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
№ 7

Communication, informatization and cybersecurity systems and technologies
№ 7

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

The book containes 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 – 2025 – Kyiv

УДК 621
ББК Ц4 (4Укр) 39
З – 415

Системи і технології зв'язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. – Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. – 2025. – № 7. – 264 с. – DOI: 10.58254/viti.7.2025.

ISSN 2786-6610

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

При передрукуванні 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 № 11 від 30.04.2025).

Науковий профіль видання:
125 Кібербезпека;
126 Інформаційні системи та технології;
255 Озброєння та військова техніка

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

Відповідальний за випуск: Куцаєв В. В.
Зам. № 129. Друк. арк. 33,00. Ум.-друк. арк. 30,69. Обл.-вид. арк. 28,54.
Формат паперу 60×84/8. Тираж 57 прим.
Адреса друкарні ВІТІ імені Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

З М І С Т

1	**Бернацький А. П., Коваленко О. О.** Адаптивне керування бойовим середовищем на основі просторово-часової ентропії	5
2	**Волошин В. В., Ковальчук Б. П., Зінченко М. О., Шаповал В. М., Макарчук В. І.** Методика відокремлення шумів у спектрограмі від реальних даних за допомогою порогової бінаризації	19
3	**Данилюк І. А., Лазута Р. Г., Куцаєв В. В., Цимбал І. В.** Дослідження перспектив застосування квантових технологій у Збройних Силах України	28
4	**Корольов А. П., Мацаєнко А. М., Роскошний Д. В.** Особливості розрахунку часу обчислень під час проєктування цифрових фільтрів на мікроконтролерах	44
5	**Креденцер Б. П., Унтілова О. О.** Модель надійності системи безперервного використання зі структурною надлишковістю з паралельною витратою складових резервного часу	53
6	**Кузавков В. В., Ланко А. В.** Застосування безконтактного індукційного методу при визначенні показників надійності об’єкта контролю	65
7	**Кузавков В. В., Тлустий А. О.** Аналіз статистичних тестів псевдовипадкових послідовностей	74
8	**Любарський С. В., Кондратюк А. Г., Шарнін С. А., Здоренко Ю. М.** Функціональна модель рефакторингу об’єктно-орієнтованого коду на основі методів штучного інтелекту для забезпечення завдання безпеки програмного коду	81
9	**Масесов М. О.** Концептуальна модель предметної області системи зв’язку	92
10	**Нестеренко І. К.** Спрощений метод розрахунку коефіцієнта частотної вибірковості приймача	100
11	**Панченко І. В., Бондаренко Д. М., Липський О. А., Стефанишин Я. І., Ушаков В. Д.** Підвищення захищеності радіоліній спеціального зв’язку БпЛА	110
12	**Радзівілов Г. Д., Думітраш О. В.** Характеристика спроможності існуючих рішень управління радіозв’язністю бездротових сенсорних мереж тактичної ланки управління	122
13	**Руденко В. І., Зінченко М. О., Яковчук О. В., Плугова О. Б.** Концептуальні аспекти щодо розробки перспективної моделі системи супутникового зв’язку спеціального призначення в умовах впливу засобів радіоелектронної боротьби	130
14	**Савченко В. А., Хавер А. В.** Метод розрахунку кіберстійкості 2-1 рівнів моделі Purdue проти спеціалізованого технологічного троянського програмного забезпечення	147
15	**Сайко В. Г., Радзівілов Г. Д., Комаров В. О.** Спосіб та інтегрований комплекс визначення місцезнаходження наземних джерел радіовипромінювання на базі БпЛА спеціального призначення	165
16	**Сайко В. Г., Станілога О. О.** Аналіз тенденцій розвитку та модель оцінки характеристик ефективності безпроводових мереж систем когнітивного радіо спеціального призначення	177
17	**Фесенко О. Д., Колтовсков Д. Г., Остапчук В. М., Макаренко О. О.** Аналіз динаміки кібератак на об’єкти критичної інфраструктури в умовах геополітичної напруженості	187
18	**Фесьоха В. В., Кисиленко Д. Ю.** Метод самонавчання системи кіберзахисту на основі інваріантів поведінки поліморфного та метаморфного шкідливого програмного забезпечення	202
19	**Фомкін Д. В., Шемендюк О. В., Ткач В. О., Балан Д. Д.** Аналіз моделей машинного навчання для виявлення шкідливого програмного коду в файлах PDF: вибір оптимальної моделі	213
20	**Хоменко П. В., Радзівілов Г. Д., Ільїнов М. Д.** Аналіз функціональних характеристик сучасних радіозасобів класу Manet	222
21	**Хусаінов П. В., Черниш Ю. О., Терещенко Т. П.** Зменшення невизначеності оцінки часу компрометації Server-side Web Application об’єкта критичної інфраструктури	232
22	**Штаненко С. С., Толюпа С. В., Самохвалов Ю. Я.** Діагностична модель розпізнавання технічного стану мікропроцесорних систем з елементами штучного інтелекту	243
	Автори номера	259
	Пам’ятка автору	263

C O N T E N T S

1	**A. Bernatskyi, O. Kovalenko** Adaptive control of the combat environment based on spatio-temporal entropy	5
2	**V. Voloshyn, B. Kovalchuk, M. Zinchenko, V. Shapoval, V. Makarchuk** Method of separation of noise in spectrograms from real data using threshold binarization	19
3	**I. Danyliuk, R. Lazuta, V. Kutsaiev, I. Tsymbal** Research into the prospects of application of quantum technologies in the Armed Forces of Ukraine	28
4	**A. Korolov, A. Matsayenko, D. Roskoshniy** Features of calculating computing time when designing digital filters on STM32F103 microcontrollers from STMicroelectronics Corporation	44
5	**B. Kredenzer, O. Untilova** Reliability model of a continuously operating system with structural redundancy and parallel consumption of reserve time components	53
6	**V. Kuzavkov, A. Lanko** Application of non-contact induction method in determining reliability indicators of the control object	65
7	**V. Kuzavkov, A. Tlustyi** Analysis of statistical tests of pseudorando sequences	74
8	**S. Liubarskyi, A. Kondratiuk, S. Sharnin, Y. Zdorenko** Functional model of object-oriented code refactoring based on artificial intelligence methods to provide security tasks of software code	81
9	**M. Masesov** Conceptual model of the subject area of communication systems	92
10	**I. Nesterenko** Simplified method of calculation coefficient of frequency selectivity of the receiver	100
11	**I. Panchenko, D. Bondarenko, O. Lypskyi, Ya. Stefanyshyn, V. Ushakov** Increasing the security of UAV special communication radio lines	110
12	**H. Radzivilov, O. Dumitrash** Assessment of the capabilities of existing radio connectivity management solutions for tactical-level wireless sensor networks	122
13	**V. Rudenko, M. Zinchenko, O. Yakovchuk, O. Plugova** Conceptual aspects of developing a promising model of a special-purpose satellite communication system under the influence of electronic warfare means	130
14	**V. Savchenko, A. Khaver** Method for calculating the cyber resilience of levels 2-1 of the Purdue model against specialized technological trojan software	147
15	**V. Saiko, G. Radzivilov, V. Komarov** Method and integrated complex for determining the location of terrestrial sources of radio radiation based on special-purpose UAVs	165
16	**V. Sayko, O. Staniloha** Analysis of trends in development and a model for evaluating the performance characteristics of wireless networks used in special purpose cognitive radio systems	177
17	**O. Fesenko, D. Koltovskov, V. Ostapchuk, O. Makarenko** Analysis of the dynamics of cyberattacks on critical infrastructure objects under geopolitical tensions	187
18	**V. Fesokha, D. Kysylenko** A method of self-learning of a cyber defence system based on behavioural invariants of polymorphic and metamorphic malware	202
19	**D. Fomkin, O. Shemendyk, V. Tkach, D. Balan** Comparative analysis of machine learning models for malware detection in PDF: evaluation of training and testing criteria	213
20	**P. Khomenko, H. Radzivilov, M. Ilinov** Analysis of the functionality of Manet tactical radio systems	222
21	**P. Khusainov, Y. Chernysh, T. Tereshchenko** Decreasing an indetermination of evaluation of time to compromise Server-Side Web Application of Industrial Control System	232
22	**S. Shtanenko, S. Toliupa, Y. Samokhvalov** Diagnostic model for identifying the technical condition of microprocessor systems with elements of artificial intelligence	243
	About authors	259
	Memo to the author	263

DOI: 10.58254/viti.7.2025.01.05

УДК 621.3:623.4:629.07-044.4

PhD Бернацький А. П. ORCID: 0000-0003-0379-075X (ВІТІ ім. Героїв Крут)
Коваленко О. О. ORCID: 0009-0008-4087-8770 (ВІТІ ім. Героїв Крут)

АДАПТИВНЕ КЕРУВАННЯ БОЙОВИМ СЕРЕДОВИЩЕМ НА ОСНОВІ ПРОСТОРОВО-ЧАСОВОЇ ЕНТРОПІЇ

У роботі запропоновано концепцію ентропійного аналізу бойового середовища, яка інтерпретується як багаторівнева термодинамічно замкнута система з динамічно змінною структурою. Визначено, що ключовим викликом сучасного поля бою є високий рівень невизначеності, який унеможливлює класичне централізоване управління. У цьому контексті ентропія розглядається як операційна змінна, що дозволяє кількісно описати ступінь організованості, хаотичності, інформаційної фрагментації та структурної стабільності військової обстановки. З метою формалізації цього підходу побудовано просторово-часовий ентропійний функціонал, який містить термодинамічну та інформаційну компоненти. Запропоновано варіант побудови ентропійної карти середовища та механізмів автоматизованої реакції автономних БпЛА, РНС(К), з подальшою реалізацією моделі у симуляційному середовищі Gazebo, де простір бойових дій відображається у вигляді воксельної сітки з динамічним оновленням ентропійних показників. Введено концепцію змінної ентропійної метрики, що дозволяє адаптувати ваги впливу кожного з типів ентропії залежно від конкретного типу бойового середовища та фаз операції. Такий підхід забезпечує системний перехід від реактивного до проактивного управління, що базується на прогнозуванні ентропійної динаміки та своєчасному перерозподілі ресурсів.

Представлено результати симуляцій трьох типових сценаріїв: оборони стратегічного об'єкта, наступальної операції та евакуації поранених, які демонструють зменшення системного хаосу на 45–56 % з покращенням ситуаційної обізнаності, зниження ентропійного ризику під час навігації та посилення тактичної стійкості системи.

Таким чином, запропонована парадигма формує наукове й прикладне підґрунтя для створення універсальної системи ентропійного керування в багатоплатформних автономних бойових операціях нового покоління.

Ключові слова: *автономні бойові платформи, адаптивне управління, багаторівнева система, безпілотний агент, БпЛА, воксельна сітка, ентропія, інформаційна невизначеність, карта, метрика, НРС(К), просторово-часова ентропія, симуляційне середовище, термодинамічна модель.*

A. Bernatskyi, O. Kovalenko. Adaptive control of the combat environment based on spatio-temporal entropy

This study proposes a novel concept of entropic analysis of the battlefield environment, interpreted as a multi– layered, thermodynamically closed system with a dynamically evolving structure. It identifies a high level of uncertainty as a key challenge of modern combat zones, which renders classical centralized control approaches ineffective. In this context, entropy is treated as an operational variable that enables the quantitative assessment of system organization, chaoticity, informational fragmentation, and structural stability of the operational environment. To formalize this approach, a spatio– temporal entropic functional is developed, comprising both thermodynamic and informational components. A method for constructing an entropy map of the environment and mechanisms for autonomous UAV and UGV reaction is proposed, followed by the implementation of the model in the Gazebo simulation platform. In this setting, the battlefield is represented as a voxel– based grid with dynamic updates of entropy indicators. The study introduces the concept of a variable entropic metric that adapts the weighting of different entropy components based on the type of combat environment and operational phase. This approach facilitates a systemic transition from reactive to proactive command and control, grounded in the prediction of entropic dynamics and real– time resource redistribution.

Simulation results for three typical scenarios – defense of a strategic object, offensive operation, and casualty evacuation – demonstrate a reduction in systemic chaos by 45–56 %, improved situational awareness, reduced entropic navigation risk, and enhanced tactical resilience.

Thus, the proposed paradigm provides a theoretical and applied foundation for the development of a universal entropic control system in next– generation multi– platform autonomous combat operations.

Keywords: *autonomous combat platforms, adaptive control, multi-layered system, unmanned agent, unmanned aerial vehicle (UAV), voxel grid, entropy, informational uncertainty, map, metric, unmanned ground vehicle (UGV), spatio-temporal entropy, simulation environment, thermodynamic model.*

Постановка проблеми

У сучасному театрі бойових дій, який характеризується високим ступенем динамічності, невизначеності та багатофакторності, поняття ентропії середовища набуває фундаментального значення. Ентропія як міра невпорядкованості або інформаційної складності системи дозволяє кількісно оцінювати ступінь організованості або хаосу у бойовому просторі. Висока ентропія може свідчити про непередбачуваність обстановки, порушення логістичних ланцюгів, втрату контролю над інформаційними потоками чи зростання загрози з боку асиметричних чинників, що особливо критично в умовах гібридної війни.

Розуміння та аналіз ентропії середовища в режимі реального часу дозволяє командним центрам та роботизованим автономним системам приймати обґрунтовані рішення в реальному часі, адаптуючись до змін і попереджаючи системні збої. Зокрема, в умовах інформаційної війни, кіберзагроз та багаторівневої взаємодії між людиною і машиною, здатність до ідентифікації “гарячих точок” ентропії у фізичному чи віртуальному середовищі може бути вирішальною для збереження оперативної переваги. Аналіз ентропії допомагає також оцінити стабільність логістичних маршрутів, ефективність розвідки, ступінь демаскування підрозділів і навіть вірогідність появи нових загроз.

Аналіз останніх досліджень і публікацій

Проведений аналіз наукових джерел свідчить про зростаючий інтерес до застосування ентропійних підходів у військовій справі, зокрема у сфері ситуаційної обізнаності, автономного управління та бойового моделювання. Дослідження демонструють, що ентропія активно використовується для кількісної оцінки невизначеності в даних сенсорного спостереження, розвідки, планування маршрутів та оцінки ризиків у складних операційних середовищах. Наприклад, у контексті автономних безпілотників ентропія дозволяє визначити області з найменшою інформативністю для цілеспрямованої розвідки (exploration vs. exploitation), підвищуючи ефективність розподілу ресурсів у розвідувальних місіях.

Так, наприклад, автори А. О. Подорожняк і Г. В. Земляна в [1] розглядають методи впливу на БпЛА, включно із застосуванням технологій Data Mining для аналізу та прогнозування їх поведінки. Під час дослідження використання ентропійних підходів для оцінки невизначеності в даних сенсорного спостереження та розвідки, автори розглядають ентропію переважно в інформаційному сенсі, як інструмент оцінки невизначеності. Тобто, ентропія для них – це локальна інформаційна характеристика, що допомагає фільтрувати чи уточнювати дані. Стаття-дослідження [2] автора Ю. І. Приходько присвячена теоретичним основам та методологічним засадам трансформації систем під впливом зовнішніх і внутрішніх чинників. Автор проводить обґрунтування закономірності та принципів трансформації, визначає чинники цього процесу, включно з аналізом ентропійних характеристик систем у контексті їхньої еволюції та самоорганізації. Причому основний фокус зроблено на еволюції складних систем і трансформації їхніх структур у відповідь на зовнішні збурення. Автор вводить ентропію в рамках загальної теорії систем, описуючи її вплив на динаміку організації. У своїй праці [3] автори М. І. Трєбін і О. В. Трєбін проводять аналіз феномену гібридної війни з акцентом на контекст збройної агресії рф проти України, де розглядається роль інформаційної складової та ентропійних процесів у сучасних військових конфліктах і підкреслюється важливість розуміння невизначеності та хаосу в бойових діях для розробки ефективних стратегій протидії. Автори визначають ентропію як синонім до хаосу, інформаційної плутанини, медійної невизначеності. Аналіз ґрунтується більше на якісному, політико-соціальному підході, ніж на формальному моделюванні.

Сучасні дослідження ентропії в контексті бойових середовищ хоча й демонструють зростаючий інтерес застосування ентропійних методів у контексті сучасних бойових дій, але наявні підходи залишаються фрагментарними та переважно зосередженими на локальному

інформаційному аналізі. Здебільшого ентропія розглядається як характеристика невизначеності сенсорних даних, розвідувальної інформації або кіберпростору, без належної уваги до її потенціалу як глобального системного показника впорядкованості бойового середовища. Водночас бойове середовище є багаторівневою, динамічною та просторово розподіленою системою, яка охоплює взаємодію автономних платформ, інфраструктурних об'єктів, інформаційних мереж і факторів зовнішнього впливу. Відсутність термодинамічно обґрунтованих моделей, здатних кількісно описувати зміну ентропії в таких системах, обмежує можливості адаптивного управління та прогнозування розвитку бойової ситуації [10]. Крім того, бракує формалізованих підходів до інтеграції ентропійного аналізу в середовища моделювання та симуляції, що унеможливлює тестування стратегій зниження хаосу та підвищення структурної стійкості у бойових сценаріях. Таким чином, актуальним є формування нової наукової парадигми, яка б поєднувала інформаційні, просторові та фізичні аспекти ентропії для системного аналізу й оптимізації бойових середовищ як складних, замкнутих, термодинамічно керованих систем.

Метою статті є розробка теоретико-методологічних засад і формалізованої моделі ентропії бойового середовища як багаторівневої замкнутої системи, з урахуванням її термодинамічних, просторових та інформаційних характеристик. Запропонована концепція має на меті забезпечити кількісну оцінку впорядкованості бойової ситуації в динаміці, інтегрувати ентропійний аналіз у сучасні симуляційні платформи (напр., Gazebo, Webots та ін.), а також сформувати підґрунтя для розробки адаптивних стратегій управління бойовими операціями, спрямованих на мінімізацію системного хаосу та підвищення структурної стійкості операційного середовища.

Виклад основного матеріалу

Бойове середовище сучасного театру воєнних дій є складною багатокомпонентною системою, що містить фізичні, інформаційні, когнітивні та кібернетичні рівні взаємодії. У термінах системного аналізу таке середовище можна трактувати як замкнуту або умовно замкнуту динамічну систему, в межах якої відбувається постійний обмін енергією, інформацією та структурними змінами між її підсистемами: бойовими платформами (UGV, UAV, USV – які в подальшому будемо називати безпілотними агентами (БА) відповідного типу), командними центрами, логістичними каналами, об'єктами інфраструктури тощо. Внаслідок взаємодії цих елементів середовище демонструє складну поведінку, що характеризується як впорядкованими, так і хаотичними процесами.

У цьому контексті доцільно розглядати ентропію бойового середовища як узагальнену міру його впорядкованості або невизначеності, що відображає поточний стан системної організації. З одного боку, високий рівень впорядкованості, а саме низька ентропія, свідчить про структурну стабільність, передбачуваність маршрутів, контрольованість комунікацій та взаємодій. З іншого боку, підвищення ентропії свідчить про зростання невизначеності, збої у командному управлінні, порушення логістичних структур або появу асиметричних загроз. Відтак, ентропія бойового середовища може бути розглянута як операційна змінна, що відображає стан функціональної цілісності бойової системи.

Для забезпечення формалізації цього підходу введемо поняття просторово-часового ентропійного функціонала $S(x, y, z, t)$, що описує локальну або глобальну ентропію середовища з урахуванням тривимірної топології, часової динаміки та множини взаємодіючих об'єктів. Такий функціонал може бути побудований на основі поєднання термодинамічної ентропії на основі розподілу енергетичних впливів та інформаційної ентропії на основі розподілу ймовірностей станів об'єктів або інформаційних потоків [5]. Таким чином, запропонована теоретична база дозволяє перейти від інтуїтивного розуміння невизначеності до її кількісного аналізу, що є необхідною умовою для моделювання, прогнозування та адаптивного керування бойовими діями у складних сценаріях.

З метою переходу від концептуального розуміння до практичного використання ентропійної характеристики бойового середовища проведемо формалізацію та опишемо математичну модель ентропії бойового середовища. Запропонований підхід ґрунтується на уявленні бойового простору як багаторівневої системи, у якій кожен рівень (тактичний, оперативний, стратегічний) може бути змодельований у вигляді просторової області $\Omega \subset R^3$ з дискретною або неперервною динамікою об'єктів, що діють у часі $t \in [0, T]$.

Нехай система складається з множини бойових агентів $A = \{a_1, a_2, \dots, a_n\}$, кожен з яких перебуває у деякому стані $s_i(t)$, визначеному параметрами позиції, швидкості, ролі, рівнем енергії та функціонального навантаження. Визначимо ймовірність $p_i(t)$ перебування агента a_i у певному критичному або "хаотичному" стані в момент часу t. Тоді інформаційна ентропія системи може бути визначена за формулою Шеннона [4]:

$$S_{info}(t) = -\sum_{i=1}^{n} p_i(t) \log p_i(t) \,. \tag{1}$$

Однак для моделювання просторово-часової динаміки впорядкованості середовища ми розширимо підхід, увівши розподілену ентропійну щільність $\rho_S(x, y, z, t)$, що визначає локальну "ентропійну напругу" у середовищі. Тоді *глобальна бойова ентропія середовища* визначатиметься як інтеграл по області:

$$S(t) = \iiint_{\Omega} \rho_S(x, y, z, t)\, dx\, dy\, dz. \tag{2}$$

Джерелами росту ρ_S у кожній точці можуть виступати: невизначеність щодо позицій і намірів противника, порушення структур взаємодії , наприклад, розрив зв'язку між безпілотним агентом (БА) і командним пунктом, руйнування інфраструктури, а також непередбачувані події, що змінюють доступність або топологію простору. Для оцінки таких впливів можна застосувати рівняння реакції-дифузії або потік ентропії у вигляді:

$$\frac{\partial \rho_S}{\partial t} = D\nabla^2 \rho_S + \Phi(x, y, z, t) \,, \tag{3}$$

де D – коефіцієнт дифузії (розповсюдження ентропійних впливів), а Φ – джерело локального збурення, наприклад, вибух, втрата каналу зв'язку, знищення безпілотного агента. Таким чином, ми отримуємо *динамічну модель бойового середовища* як еволюційну систему, де ентропія слугує головною змінною, що дозволяє оцінювати його структурну цілісність.

Для практичного застосування запропонованої ентропійної моделі в контексті сучасного бойового моделювання необхідна її інтеграція в симуляційні платформи, які підтримують мультиагентні системи, динаміку середовища та взаємодію з AI/ROS-архітектурами. У цьому дослідженні розглянуто можливість реалізації моделі в середовищі Gazebo, яке завдяки підтримці фізики, сенсорів, сценарного керування та інтеграції з ROS2, є оптимальним для тестування бойових дій у реальному масштабі часу.

У рамках симуляції бойового середовища простір Ω розбивається на воксельну сітку, кожен воксель якої асоціюється з локальним значенням $\rho S(x_i, y_j, z_k, t)$. Значення ентропійної щільності $\rho_S(x, y, z, t)$ у кожній точці бойового середовища динамічно обчислюються з урахуванням ключових факторів, що впливають на рівень невизначеності та впорядкованості простору [11]. Зокрема, до основних детермінантів належить: присутність ворожих об'єктів, як підтверджених, так і гіпотетичних, що спричиняє зростання ентропії через непередбачуваність їхньої поведінки; топологічні збої, викликані руйнуванням, блокуванням або частковою втратою прохідності ключових маршрутів, які ускладнюють маневрування та змінюють динаміку простору; інформаційна фрагментація, що проявляється

у втраті зв'язку, затримках даних або обмеженому охопленні сенсорної мережі, що знижує ситуаційну обізнаність системи; вразливість до атаки, яка зростає в умовах зменшення щільності або боєздатності дружніх платформ у конкретній зоні, що призводить до локального підвищення ентропії як прояву структурної нестабільності системи.

Ці значення передаються через ROS2 – повідомлення у вигляді окремих топіків entropy_map, entropy_gradient та entropy_alerts, які можуть бути використані для адаптивного планування маршрутів БА на основі градієнтного спуску до зон з мінімальною ентропією і тактичного аналізу ситуації командним центром або AI – навігації рою.

Для практичної реалізації ентропійної моделі у бойовому симуляційному середовищі було обрано платформу Gazebo з інтеграцією в ROS2 [6] – архітектуру, яка забезпечує гнучке керування агентами, підтримку фізики, сенсорів, а також динамічну реконфігурацію простору. Віртуальне бойове середовище Ω моделюється як тривимірна воксельна сітка, в якій кожному вокселю присвоюється значення ентропійної щільності $\rho_S(x, y, z, t)$, що оновлюється з частотою $f = 5 - 10$ Гц на основі багатофакторного аналізу подій у сцені. Інформація про ентропійний розподіл транслюється через спеціалізовані топіки ROS /entropy_map [9], /entropy_gradient, /entropy_alerts у вигляді 3D-масивів або heatmap-проєкцій.

