукової роботи, м. Київ, Україна.

54. **Рибка Євгеній Миколайович** – начальник факультету Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

55. **Романенко Марія Михайлівна** – доктор філософії, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

56. **Руденко Володимир Іванович** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

57. **Сайко Володимир Григорович** – доктор технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

58. **Самохвалов Юрій Якович** – доктор технічних наук, професор кафедри інтелектуальних технологій Київського національного університету імені Тараса Шевченка, м. Київ, Україна.

59. **Семитківська Ірина Володимирівна** – старший помічник начальника науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
60. **Симоненко Олександр Анатолійович** – кандидат технічних наук, доцент, начальник науково-методичного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
61. **Сінько Вікторія Володимирівна** – доктор філософії, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
62. **Скоропад Сергій Іванович** – старший викладач кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, м. Київ, Україна.
63. **Слюсар Петро Петрович** – науковий співробітник Науково-дослідного інституту воєнної розвідки, м. Київ, Україна.
64. **Солодовник В'ячеслав Ігорович** – доктор філософії, заступник начальника кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
65. **Станілога Олександр Олександрович** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
66. **Стефанишин Ярослав Іванович** – науковий співробітник Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, м. Київ, Україна.
67. **Тлустий Андрій Олександрович** – ад'юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
68. **Троцько Олександр Олександрович** – кандидат технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
69. **Устинов Дмитро Андрійович** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
70. **Ушань Владислав Миколайович** – кандидат технічних наук, доцент кафедри тактики Військового інституту танкових військ Національного технічного університету «Харківський політехнічний інститут», м. Харків, Україна.
71. **Фесенко Олексій Дмитрович** – доктор філософії, доцент кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
72. **Фесьоха Віталій Вікторович** – доктор філософії, доцент, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
73. **Фесьоха Надія Олександрівна** – доктор філософії, доцент, провідний науковий співробітник науково-методичного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
74. **Хавер Анюта Вячеславівна** – аспірант Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.
75. **Хусаїнов Павло Валентинович** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
76. **Цимбал Ірина Володимирівна** – науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.
77. **Чурілова Ірина Сергіївна** – незалежний науковець, м. Київ, Україна.
78. **Штаненко Сергій Станіславович** – кандидат технічних наук, доцент, заступник начальника центру Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

79. **Яковчук Олександр Вікторович** – начальник науково-дослідного відділу – заступник начальника науково-дослідного управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

80. **Яровий Віталій Сергійович** – доктор філософії, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Наукові статті у фахових виданнях повинні мати такі необхідні елементи:

анотація як стисла стаття;

постановка проблеми у загальному вигляді та її зв'язок із важливими науково-практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано розв'язання зазначеної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується стаття;

формулювання мети статті (постановка наукового завдання);

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів;

висновки з цього дослідження і **перспективи** подальших досліджень у зазначеному напрямку;

список використаних джерел: 10–15 посилань терміном **не більше 10 років**.

Редакція не рекомендує використання джерел інформації держав-агресорів.

До друку приймаються оригінальні наукові праці, які не було відправлено до інших редакцій та не опубліковано раніше в інших виданнях.

Рукопис статті потрібно подавати разом з наступними документами:

довідка про результати перевірки на академічний плагіат;

акт експертної оцінки про можливість відкритого опублікування (1 примірник);

згода на публікацію статті та оприлюднення персональних даних;

відомості про автора (авторів) за формою: прізвище, ім'я та по батькові; науковий ступінь, вчене звання, посада; назва установи, де працює автор, її місце розташування (місто, країна); обліковий запис автора ORCID, електронна адреса та номер телефону.

Відомості про автора (авторів) подаються окремим супровідним файлом. Наприклад:

№ з/п	Українська мова	Англійська мова
1	Шевченко Олександр Іванович Кандидат технічних наук Доцент Старший викладач Військовий інститут телекомунікацій та інформатизації імені Героїв Крут; м. Київ, Україна https://orcid.org/0000-0000-0000-0000 e-mail _____, телефон _____	Shevchenko Oleksandr Candidate of Technical Sciences Associate Professor Senior Lecturer Military Institute of Telecommunications and Informatization Technologies named after Heroes of Kruty; Kyiv, Ukraine https://orcid.org/0000-0000-0000-0000

Рукопис подається в друкованому та електронному вигляді у текстовому редакторі Microsoft Word, а також може бути надісланий за електронною адресою: naukaviti@viti.edu.ua.

Якщо стаття подається в електронному вигляді, супровідні документи подаються у сканованому вигляді.

Обсяг рукопису – не менше 7 повних аркушів українською або англійською мовами.

Формат аркушу – А4 (210 мм × 297 мм).

Параметри сторінки: зліва – 20 мм, справа – 20 мм, зверху – 20 мм, знизу – 20 мм.

Основний шрифт статті – Times New Roman, розмір 12 пт, міжрядковий інтервал – 1,0; абзацний відступ – 1,0 см; вирівнювання – по ширині; із виключенням переносів.

У лівому кутку першої сторінки на першому рядку друкується шифр УДК, розмір 12 пт, у правому кутку першої сторінки на другому рядку – дані про авторів: науковий ступінь, вчене звання, ініціали і прізвище автора, ORCID, в дужках назва установи, де він працює. Наприклад: к. т. н. Шевченко О. І. ORCID: 0000-0000-0000-0000 (ВІТІ ім. Героїв Крут). Далі через рядок друкується назва статті (відцентрована, великими напівжирними літерами).

Пропуск (перед і після назви статті та кожного розділу) – 1 рядок.

Анотацію друкують курсивом, шрифт Times New Roman, розмір 10 пт. Анотацію та ключові слова приводять українською та англійською мовами. Обсяг кожної з них не менше **1800 знаків з пробілами**, включаючи ключові слова. Анотація повинна бути структурована таким чином: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після анотації вказати 6–8 ключових слів окремо українською та англійською мовами.

Список використаних джерел оформлюється шрифтом Times New Roman, розмір 11 пт, та складається з урахуванням Національного стандарту України ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання».

Посилання на використані джерела наводяться у тексті статті у квадратних дужках [...] із зазначенням порядкового номеру бібліографічного посилання у списку.

Редакційна колегія залишає за собою право вносити зміни в рукопис редакційного характеру.

Телефон для довідок: (044) 256-22-37.

Адреса сайту збірника: <https://journal.viti.edu.ua/index.php/cicst/issue/archive>.

Електронна адреса для надання статей: naukaviti@viti.edu.ua.