Для демонстрації ефективності підходу було реалізовано три типові бойові сценарії, а саме: оборона критичного об'єкта, атака ворожого об'єкта й евакуація поранених. Проведемо опис важливих результатів симуляцій і перевірок.

Сценарій "Оборона бази". У цьому сценарії дружні БА наземного та повітряного типу патрулюють периметр критичного об'єкта. Виникнення підозрілої активності за межами бази викликає локальне зростання ентропії в суміжних вокселях. При перевищенні порогового значення ρ_S^{thresh} система автоматично змінює маршрути патрулювання, збільшує частоту сканування сенсорів і спрямовує найближчі платформи на зону підвищеної невизначеності. Таким чином, механізм *градієнтного реагування на ентропію* забезпечує передбачувану і координовану оборонну реакцію без централізованого втручання. А математична модель буде виглядати наступним чином. З урахуванням, що метою завдання постає підтримувати ентропію у визначеній критичній зоні Ω_{base} нижчою за порогове значення ρ_S^{thresh}.

Цільова функція буде мати вигляд:

$$\min_{u(t)} \int_{\Omega_{base}} \rho_S(x, y, z, t)\, dx\, dy\, dz. \tag{4}$$

Додатковими обмеженнями буде:

1. u(t)– керування маршрутом патрулювання дружніх агентів;
2. $\frac{\partial \rho_S}{\partial t} = D\nabla^2 \rho_S + \Phi_{threat}(x, y, z, t) - \Psi_{response}(x, y, z, t, u(t))$,

де Φ_{threat} – надходження зовнішніх загроз;

$\Psi_{response}$ – зменшення ентропії внаслідок присутності/дій дружніх агентів.

Сценарій "Атака на ворожу позицію". Цей сценарій моделює наступальну операцію, в якій рій автономних роботів просувається через складну територію до ворожої цілі. У реальному часі ентропія в середовищі оновлюється залежно від інтенсивності вогневого супротиву, втрати зв'язку, руйнування інфраструктури або непередбачуваних змін у топографії. Навігаційна підсистема використовує карту градієнтів ентропії для *адаптивного планування маршруту з найменшим ентропійним ризиком*, обходячи "зони хаосу", які класифікуються як стратегічно небезпечні [7]. Це дає змогу зменшити втрати та підвищити ефективність наступу.

Математична модель для сценарію "Атака", метою якої є пошук маршруту $\gamma(t)$ з точки x_0 до цілі x_T, який мінімізує сумарну ентропію на шляху [12]:

$$\min_{\gamma(t)} \int_0^T \rho_S(\gamma(t), t)\, dt. \quad (5)$$

Обмеження:

1. $\gamma(0) = x_0, \gamma(T) = x_T$.
2. $\gamma(t) \in \Omega$.
3. $\| \dot{\gamma}(t) \| \leq v_{max}$.

Фізична інтерпретація полягає в тому, що агент ухвалює рішення стосовно руху, враховуючи мінімізацію ентропійного ризику, обходячи "гарячі зони" і адаптуючи маршрут в реальному часі на основі оновленої карти ρ_S.

Сценарій "Евакуація поранених". У сценарії евакуації в симульованій зоні бойових дій поранений солдат виявляється в секторі з високою ентропією, спричиненою втратою зв'язку, наявністю ворога та складною топологією, наприклад завали, руйнації тощо. Система формує *оптимальний евакуаційний маршрут* на основі градієнта ентропії, спрямовуючи медичний БА (БпЛА, РНС(К)) через найбільш стабільні ділянки середовища. Зміна рівня ρ_S в режимі реального часу дає змогу адаптувати маршрут у разі появи нових загроз. У разі блокування основного шляху активується механізм повторної маршрутизації на основі зменшеного функціоналу ентропійних варіацій.

Математична модель для сценарію "Евакуація поранених", з метою транспортування пораненого із зони вогневого контакту $x_0 \in \Omega_{hot}$ до медичної точки $x_T \in \Omega_{safe}$, по маршруту мінімального ентропійного ризику, при цьому враховуючи час реагування. Тоді цільовий функціонал, а саме компроміс між ентропією і часом буде мати вигляд:

$$\min_{\gamma(t)} \left[\alpha \int_0^T \rho_S(\gamma(t), t)\, dt + \beta T \right], \quad (6)$$

де $\alpha, \beta > 0$ – вагові коефіцієнти, що балансують між безпекою маршруту і швидкістю евакуації.

Для того, щоб модель реагувала на реалістичну динаміку бойового середовища і могла адаптувати поведінку БА у відповідь на зміни ситуації, врахуємо додаткові умови.

1. Перешкоди та блоковані ділянки простору відображаються як області з $\rho_S \to \infty$.
2. За потреби система виконує перепланування при зміні ρ_S в окремих ділянках.

Наведемо приклад практичного застосування запропонованої моделі просторово-часової ентропії, що була використана для перевірки реалізації сценарію "оборона бази" в симуляційному середовищі Gazebo з інтеграцією в ROS2. Середовище побудовано з використанням набору елементів, а саме – в геометричному центрі розташована ціль захисту, наприклад, *штабний модуль*. Периметр середовища обмежений парканами та блокпостами. Здійснено секторальне розбиття $\Omega = \bigcup_i \Omega_i$, де кожен сектор – це воксель 10×10 м. Також, задано, що зовнішня зона охоплює симуляційні можливості появи ворожих об'єктів. Патрулювання здійснюється автономними БА наземного та повітряного типів, які обладнані наборами сенсорів LiDAR, GPS, камери та працюють під керуванням ROS2 вузлів.

Модель просторової ентропії реалізована у вигляді динамічної карти $\rho_S(x, y, t)$, що оновлюється з частотою 5 Гц на основі даних про ситуаційну обстановку [13]. Зокрема, для кожного сектора середовища значення ентропійної щільності розраховується як зважена сума кількох факторів: ймовірності присутності ворожого об'єкта, індикатора втрати зв'язку, інверсної щільності розподілу дружніх агентів. Порогове значення ρ_S^{thresh} встановлюється на рівні 0,6; перевищення цього рівня ініціює локальну тривогу та автоматичне перенаправлення найближчої платформи до зони підвищеної ентропії.

Система управління патрулюванням реалізована у вигляді ROS2 вузла /patrol_manager, який формує цільові точки для агентів залежно від карти ентропії, що надходить з вузла /entropy_monitor. Останній агрегує телеметрію роботів, стан зв'язку, а також інформацію з сенсорів. Усі обміни реалізовані через спеціалізовані топіки [9] /entropy_map, /entropy_alerts, /agent_status. У результаті моделювання показано, що запропонований підхід дозволяє ефективно виявляти та локалізувати загрози на ранніх етапах, адаптивно змінювати поведінку роботизованих платформ у реальному часі та знижувати структурну ентропію середовища в критичних секторах.

Логіка оновлення ентропії застосовується для кожного сектора Ω_i в сцені:

$$\rho_S(\Omega_i, t) = w_1 \cdot threati(t) + w_2 \cdot comm\_loss_i(t) + w_3 \cdot agent\_density_i^{-1}(t), \quad (7)$$

де $threat_i(t)$ – ймовірність присутності ворожого об'єкта;

$comm\_loss_i(t)$ – індикатор втрати зв'язку;

$agent\_density_i(t)$ – кількість дружніх агентів у секторі.

При цьому порогове значення визначається як $\rho_S^{thresh} = 0{,}6$.

Архітектура вузлів ROS2 має визначену структуру та призначення. Так:

– Вузол /patrol_manager_node виконує планування маршрутів для БА різних типів (наземних/повітряних), здійснює підписку до /entropy_map і публікує в /patrol_goal_{id}.

– Вузол /entropy_monitor_node будує карту ρ_S, здійснює підписку до /agent_status і /sensor_data, публікує /entropy_map (grid_msg) і /entropy_alerts.

– Вузол /agent_node_{i} виконує навігацію і роботу сенсорів всіх БА, здійснює підписку до /patrol_goal_{i}, /entropy_map і публікує /agent_status і /sensor_data.

Повідомлення мають спрощену структуру, що показано в таблиці 1.

Таблиця 1

Структура файлів повідомлень

/entropy_map	/entropy_alerts	/agent_status
std_msgs/Header float32[] entropy_values int32 width, height float32 resolution	std_msgs/Header string[] alert_sectors	std_msgs/Header string id geometry_msgs/Point position float32 battery bool connected

Враховуємо, що float32[] entropy_values виконано у вигляді рядка для кожного сектора, а string[] alert_sectors – це список секторів, де $\rho_S >$ порогове.

Виконання умови, коли entropy_monitor_node фіксує, що $\rho_S(\Omega_k, t) > \rho_S^{thresh}$ буде реакцією на зростання ентропії. І тоді він публікує попередження і /patrol_manager_node перепризначає найближчого БА в цей сектор. Повітряні БА можуть автоматично змінити висоту або швидкість, а наземні БА можуть зупинити звичайне патрулювання і виконати переміщення в зону ризику.

На завершальному етапі симуляції сценарію "Оборона бази" система досягає стану стабілізації ентропійного розподілу в межах критичної зони Ω_{base}. Протягом першої третини симуляції ($t \in [0, 60]$ с), внаслідок моделювання ворожої активності за межами бази, спостерігалося поступове зростання ентропійної щільності в зовнішніх секторах до пікових значень $\rho_S^{peak} \approx 0{,}83$. Це спричинило активацію системи тактичного реагування: два патрульні UGV були перенаправлені до секторів з аномальним зростанням ентропії, а один UAV здійснив висотне сканування зазначеної області.

Після 30 секунд активного реагування, середня ентропія в зоні підвищеного ризику знизилася з 0,76 до 0,42, що становить приблизно 45 % зменшення рівня невизначеності в проблемних секторах. Загальна ентропія середовища, інтегрована по Ω, знизилася на 21 % порівняно з піковими значеннями. Одночасно було зафіксовано покращення щільності покриття дружніми агентами в зоні порушення з 0,33 до 0,68 (у нормалізованих одиницях), що підтверджує активне переорієнтування ресурсів.

Фінальний етап симуляції ($t \in [90, 120]$ с) продемонстрував стабілізацію карти $\rho_S(x, y, t)$, при якій жоден із секторів не перевищував порогового значення $\rho_S^{thresh} = 0{,}6$. Це дозволило автоматично повернути наземний БА до базових маршрутів, а повітряному БА перейти в режим стандартного моніторингу. Отримані результати підтверджують здатність запропонованої моделі до динамічного виявлення локальних "вузлів хаосу", їхньої стабілізації за допомогою автономних агентів та підтримання функціональної впорядкованості бойового середовища шляхом ентропійного управління.

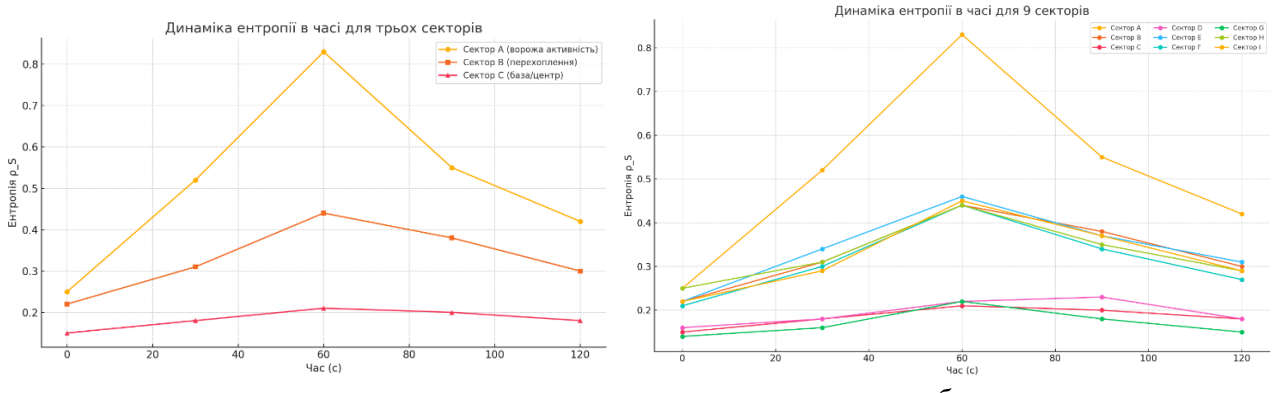
Таблиця 2 містить результати динаміки зміни рівня ентропії протягом всієї симуляції для трьох секторів при симуляції сценарію "Оборона бази", включно із середнім значенням по всьому бойовому середовищу.

Таблиця 2

Динаміка ентропії у сценарії "Оборона бази"

Час (с)	**Сектор A (ворожа активність)**	**Сектор B (перехоплення)**	**Сектор C (база/центр)**
0	0,25	0,22	0,15
30	0,52	0,31	0,18
60	0,83	0,44	0,21
90	0,55	0,38	0,2
120	0,42	0,3	0,18

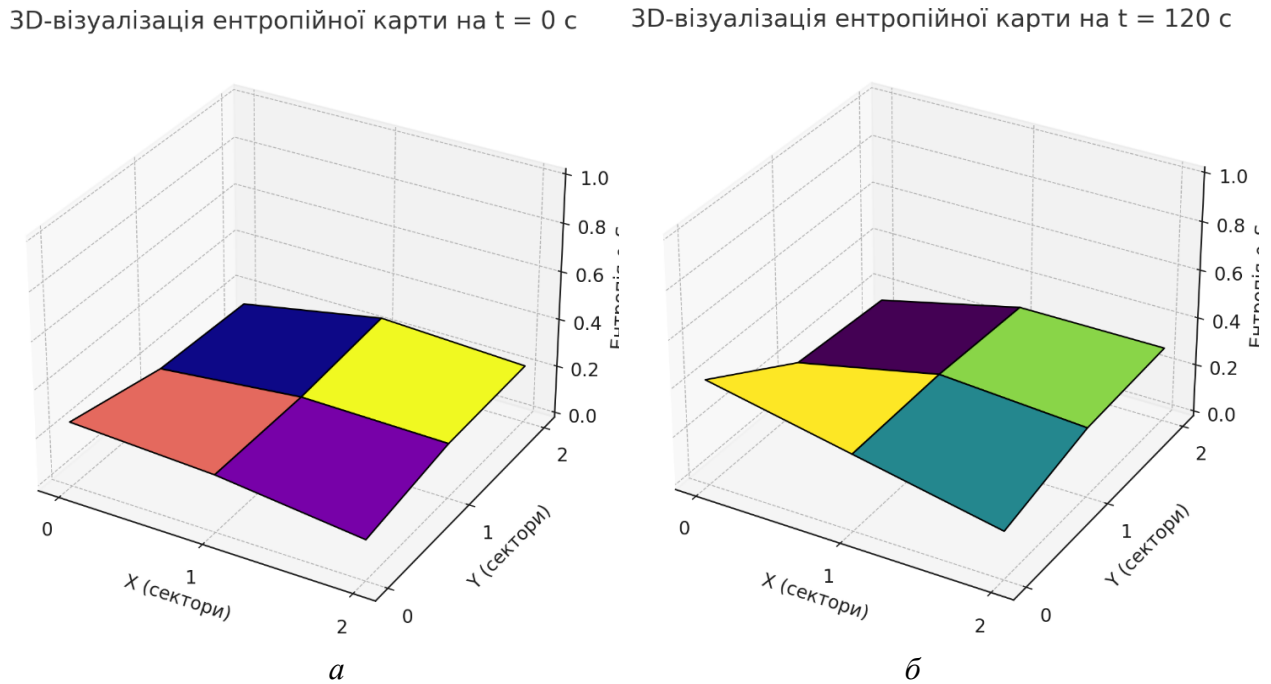
Графічне зображення результатів (рис. 1, *а*) показує зростання невизначеності у секторі A під час активної фази реагування та поступову стабілізацію середовища до завершення симуляції. Тоді як графік на рисунку 1, *б* демонструє зміну ентропії в часі. Застосування розширення секторального аналізу дозволяє оцінити просторову неоднорідність динаміки невизначеності та виявити ключові "вузли хаосу" або стабільності під час сценарію оборони.



а *б*

Рис. 1. Графік, що ілюструє зміну ентропії в часі бойового середовища у сценарії "Оборона бази": *а* – для трьох секторів; *б* – для дев'яти секторів

Побудова 3D-візуалізації ентропійної карти (рис. 2, *а, б*) для різних етапів симуляції сценарію “Оборона бази” демонструє відносно низький і рівномірний рівень ентропії в усіх секторах, що відповідає спокійному стану системи до початку загрозливих подій, та розподіл просторової невизначеності в бойовому середовищі активної фази, що дозволяє швидко виявити залишкові “гарячі зони”.



а *б*

Рис. 2. 3D-візуалізація ентропійної карти сценарію “Оборона бази”:
а – на початковому етапі симуляції t = 0 с; *б* – на завершальному етапі симуляції при t = 120 с

Динаміка та результати фінальної фази сценарію атаки.

У заключній фазі сценарію “Атака на ворожу позицію” здійснюється завершальний прорив бойових автономних платформ до заданої цілі в секторі Ω_{target}, що знаходився в зоні з підвищеним рівнем ентропії. Початково, протягом першої третини симуляції ($t \in [0, 60]$ с), унаслідок ворожого вогню та втрати зв’язку з двома агентами, середня ентропія у зоні наступу зросла до $\rho_S = 0{,}81$, що становило понад 160 % від базового (0,31) рівня середовища. Це спричинило активацію алгоритму маршрутизації з уникненням ентропійного максимуму та використанням бокових обхідних векторів просування.

Після реалізації обхідного маневру і повторного формування рою [8], протягом наступних 40 секунд, система продемонструвала поступове зниження локальної ентропії до $\rho_S = 0{,}49$, що еквівалентно зменшенню на 39,5 % від пікового значення. Це зумовлено як стабілізацією інформаційної структури середовища, так і збільшенням щільності дружніх агентів поблизу зони цілі, що позитивно вплинуло на спостережуваність та контроль ситуації.

На завершальному етапі ($t \in [100, 120]$ с), завдяки успішному прориву та підтвердженню нейтралізації об’єкта, ентропія в секторі Ω_{target} знизилася до рівня 0,36, порівнянного з початковими стабільними зонами середовища. Таким чином, повна динаміка зниження ентропії становила ~56 %, а система довела здатність адаптивно реагувати на флуктуації середовища, зберігаючи стратегічну ціль атаки без входу в критично невизначені зони. Це демонструє ефективність ентропійно-орієнтованої навігації як критерію ризик-адаптивного управління в бойовому полі.

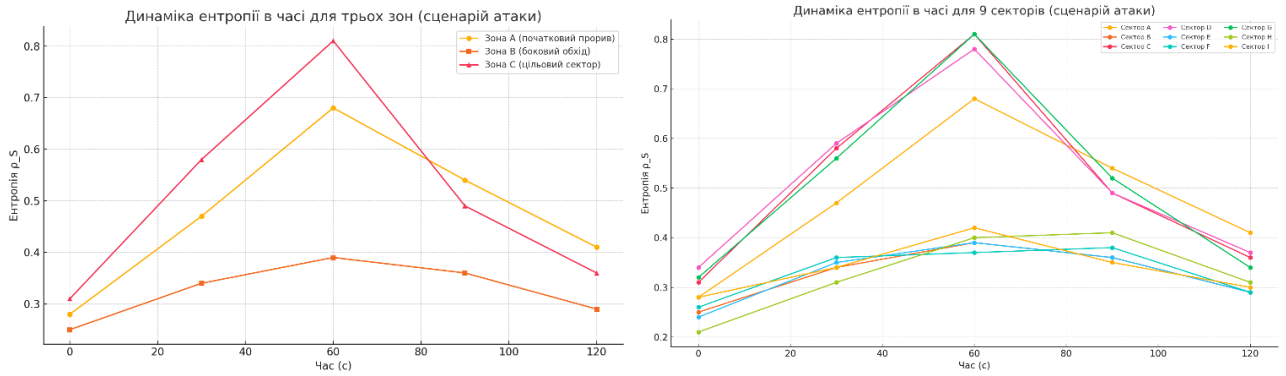
У таблиці 3 показано результати динаміки ентропії для трьох секторів при симуляції сценарію "Атака на ворожу позицію", що дозволяє простежити зміну рівнів невизначеності в ключових ділянках бойового простору та оцінити ефективність реакції системи у часі.

Таблиця 3

Динаміка ентропії у сценарії "Атака на ворожу позицію"

Час (с)	**Зона А (початковий прорив)**	**Зона В (боковий обхід)**	**Зона С (цільовий сектор)**
0	0,28	0,25	0,31
30	0,47	0,34	0,58
60	0,68	0,39	0,81
90	0,54	0,36	0,49
120	0,41	0,29	0,36

Графік на рисунку 3, *а* показує різке зростання ентропії у цільовому секторі (Зона С) під час бойового контакту, а також поступову стабілізацію після обхідного маневру. Графік на рисунку 3, *б* дозволяє оцінити, як поширюється або локалізується невизначеність у просторі протягом наступу.



а *б*

Рис. 3. Графік демонстрації зміни ентропії в часі бойового середовища у сценарії "Атака на ворожу позицію":
а – для трьох ключових зон; *б* – для дев'яти секторів

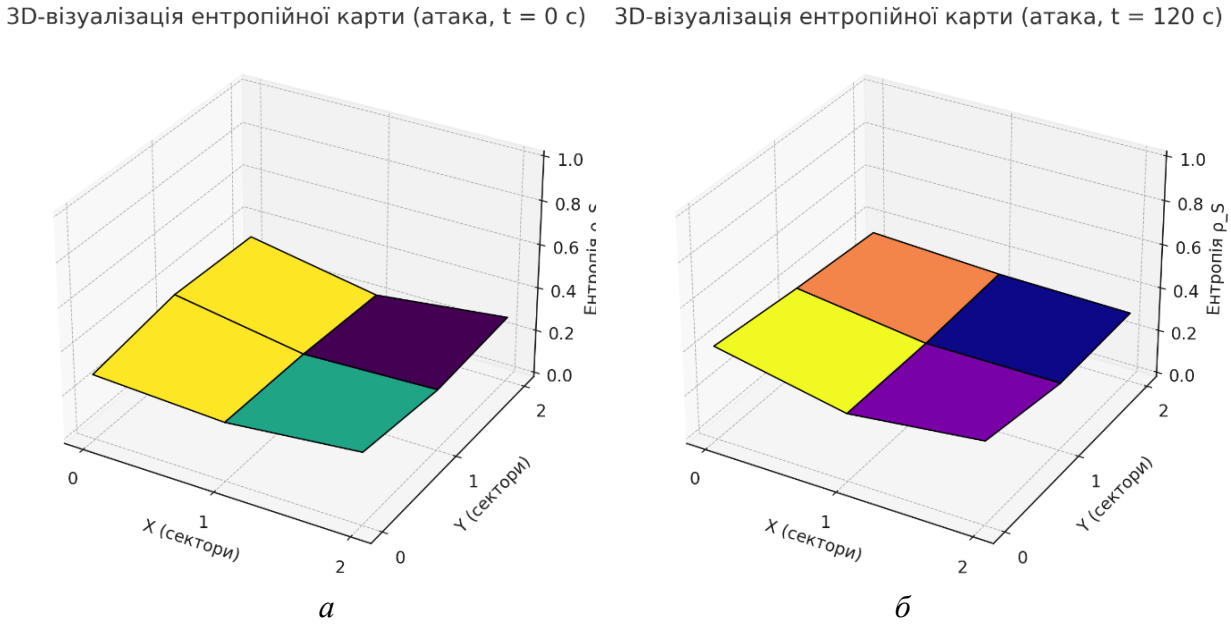
Побудована 3D-візуалізація ентропійної карти (рис. 4, *а, б*) для різних етапів симуляції сценарію "Атака на ворожу позицію" відображає відносно низький рівень ентропії у всіх секторах перед початком наступу, що свідчить про стабільний і впорядкований стан середовища, зниження ентропії у зоні цілі після прориву на завершальному етапі. Також легко бачимо залишкові хвилі невизначеності в суміжних секторах.

Така візуалізація дозволяє порівняти просторову динаміку змін невизначеності до та після бойового контакту й верифікувати ефективність адаптивної навігації та контроль бойового простору.

Динаміка та результати фінальної фази сценарію "Евакуація поранених"

На завершальному етапі сценарію "Евакуація поранених" симуляційна система автономного медичного транспорту БА наземної або повітряної компоненти успішно виконує місію з виведення пораненого із зони підвищеної невизначеності до стабільного тилового сектора. Початково, у момент виявлення пораненого ($t = 0$ с), сектор $\Omega_{injured}$ характеризувався ентропією $\rho_S = 0{,}67$, що вказує на нестабільність, викликану частковою

втратою зв’язку, пошкодженнями навколишньої інфраструктури та наявністю потенційної ворожої активності. Навколишні сектори також демонстрували високий рівень ентропії, що суттєво ускладнювало побудову безпечного евакуаційного маршруту.



а *б*

Рис. 4. 3D-візуалізація ентропійної карти сценарію “Атака на ворожу позицію”:
а – на початковому етапі симуляції t = 0 с; *б* – на завершальному етапі симуляції при t = 120 с

Завдяки реалізації алгоритму градієнтної маршрутизації з динамічним реагуванням на карту $\rho_S(x, y, t)$, евакуаційна система обрала маршрут через бічні сектори зі зниженим ентропійним градієнтом. Протягом активної фази евакуації (t ∈ [30, 90] с) спостерігалося поступове зниження ентропії у відповідних зонах на 34–48 % внаслідок переміщення агентів, покращення зв’язку та відновлення оглядовості середовища. У цільовому секторі Ω_{safe}, куди було доставлено пораненого, ентропія зберігалася в межах $\rho_S < 0{,}22$, що на 67 % нижче за початкове значення в зоні ризику.

На фінальному етапі ($t = 120$ с) загальний інтегральний рівень ентропії по маршруту евакуації знизився з 0,54 до 0,31, що становить зменшення на 42,6 %. Це свідчить про ефективність ентропійно-керованої навігації в умовах часткової інформаційної ізоляції та дозволяє вважати такий підхід придатним для динамічного управління евакуаційними місіями в бойовому середовищі зі змінною структурною впорядкованістю.

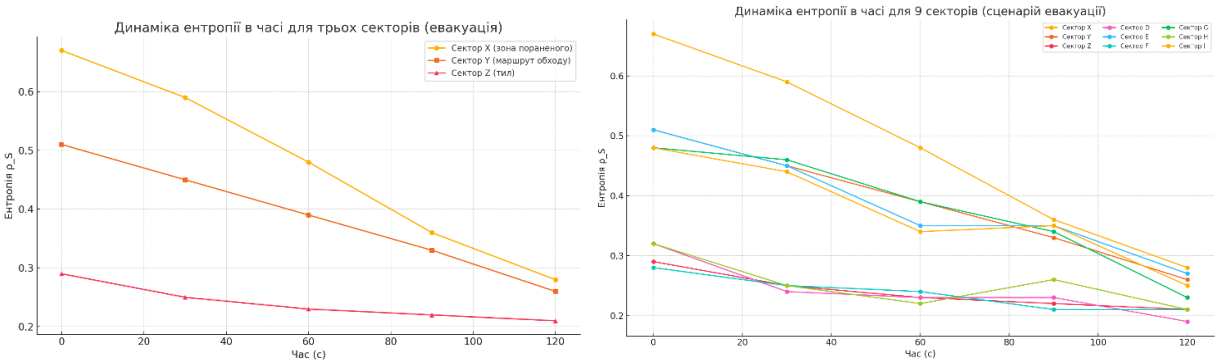
У таблиці 4 показано результати динаміки ентропії в ключових зонах під час сценарію “Евакуація поранених”. Ці дані наочно ілюструють зменшення рівня невизначеності вздовж евакуаційного маршруту, що відображає ефективність адаптивного ентропійного управління.

Таблиця 4

Динаміка ентропії у сценарії “Евакуація поранених”

Час (с)	**Сектор X (зона пораненого)**	**Сектор Y (маршрут обходу)**	**Сектор Z (тил/евакуаційна точка)**
0	0,67	0,51	0,29
30	0,59	0,45	0,25
60	0,48	0,39	0,23
90	0,36	0,33	0,22
120	0,28	0,26	0,21

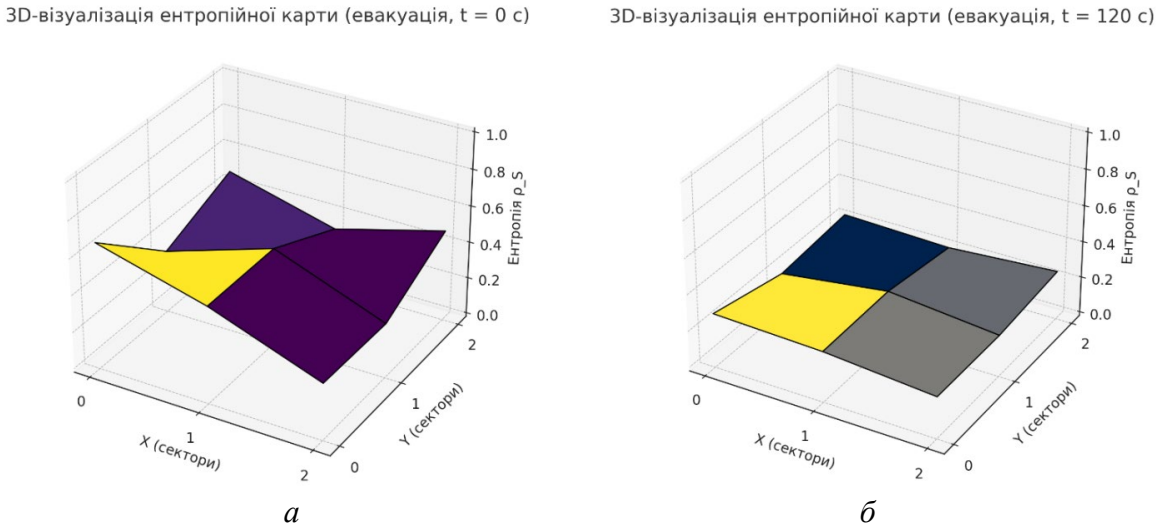
Графік динаміки ентропії в часі для трьох ключових секторів у сценарії “Евакуація поранених” (рис. 5, *а*) демонструє стабілізацію ситуації уздовж маршруту: від хаотичної зони пораненого (сектор X) до контрольованої евакуаційної точки (сектор Z). Графік на рисунку 5, *б* демонструє поступове зниження ентропії у критичних зонах і стабілізацію середовища вздовж усього евакуаційного маршруту.



а *б*

Рис. 5. Графік демонстрації зміни ентропії в часі бойового середовища у сценарії “Евакуація поранених”:
а – для трьох ключових зон; *б* – для дев’яти секторів

3D-візуалізація ентропійної карти на початку сценарію “Евакуація поранених” (рис. 6, *а*) показує підвищену ентропію в секторі X, зони, де перебуває поранений, та більш помірні значення в тилових секторах. При цьому рисунок 6, *б* демонструє зниження ентропії вздовж маршруту переміщення, від зони вогневого ураження, тобто нестабільної зони пораненого до тилового безпечного сектору.



а *б*

Рис. 6. 3D-візуалізація ентропійної карти сценарію “Евакуація поранених”:
а – на початковому етапі симуляції t = 0 с; *б* – на завершальному етапі симуляції при t = 120 с

Ця демонстрація створює чіткий контраст із фінальним станом і демонструє, як система впливає на просторову стабілізацію середовища. Це підтверджує ефективність динамічного маршрутизаційного реагування системи на ентропійні умови.

Об’єднана порівняльна таблиця 5 демонструє динаміку ентропії у характерних секторах для кожного з трьох бойових сценаріїв: оборони, атаки та евакуації. Вона дозволяє чітко

простежити, як змінюється рівень невизначеності в найбільш критичних точках під час реалізації різних типів бойових дій. У разі потреби можемо також побудувати порівняльний графік цих трьох ліній у часі.

Таблиця 5

Порівняльна таблиця ентропії для трьох бойових сценаріїв

Час (с)	**Оборона Сектор А (ворожа активність)**	**Атака Сектор С (цільова позиція)**	**Евакуація Сектор Х (зона вогневого контакту)**
0	0,25	0,31	0,67
30	0,52	0,58	0,59
60	0,83	0,81	0,48
90	0,55	0,49	0,36
120	0,42	0,36	0,28

А узагальнений порівняльний графік рівня ентропії у найбільш критичних точках для трьох бойових сценаріїв – оборони, атаки та евакуації пораненого – показано на рисунку 7.

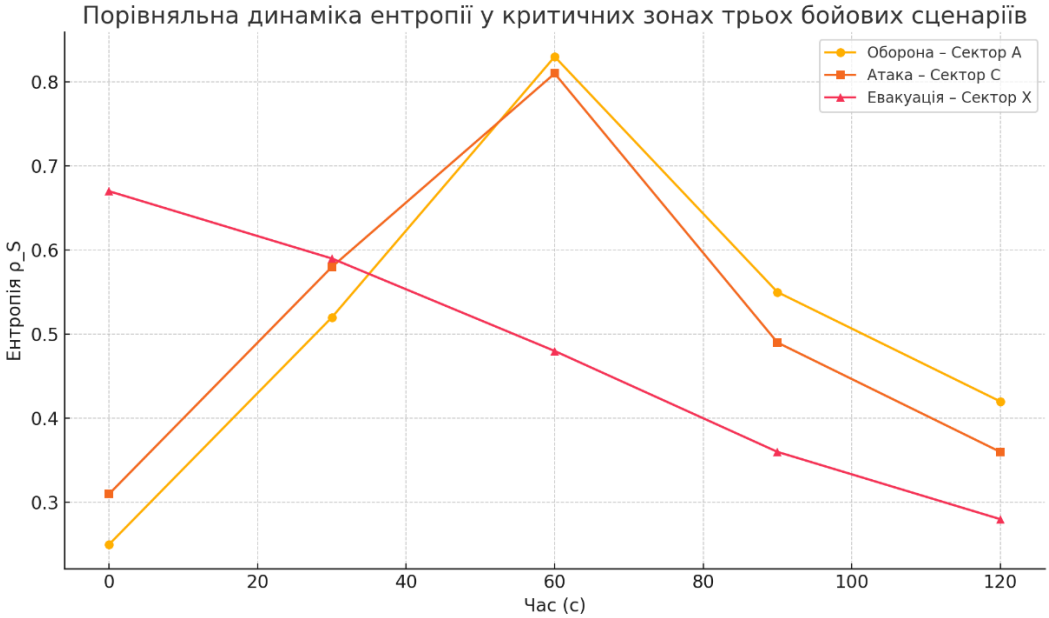


Рис. 7. Графік порівняльної динаміки ентропії у критичних зонах трьох бойових сценаріїв

Узагальнений графік наочно демонструє характер зростання й зниження невизначеності в часі залежно від типу місії та початкових умов.

Висновки та напрями подальших досліджень

У проведеному дослідженні обґрунтовано доцільність використання просторово-часової ентропії як операційної змінної для аналізу, оцінки та адаптивного управління бойовим середовищем. Розроблена модель дозволила поєднати термодинамічне трактування впорядкованості з практичною реалізацією в симуляційному середовищі Gazebo, демонструючи ефективність автономного реагування у трьох ключових сценаріях: оборони, атаки та евакуації. Досвід симуляцій підтвердив, що ентропійне управління забезпечує суттєве зменшення рівня невизначеності в критичних секторах, сприяючи покращенню ситуаційної обізнаності та зниженню ризику втрати контрольованості.

Разом з тим, результати роботи окреслюють і важливі перспективи розвитку даної парадигми. Подальші дослідження передбачають формалізацію різновидів ентропії, що відповідають структурним і функціональним особливостям різних типів бойових середовищ: відкритих, урбанізованих, напівструктурованих, а також динамічно змінних з урахуванням погоди, часу доби, інформаційних ускладнень. З цією метою пропонується ввести класифікацію на просторову, інформаційну, топологічну, когнітивну, взаємодійну та контекстуальну ентропії, кожна з яких фіксує окремий клас невизначеності. Крім того, доцільним є впровадження змінної ентропійної метрики, яка адаптивно підлаштовується під тип середовища та сценарій, автоматично переналаштовуючи ваги впливу відповідних ентропійних компонентів.

Такий підхід закладає основу для створення універсальної системи ентропійного керування у багатоплатформних роботизованих системах нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Подорожняк А. О., Земляна Г. В. Методи ефективного впливу на БпЛА // Збірник наукових праць. 2020. № 3 (45). С. 102–107.

2. Приходько Ю. І. Трансформація систем: основи теорії та методології. Київ: Інститут системного аналізу, 2018. 312 с.

3. Трєбін М. І., Трєбін О. В. Гібридна війна як нова українська реальність. Харків: Право, 2016. 254 с.

4. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. 1948. Vol. 27. P. 379–423. DOI: 10.1002/j.1538–7305.1948.tb01338.x.

5. Jaynes E. T. Information Theory and Statistical Mechanics // Physical Review. 1957. Vol. 106, No. 4. P. 620–630. DOI: 10.1103/PhysRev.106.620.

6. Quigley M., Conley K., Gerkey B. et al. ROS: An Open-Source Robot Operating System // ICRA Workshop on Open Source Software. 2009. Vol. 3. P. 1–6. [DOI не знайдено].

7. Parker G. Entropic Risk in Autonomous Systems: Modeling, Mapping, Mitigation // Journal of Defense Modeling and Simulation. 2021. Vol. 18, No. 3. P. 199–212. DOI: 10.1177/15485129211006492.

8. Zheng F., Liu J., Wang H. Entropy-Based Multi–Agent Coordination in Dynamic Battlefield Environments // Sensors. 2023. Vol. 23, No. 8. P. 4211. DOI: 10.3390/s23084211.

9. Kobayashi T., Tanaka Y., Saito H. Real-Time Entropy Mapping for UAV Swarms Using Distributed Sensor Networks // IEEE Access. 2022. Vol. 10. P. 65123–65134. DOI: 10.1109/ACCESS.2022.3183487.

10. Škoda P., Hruban P., Hromada M. Application of Thermodynamic Principles in Military Decision Support Systems // Military Technical Courier. 2020. Vol. 68, No. 4. P. 881–894. DOI: 10.5937/vojtehg68–23493.

11. Hodo E., Paspulis D., Triantafyllou A. Modeling Uncertainty in Cyber–Physical Battlefields Using Spatio-Informational Entropy // ACM Transactions on Cyber–Physical Systems. 2022. Vol. 6, No. 2. P. 1–20. DOI: 10.1145/3491234.

12. Li Y., Xu Z., Chen J. Dynamic Entropy Fields in Multi–Robot Systems for Adaptive Path Optimization // Robotics and Autonomous Systems. 2023. Vol. 163. P. 104360. DOI: 10.1016/j.robot.2023.104360.

13. Гончарук В. П. Ентропійні моделі управління складними динамічними об’єктами // Системні дослідження та інформаційні технології. 2019. № 1. С. 21–30. DOI: 10.20535/SRIT.2308-8893.2019.1.02.

DOI: 10.58254/viti.7.2025.02.19

УДК 004.67

Волошин В. В. ORCID: 0009-0004-7121-0950 (ВІТІ ім. Героїв Крут)
канд. фіз.-мат. наук Ковальчук Б. П. ORCID: 0000-0001-5219-7624 (ВІТІ ім. Героїв Крут)
Зінченко М. О. ORCID: 0000-0002-1428-8231 (ВІТІ ім. Героїв Крут)
Шаповал В. М. ORCID: 0000-0003-4637-9362 (ВІТІ ім. Героїв Крут)
Макарчук В. І. ORCID: 0000-0002-3997-4684 (ВІТІ ім. Героїв Крут)

МЕТОДИКА ВІДОКРЕМЛЕННЯ ШУМІВ У СПЕКТРОГРАМІ ВІД РЕАЛЬНИХ ДАНИХ ЗА ДОПОМОГОЮ ПОРОГОВОЇ БІНАРИЗАЦІЇ

Спектральний аналіз є важливим інструментом у багатьох наукових і технічних дисциплінах, таких як радіотехніка, акустика, телекомунікації та медична діагностика. Однак основною проблемою, що знижує ефективність цього аналізу, є наявність шумових компонент у спектрограмі, які можуть суттєво спотворювати результати й ускладнювати подальшу обробку сигналів. Присутність шумів, що мають різні характеристики, може негативно впливати на точність визначення корисного сигналу, створюючи додаткові труднощі при його інтерпретації та використанні.

Традиційні методи фільтрації не завжди ефективні для усунення шумових компонент, особливо коли вони мають складну структуру або змінюються в реальному часі. Зокрема, звичайні фільтри можуть не враховувати локальні варіації рівня шуму, що призводить до зниження якості очищених даних. Тому пошук нових методів для ефективного виділення корисного сигналу і фільтрації шумів є актуальним завданням.

У статті запропоновано новий алгоритм обробки спектрограм, заснований на пороговій бінаризації, який дозволяє ефективно виділяти активні сигнали та усувати фонові шумові компоненти. Для реалізації алгоритму використано поєднання двох бібліотек для обробки зображень – SkiaSharp та OpenCV. Це забезпечує не тільки гнучкість і високу продуктивність під час обробки спектрограм, але й можливість адаптації до різних умов спектрального середовища.

Запропонований метод дозволяє значно зменшити вплив випадкових флуктуацій рівня шуму, підвищуючи точність аналізу і достовірність результатів. Використання порогової бінаризації з адаптивним визначенням порогових значень дає змогу зберегти важливі частотні компоненти сигналу та ефективно усувати зайві шумові елементи. Застосування цієї технології може значно покращити спектральний аналіз у реальному часі, забезпечуючи підвищену стійкість до змін умов навколишнього середовища.

Таким чином, запропонований алгоритм є перспективним для подальшого застосування у різних сферах, де важливим є точний аналіз частотних характеристик сигналів. Окрім того, метод може бути використаний для покращення якості спектрального моніторингу, акустичного аналізу, а також у задачах розпізнавання сигналів у радіоелектронних системах.

Ключові слова: *спектральний аналіз, порогова бінаризація, шумопригнічення, спектрограма, цифрова обробка сигналів, обробка зображень, SkiaSharp, OpenCV.*

V. Voloshyn, B. Kovalchuk, M. Zinchenko, V. Shapoval, V. Makarchuk. Method of separation of noise in spectrograms from real data using threshold binarization

Spectral analysis is an important tool in many scientific and technical disciplines, such as radio engineering, acoustics, telecommunications, and medical diagnostics. However, one of the main challenges that reduces the effectiveness of this analysis is the presence of noise components in the spectrogram, which can significantly distort the results and complicate further signal processing. The presence of noise, which has different characteristics, can negatively affect the accuracy of identifying the useful signal, creating additional difficulties in its interpretation and use. Traditional filtering methods are not always effective in removing noise components, especially when they have a complex structure or vary in real-time. In particular, conventional filters may not account for local variations in the noise level, which leads to a decrease in the quality of the processed data. Therefore, the search for new methods for effectively extracting the useful signal and filtering noise remains a relevant task.

This article proposes a new method for processing spectrograms based on threshold binarization, which allows for the efficient isolation of active signals and the removal of background noise components. The algorithm implementation utilizes a combination of two powerful image processing libraries, SkiaSharp and OpenCV. This provides not only flexibility and high performance during spectrogram processing but also adaptability to various spectral environment conditions. The proposed method significantly reduces the impact of random fluctuations in the noise level, improving the accuracy of analysis and the reliability of results. The use of threshold binarization with adaptive threshold value determination enables the preservation of important frequency components of the signal while

effectively removing unnecessary noise elements. The application of this technology can substantially improve real-time spectral analysis, providing increased resilience to environmental changes.

Thus, the proposed approach holds promise for further application in various fields where precise frequency characteristic analysis of signals is crucial. Furthermore, the method can be used to improve the quality of spectral monitoring, acoustic analysis, as well as in signal recognition tasks within radio-electronic systems.

Keywords: *spectral analysis, threshold binarization, noise suppression, spectrogram, digital signal processing, image processing, SkiaSharp, OpenCV.*

Постановка завдання в загальному вигляді. Проблема виділення корисного сигналу на спектрограмі полягає у забезпеченні точного спектрального аналізу в умовах наявності фонових шумів, які можуть суттєво спотворювати результати вимірювань. У традиційних методах цифрової обробки сигналів використовуються різні алгоритми до фільтрації шумів, однак вони не завжди забезпечують ефективне відокремлення слабких корисних сигналів від випадкових завад. Особливо актуальною ця проблема є для сфер радіочастотного моніторингу, акустичного аналізу, а також телекомунікацій, де точність визначення параметрів сигналу має критичне значення.

Однією з ключових завад у цьому процесі є змінний характер шумів, які можуть мати нерівномірний розподіл і динамічні характеристики, що ускладнює їх фільтрацію класичними методами. Зокрема, у спектрограмах шумові артефакти можуть накладатися на корисний сигнал або маскувати його, що призводить до хибних результатів аналізу.

У публікації запропоновано метод бінаризації спектрограм, який базується на адаптивному визначенні порогових значень для відокремлення корисного сигналу від фонового шуму. Використання бібліотек SkiaSharp та OpenCV дозволяє здійснювати швидку та ефективну обробку зображень спектрограм у реальному часі. Запропонований алгоритм забезпечує автоматичну адаптацію до умов змінної зашумленості та покращує точність аналізу спектральних характеристик сигналів.

Отже, актуальним є розроблення ефективного алгоритму обробки спектрограм, здатного підвищувати точність спектрального аналізу шляхом усунення завад та виділення корисного сигналу. Це дозволить покращити якість обробки радіосигналів, підвищити ефективність моніторингу частотного спектра та зробити аналіз більш надійним у складних умовах.

Розробка ефективних методів фільтрації шумів у спектральному аналізі є важливою науковою проблемою, яка активно досліджується в різних галузях, таких як цифрова обробка сигналів, машинне навчання та комп’ютерний зір. Аналіз наукових публікацій показує, що існують різні алгоритми до відокремлення корисного сигналу від шуму, серед яких найбільш поширеними є методи порогової бінаризації, вейвлет-перетворення, нейронні мережі та адаптивна обробка спектрограм.

Аналіз останніх публікацій. Методи відокремлення шумів у спектрограмі від реальних даних є предметом досліджень у багатьох сучасних наукових публікаціях. Значна частина робіт зосереджена на вдосконаленні алгоритмів спектрального аналізу та бінаризації для підвищення точності виявлення сигналів на зашумленому фоні.

У роботі [1] розглянуто удосконалення технічних характеристик аналізаторів спектра сигналів, що може бути корисним для розробки методів виявлення небезпечних сигналів. Запропоновані алгоритми дозволяють ефективніше оцінювати параметри сигналів в умовах завад.

Дослідження [2] присвячене комплексуванню візуальних даних з далекомірними вимірюваннями для позиціонування та картографування. У роботі розглянуто методи порогової бінаризації та виділення країв, що дозволяють покращити виявлення характерних об’єктів, що може бути застосовано для спектрального аналізу.

Аналіз методів бінаризації зображень проведено в [3]. У роботі оцінено ефективність різних алгоритмів, таких як адаптивна бінаризація Бредлі – Рота, медіанна фільтрація,

методи збалансованих гістограм та дискримінантний аналіз. Ці методи можуть бути застосовані для покращення спектральної бінаризації сигналів.

Спектральна денойзингова обробка також досліджується в [4], де реалізовано простий метод спектрального шумопригнічення для аудіозаписів довкілля.

Робота [5] застосовує генеративні змагальні мережі (GAN) для покращення мікро-доплерівської спектрограми, що демонструє перспективність машинного навчання для очищення спектральних даних. Автоматизоване виділення основної частоти сигналів морських ссавців за допомогою спектральної бінаризації досліджується в [6].

Подібний алгоритм застосовано в [7] для автоматизованого розпізнавання вокалізацій морських ссавців, що підтверджує ефективність спектральної обробки у складних акустичних умовах.

Узагальнення методів бінаризації та їх кількісне оцінювання представлене в [8].

Дослідження [9] розглядає гібридний алгоритм до очищення мовних сигналів, що поєднує спектральний і хвильовий алгоритми.

Робота [10] аналізує багатокомпонентну обробку сигналів у часово-частотному просторі, що може бути корисним для розробки нових алгоритмів спектрального аналізу. Загалом, аналіз останніх публікацій свідчить про активний розвиток методів спектральної обробки сигналів, включно з пороговою бінаризацією, що дозволяє ефективніше виокремлювати корисні дані від шумів.

Проаналізовані роботи підтверджують ефективність порогової бінаризації та методів комп’ютерного зору для відокремлення шуму у спектральному аналізі.

Метою статті є обґрунтування методики, яка дозволить більш ефективно обробляти спектрограми для відокремлення реальних сигналів від шумів.

Виклад основного матеріалу. Обробка спектральних даних є важливою складовою аналізу сигналів у різних наукових і технічних дисциплінах, включаючи радіофізику, акустику, телекомунікації, а також системи спостереження й аналізу радіочастотного середовища.

Для обробки спектральних даних вже існує низка традиційних алгоритмів, кожен з яких має свої переваги та обмеження.

Фільтрація за допомогою швидкого перетворення Фур’є (ШПФ) та хвильового перетворення – застосовується для аналізу частотного складу сигналів, дозволяючи виділяти окремі компоненти. ШПФ ефективне для стаціонарних сигналів, тоді як хвильове перетворення краще підходить для обробки нестаціонарних сигналів.

Кореляційний аналіз – використовується для виявлення корисних сигналів шляхом оцінки їхньої подібності до еталонних зразків. Однак він потребує значних обчислювальних ресурсів і не завжди дає чітке розділення сигналу від шуму.

Метод Оцу – автоматично визначає порогове значення для бінаризації зображень, що може бути корисним для сегментації спектрограм. Проте цей метод ефективний лише тоді, коли розподіл сигналу та шуму є чітко вираженим, що не завжди відповідає реальним умовам.

Адаптивні фільтри Калмана – використовуються для оцінки та прогнозування параметрів сигналу, зокрема відстеження змін частоти в часі. Хоча вони є потужним інструментом, їх застосування потребує попереднього моделювання динаміки сигналу, що ускладнює їхню адаптацію до нових умов.

Незважаючи на ефективність цих методів у певних випадках, вони мають свої обмеження. Зокрема, ШПФ недостатньо добре працює для змінних спектрів, кореляційний аналіз є ресурсозатратним, метод Оцу не завжди забезпечує точне розділення спектрограми, а фільтри Калмана вимагають детального знання характеристик сигналу, що не завжди доступне.

У цій роботі представлено алгоритм, який ідентифікує та сегментує активні частоти за допомогою адаптивної порогової бінаризації, а також виконує фільтрацію шумів на основі статистичних характеристик спектрограми.

На відміну від класичних методів, запропонований алгоритм працює поетапно, зосереджуючись на ефективному відокремленні корисних сигналів від шуму шляхом порогової бінаризації спектрограми.

Автори пропонують наступний алгоритм: відокремлення шумів у спектрограмі від реальних даних за допомогою методу порогової бінаризації:

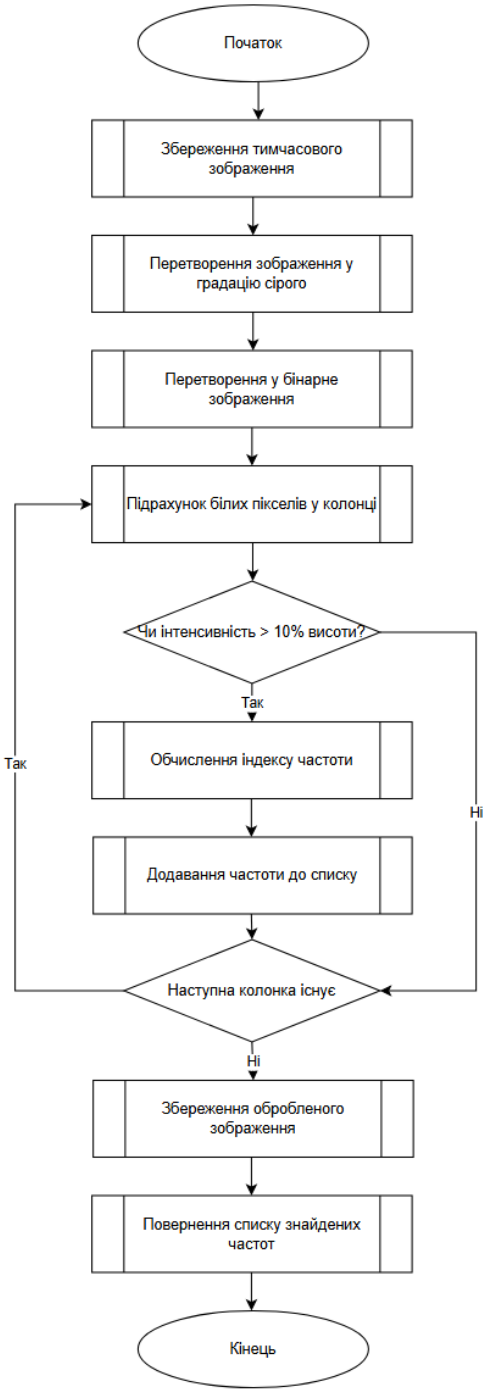


Рис. 1. Алгоритм відокремлення шумів у спектрограмі від реальних даних за допомогою порогової бінаризації

Методика відокремлення шумів у спектрограмі від реальних даних за допомогою порогової бінаризації передбачає наступні крокі:

Перший етап. Перший етап передбачає отримання спектрограми сигналу, яка є візуальним представленням змін частотного спектра в часі. Для отримання спектрограми було використано спектроаналізатор частот TinySA Ultra (рис. 2), який забезпечує високу точність вимірювання та дозволяє здійснювати моніторинг широкого діапазону частот.

Рис. 2. Спектроаналізатор частот TinySA Ultra

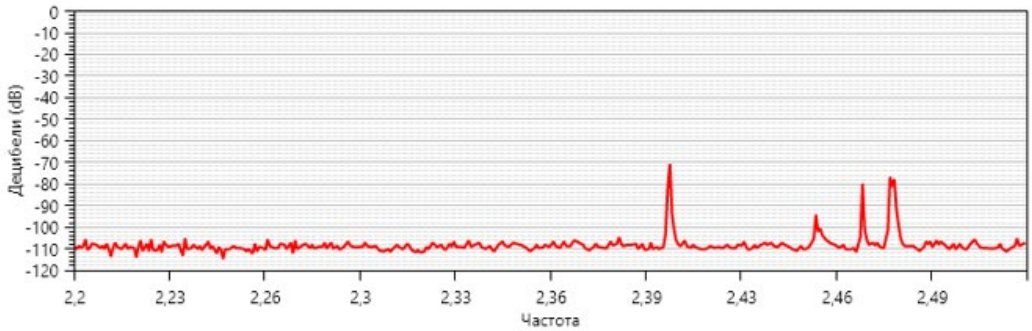


Рис. 3. Спектр сигналів, зчитаний за допомогою TinySA Ultra

Для побудови спектрограми програма здійснювала зчитування радіочастотного спектра з інтервалом 1 секунда (рис. 3), після чого на основі отриманих даних було сформовано спектральне зображення. Для її побудови використовується короткочасне перетворення Фур’є (КПФ) [11], що розбиває сигнал на віконні відрізки та обчислює їхні частотні характеристики згідно з виразом (1):

$$X_m(\omega) = \sum_{n=-\infty}^{\infty} x(n)w(n - mR)e^{-j\omega n}, \quad (1)$$

де $w(n)$ – віконна функція довжиною M;

$X_m(\omega)$ – образ функції $x(n)$ у частотній області, отриманий ШПФ добутку функції $x(n)$ і віконної функції $w(n)$, центрованої у моменті часу mR;

R – довжина стрибка (зсуву) вікна.

Застосування КПФ дозволяє отримати часово-частотне представлення сигналу, що є основою для побудови спектрограми.

Другий етап. Оскільки спектрограми часто містять кольорову шкалу для відображення інтенсивності сигналу, наступним етапом є її перетворення у градації сірого. Це зменшує розмірність даних і спрощує обробку. Кожен піксель спектрограми обчислюється за формулою (2):

$$I_{gray} = 0.299R + 0.587G + 0.111B, \tag{2}$$

де R, G, B – інтенсивності червоного, зеленого і синього каналів відповідно;

I_{gray} – отримане значення в градаціях сірого.

Коефіцієнти 0.299, 0.587 і 0.111 визначені на основі сприйняття людським оком різних кольорів. Червоний канал має найбільшу вагу (0.299), оскільки людське око менш чутливе до червоного світла. Зелений канал має найбільший внесок (0.587), оскільки він є найбільш сприйнятливим для людського зору. Синій канал має найменшу вагу (0.111), оскільки людське око найменш чутливе до синього світла. Таке перетворення дозволяє отримати більш коректне відображення яскравості зображення в градаціях сірого.

Зазначені коефіцієнти визначено відповідно до стандарту ITU-R BT.601, який використовується для перетворення кольорових зображень у відтінки сірого в системах обробки відеосигналів.

Третій етап. Порогова бінаризація, яка дозволяє розділити спектрограму на дві області: сигнальну (білу) та фонову (чорну). Вона виконується шляхом застосування порогового значення, обраного на основі статистичних параметрів спектрограми згідно з правилом (3):

$$I' = \begin{cases} 255, & I_{gray} > T \\ 0, & I_{gray} \le T \end{cases}, \tag{3}$$

де I_{gray} – інтенсивність пікселя у відтінках сірого;

I' – результуюче бінаризоване зображення;

T – порогове значення, яке визначає межу між сигнальною та фоновою областями;

255 – значення, що присвоюється сигнальній області (білий колір);

0 – значення, що присвоюється фоновій області (чорний колір).

Точне визначення порогу є критичним, оскільки занадто високе значення може призвести до втрати слабких сигналів, а занадто низьке – до збереження шуму. Оптимізація може здійснюватися за допомогою методу Оцу або адаптивної бінаризації, що враховує локальні особливості спектрограми.

Четвертий етап. Після виконання бінаризації зображення, на якому відображається спектрограма сигналу, здійснюється наступний етап аналізу, що полягає у виявленні частот, які містять корисний сигнал. Це досягається шляхом аналізу вертикальних стовпців бінаризованого зображення. Кожен стовпець спектрограми відповідає певній частоті, а його висота залежить від кількості білих пікселів у зображенні, що, у свою чергу, відображає рівень енергії сигналу в конкретній частотній смузі.

Зокрема, на цьому етапі підраховується кількість білих пікселів у кожному вертикальному стовпці спектрограми, що дозволяє визначити наявність активних частот, які можуть містити корисний сигнал. Для цього використовується наступна функція (4):

$$N_{active}(f) = \sum_{i=1}^{h} I'_{i,j}, \tag{4}$$

де h – висота зображення, що відповідає максимальній кількості пікселів у вертикальному напрямку спектрограми;

j – номер стовпця, який відповідає частоті f;

$I'_{i,j}$ – бінаризоване значення пікселя на перехресті i-го ряду та j-го стовпця. Якщо піксель білий, то його значення дорівнює 1, якщо чорний – 0.

Якщо у стовпці виявляється велика кількість білих пікселів, це свідчить про те, що на відповідній частоті є значний рівень активності, що вказує на наявність корисного сигналу. Таким чином, на цьому етапі здійснюється виявлення частот, де присутній активний сигнал, що може бути використано для подальшого аналізу або фільтрації сигналів.

П'ятий етап. Останнім етапом є відсікання шумових компонент на основі аналізу щільності активних пікселів у кожному стовпці. Вводиться мінімальний поріг, який визначає необхідну кількість білих пікселів у стовпці, щоб вважати його частиною реального сигналу відповідно до правила (5):

$$N_{active}(f) = N_{min} \Rightarrow \text{фіксація сигналу на частоті } f. \quad (5)$$

Якщо кількість білих пікселів у стовпці менша за N_{min}, то ця частота вважається шумом і виключається з подальшого аналізу. Такий алгоритм дозволяє знижувати вплив шумових компонент на результати обробки сигналу, підвищуючи точність виявлення корисного сигналу.

N_{min} є ключовим параметром для налаштування чутливості до сигналу та визначення порогу для відсікання шуму. Значення цього порогу зазвичай вибирається експериментально залежно від характеристик сигналу і рівня шуму в конкретній задачі.

Для практичної реалізації даного алгоритму була написана програма мовою програмування C#, яка використовує бібліотеки для обробки графіки SkiaSharp та OpenCV.

```
using (var img = SKImage.FromBitmap(originalImage))
using (var data = img.Encode(SKEncodedImageFormat.Png, 100))
using (var stream = File.OpenWrite(tempPath))
{
    data.SaveTo(stream);
}

Mat image = CvInvoke.Imread(tempPath, ImreadModes.Grayscale);
double threshold = 150;
Mat binaryImage = new Mat();
CvInvoke.Threshold(image, binaryImage, threshold, 255, ThresholdType.Binary);

var imageData = (byte[,])binaryImage.GetData();
List<double> activeFrequencies = new List<double>();

for (int x = 0; x < binaryImage.Width; x++)
{
    int signalIntensity = 0;

    for (int y = 0; y < binaryImage.Height; y++)
    {
        byte pixelValue = imageData[y, x];
        if (pixelValue == 255)
        {
            signalIntensity++;
        }
    }

    if (signalIntensity > binaryImage.Height * 0.1)
    {
        int frequencyIndex = (int)((double)x / binaryImage.Width * Frequencies.Count);

        if (frequencyIndex >= 0 && frequencyIndex < Frequencies.Count)
        {
            double frequency = Frequencies[frequencyIndex];
            activeFrequencies.Add(frequency);
        }
    }
}

CvInvoke.Imwrite(processedFilePath, binaryImage);

ActiveFrequencies?.Invoke(activeFrequencies);
ProceedImage?.Invoke(processedFilePath);
```

Програма здійснює зчитування радіосигналу за допомогою спектроаналізатора TinySA, після чого отримані дані перетворюються на спектрограму. Для аналізу спектральної структури застосовується запропонований алгоритм, який дозволяє відокремлювати корисний сигнал від фонового шуму. У процесі виконання програми було здійснено детальний аналіз спектральної діаграми та відокремлено шумові компоненти від корисного сигналу. Застосування алгоритму бінаризації з пороговим значенням T сприяло виділенню областей із суттєвою амплітудою сигналу, мінімізуючи вплив випадкових флуктуацій. На рисунку 5 зображено два графіки, які створюються програмою та демонструють процес виділення шумів на спектрограмі за допомогою методу порогової бінаризації.

Верхній графік – це оригінальна спектрограма, де показано розподіл сили сигналу (в dBm) за частотою (в ГГц). Кольорова шкала праворуч відображає рівень сигналу: від 100 dBm (синій колір) до 0 dBm (червоний колір). На спектрограмі чітко видно області з високим рівнем сигналу (жовті та червоні), що відповідають корисним даним, а також області з низьким рівнем сигналу (сині), де присутні шуми.

Нижній графік – результат застосування порогової бінаризації до оригінальної спектрограми. Цей метод дозволяє розділити сигнал на два класи: корисний сигнал та шум. У даному випадку порогове значення було встановлено так, щоб відокремити шуми (відображені білим кольором) від корисних даних (чорний колір). Як видно з графіку, бінаризація успішно видалила шуми.

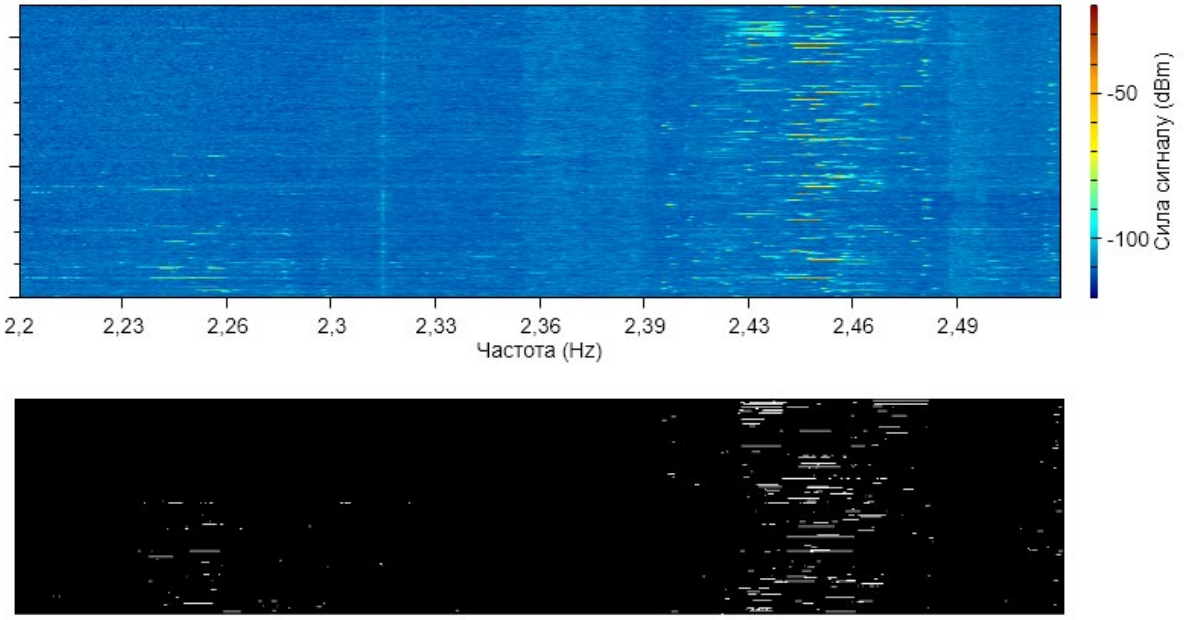


Рис. 5. Візуалізація порогової бінаризації для виділення шумів на спектрограмі

Отримані результати демонструють, що застосований алгоритм забезпечує відокремлення шумів та дозволяє виділити структурні особливості сигналу, що спрощує його подальший аналіз. Таким чином, алгоритм дозволяє підвищити якість спектральної обробки та точність подальшої ідентифікації характерних частотних компонент.

Ефективність запропонованої методики полягає в її здатності виділяти частотні компоненти зі спектрограми у структурованому форматі, придатному для подальшого аналізу. Це забезпечує автоматизацію обробки спектральних даних, мінімізуючи вплив людського фактора та підвищуючи точність і відтворюваність результатів аналізу.

Реалізований алгоритм дозволяє усувати шуми, що підтверджено експериментами із реальними спектрограмами. Аналіз результатів показав, що використання порогової бінаризації дозволяє зменшити рівень завад і виділити основні сигнали у спектрі.

Висновки. Запропонований алгоритм обробки продемонстрував високу ефективність у виділенні активних сигналів і фільтрації шумових компонент. Алгоритм забезпечує точне розпізнавання корисного сигналу завдяки застосуванню аналізу спектральних характеристик, що дозволяє значно покращити якість обробки даних.

Основними перевагами запропонованого алгоритму є:

використання локально адаптивних методів для визначення порогу бінаризації підвищує стійкість алгоритму до флуктуацій рівня шуму, що є важливим при роботі з реальними сигналами, де рівень шуму може змінюватися залежно від умов середовища. Це дозволяє забезпечити виділення активних частот навіть у складних умовах;

алгоритм здійснює детальний аналіз просторової структури бінаризованого зображення, що дозволяє зберігати важливі частотні компоненти сигналу, уникаючи їх втрат. Це важливо для подальшої обробки та інтерпретації сигналів, оскільки дозволяє зберегти їхню цілісність і точність для подальших етапів аналізу.

Запропонований алгоритм є корисним для обробки частотних характеристик у радіотехніці, акустиці, розпізнаванні мовлення та спектральному моніторингу.

Подальший розвиток може включати інтеграцію методів машинного навчання для автоматичної класифікації та адаптації до складніших сигналів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конотопець М., Самойлов І., Сторчак А., Смольков О. Пропозиції з удосконалення технічних характеристик аналізаторів спектру сигналів // Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 50 (2). С. 118–128. DOI: 10.33099/2311-7249/2024-50-2-118-128.

2. Мухіна М. П. Алгоритм комплексування візуальних даних з далекомірними вимірюваннями для одночасного позиціонування та картографування (SLAM) // Електроніка та системи управління. 2010. № 1. С. 75–81.

3. Зубик Л., Пужай-Череда С., Сапельников О., Калугін Д., Котляр М. Аналіз методів і алгоритмів розпізнавання та ідентифікації зображень за їх окремими фрагментами // Кібербезпека: освіта, наука, техніка. 2024. № 4 (24). С. 363–375. DOI: 10.28925/2663-4023.2024.24.363375.

4. Dias F. F., Ponti M. A., Minghim R. Implementing simple spectral denoising for environmental audio recordings // arXiv preprint. 2022. arXiv:2201.02099.

5. Zhang Y., Wu L. Micro-Doppler Spectrogram Denoising Based on Generative Adversarial Network // IEEE Radar Conference (RadarConf18). 2018. С. 932–935.

6. Kandia V., Stylianou Y. Spectrogram denoising and automated extraction of the fundamental frequency variation of dolphin whistles // The Journal of the Acoustical Society of America. 2006. Т. 120 (5). С. 3435–3446.

7. Kuklasinski A., Lavesson N., Ulén J. Spectrogram denoising for the automated detection of marine mammal vocalizations // Applied Acoustics. 2015. Т. 97. С. 127–134.

8. Sezgin M., Sankur B. Survey over image thresholding techniques and quantitative performance evaluation // Journal of Electronic Imaging. 2004. Т. 13 (1). С. 146–165.

9. Kong Z., Ping W., Dantrey A., Catanzaro B. CleanUNet 2: A Hybrid Speech Denoising Model on Waveform and Spectrogram // arXiv preprint. 2023. arXiv:2309.05975.

10. Miramont J. M., Bardenet R., Chainais P., Auger F. Benchmarking multi-component signal processing methods in the time-frequency plane // arXiv preprint. 2024. arXiv:2402.08521.

11. Гаврилюк В., Мелешко В. Вибір параметрів перетворення Фур'є для спектрального аналізу тягового струму // Електромагнітна сумісність та безпека на залізничному транспорті. 2019. № 17. С. 11–19. DOI: 10.15802/ecsrt2019/225841.

DOI: 10.58254/viti.7.2025.03.28

УДК 004.056(075.8)

канд. техн. наук Данилюк І. А. ORCID: 0000-0003-0955-0108 (ВІТІ ім. Героїв Крут)
Лазута Р. Г. ORCID: 0000-0002-8584-1110 (ВІТІ ім. Героїв Крут)
Куцаєв В. В. ORCID: 0000-0001-8213-4739 (ВІТІ ім. Героїв Крут)
Цимбал І. В. ORCID: 0000-0001-7294-3794 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ ПЕРСПЕКТИВ ЗАСТОСУВАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Стрімкий розвиток квантових технологій відкриває нові можливості для військової сфери, зокрема у галузях кібербезпеки, комунікацій, навігації, розвідки та моделювання складних бойових сценаріїв. У статті проведено аналіз сучасного стану досліджень у сфері квантових обчислень, квантової криптографії, квантових датчиків і сенсорики, а також їхнього потенційного застосування для підвищення боєздатності Збройних Сил України. Розглянуто можливості використання квантових алгоритмів для розв'язання складних оптимізаційних завдань, що можуть бути корисними у військовій логістиці, управлінні військовими ресурсами та прогнозуванні загроз.

Окрему увагу приділено перспективам впровадження квантових технологій для створення захищених каналів зв'язку, що унеможливлюють несанкціоноване перехоплення інформації, а також для розробки нових систем навігації, які не залежать від супутникових сигналів і здатні працювати в умовах радіоелектронної боротьби. У роботі також розглянуто основні виклики, що стоять перед впровадженням квантових технологій у військову сферу, зокрема технічні, фінансові та організаційні бар'єри.

На основі проведеного аналізу визначено ключові напрями подальших досліджень, що сприятимуть ефективному впровадженню квантових технологій у сферу оборони України. Запропоновано підходи до створення інноваційної стратегії розвитку квантових технологій у військовій сфері, яка передбачає як наукові дослідження, так і практичну реалізацію їхніх результатів у військових інформаційних системах, системах зв'язку та засобах розвідки.

Ключові слова: *квантові технології, квантові обчислення, квантовий зв'язок, квантові сенсори, квантова суперпозиція, квантова заплутаність, квантовий генератор випадкових чисел.*

I. Danyliuk, R. Lazuta, V. Kutsaiev, I. Tsymbal. Research into the prospects of application of quantum technologies in the Armed Forces of Ukraine

The rapid development of quantum technologies opens up new opportunities for the military sphere, in particular in the fields of cybersecurity, communications, navigation, intelligence and modelling of complex combat scenarios. The article analyses the current state of research in the field of quantum computing, quantum cryptography, quantum sensors and sensors, as well as their potential application to increase the combat capability of the Armed Forces of Ukraine. The possibilities of using quantum algorithms to solve complex optimization problems that can be useful in military logistics, military resource management and threat forecasting are considered.

Particular attention is paid to the prospects for the implementation of quantum technologies to create secure communication channels that prevent unauthorized interception of information, as well as for the development of new navigation systems that do not depend on satellite signals and are capable of operating in electronic warfare conditions. The paper also examines the main challenges facing the introduction of quantum technologies into the military sphere, in particular technical, financial and organizational barriers.

Based on the analysis, key areas of further research have been identified that will contribute to the effective introduction of quantum technologies into the defense sector of Ukraine. Approaches to creating an innovative strategy for the development of quantum technologies in the military sphere, which involves both scientific research and the practical implementation of their results in military information systems, communication systems and intelligence means, have been proposed.

Keywords: *quantum technologies, quantum computing, quantum communication, quantum sensors, quantum superposition, quantum entanglement, quantum random number generator.*

Вступ

За останнє десятиліття квантові технології стали однією з найдинамічніших галузей наукових досліджень, що підтверджується значним зростанням кількості публікацій та міжнародних дослідницьких проєктів. Дослідження у сфері квантових обчислень уже продемонстрували можливість квантової переваги, коли квантові процесори перевершують

класичні суперкомп’ютери у виконанні спеціалізованих обчислювальних задач. Водночас у квантовій криптографії досягнуто значного прогресу, зокрема реалізовано практичні системи квантової комунікації, що підтверджено успішними експериментами в різних країнах.

Значна увага приділяється і підготовці квантових спеціалістів, що знайшло відображення у зростанні кількості освітніх програм, курсів та досліджень, присвячених методикам навчання у цій сфері. Проведені роботи підкреслюють важливість міждисциплінарного підходу, що включає знання з фізики, математики, комп’ютерних наук та інженерії, а також необхідність розвитку лабораторної інфраструктури й тісної співпраці між науковими установами та промисловістю. Усі ці аспекти активно досліджуються та відображені в численних наукових публікаціях, що висвітлюють сучасний стан і перспективи розвитку квантових технологій.

Аналіз публікацій за темою дослідження

У роботі [1] викладено історію квантових обчислень, основи квантової інформації, квантові алгоритми та квантові криптографічні системи.

У роботі [2] авторами запропоновано послідовний виклад фізичних основ і математичного апарату квантової механіки та їх застосування до різних задач, що є гарною основою для початкової підготовки військових квантофахівців.

Робота [3] представляє квантовий алгоритм розпізнавання оптичних образів на растрових зображеннях, який реалізується на основі квантових логічних елементів Тоффолі та оператора Гровера. Показано, що реалізація квантового алгоритму розпізнавання образів дає змогу порівняно із класичними алгоритмами експоненційно скоротити обсяг необхідної пам’яті та поліноміально зменшити час виконання алгоритму внаслідок реалізації квантового паралелізму. Автори вважають, що застосування схожих алгоритмів надасть можливість використати квантовий комп’ютер, складений з 1–2 млн. кубітів, який буде здатен розв’язувати складні питання планування, розвідки, логістики, криптографії в інтересах Збройних Сил України.

У роботі [4] автори розглядають проблеми квантових обчислень, квантові алгоритми Шора, Гровера та квантове перетворення Фур’є, що також є основою для сучасних досліджень, стосовно використання квантових технологій в Збройних Сил України.

У роботі [5] автори розглядають фотонні системи з однокубітними квантовими обчисленнями, що може стати корисним при підготовці військових квантофахівців.

У роботі [6] пропонується нове ефективне перетворення великого об’єму неструктурованих текстових даних на просторову. Це дозволить здійснювати конверсію великих наборів текстової інформації, таких як звіти, замовлення, листи й інші документи, на точкові класи просторових об’єктів у географічних інформаційних системах. Для опрацювання цієї проблеми у новому перспективному підході авторами пропонується поєднання гібридних квантово-класичних нейронних мереж із геоінформаційними технологіями.

У роботі [7] викладено питання, які стосуються нестаціонарного та стаціонарного рівнянь Шредінгера, фізичного змісту хвильової функції. Проаналізовано співвідношення невизначеностей Гайзенберга та принцип доповнювальності Бора. Це надає можливість військовим квантофахівцям ефективно опанувати принципи фізики квантових частинок та приєднатись до використання квантових технологій в інтересах Сил оборони України.

У роботі [8] викладено основи виконання квантових розрахунків за допомогою квантових процесорів, із суттєвим використанням їх квантових властивостей. У роботі розглянуто поняття розрахунку функцій, складності алгоритмів, класичної та квантової машин Тюринґа, квантових бітів, квантових логічних елементів, квантових обчислювальних мереж. З’ясовано, на яких ефектах ґрунтується надефективність квантових комп’ютерів порівняно з класичними. Наведено приклади ефективних квантових алгоритмів.

У роботі [9] викладено основні положення та методи квантової механіки, які необхідні для більш глибокої підготовки до опанування та застосування можливостей застосування квантових технологій у Збройних Силах України.

У роботі [10] запропоновано узагальнення булевих операцій для квантових обчислень, а також розглянуто 9 квантових операцій додатково до 7-ми класичних. Отримано повний набір 16 однокубітних операцій, що відповідає кількості базових станів 16-кубітного квантового процесора, що дозволить підвищити продуктивність квантових обчислень у цифрових симуляторах квантових процесорів, з точки зору паралельності обчислень та скорочення програмного коду. Дані дослідження можуть бути використані для підготовки квантофахівців-програмістів на квантових засобах інформаційних технологій або квантових симуляторах.

У роботі [11] висвітлено сучасні проблеми створення стандартів перспективних криптографічних перетворень та хід їх вирішення, які необхідні для аналізу криптографічної стійкості алгоритмів, у тому числі і квантових, що може бути використано для аналізу стійкості постквантових алгоритмів.

Таким чином, проведений аналіз літератури, зокрема робіт [1–11], надає достатнє підґрунтя для підготовки військових квантофахівців до ефективного використання сучасних інноваційних квантових технологій у військовій сфері. Це стосується квантових обчислень, квантового зв’язку та квантових сенсорів, що, у свою чергу, сприятиме підвищенню боєздатності Збройних Сил України.

Метою статті є дослідження сучасного стану квантових технологій у контексті можливості використання квантових технологій і підготовки квантофахівців в інтересах Збройних Сил України для підвищення їх боєздатності.

Основна частина

Аналіз сучасного стану досліджень у сфері квантових обчислень, необхідний для підвищення боєздатності Збройних Сил України

Квантові обчислення є однією з найперспективніших технологій, що здатна радикально змінити підхід до вирішення складних завдань у військовій сфері. Уряди провідних країн світу, включно із США, Китаєм, Великобританією та країнами ЄС, активно фінансують дослідження та розробки в галузі квантових технологій для оборонного сектору. Зокрема, військові програми зосереджені на застосуванні квантових обчислень для оптимізації військових операцій, розробки нових систем шифрування та моделювання складних фізичних процесів.

Одним із ключових напрямів є використання квантових алгоритмів для військової логістики та планування бойових дій [8]. Такі алгоритми, як квантовий відпал (Quantum Annealing), уже тестуються оборонними агентствами США та Великобританії для вирішення задач оптимального розподілу ресурсів [12]. Наприклад, Агентство перспективних дослідницьких проєктів оборони США (DARPA) фінансує проєкти, спрямовані на інтеграцію квантових обчислень у військове управління.

Квантові комп’ютери також мають значний потенціал у сфері криптографії. Використання алгоритму Шора дозволяє розкладати великі числа на прості множники експоненційно швидше, ніж класичні алгоритми, що ставить під загрозу традиційні криптографічні методи, такі як RSA. У відповідь військові відомства активно розробляють квантостійкі алгоритми шифрування, які здатні забезпечити безпечний зв’язок навіть у разі появи потужних квантових обчислювальних систем [4].

Ще один перспективний напрямок досліджень – це квантові сенсори, які можуть забезпечити високоточне визначення положення військової техніки без використання супутникових систем. У 2022 році Міністерство оборони Великобританії заявило про успішні випробування квантових інерціальних навігаційних систем, які дозволяють

кораблям і підводним човнам орієнтуватися без GPS. Такі розробки є критично важливими в умовах радіоелектронної боротьби, коли традиційні навігаційні засоби можуть бути виведені з ладу.

Китай також активно розвиває військові квантові технології. У 2017 році країна запустила супутник Micius, який здійснив першу у світі квантову телепортацію та захищену передачу інформації між віддаленими точками. Це демонструє потенціал квантової комунікації для створення нерозшифровуваних каналів зв’язку між військовими об’єктами.

Таким чином, сучасні дослідження в галузі квантових обчислень у військовій сфері перебувають на стадії активного розвитку. Провідні держави спрямовують значні ресурси на інтеграцію цих технологій у свої оборонні стратегії, що створює нові виклики та можливості для України. Подальші дослідження та інвестиції у квантові обчислення можуть стати важливим чинником зміцнення обороноздатності нашої держави. У контексті підвищення боєздатності Збройних Сил України. Ці технології відкривають можливості для оптимізації логістики, розробки нових систем озброєння, аналізу великих даних та забезпечення кібербезпеки. Сучасний стан досліджень у цій сфері демонструє значний прогрес, однак потребує адаптації до специфічних потреб військової сфери, особливо в умовах війни.

Перш за все, потрібно звернути увагу на відмінність теоретичних основ квантових обчислень від сучасних класичних, що суттєво впливає на вирішення проблемних питань.

Квантові комп’ютери базуються на принципах квантової механіки, таких як суперпозиція, заплутаність та інтерференція, порівняно з класичними бітами, які мають значення 0 або 1.

Кубіти – квантові біти [1–5] можуть перебувати в суперпозиції станів [2] згідно з виразом (1):

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle, \tag{1}$$

де α та β – комплексні амплітуди, що задовольняють умові нормалізації (2):

$$|\alpha|^2 + |\alpha|^2 = 1. \tag{2}$$

Суперпозиція. Принцип суперпозиції дозволяє квантовому комп’ютеру одночасно обробляти велику кількість станів, що суттєво прискорює виконання складних обчислювальних задач [2].

Другою ключовою властивістю є квантова **заплутаність**, яка забезпечує миттєву кореляцію між кубітами незалежно від відстані [1–5]. Якщо два кубіти знаходяться у заплутаному стані, їх хвильова функція має вигляд (3):

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{3}$$

Ця особливість використовується у квантовій криптографії для забезпечення безпечного зв’язку, а також у військових інформаційних системах.

Квантова **інтерференція.** Ще однією важливою властивістю є квантова інтерференція, яка відіграє ключову роль у роботі квантових алгоритмів. Використання оператора Унітарного перетворення дозволяє маніпулювати станами кубітів за допомогою квантових вентилів. Наприклад, квантове перетворення Фур’є, яке використовується в алгоритмі Шора для факторизації чисел [4], визначається виразом (4):

$$QFT|x\rangle \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i x k/N} |k\rangle. \tag{4}$$

Цей механізм дозволяє вирішувати криптографічні задачі експоненційно швидше за класичні методи, що є важливим у військовій сфері для розробки нових засобів шифрування та дешифрування інформації.

Таким чином, завдяки принципам суперпозиції, заплутаності та інтерференції, квантові обчислення відкривають нові можливості для оптимізації військових операцій, забезпечення безпеки комунікацій і швидкої обробки великих масивів даних.

Квантова перевага. Авторами було досліджено, проаналізовано та встановлено, що на глобальному рівні лідерами у сфері квантових обчислень є компанії Google, IBM, D-Wave, Microsoft та Intel. У 2019 році Google оголосила про досягнення «квантової переваги» з їхнім процесором Sycamore, який виконав задачу за 200 секунд, що для класичного суперкомп'ютера потребувало б 10 тис. років. Час виконання задачі для квантового комп'ютера можна оцінити згідно з виразом (5):

$$T_q = O(2^n/p), \tag{5}$$

де n – кількість кубітів;

p – кількість паралельних квантових операцій.

Для класичних суперкомп'ютерів час обчислення такої самої задачі визначається виразом (6):

$$T_c = O(2^n P), \tag{6}$$

де P – кількість класичних процесорів, що працюють паралельно.

У випадку експерименту Google процесор Sycamore мав 53 кубіти та виконав задачу вибірки випадкових чисел у квантовій системі за 200 секунд. Для класичного суперкомп'ютера ця задача має експоненційну складність, що призводить до оцінки часу (7):

$$T_c \approx 10^4 \text{років}. \tag{7}$$

Цей результат підтверджує значну перевагу квантових обчислень у специфічних класах задач, таких як моделювання квантових систем і оптимізаційні завдання.

Компанія IBM [5], у свою чергу, розвиває підхід до квантових обчислень на основі гібридних систем, де класичні алгоритми доповнюються квантовими прискорювачами. Основною метою є зниження рівня квантового шуму, який моделюється рівнянням (8):

$$\varepsilon = e^{-\lambda t}, \tag{8}$$

де λ – коефіцієнт затухання кубітного стану;

t – час виконання обчислень.

Зменшення цього шуму є ключовою проблемою для масштабування квантових процесорів.

Компанія D-Wave розвиває інший підхід – квантове відпалювання (Quantum Annealing), який використовується для оптимізаційних задач. Його математична модель описується гамільтоніаном (9):

$$H(t) = A(t)H_i + B(t)H_j, \tag{9}$$

де H_i – початковий гамільтоніан;

H_j – фінальний гамільтоніан;

A(t) та *B(t)* – функції часу, які поступово змінюються так, щоб система еволюціонувала до розв'язку задачі.

Квантовий комп'ютер Microsoft в рамках Azure Quantum працює на основі топологічного кубіту, що використовує майоранові квазічастинки для підвищення стабільності квантових обчислень. Квантові стани в такій системі описуються хвильовою функцією Ψ, що еволюціонує згідно з рівнянням Шредінгера (10):

$$i\hbar\frac{\partial}{\partial t}\Psi(t) = H\Psi(t), \tag{10}$$

де *H* — гамільтоніан системи.

В основі квантових операцій лежать унітарні перетворення, які забезпечують когерентну еволюцію кубітів (11):

$$U = e^{-iHt\hbar}. \tag{11}$$

Microsoft також використовує гібридну квантово-класичну обчислювальну модель, де квантові алгоритми, такі як квантовий алгоритм Гровера, використовуються для пошуку в невпорядкованих базах даних, де складність відповідає виразу квадратичного прискорення (12):

$$O = \left(\sqrt{N}\right), \tag{12}$$

де *N* – розмірність бази даних.

Також використовується квантовий алгоритм Шора для факторизації чисел, де складність *O* відповідає виразу (13):

$$O = ((\log N)^3). \tag{13}$$

Розрахунки інтегруються з класичними обчисленнями через платформу Azure Quantum. Це дозволяє ефективно вирішувати задачі оптимізації, криптографії та симуляції фізичних процесів, використовуючи різні апаратні реалізації, включаючи іонні пастки, надпровідникові кубіти та перспективні топологічні процесори, що може бути використано для підвищення обороноздатності держави.

Компанія Intel розробила квантовий комп'ютер, заснований на технології кремнієвих спінових кубітів, які використовують спін електрона у квантовій точці як носій інформації. Динаміка квантового стану таких кубітів описується рівнянням Шредінгера (14):

$$i\hbar\frac{\partial}{\partial t}\Psi(t) = H\Psi, \tag{14}$$

де гамільтоніан системи має вигляд (15):

$$H = g\mu_B BS_z + JS_1 \cdot S_2, \tag{15}$$

де g – фактор Ланде;

μ_B – магнетон Бора;

B – зовнішнє магнітне поле;

J – обмінна взаємодія між спінами кубітів;

S_2 – оператор спіну.

Intel використовує технологію Horse Ridge, яка дозволяє ефективно керувати квантовими станами при температурі < 1K, що спрощує масштабування квантових систем.

Перспективи використання у Збройних Силах включають криптографічні операції (захист інформації за допомогою постквантових алгоритмів), оптимізацію логістичних процесів (швидкий розподіл ресурсів у реальному часі) та аналіз великих даних для розвідки (квантові алгоритми прискорюють розпізнавання об'єктів на супутникових знімках). Використання квантових технологій Intel може значно підвищити ефективність обчислень у військовій сфері, забезпечуючи перевагу в інформаційних і стратегічних операціях.

Таким чином, технологічно розвинені країни світу намагаються втілювати принципи квантової технологій для підвищення якісного та ефективного розвитку своїх Збройних сил.

Автори намагалися вивчити досвід розвинутих країн світу та визначитися з можливими основними напрямками, які зможуть підвищити ефективність використання Збройних Сил України для досягнення перемоги у сучасній війні, в першу чергу, з метою збереження особового складу.

Квантові технології можуть значно покращити точність та швидкість прогнозування загроз завдяки застосуванню квантових алгоритмів для аналізу великих масивів даних, розпізнавання закономірностей та моделювання складних систем.

Проведено аналіз можливостей використання досягнень квантових технологій у військовій галузі та визначено напрямки використання квантових технологій для підвищення ефективності використання військових ресурсів (людських та матеріальних), що набуває особливої потреби в сучасних умовах війни проти рф.

Оптимізаційні завдання відіграють ключову роль у військовій сфері, оскільки дозволяють підвищити ефективність логістики, управління військовими ресурсами, розподілу сил та планування бойових операцій. Традиційні методи часто стикаються з обмеженнями обчислювальної потужності при розв'язанні задач великої розмірності, що ускладнює швидкий аналіз бойової обстановки. У цьому контексті квантові алгоритми відкривають нові перспективи, оскільки здатні значно прискорювати розв'язання складних комбінаторних задач.

Квантові технології можуть бути використані для розв'язання складних оптимізаційних завдань, що можуть бути корисними у військовій логістиці, управлінні військовими ресурсами та прогнозуванні загроз.

Проаналізовано основні можливі напрямки оптимізації військових стратегій, які можливо вирішити за допомогою використання квантових технологій.

Одним із найперспективніших напрямів є використання квантового відпалу (Quantum Annealing) для розв'язання задач маршрутизації та розподілу ресурсів. Такі задачі можуть бути сформульовані у вигляді задачі квадратичного двоїстого програмування (Quadratic Unconstrained Binary Optimization, QUBO) (16):

$$H(x) = \sum_i Q_{ii} x_i + \sum_i Q_{ij} x_i x_j, \tag{16}$$

де x_i – двійкові змінні (0 або 1), що представляють вибір конкретного маршруту чи ресурсу;

Q_{ii} та Q_{ij} – коефіцієнти, що відображають вагу та взаємозв'язки між змінними.

Квантові пристрої, такі як D-Wave, здатні знаходити глобальний мінімум функції, що дозволяє оптимально розподіляти ресурси в реальному часі.

Таким чином, оптимізація логістичних операцій щодо розподілу ресурсів у бойових умовах можна сформулювати у вигляді задачі квадратичного двоїстого програмування (QUBO). При цьому оптимізація військових перевезень може бути розв'язана за допомогою алгоритму квантового відпалу, де транспортна задача формулюється наступним чином (17):

$$\min \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} xij \tag{17}$$

за умов:

$$\sum_{j=1}^{n} x_{ij} = a_i, i = 1,2, \dots, m,$$
$$\sum_{i=1}^{m} x_{ij} = b_j, j = 1,2, \dots, n,$$

де c_{ij} – вартість транспортування військових ресурсів між пунктами *ii* та *jj*;

x_{ij} – кількість ресурсів, що транспортується;

a_i – запаси у відправних пунктах;

b_j – потреби в пунктах призначення.

Квантові алгоритми можуть швидко знаходити рішення подібних задач навіть при великій кількості змінних.

Даний метод може бути застосований для розподілу військових підрозділів, маршрутизації техніки та обчислення оптимального використання пального.

Ще одним перспективним напрямком застосування квантових технологій авторами був запропонований квантовий пошук у військовій розвідці. Для його реалізації запропоновано використовувати алгоритм Гровера для пошуку в невпорядкованих базах даних. Цей алгоритм здатний прискорювати виявлення критично важливих цілей. Часова складність класичного пошуку складає, тоді як алгоритм Гровера виконує пошук за складності $O(\sqrt{N})$. Основний оператор алгоритму описується наступним рівнянням (18) [5]:

$$U = (2|\psi><\psi| - I)O, \tag{18}$$

де |ψ⟩ – початковий стан суперпозиції;

O – оператор пошуку;

I – одиничний оператор.

Таким чином, автори пропонують використовувати алгоритм Гровера для аналізу великих обсягів розвідувальної інформації, значно скорочуючи час на обробку даних [4; 5].

Ще одним із можливих ключових напрямків, на думку авторів, є використання нейромереж і методів машинного навчання для аналізу даних розвідки при використанні квантових алгоритмів. Наприклад, Варіаційний квантовий алгоритм наближення (VQE) та Квантова підтримка векторних машин (QSVM), можуть значно прискорити обробку великих розвідувальних даних.

Класичне оновлення параметрів у нейромережах описується градієнтним спуском (19):

$$\Theta_{t+1} = \Theta_t - \eta \nabla L(\Theta_t), \tag{19}$$

де η – швидкість навчання;

Θ_t – функція втрат;

$\nabla L(\Theta_t)$ – градієнт функції втрат.

Запропоновані квантові алгоритми можуть пришвидшити цей процес завдяки швидкому розрахунку квантових градієнтів та експоненційному масштабуванню обчислювальних можливостей**.**

Ще одним можливим варіантом використання квантових технологій є моделювання можливих дій противника за допомогою квантових стохастичних алгоритмів [8].

Для прогнозування можливої поведінки противника можна використовувати квантову Марковську модель, яка визначається рівнянням еволюції (20):

$$\rho(t) = e^{-iHt}\rho(0)e^{iHt}, \tag{20}$$

де $\rho(t)$ – щільнісний оператор стану системи;

H – гамільтоніан, що описує динаміку змін;

t – час.

Ця модель дозволяє аналізувати ймовірності різних сценаріїв розвитку подій та визначати оптимальні стратегії реагування.

Автори вважають, що застосування квантових алгоритмів [8] у прогнозуванні загроз відкриває нові можливості для військової аналітики, зменшуючи час обчислень та покращуючи точність оцінки ризиків. У подальшому військові аналітики зможуть швидше реагувати на нові загрози, оптимізувати використання ресурсів та розробляти ефективні оборонні стратегії.

Таким чином, застосування квантових алгоритмів у військових оптимізаційних задачах дозволяє значно підвищити ефективність логістичних операцій, аналіз розвідувальних даних та управління ресурсами. Подальші дослідження в цій сфері сприятимуть швидшому впровадженню квантових технологій у Збройні Сили України.

Наступною областю впровадження квантових технологій у військову галузь є використання квантових алгоритмів для криптографії та військового зв’язку [8].

Традиційна криптографія базується на факторизації великих чисел, що є складним завданням для класичних комп’ютерів. Однак алгоритм Шора дозволяє розкласти число N на прості множники за час згідно з виразом (21) [4]:

$$T = O((\log N)^3), \tag{21}$$

що експоненційно швидше за класичні методи. Це загрожує безпеці існуючих криптографічних протоколів.

Телепортація. Для захищеного зв’язку військові досліджують квантову телепортацію, яка базується на передачі квантового стану між двома віддаленими точками за допомогою сплутаних кубітів. Основна формула квантової телепортації виглядає так (22) [1; 2]:

$$|\psi\rangle_A=\alpha|0\rangle+\beta|1\rangle. \tag{22}$$

Після передачі квантового стану між точками А і В можна створювати нерозшифровувані канали зв’язку.

Перспективи впровадження квантових технологій для створення захищених каналів зв’язку.

Сучасний розвиток інформаційних технологій ставить перед суспільством нові виклики у сфері кібербезпеки, зокрема щодо захисту даних від несанкціонованого доступу. Традиційні методи шифрування, такі як RSA або AES, базуються на обчислювальній складності певних математичних задач (наприклад, факторизації великих чисел). Проте поява квантових комп’ютерів, здатних реалізовувати алгоритм Шора [4], загрожує зламати ці системи за поліноміальний час $O\big((\log N)^2(\log\log N)(\log\log\log N)\big)$, де N – число, яке потрібно факторизувати. У цьому контексті квантові технології відкривають нові горизонти у сфері інформаційної безпеки, зокрема у створенні захищених каналів зв’язку, що унеможливлюють несанкціоноване перехоплення інформації. Основою таких систем є принципи квантової механіки, які гарантують безпеку передачі даних завдяки унікальним властивостям квантових станів. Авторами пропонується впровадження квантових технологій, таких як квантова криптографія та квантовий розподіл ключів (Quantum Key Distribution, QKD) для забезпечення конфіденційності зв’язку.

Одним із ключових принципів квантової криптографії є використання квантової суперпозиції та заплутаності [1]. Квантовий стан частинки, наприклад, фотона [5], може перебувати у суперпозиції станів |0⟩ та |1⟩, що описується виразами (23) та (24):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{23}$$

$$|\alpha|^2 + |\beta|^2 = 1, \tag{24}$$

де α і β – комплексні амплітуди.

При спробі вимірювання цього стану сторонньою особою (перехоплювачем) квантовий стан колапсує до одного з базисних станів, що порушує початкову інформацію та робить перехоплення помітним для легітимних користувачів.

Найвідомішим протоколом QKD є BB84, запропонований Чарльзом Беннеттом і Жилем Брассаром у 1984 році. У цьому протоколі відправник (*A*) кодує біти ключа у поляризаційних станах фотонів, наприклад, горизонтальному (|*H*⟩) або вертикальному (|*V*⟩), а також у діагональних базисах (25) та (26):

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, \tag{25}$$

$$|A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}. \tag{26}$$

Отримувач (**Б**) випадково обирає базис для вимірювання. Після передачі отримувач (**А**) та відправник (**Б**) порівнюють базиси через відкритий канал і зберігають лише ті біти, де базиси збіглися. Будь-яке втручання, наприклад, вимірювання посередником (В), вносить помилки, які виявляються через перевірку підмножини бітів. Рівень помилок у ключі (Quantum Bit Error Rate, *QBER)* розраховується виразом (27):

$$QBER = \frac{D}{DD}, \tag{27}$$

де *D* – кількість помилок;

DD – загальна кількість бітів.

Якщо *QBER* перевищує певний поріг (зазвичай 11 % для BB84), це свідчить про присутність перехоплювача.

Перспективи впровадження квантових технологій включають інтеграцію QKD у сучасні оптоволоконні мережі та супутникові системи зв’язку. Наприклад, китайський супутник Micius у 2017 році продемонстрував успішну передачу квантового ключа на відстань понад 1200 км. Це стало проривом у глобальній квантовій комунікації, що використовує супутниковий зв’язок для передачі ключів між континентами. Ключова перевага полягає в тому, що будь-яка спроба перехоплення квантового сигналу змінює його стан, що описується принципом клонування квантових станів: жодна квантова система не може бути скопійована без порушення оригіналу (теорема про заборону клонування). Однак існують і виклики: висока вартість обладнання, обмеження дальності передачі через втрати у волокнах (приблизно 0,2 дБ/км для стандартних оптоволоконних ліній), які описуються законом Бугера – Ламберта – Бера, який описує залежність інтенсивності світла від товщини середовища та концентрації поглинаючої речовини при його проходженні через поглинаюче середовище. Його математичний вираз має вигляд (28):

$$I = I_0 e^{-\alpha L}, \tag{28}$$

або у логарифмічній формі (29):

$$A = \log \frac{I_0}{I} = \varepsilon c L, \tag{29}$$

де I_0 – початкова інтенсивність світла;

α – коефіцієнт поглинання середовища;

I – інтенсивність світла після проходження середовища;

L – товщина поглинаючого шару;

A – оптична густина (абсорбція);

ε – молярний коефіцієнт поглинання (залежить від довжини хвилі світла речовини);

c – концентрація поглинаючої речовини.

Практичне застосування закону Бугера – Ламберта – Бера може бути використане у спектроскопії, аналітичній хімії та біофізиці для визначення концентрації речовин у розчинах. У військовій сфері він застосовується для аналізу диму, газів та забруднень в атмосфері, а також у лазерних технологіях, зокрема для оцінки ефективності маскувальних аерозолів та оптичного виявлення хімічних речовин.

Для зменшення втрат активно розробляються квантові повторювачі (quantum repeaters), які використовують заплутані фотони для подовження дистанції передачі (телепортацію квантового стану) [1; 2].

У майбутньому вдосконалення квантових повторювачів, які використовують квантову телепортацію для подолання втрат сигналу, може розширити масштабність таких систем. Процес телепортації квантового стану описується оператором заплутаності, наприклад, для стану Белла [1; 7; 9] виглядає, як у виразі (30):

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{30}$$

де стан однієї частинки передається іншій через спільний заплутаний стан і класичний канал зв’язку.

Ще одним видом використання квантових технологій може бути квантовий зв’язок, в основу якого покладена квантова сплутаність (заплутаність) [1–8] – це квантовомеханічне явище, коли існує взаємозв’язок та залежність між квантовими частками, навіть рознесеними у просторі. Головним при цьому є використання так званих сплутаних квантових станів [5–8]. На рисунку 1 зображено процес утворення зв’язаних частинок фотона шляхом їх пропускання скрізь кристал бета-барата-барія світового потоку або одного фотону.

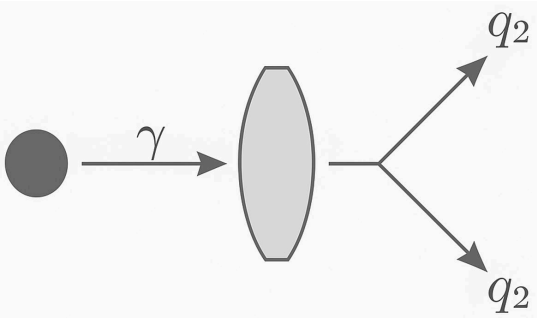


Рис. 1. Графічне представлення процесу утворення заплутаних кубітів (фотонів) шляхом їх розкладання в лінзі

На рисунку 2 пояснюється процес вимірювання стану частки. Зв’язані або заплутані квантові частки захоплюються в пастку, яка вимірює їх стан, але далі ці частки вже не поширюються.

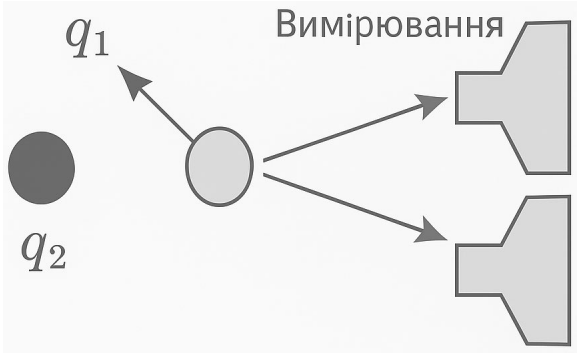


Рис. 2. Графічне представлення вимірювання (та руйнування)
стану заплутаних кубітів спеціальними пастками

Рисунок 3 пояснює, як крізь канал, побудований на основі заплутаних частинок ***A***, ***B***, передається інформаційна частка ***C***.

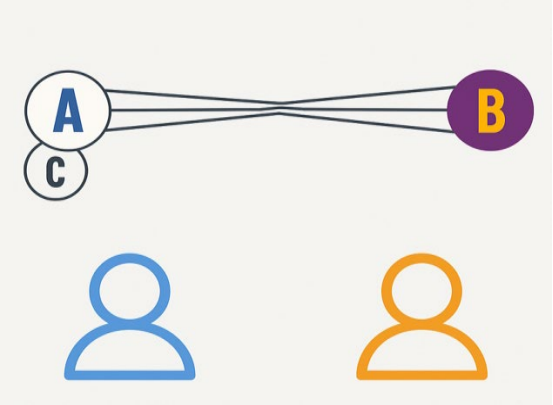


Рис. 3. Принцип передачі даних каналом, утвореним між пов’язаними частками *A, B*

Квантовий генератор випадкових чисел (КГВЧ). Однією із важливих складових криптографічних систем є генератори псевдовипадкових чисел, необхідні для створення ключів шифрування. КГВЧ використовує квантові явища, такі як суперпозиція і заплутаність, для створення чисел, які є абсолютно випадковими і не підлягають детермінізму, забезпечуючи високий рівень ентропії і непередбачуваності, що є критично важливим для криптографії та інших безпекових застосувань, особливо у військові сфері. На рисунку 4 визначено принцип утворення потоку випадкових чисел за рахунок утворення та контролю збуджених станів квантових часток. Очікувано, що Збройні сили використають КГВЧ для здійснення більш надійного захисту інформації.

Перспективним для військового використання є *квантовий датчик Рідберга* (КДР), який здатен перевершити можливості сучасних засобів електроніки за чутливістю, смугою пропускання і частотним діапазоном. Це в перспективі надасть можливість розробити нові ефективні засоби радіоелектронної боротьби. Рисунок 5 пояснює принцип роботи квантових часток у різноманітних сенсорах або засобах, реалізуючи квантові датчики.

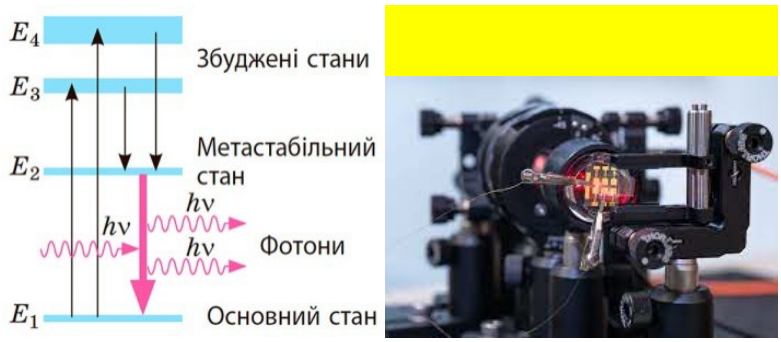


Рис. 4. Принцип роботи квантового генератора випадкових чисел

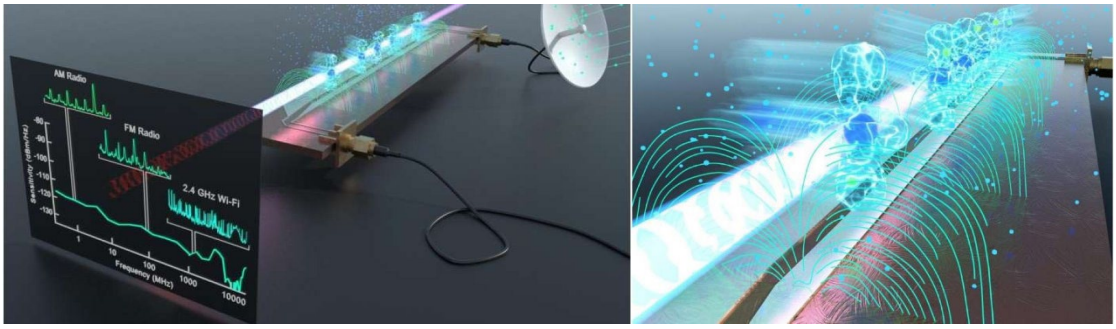


Рис. 5. Надчутливі квантові датчики

КДР здатен вловлювати й аналізувати весь спектр радіочастотних сигналів та допоможе виявити ворожі електронні засоби. КДР здатен фіксувати від нульової частоти до 19 ГГц, АМ- та FM-хвилі, Bluetooth, Wi-Fi та інші сигнали зв’язку. Наразі застосовують лазерні промені для створення атомів Рідберга, зовнішні електрони яких знаходяться у високозбудженому стані. Це робить датчик надчутливим до широкого діапазону сигналів у радіочастотному спектрі.

КДР значно перевищує сучасну електроніку за чутливістю, смугою пропускання і частотним діапазоном. Таким чином, можливо розробити військові засоби радіоелектронної боротьби та виявлення засобів зв’язку в рази ефективнішими, що є частиною стратегії модернізації армії.

Кульмінацією розвитку військового квантового зв’язку стане створення військового квантового Інтернету, коли передача буде здійснюватися у вигляді кубітів між розподіленими квантовими процесорами. Надалі військові побудують квантовий зв’язок між командними пунктами та вузлами управління, використовуючи субатомні частинки, такі як фотони [5], для передачі інформації на принципах квантової механіки. Квантова криптографія забезпечить таємність даних, тому що ці частинки неможливо знищити, скопіювати або відслідити. Квантовий розподіл ключів передбачає передачу ключової інформації заплутаними фотонами, що унеможлює перехоплення даних, тому що при їх вимірюванні вони руйнуються. Рисунок 6 відображає схему утворення глобального квантового Інтернету на основі супутникової мережі.

Рис. 6. Принцип формування та роботи глобального квантового Інтернету

Квантова телепортація [2–7] дозволить передавання квантового стану від однієї частинки до іншої на відстані без фізичного переміщення самої частинки. У квантовій телепортації не передається сама інформація чи матеріал, а лише квантовий стан, що робить її важливою для майбутніх технологій, зокрема для квантової комунікації та обчислень[1; 10; 11]. Рисунок 7 дає уяву про принципи роботи квантової телепортації на основі супутникових каналів зв’язку, утвореними між заплутаними частками.

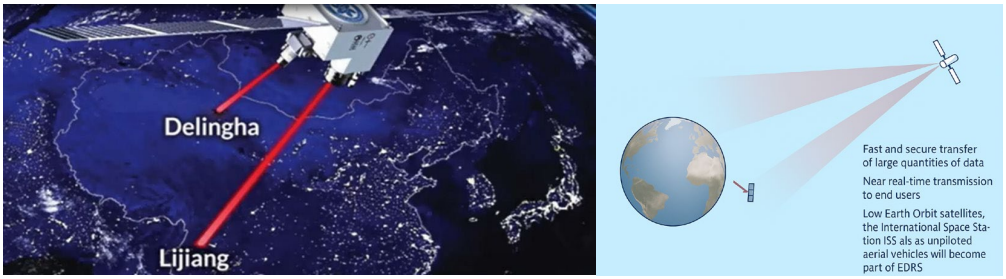


Рис. 7. Принципи роботи квантової телепортації на базі утворених супутникових каналів між заплутаними частками

Квантова телепортація є фундаментальною технологією для створення захищених каналів зв’язку у військовій галузі. Вона дозволить передавати квантовий стан між віддаленими військовими об’єктами без фізичного переміщення носія інформації. Основна ідея базується на квантовій заплутаності, що дозволяє миттєво передавати інформацію. У майбутньому квантові технології можуть стати основою військових мереж зв’язку, стійких до атак квантових комп’ютерів, які здатні зламувати традиційні криптосистеми (RSA, ECC) за допомогою алгоритму Шора [4–7]. Таким чином, впровадження квантових каналів зв’язку обіцяє революцію в кібербезпеці, забезпечуючи абсолютну конфіденційність передачі даних.

Перспективним напрямком автори статті вважають використання квантових сенсорів та військової навігації.

Наприклад, традиційні GPS-системи можуть бути заблоковані радіоелектронною боротьбою. Альтернативою є квантові інерціальні сенсори, що базуються на принципі атомної інтерферометрії. Основне рівняння руху квантових частинок у такій системі має вигляд (31):

$$S = \int L dt, \tag{31}$$

де S – дія;

L – лагранжіан;

dt – елемент часу.

У квантовій механіці лагранжіан можна представити у вигляді (32):

$$L = \frac{1}{2}mv^2 - \mathcal{V}, \tag{32}$$

де m – маса атома;

v –швидкість атома;

$\mathcal{V}$ – потенціальна енергія в системі.

Завдяки вимірюванню фазового зсуву між хвильовими функціями атомів можна з високою точністю визначати параметри руху, включаючи прискорення та кутову швидкість.

Квантові інерціальні сенсори забезпечують надвисоку точність визначення координат, що дозволяє військовим об’єктам, таким як підводні човни, безпілотники та ракетні комплекси, автономно орієнтуватися без використання GPS. Точність таких систем може сягати нанометрів на секунду, що значно перевершує традиційні інерціальні навігаційні системи.

Крім того, квантові сенсори можуть працювати в умовах, де традиційні системи втрачають ефективність, наприклад, під водою, у глибоких підземних тунелях або в середовищі із сильними радіоперешкодами.

Таким чином, застосування квантових сенсорів у військовій навігації відкриває нові можливості для Збройних сил, що забезпечує незалежність від супутникових систем (наприклад, нещодавній випадок відключення функціонування супутникової системи Starlink під час проведення бойових дій Збройними Силами України в окупованому Криму та в Курській операції) та підвищує точність автономного руху військової техніки. Це робить квантові технології критично важливим напрямом розвитку оборонних систем майбутнього.

Висновки

Таким чином, використання квантових технологій демонструє значний прогрес і потенціал для застосування у військових галузях, таких як зв’язок, криптографія та оптимізація військових операцій. Інтеграція квантових технологій у військову сферу може докорінно змінити принципи ведення бойових дій, забезпечуючи технологічну перевагу над супротивником.

У майбутньому для повноцінного використання квантових технологій у секторі оборони України необхідно продовжувати дослідження, створювати необхідну матеріально-технічну базу та подальше впровадження підготовки професійних і досвідчених квантофахівців, що передбачає розробку сучасних освітніх програм у галузі квантової фізики, обчислень та безпеки, використання в освітньому процесі інноваційних методів та забезпечення новітніми технічними засобами.

З огляду на стрімкий розвиток квантових технологій, держави, які першими зможуть ефективно їх інтегрувати у військову інфраструктуру, отримають стратегічну перевагу у майбутніх конфліктах та значно змінять власну обороноздатність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карлаш Г. Ю. Квантові інформаційні системи: навч. посіб. для спеціальності «Прикладна фізика та наноматеріали». Київ, 2018. С. 12, 18, 33.

2. Вакарчук І. О. Квантова механіка: підруч. / І. О. Вакарчук. 4-те вид., доп. Львів: ЛНУ ім. Івана Франка, 2012. С. 747–749.

3. Павлишенко Б. Квантовий алгоритм розпізнавання образів на растрових зображеннях // Львівський національний університет ім. Івана Франка. Львів. Серія Фіз. 2010. Вип. 45. С. 24–30.

4. Крохмальський Т. Є. Вступ до квантових обчислень: навч. посіб. Львів: ЛНУ ім. Івана Франка, 2018. С. 107–120.

5. Філоненко Є. О., Королюк Д. В. Фотонні системи з однокубітними квантовими обчисленнями. Київ: Кафедра мікроелектроніки НТУ України «КПІ ім. Ігоря Сікорського», Факультет електроніки. Київ, 2021. С. 44–45, 50–51, 107–120.

6. Старовойт Тетяна, Зайченко Юрій. Гібридна квантово-вдосконалена модель штучного інтелекту в задачі автоматичного розпізнавання та швидкого перетворення неструктурованої текстової інформації на просторову // Advanced Information Technology. 2023. № 1 (2).

7. Боровий М. О., Оліх О. Я. Фізичні основи квантової механіки. Частина 1. К.: КНУ ім. Тараса Шевченка, 2011. С. 19–22, 56–65.

8. Крохмальський Т. Квантові комп’ютери: основи й алгоритми (короткий огляд) / Т. Крохмальський // Журн. фіз. досліджень. 2004. Т. 8, № 4. С. 1–15.

9. Кобушкін О. П. Квантова механіка: навч. посіб. Київ, 2016. С. 1–15.

10. Будник Микола. Булеві квантові логічні операції // Фізико-математичне моделювання та інформаційні технології. 2023. Вип. 36. С. 38–42. URL: doi.org/10.15407/fmmit2023.36.038.

11. Горбенко І. Д., Качко О. Г., Кузнєцов О. О., Потій О. В., Горбенко Ю. І., Пономар В. А., Єсіна М. В. Проблеми створення стандартів перспективних криптографічних перетворень та хід їх вирішення // Доповідь на конференції ВІТІ, 2018 URL: https://iit.com.ua/.

12. Корольов В. Ю., Ходзінський О. М. Дослідження впливу параметрів квантового відпалу на якість розв’язку задачі факторизації чисел // Cybernetics and Computer Technologies. 2023. Вип. 1. С. 13–22. URL: https://doi.org/10.34229/2707-451X.23.1.2.

DOI: 10.58254/viti.7.2025.04.44

УДК 62-23

канд. техн. наук, доцент Корольов А. П. ORCID: 0000-0001-6281-063X (ВІТІ ім. Героїв Крут)
канд. техн. наук Мацаєнко А. М. ORCID: 0000-0003-1149-7318 (ВІТІ ім. Героїв Крут)
Роскошний Д. В. ORCID: 0000-0002-4432-6630 (ІТС НТУУ«КПІ ім. Ігоря Сікорського»)

ОСОБЛИВОСТІ РОЗРАХУНКУ ЧАСУ ОБЧИСЛЕНЬ ПІД ЧАС ПРОЄКТУВАННЯ ЦИФРОВИХ ФІЛЬТРІВ НА МІКРОКОНТРОЛЕРАХ

Стаття присвячена створенню методики оцінки частотного діапазону сигналів під час проєктування цифрового фільтра шляхом вимірювання часу калькуляції поточного відліку в системі цифрового фільтра нижніх частот із кінцевою імпульсною характеристикою на мікроконтролері STM32F103C8T6.

Розроблено установку для дослідження фільтра, яка включає в себе: генератор синусоїдальних сигналів; вхідне коло для забезпечення подачі додатних значень на вхід АЦП; модуль самого мікроконтролера STM23F103C8T6, який обробляє вхідний сигнал у реальному часі та реалізує функцію фільтрації.

Таймер мікроконтролера налаштований на генерацію переривань для вибірки вхідного сигналу з частотою дискретизації 35,15 кГц. Створено програмний код для забезпечення мінімального часу перетворення у процесі фільтрації.

Виконано програмну реалізацію кінцевої імпульсної характеристики фільтра нижніх частот із частотою зрізу 800 Гц. Забезпечено реалізацію даного фільтра порядком від одиниць до сотень. Проаналізовано амплітудно-частотні характеристики фільтрів низького та високого порядків. Розроблено методику визначення періоду виконання мікроконтролером обчислення згортки, яка є основою процесу фільтрації. Розроблено код налаштування таймера для вимірювання часу та виводу результату на дисплей у режимі реального часу.

Обрано найпростіший алгоритм обчислення згортки і реалізовано мовою програмування С++. Отримано результати вимірювань часу калькуляції згортки мікроконтролером STM32F10C8T6 залежно від різних порядків цифрового фільтра. Результати можуть бути використані для визначення необхідного періоду (частоти) дискретизації сигналу. Відповідно, вони дозволяють оцінити максимальний частотний діапазон сигналу, який може бути оброблений у режимі реального часу цифровим фільтром обраного порядку.

Ключові слова: *цифрові фільтри, STM мікроконтролер, операція згортки, час розрахунку, час процесора, режим реального часу, діапазон частот.*

A. Korolov, A. Matsayenko, D. Roskoshniy. Features of calculating computing time when designing digital filters on STM32F103 microcontrollers from STMicroelectronics Corporation

The article is devoted to the creation of a method for estimating the frequency range of signals when designing a digital filter (DF) by measuring the calculation time of the current reference in the system of a digital low-pass filter (LPF) with a finite impulse response (FIR) on the STM32F103C8T6 microcontroller.

A setup for studying the filter has been developed, which includes: a generator of sinusoidal signals; an input circuit to ensure the supply of positive values to the ADC input; the STM23F103C8T6 microcontroller module itself, which processes the input signal in real time and implements the filtering function.

The microcontroller timer is configured to generate interrupts for sampling the input signal with a sampling frequency of 35.15 kHz. A program code has been created to ensure the minimum conversion time during the filtering process.

A software implementation of the FIR low-pass filter with a cutoff frequency of 800 Hz has been performed. The implementation of a filter with an order from units to hundreds is provided. The amplitude-frequency characteristics (AFC) of low- and high-order filters have been analyzed. A method has been developed for determining the period of execution of the convolution calculation by the microcontroller, which is the basis of the filtering process. A timer setting code has been developed for measuring time and displaying the result on the display in real time.

The simplest convolution calculation algorithm has been selected and implemented in the C++ programming language. The results of measurements of the convolution calculation time by the STM32F10C8T6 microcontroller have been obtained depending on different orders of the digital filter. The results can be used to determine the required period (frequency) of signal sampling. Accordingly, they allow us to estimate the maximum frequency range of the signal that can be processed in real time by a digital filter of the selected order.

Keywords: *digital filters, STM microcontroller, convolution operation, calculation time, processor time timing, real-time mode, frequency range.*

Постановка задачі в загальному вигляді. Цифрова обробка сигналів (ЦОС) є критично важливою технологією в сучасній електроніці, яка дозволяє аналізувати сигнали та використовувати отриману інформацію в різноманітних сферах застосування, таких як обробка аудіо, фото і відео, телекомунікації, медична діагностика, системи управління [1, 2]. Цифрова фільтрація (ЦФ) є одним з основних напрямів ЦОС. ЦФ є важливим компонентом в обробці цифрових сигналів, призначенням яких є виділення корисного сигналу та придушення небажаних складових із його спектра [3].

На сьогодні способи реалізації ЦФ є доволі різноманітними. Мікроконтролери (МК) – одне з апаратних рішень для реалізації ЦФ, які стали популярним вибором для виконання завдань ЦОС у вбудованих системах завдяки своїй доступності, універсальності та енергоефективності. Однією з проблем такої реалізації є забезпечення обробки сигналу у режимі реального часу, що означає завершення обробки поточного відліку сигналу протягом періоду дискретизації до надходження наступного відліку [3].

Відомо, що обчислювальна ефективність фільтра, тобто швидкість обробки дискретних вибірок сигналу, напряму залежить від кількості операцій множення з накопиченням. Вони є основою згортки сигналу з імпульсною характеристикою фільтра. Чим більше порядок ЦФ, тим більшою буде кількість операцій і відповідно часовий інтервал, необхідний для виконання операції згортки. При збільшенні частоти сигналу, що підлягає фільтрації, необхідно збільшувати частоту дискретизації, що зменшує часовий інтервал для обробки відліку сигналу. Тому під час практичної реалізації ЦФ необхідно правильно розраховувати період виконання мікроконтролером операції згортки.

У статті розглянуто особливості розрахунку таймінгу процесорного часу цифрового фільтра на прикладі фільтра низьких частот (ФНЧ) на мікроконтролері *STM32F103C8T6* (*Cortex-M3*). Увагу приділено дослідженню періоду виконання мікроконтролером обчислень згортки, що лежать в основі процесу фільтрації. В якості зразка було використано ФНЧ із кінцевою імпульсною характеристикою (КІХ) (*Low Pass FIR-filtering*) зі смугою пропускання 0…800 Гц. Досліджувались варіанти реалізації такого фільтра різного порядку – від одиниць до сотень.

Аналіз публікацій за темою дослідження. Дана проблема є актуальною з погляду необхідності побудови ефективного пристрою ЦФ під час роботи з різними за частотою сигналами. Цій проблемі присвячено низку робіт.

У роботі [4] досліджено, яким є вплив рівня оптимізації коду відповідного середовища розробки (*STM32Cube IDE*) на час виконання операції фільтрації. Наведено таблиці з отриманими часовими інтервалами та зроблено висновок, який рівень оптимізації дає виграш у часі. Але при цьому не взято до уваги вплив порядку фільтра. А саме порядок визначає вигляд *амплітудно-частотної характеристики* (АЧХ) фільтра.

У роботі [5] приділено увагу дослідженню впливу різних алгоритмів обчислення згортки на швидкість обчислень у мікроконтролерах на ядрах *ARM Cortex-M4* і *Cortex-M7*. Авторами визначено прискорення роботи мікроядер і представлено графіки залежності для трьох різних обраних мікроконтролерів. Але не вказано на залежність обчислень від кількості відліків при обчисленні згортки.

Публікація [6] знайомить із результатами дослідження тестових програм для мікроконтролерів на ядрах *ARM Cortex-M4* і *Cortex-M0+*. Тестові програми дозволяють вимірювати затримку критичних у часі операцій. Це дозволить оцінити обчислювальні можливості того чи іншого мікроконтролера, але не відображено конкретну порівняльну таблицю для обчислень, зокрема згортки сигналів.

У дослідженні [7] представлено та проаналізовано декілька структур побудови КІХ-фільтрів з метою оптимізації часу і складності обчислювальних процесів. Але автори

не представили залежність впливу кількості коефіцієнтів імпульсної характеристики на час обчислення і виведення кожного поточного відліку.

Дослідження чинників, які впливають на часові параметри під час проєктування і реалізації цифрових фільтрів, як бачимо, є актуальною задачею. В рамках даного дослідження вирішено зосередитись на вимірюванні часу такої математичної операції, як згортка, що виконується мікроконтролером сучасної корпорації *STMicroelectronic*. Вибір мікроконтролера *STM32F103C8T6* обумовлений його кращими характеристиками за співвідношенням параметрів ціна/можливості/продуктивність.

Метою статті є створення методики оцінки частотного діапазону сигналів під час проєктування цифрового фільтра шляхом вимірювання часу калькуляції поточного відліку в системі цифрового КІХ-фільтра нижніх частот на мікроконтролері *STM32F103C8T6*.

Виклад основного матеріалу. В якості зразка на мікроконтролері *STM32F103C8T6* (*Cortex-M3*) було створено цифровий КІХ-фільтр нижніх частот та установка для його дослідження. Структурна схема установки представлена на рисунку 1.

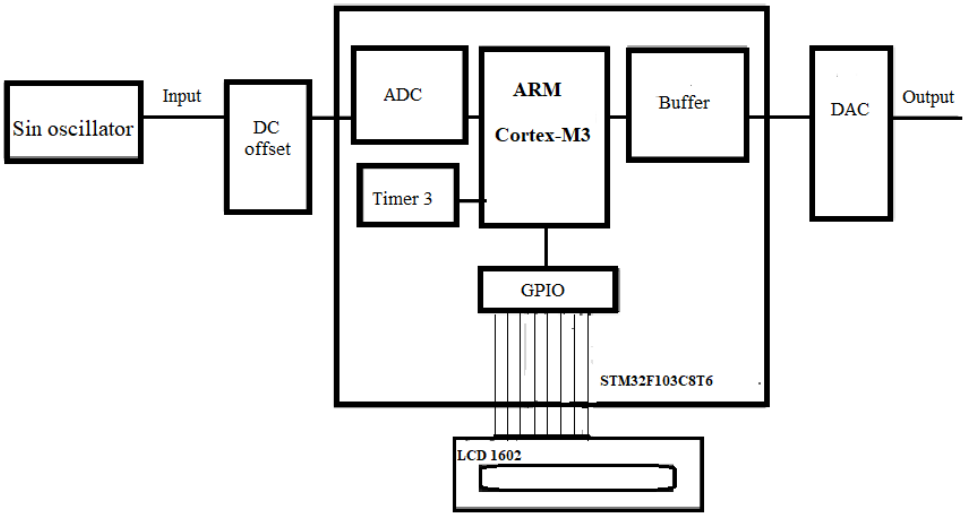


Рис. 1. Структурна схема установки для дослідження КІХ-фільтра на мікроконтролері *STM32F103C8T6*

Перша частина структури – це вхідне коло. Функція його полягає в додаванні постійного зміщення до вхідного сигналу. Це необхідно, оскільки вхідний сигнал є сигналом змінного струму, який складається як із додатних, так і з від'ємних значень напруги. Аналого-цифровий перетворювач мікроконтролера (АЦП) може працювати тільки з додатними значеннями. Сигнал на виході вхідного кола є сигналом змінного струму, який приймає значення від 0 до 3.3 В і готовий до подачі на АЦП мікроконтролера *STM32F103C8T6*.

Друга частина структури – це модуль самого мікроконтролера *STM23F103C8T6*, який обробляє вхідний сигнал в реальному часі. АЦП здійснює дискретизацію вхідного сигналу з роздільною здатністю 10 біт. Таймер *T3* використовується для генерації переривань для вибірки вхідного сигналу з частотою дискретизації 35,15 кГц, а також для вимірювання часу обрахунку математичної операції згортки.

Поточний час калькуляції, зміна якого є предметом дослідження, вимірюється в мікросекундах і виводиться на *LCD* символьний дисплей типу 1602 на основі інтерфейсу *HD*44780. Алгоритм вимірювання часу процедури представлений блок-схемою на рисунку 2.

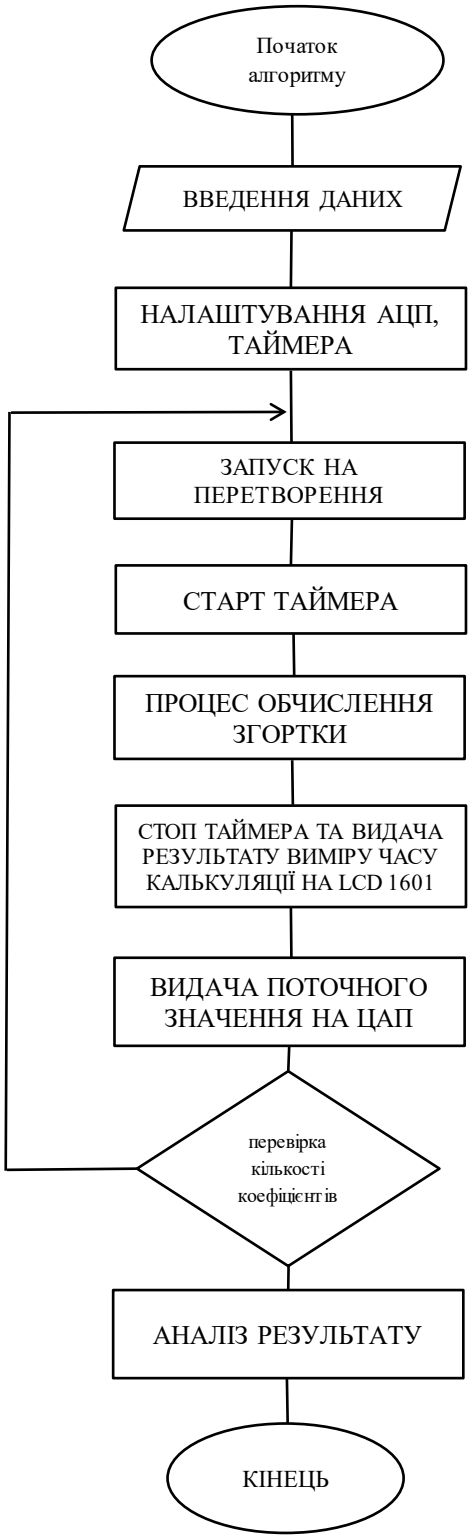


Рис. 2. Блок-схема алгоритму виміру часу калькуляції згортки

Особливість налаштування АЦП самого мікроконтролера *STM32F103C8T6* полягає в тому, щоб вийти на мінімальний час перетворення у процесі фільтрації.

Приклад коду з коментарями, що забезпечує налаштування аналогово-цифрового перетворювача, представлено нижче.

```
#include "stm32f10x.h" // Бібліотека CMSIS для STM32F10...

void ADC1_Init(void) {
   // Увімкнення тактування ADC1 та GPIOA (для каналу 0 - PA0)
   RCC->APB2ENR |= RCC_APB2ENR_ADC1EN | RCC_APB2ENR_IOPAEN;
   // Налаштування PA0 у аналоговий режим (ADC_IN0)
   GPIOA->CRL &= ~(GPIO_CRL_MODE0 | GPIO_CRL_CNF0);
   // Налаштування тактової частоти АЦП (PCLK2/6 = 12 МГц)
   RCC->CFGR &= ~RCC_CFGR_ADCPRE;              // Очистити біти ADCPRE
   RCC->CFGR |= RCC_CFGR_ADCPRE_DIV6;  // Встановити дільник на 6 , тобто 12 МГц)
   // Налаштування АЦП
   ADC1->CR2 |= ADC_CR2_ADON;  // Увімкнути АЦП
   for (volatile int i = 0; i < 10000; i++);  // Затримка (необхідна для стабілізації)
   ADC1->SMPR2 &= ~ADC_SMPR2_SMP0;  // Очистити біти часу вибірки
   ADC1->SMPR2 |= ADC_SMPR2_SMP0_0; // Встановити мінімальний час вибірки: 1.5 такт
   ADC1->SQR1 &= ~ADC_SQR1_L;  // Один канал у послідовності (L = 0)
   ADC1->SQR3 &= ~ADC_SQR3_SQ1;
   ADC1->SQR3 |= 0;  // Канал 0 (ADC_IN0)
   // Калібрування АЦП
   ADC1->CR2 |= ADC_CR2_CAL;
   while (ADC1->CR2 & ADC_CR2_CAL);  // Очікування завершення калібрування
}
uint16_t ADC1_Read(void) {// Функція для запуску АЦП і отримання результату
   ADC1->CR2 |= ADC_CR2_ADON;                // Запуск перетворення
   while (!(ADC1->SR & ADC_SR_EOC));         // Очікування завершення
   return ADC1->DR;                          // Читання результату
}
```

Було створено відповідний код, що реалізує функцію фільтрації для представленої схеми.

Цифровий КІХ-фільтр являє собою певну дискретну систему, в якій вираз (1) визначає співвідношення між вхідною x_n та вихідною y_n послідовностями:

$$y_n = \sum_{k-0}^{N} h_k * x_{n-k} , \quad (1)$$

де постійні коефіцієнти h_k – це відліки імпульсної характеристики фільтра. Вхідне вікно фільтра, тобто кількість відліків вхідного сигналу, що обробляються для отримання одного відліку вихідного сигналу, складає $N + 1$. Число N визначає порядок фільтра.

Системна (передатна) функція КІХ-фільтра має наступний вид:

$$H(z) = \sum_{i-0}^{N} h_i * z^{-i},$$

де $z = e^{jw}$.

Щодо комплексної частотної характеристики фільтра, то вона може бути представлена поліномом наступного вигляду:

$$H\left(e^{jw}\right) = \sum_{k-0}^{N} h_k e^{jwk} = \left|H\left(e^{jw}\right)\right| e^{j\varphi(w)}, \quad (2)$$

де $|H(e^{jw})|$ – амплітудно-частотна характеристика (АЧХ);

$\varphi(w)$ – фазо-частотна характеристика (ФЧХ) фільтра.

Для розрахунку коефіцієнтів КІХ-фільтра з частотою зрізу 800 Гц було використано відповідний додаток із пакету *Matlab*.

Так, наприклад, для ФНЧ 7-го порядку коефіцієнти імпульсної характеристики будуть наступними:

0.02; 0.0647; 0.1664; 0.2489; 0.2489; 0.1664; 0.0647; 0.02.

За допомогою програмного пакету *Mathcad* була розрахована його АЧХ, вигляд якої представлено на рисунку 3.

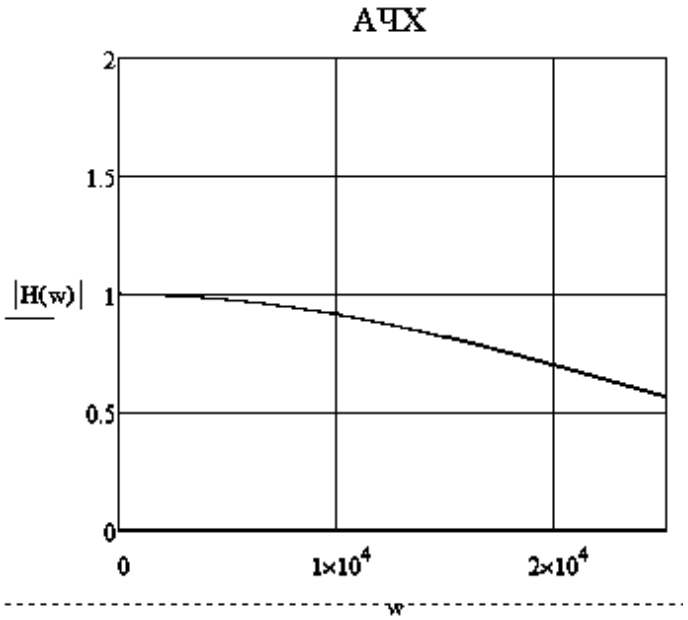


Рис. 3. АЧХ КІХ-фільтра 7-го порядку

Для ФНЧ 19-го порядку коефіцієнти КІХ-фільтра складають наступний масив:

0.4620514531395525; 1.5242017614706227; 3.793161197453402; -7.016345527025121;
11.042184667369394; -14.442346816573414; 16.30850577885218; -15.069991485222175;
10.861863005754623; -3.853269786474018; -3.853269786474018; 10.861863005754623;
-15.069991485222175; 16.30850577885218; -14.442346816573414; 1 1.042184667369394;
-7.016345527025121; 3.793161197453402; -1.5242017614706227; 0.4620514531395525.

АЧХ такого фільтра представлена на рисунку 4.

Аналіз отриманих характеристик підтверджує, що вони відповідають характеристикам ФНЧ з частотою зрізу 800 Гц. Очевидно, що збільшення порядку фільтра призводить до звуження смуги переходу від смуги пропускання до смуги затримування. Також змінюються величини відхилень АЧХ від ідеальної у смугах пропускання та затримування. Тому порядок фільтра слід обирати з вимог до граничної частоти смуги затримування та припустимих нерівномірностей АЧХ.

З практичного досвіду відомо – для ґрунтовного обмеження небажаних частот спектра потрібно використовувати масив 60…100 відліків імпульсної характеристики фільтра, тобто використовувати ЦФ такого порядку.

Як відомо, час для формування кожного вихідного відліку y_n складається з двох складових:

- часу перетворення T_{ADC};
- часу калькуляції згортки T_C.

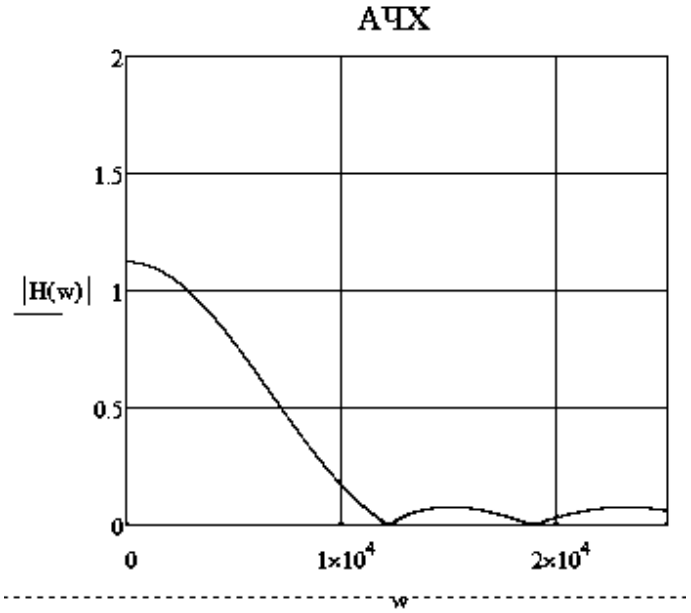


Рис. 4. АЧХ КІХ-фільтра 19-го порядку

Якщо час перетворення однозначно визначається режимом налаштування АЦП мікроконтролера, то час калькуляції згортки залежить від алгоритму, типу змінних, порядку фільтра, деяких особливостей написання програми, від рівня оптимізації компілятора робочої *IDE* [4].

Частину програмного забезпечення було присвячено вимірюванню часу, який витрачався на обчислення згортки і формування поточного вихідного відліку y_n.

Дані вимірювання часу виводились на дисплей у режимі реального часу.

Код налаштування таймера Т3 має наступний вигляд:

```
void TIM3_Config(void) {
RCC_APB1PeriphClockCmd(RCC_APB1Periph_TIM3, ENABLE);
TIM_TimeBaseInitTypeDef TIM_TimeBaseStructure;
TIM_TimeBaseStructure.TIM_Period = 0xFFFF;       // Максимальне значення лічильника
TIM_TimeBaseStructure.TIM_Prescaler = 71;        // Переддільник для частоти 1 МГц
TIM_TimeBaseStructure.TIM_ClockDivision = 0;
TIM_TimeBaseStructure.TIM_CounterMode = TIM_CounterMode_Up;
 TIM_TimeBaseInit(TIM3, &TIM_TimeBaseStructure); /
TIM_Cmd(TIM3, ENABLE);    }
```

Точність вимірювань часу калькуляції визначається тривалістю тактового імпульсу, які використовує таймер/лічильник *T*3 і дорівнює приблизно 14 нс.

Алгоритм обчислення згортки було обрано найпростіший і реалізовано мовою програмування *C++*. Рівень оптимізації компілятора *GCC* обраний мінімальним.

Результати вимірювань часу калькуляції згортки мікроконтролером *STM32F10C8T6* залежно від порядку *N* цифрового КІХ-фільтра наведено в таблиці 1.

Таблиця 1

Кількість коефіцієнтів ІХ ($N+1$)	6	10	20	50	100	200
Час калькуляції, мкс	29	46	89	210	439	822

Графічно побудована діаграма залежності зростання часу калькуляції від кількості коефіцієнтів КІХ цифрового фільтра НЧ на мікроконтролері представлена на рисунку 5.

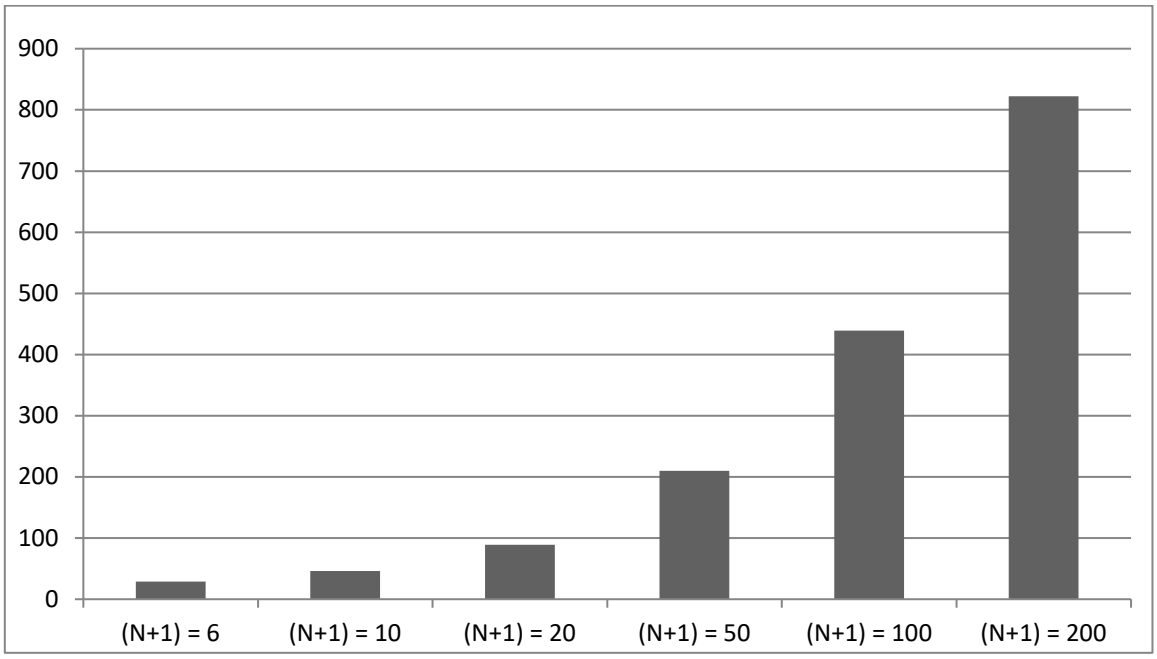


Рис. 5.Діаграма залежності часу калькуляції від кількості коефіцієнтів

1. Отримані результати вимірів часу калькуляції свідчать про вельми суттєвий час, який витрачається для формування кожного поточного відліку вихідного сигналу y_n. Зростання цього необхідного часу напряму пов’язано зі зростанням порядку фільтра. Так, для фільтра 5-го порядку час калькуляції складає 29 мкс, а для фільтра 199-го порядку – 822 мкс.

2. Якщо взяти до уваги час перетворення АЦП мікроконтролера, який розраховується за формулою

$$Tconv = (12.5 + 1.5) \times 112 \text{ МГц} \approx 1.17 \text{ мкс},$$

тобто триває приблизно 2 мкс, то є можливість оцінити, безпосередньо для якого саме діапазону частот може бути створений цифровий фільтр обраного порядку на мікроконтролері *STM32F10C8T6*.

3. Порядок фільтра впливає на крутизну АЧХ фільтра і звужує ширину перехідної області частот між смугою пропускання і смугою затримування, що покращує його вибірковість. З іншого боку, високий порядок потребує підвищеного часу обчислення кожного наступного значення на виході фільтра. Даний факт свідчить про необхідність пошуку оптимального вибору як алгоритму реалізації ЦФ, так і безпосередньо мікроконтролера з потрібними характеристиками.

Висновки. Таким чином, можна стверджувати, що отримані значення показників часу калькуляції можуть бути використані для оцінки можливого періоду (частоти) дискретизації сигналу. Відповідно можна визначити максимальний частотний діапазон сигналу, який може бути оброблений у режимі реального часу цифровим фільтром обраного порядку.

Майбутні напрямки досліджень передбачають пошук нових схемних рішень під час проєктування цифрових фільтрів, а також удосконалення алгоритмів обрахунку операції згортки. При цьому мають враховуватись можливості сучасних мікроконтролерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рудик А. В. Синтез та моделювання цифрових фільтрів програмними засобами MATLAB // Інформаційно-вимірювальні та обчислювальні системи і комплекси в технологічних процесах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2017. № 3. С. 87–93.

2. Smith J. Future Directions in Realizing Numerical Filters on STM32F103 Microcontrollers // Journal of Embedded Systems. 2023. No. 10 (2). P. 123–135.

3. 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.

4. Vorgul O., Zubkov O., Svyd I. Features of the Digital Filters Implementation on STM32 Microcontrollers. URL: https://mcfpga.nure.ua/en/conf-en/2021-mc-fpga/10-35598-mcfpga-2021-001.

5. Antonio Maciá-Lillo, Sergio Barrachina, Germán Fabregat, Manuel F. Dolz. Optimising Convolutions for Deep Learning Inference on ARM Cortex-M Processors // IEEE INTERNET OF THINGS JOURNAL. 2024. Vol. 11, No. 15. P. 26203–26219.

6. Ioan Ungurean. Timing Comparison of the Real-Time Operating Systems for Small Microcontrollers. Faculty of Electrical Engineering and Computer Science; Stefan cel Mare University of Suceava // Symmetry. 2020. No. 12(4). 592 p.

7. Abhishek Kumar, Suneel Yadav, Neetesh Purohit. FIR Filter Realization Under the Trade-Off Between Implementation Complexity and Computation Rate. Conference Paper. October 2019. P. 1–7.

8. Moore J. H. The DSP Handbook: Algorithms, Applications, and Design Techniques. CRC Press. 2008.

9. Welch T. B., Wright C. H. G., Morrow M. G. Embedded Signal Processing with the Micro Signal Architecture. Wiley. 2012.

10. Farag S., Khalil M. Design and Implementation of Digital Filters on FPGA // International Journal of Advanced Computer Science and Applications. 2017.

DOI: 10.58254/viti.7.2025.05.53

УДК 621.3.019.3

д-р техн. наук, професор Креденцер Б. П. ORCID: 0000-0003-1920-2107 (ВІТІ ім. Героїв Крут)
Унтілова О. О. ORCID: 0009-0003-8756-1889 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ НАДІЙНОСТІ СИСТЕМИ БЕЗПЕРЕРВНОГО ВИКОРИСТАННЯ ЗІ СТРУКТУРНОЮ НАДЛИШКОВІСТЮ З ПАРАЛЕЛЬНОЮ ВИТРАТОЮ СКЛАДОВИХ РЕЗЕРВНОГО ЧАСУ

Для обчислення нормального функціонування складних технічних систем, в тому числі автоматизованих систем управління, зв'язку, інформатизації тощо, в умовах зовнішніх впливів (відмов, перешкод) широко використовуються методи резервування: структурне, інформаційне, функціональне, навантажувальне та часове. Якщо перші чотири види резервування відомі давно, то результати дослідження надійності систем із часовою надмірністю з'явились відносно нещодавно. Резерв часу являє собою системний параметр, визначений структурою побудови і особливостями функціонування (алгоритмом використання) систем.

Аналіз відомих робіт [1–7], які були виконані в цій предметній області, показує, що більшість наукових результатів отримано при використанні окремих видів резервування, хоча комплексне використання надмірності дозволяє частково компенсувати недоліки та посилити переваги кожного окремого виду. Проте такий комплексний підхід суттєво ускладнює отримання розрахункових співвідношень для показників надійності, придатних для практичного використання.

Метою даної роботи є побудова математичної моделі надійності складної технічної системи безперервного використання, для підвищення надійності функціонування якої передбачено спільне використання структурного, навантажувального і часового резервування, яке містить дві складові резерву часу: поповнювальна ($t_Д$) та непоповнювальна ($t_Р$). У даній моделі передбачений один із ймовірних алгоритмів взаємодії складових резервного часу: інтервали відновлення системи $t_{Вi}$, в тому числі і ті, які не перевищують допустимий час $t_Д$, включаються в сумарний час простою системи та призводять до зменшення непоповнювальної складової резерву $t_Р$.

Варто зазначити, що облік трьох видів резервування в одній моделі надійності привів до помітного збільшення числа можливих станів досліджуваної системи. Для отримання більш простих розрахункових співвідношень для показників надійності використаний підхід, що базується на фазовому укрупненні станів [8; 9]. В результаті отримано відносно прості розрахункові співвідношення для вірогідності безвідмовного функціонування і середнього напрацювання до відмови системи. Проведена кількісна оцінка точності отриманих наближених формул підтвердила доцільність їх використання в інженерній практиці.

Ключові слова: *надійність функціонування, структурна надлишковість, часове резервування, завантажений, полегшений, ненавантажений резерв.*

B. Kredenzer, O. Untilova. Reliability Model of a continuously operating system with structural redundancy and parallel consumption of reserve time components

To assess the normal operation of complex technical systems, including automated control, communication, and information systems, under the influence of external faults (failures, interferences), various redundancy methods are widely used: structural, informational, functional, load-based, and temporal. While the first four types of redundancy have been known for a long time, research on the reliability of systems with temporal redundancy has emerged relatively recently. Time redundancy represents a system parameter determined by the system's structure and operational features (i.e., the algorithm of its use).

An analysis of the well-known studies [1–7] in this field shows that most scientific results have been obtained using individual types of redundancy, although integrated use of redundancy can partially compensate for the limitations and enhance the benefits of each separate type. However, such an integrated approach significantly complicates the derivation of analytical expressions for reliability indicators that are suitable for practical application.

The aim of this work is to develop a mathematical model for the reliability of a continuously operating complex technical system, in which structural, load-based, and temporal redundancy are jointly applied to improve operational reliability. The model includes two components of time reserve: replenishable ($t_Д$) and non-replenishable ($t_Р$). The model assumes one of the possible algorithms for the interaction of time reserve components: system recovery intervals t_{Bi}, including those not exceeding the permissible time $t_Д$, are included in the total system downtime and lead to a reduction in the non-replenishable component $t_Р$.

It is worth noting that accounting for three types of redundancy within a single reliability model led to a significant increase in the number of possible system states. To derive simpler analytical expressions for reliability indicators, an approach based on phase-state aggregation [8,9] was used. As a result, relatively simple analytical expressions for system reliability metrics-such as the probability of failure-free operation and the mean time to failure-

were obtained. A quantitative assessment of the accuracy of these approximate formulas confirmed their practical applicability in engineering contexts.

Keywords: *operational reliability, structural redundancy, time-based redundancy, loaded reserve, reduced-load reserve, unloaded reserve.*

Постановка завдання. Розглянемо систему, в якій передбачено спільне використання структурної, навантажувальної і часової (резерв часу комбінований) надлишковості. У цій системі об'єкт складається з n основних ($n \geq 1$) і m резервних ($m \geq 1$) ідентичних елементів, які можуть відмовляти, причому сумарна інтенсивність відмов залежить від числа непрацездатних елементів.

Позначимо через λ_k сумарну інтенсивність відмов елементів за умови, що в даний момент непрацездатні k елементів. Інтенсивність λ_k визначається числом основних і резервних елементів, а також інтенсивністю відмови окремого основного і резервного елементів. У разі змішаного резерву вважатимемо, що першочергово в системі $m_н$ елементів знаходяться в навантаженому резерві, m_0 – у полегшеному, а інші $(m - m_н - m_0)$ – у ненавантаженому. При відмові одного з основних елементів він замінюється елементом із навантаженого резерву, елемент, що відмовив, навантаженого резерву замінюється елементом з полегшеного резерву, а елементи полегшеного резерву поповнюються з ненавантаженого резерву, тобто (1)

$$\lambda_k = \begin{cases} (n + m_н + \alpha m_0)\lambda, & 0 \leq k \leq m - m_н - m_0; \\ [n + m_н + (m - m_н - k)\alpha]\lambda, & m - m_н - m_0 < k \leq m - m_н; \\ (n + m - k)\lambda, & m - m_н < k \leq m; \end{cases} \quad (1)$$

де λ – інтенсивність відмов одного елементу в навантаженому стані;

α – коефіцієнт навантаження елементів полегшеного резерву ($0 < \alpha < 1$).

Відновлення елементів, що відмовили, здійснюється ремонтним органом, що включає l ремонтних бригад ($l \geq 1$). Час відновлення одного елементу – випадкова величина $t_В$ з довільною функцією розподілу $F_В(t)$. Кожна бригада може одночасно ремонтувати тільки один елемент, що відмовив, і кожен елемент відновлюється лише однією з l бригад. Якщо всі бригади зайняті і відмовляє ще один елемент, то він стає в чергу на відновлення. Бригада, що закінчила відновлення одного з елементів, бере на ремонт перший із непрацездатних елементів, що стоять у черзі. Вважатимемо, що ремонт повністю відновлює початкові властивості елементу. Час підключення ненавантаженого резервного елементу замість основного, що відмовив, – випадкова величина $t_П$ із довільною функцією $F_П(t)$, а допустимий час підключення (використаний в системі поповнювальний резерв часу) – випадкова величина $\tau_Д$ з довільною функцією розподілу $D(t)$.

Об'єкт виконує завдання тривалістю $t_З$. Для виконання кожного завдання виділяється оперативний час t, що перевищує мінімально необхідний час $t_З$ на величину непоновлювального резерву $t_Р$, тобто $t = t_З + t_Р$.

Відмова системи може виникнути в двох випадках: при відмові $(m + 1)$-го елементу або при витраті складових резерву часу ($t_Д$ та $t_Р$). Із цього слідує, що метод витрати резерву часу на відновлення елементів, що відмовили, здійснює істотний вплив на показники надійності системи.

Взаємодія джерел комбінованого резерву часу в системі може відбуватися відповідно до однієї з двох моделей. У моделі 1 інтервали часу відновлення $t_{Вi}$, у тому числі й ті, що не перевищують допустимої величини $t_Д$, включаються в сумарний час простою і призводять до зменшення непоновлювальної складової резерву часу $t_Р$. Зрив функціонування відбувається у момент часу T_0, коли яка-небудь зі складових ($t_Р(x)$ або $t_Д(x)$) стане рівною нулю. У моделі 2

інтервали часу відновлення t_{Bi}, що не перевищують $t_Д$, включаються в корисний час і не включаються в сумарний час простою. Витрата непоновлювальної складової $t_Р$ комбінованого резерву часу починається лише тоді, коли $t_Bi > t_Д$. Зрив функціонування виникає в момент T_0, коли $t_Р(x)$ стає рівним нулю. Вибір цих моделей зумовлений, по-перше, їх широким використанням на практиці, а по-друге, одержувані результати в цьому випадку дають нижню і верхню оцінки основних показників надійності системи з комбінованим резервом часу. В даній статті розглядається взаємодія джерел комбінованого резерву часу відповідно з моделлю 1 (паралельна витрата складових резервного часу).

Припустимо, що в початковий момент всі елементи працездатні. Тоді функціонування системи відбувається таким чином. Через деякий випадковий час після включення системи виникає відмова одного з основних або резервних елементів, що знаходиться в навантаженому або полегшеному режимах. При відмові резервного елемента відразу ж починається його ремонт, після закінчення якого він повертається в резерв. Якщо відмовив основний елемент, то у момент відмови починається підключення одного з резервних елементів, що знаходяться у навантаженому режимі. В силу прийнятих припущень вважаємо, що під час підключення система не змінює свого стану. У момент закінчення підключення ремонтна бригада приступає до відновлення працездатності елементу, що відмовив. Якщо під час ремонту виникає нова відмова, то у момент відмови починається чергове підключення (при відмові основного елементу) або відновлення (якщо відмовив резервний елемент і є вільна ремонтна бригада) і т. д. Після закінчення відновлення працездатності елемент повертається в резерв. Інтервали часу підключення включаються в сумарний час простою і призводять до зменшення непоновлювальної складової резерву часу $t_Р$.

Система відмовляє в двох випадках: в момент, коли хоча б одна зі складових комбінованого резерву часу стане рівною нулю, і в момент відмови $(m + 1)$-го елементу.

Сформулюємо початкові передумови і припущення, при яких розв'язується задача:

наробіток між відмовами окремого основного елементу розподілений за експоненціальним законом з параметром λ і не залежить від номера відмови;

час відновлення одного елементу $t_В$ розподілений за експоненціальним законом із параметром μ;

час підключення резервного елементу $t_П$ розподілений за експоненціальним законом із параметром $\gamma_П$;

перемикач вважається абсолютно надійним;

допустимий час перерви у функціонуванні – випадкова величина $\tau_Д$ з експоненціальним законом розподілу і параметром $\gamma_П$ або детермінована величина $t_Д$;

при відмові $(m + 1)$-го елементу об'єкт вимикається і нові відмови не виникають; система відновлює свою роботу при закінченні ремонту одного з $(m + 1)$ непрацездатних елементів;

середня тривалість підключення і величина резерву часу значно менше середнього наробітку об'єкта між відмовами ($\bar{t}_П << 1/\lambda_k$, $t_Д << 1/\lambda_k$) і середньої тривалості ремонту $\bar{t}_В$ ($\bar{t}_П << \bar{t}_В$, $t_Д << \bar{t}_В$).

Для сформульованих умов необхідно визначити аналітичні вирази для показників надійності: ймовірність безвідмовного функціонування $P(t_З, t_Р, t_Д)$ і середній наробіток до відмови (до зриву функціонування) T_0 ($t_Р$, $t_Д$) даної резервованої системи.

Аналіз останніх публікацій. Дослідженню проблеми забезпечення надійності функціонування складних систем озброєння і військової техніки на основі використання різних видів надлишковості присвячено значну кількість наукових праць. Аналіз основних останніх публікацій у цій предметній галузі [1–7] дає змогу зробити висновок, що питанням комплексного використання декількох видів надлишковості для підвищення надійності присвячено відносно мало досліджень [5; 7]. Це пояснюється ускладненням отримання при

такому підході простих розрахункових співвідношень для показників надійності, зручних для практичного використання.

Зокрема, у роботі [5] побудована модель надійності системи епізодичного використання при спільному використанні комбінованого резерву часу, структурного та навантажувального резервування. Крім того, у цій моделі реалізовано специфічний алгоритм взаємодії поповнювальної і непоповнювальної складових резерву часу. Тому отримані в [5] результати (розрахункові співвідношення для основних показників) не можуть бути використані для оцінки надійності функціонування системи безперервного використання, що визначає актуальність тематики опублікованої статті та новизну отриманих у ній результатів. Але вищевказані роботи не встигають за швидким розвитком озброєння і військової техніки. Тому виникає наукове завдання створення наукової моделі надійності системи безперервного використання зі структурною надлишковістю з паралельною витратою складових резервного часу.

Метою статті є обґрунтування моделі надійності системи безперервного використання зі структурною надлишковістю з паралельною витратою складових резервного часу.

Виклад основного матеріалу

Процес функціонування системи можна описати однорідним марковським процесом із безперервним часом і кінцевим числом станів. Граф станів і переходів цього процесу представлений на рисунку 1, *а*, де зображено наступні стани:

$e_0 \div e_m$ – стани, в яких непрацездатні 0, 1,…, m резервних елементів;

$e_{m+1} \div e_{2m}$ – стани, в яких відбувається підключення резервного елементу після відмови основного за час, що не перевищує $\tau_Д$;

$e_{2m} \div e_{3m}$ – стани, в яких відбувається підключення резервного елементу замість основного, що відмовив, після втрати резерву часу $\tau_Д$;

e_{3m+1} – стан, в якому відбувається відновлення працездатності l елементів ($1 \le l \le m + 1$). Слід зазначити, що після відмови $(m + 1)$-го елементу система затримується в стані e_m на якийсь час $\tau_Д$. Проте через прийняті початкові умови цим часом затримки можна знехтувати. Таке припущення дозволяє спростити граф станів і переходів системи та призводить до незначної похибки.

Отримання точних розрахункових співвідношень для основних показників надійності в загальному випадку ($n \ge 1, m \ge 1$) є складним завданням, тому що введення різних видів надлишковості в систему істотно розширює фазовий простір станів випадкового процесу, що описує її поведінку в часі. При цьому для визначення основних показників надійності виникає необхідність рішення систем лінійних рівнянь великої розмірності з коефіцієнтами, які залежать від параметрів s і ω (параметрів у перетворенні Лапласа – Карсона) з подальшим оберненням одержаного перетворення Лапласа – Карсона. Навіть у найпростіших випадках, таких, наприклад, як дубльовані системи, розрахункові співвідношення виявляються дуже складними. Тому одержимо точні вирази лише для випадку одного резервного елементу ($n \ge 1, m = 1$), а для загального випадку ($n \ge 1, m \ge 1$) скористаємося алгоритмом укрупнення станів.

Граф станів і переходів системи при $m = 1$ та $n \ge 1$ представлено на рисунку 2.

Для вирішення завдання скористаємось відомими системами рівняння для визначення перетворення Лапласа – Карсона ймовірності безвідмовного функціонування $P_i(s, \omega)$ та перетворення Карсона середнього наробітку до відмови системи $\overline{T}_i(\omega)$, де s та ω – параметри в перетворенні Лапласа – Карсона; i – початковий стан системи, $i \in E_+$.

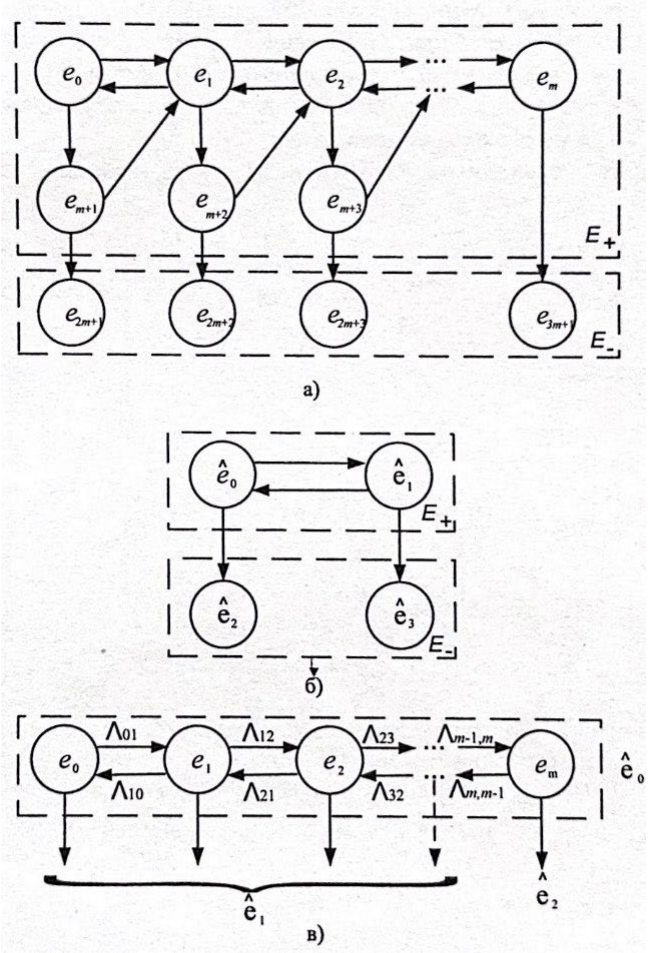


Рис. 1. Граф станів і переходів системи: *а* – початкової; *б* – після укрупнення; *в* – переходи всередині і виходи за межі укрупненої підмножини $\hat{e}_0$ (модель 1)

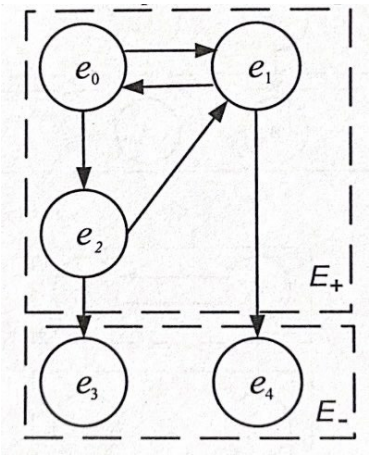


Рис. 2. Граф станів і переходів початкової системи при $m = 1$

Система рівнянь для $P_i(s, \omega)$ має вигляд (2):

$$P_i(s, \omega) = 1 - F_i(s) + \sum_{j \in E_+} P_{ij}(s)\, P_j(s, \omega),\ i \in E_+,$$
$$P_i(s, \omega) = \sum_{j \in E_+} P_{ij}(\omega)\, P_j(s, \omega),\ i \in E_+^*. \qquad (2)$$

де $F_i(s)$ – перетворення Лапласа – Карсона функція розподілу. $F_i(t)$ часу перебування системи в стані e_i, тобто (3)

$$F_i(s) = s\int_0^\infty e^{-st} F_i(t)dt; \tag{3}$$

$P_{ij}(s)$, $P_j(\omega)$ – перетворення Лапласа – Карсона перехідної імовірності $P_{ij}(t)$ (4):

$$P_{ij}(s) = s\int_0^\infty e^{-st} P_{ij}(t)td;\ P_{ij}(\omega) = \omega\int_0^\infty e^{-\omega t} P_{ij}(t)td; \tag{4}$$

E_+^* – підмножина станів з E_+, у яких об'єкт непрацездатний і відновлюється шляхом підключення резервних елементів або ремонту (при цьому відбувається витрачання обох складових резерву часу).

Запишемо тепер систему рівнянь для $\bar{T}_i(\omega)$ (5):

$$\begin{aligned} \bar{T}_i(\omega) &= a_i + \sum_{j\in E_+} p_{ij}\bar{T}_j(\omega),\ i\in E_+, \\ \bar{T}_i(\omega) &= \sum_{j\in E_+} P_{ij}(\omega)\,\bar{T}_j(\omega),\ i \in E_+^*, \end{aligned} \tag{5}$$

де a_i, p_{ij} – як і раніше, відповідно середні часи перебування в станах e_i і стаціонарна ймовірність переходу $e_i \to e_j$, при цьому $p_{ij} = \lim\limits_{t\to\infty} P_{ij}(t)$.

Для даного окремого випадку ($m = 1$, $n \geq 1$) система рівнянь для $P_i(s, \omega)$ з урахуванням графа станів (рис. 5) матиме вигляд (6):

$$\begin{aligned} &P_0(s, \omega) = 1 - F_0(s) + P_{01}(s)\,P_1(s, \omega) + P_{02}(s)\,P_2(s, \omega); \\ &P_1(s, \omega) = 1 - F_1(s) + P_{10}(s)\,P_0(s, \omega); \\ &P_2(s, \omega) = P_{21}(s)\,P_1(s, \omega). \end{aligned} \tag{6}$$

Вирішуючи систему рівнянь (6) відносно $P_0(s, \omega)$, одержимо (7):

$$P_0(s,\omega) = \frac{1-F_0(s)+(1-F_1(s))\left[P_{01}(s)+P_{02}(s)P_{21}(\omega)\right]}{1-P_{10}(s)\left[P_{01}(s)+P_{02}(s)P_{21}(\omega)\right]} \tag{7}$$

Для визначення $\bar{T}_0(\omega)$ використовується наступна система рівнянь:

$$\begin{cases} \bar{T}_0(\omega) = a_0 + p_{01}\bar{T}_1(\omega) + p_{02}\bar{T}_2(\omega); \\ \bar{T}_1(\omega) = a_1 + p_{10}\bar{T}_0(\omega); \\ \bar{T}_2(\omega) = P_{21}(\omega)\bar{T}_1(\omega). \end{cases}$$

Звідси випливає вираз (8):

$$\bar{T}_0(\omega) = \frac{a_0 + a_1(p_{01} + p_{02}P_{21}(\omega))}{1\text{-}p_{10} + (p_{01} + p_{02}P_{21}(\omega))}\ . \tag{8}$$

Використовуючи співвідношення (3) і (4), визначимо перетворення Лапласа – Карсона перехідних імовірностей і функцій розподілу, які входять до виразів (7) і (8), а також значення середнього часу перебування для випадку $D(t) = 1 - e^{-\gamma t}$, $F_П(t) = 1 - e^{-\gamma_П t}$:

$$P_{01}(s) = \frac{\alpha\lambda}{(n+\alpha)\lambda+s}; P_{02}(s) = \frac{n\lambda}{(n+\alpha)\lambda+s}; P_{10}(s) = \frac{\omega}{n\lambda+\mu+s};$$
$$F_0(s) = \frac{(n+\alpha)\lambda}{(n+\alpha)\lambda+s}; F_1(s) = \frac{n\lambda+\mu}{n\lambda+\mu+s}; F_2(s) = \frac{\gamma_П+\gamma}{\gamma_П+\gamma+\omega};$$
$$P_{21}(\omega) = \frac{\gamma_П}{\gamma_П+\gamma+\omega}; a_0 = \frac{1}{(n+\alpha)\lambda}; a_1 = \frac{1}{n\lambda+\mu}; a_2 = \frac{1}{\gamma_П+\gamma}.$$

Якщо непоповнювальний резерв часу – невипадкова величина $t_Д$ = const, то $P_{21}(\omega)$, $F_2(s)$ і a_2 слід визначати за формулами:

$$P_{21}(\omega) = \frac{\gamma_П}{\gamma_П+\omega}(1 - qe^{-\omega t_Д}); F_2(s) = \frac{1}{\gamma_П+s}(\gamma_П + sqe^{-st_Д}); a_2 = \frac{1}{\gamma_П}(1 - q),$$

де $q = P(t_П > t_Д)$.

Перейшовши від зображень по Карсону до оригіналів функцій за допомогою відомих методів [10], одержимо вирази для визначення показників надійності даної системи. Розрахункове співвідношення для $P(t_З, t_Р, \tau_Д)$ тут не наводиться, оскільки має громіздкий вигляд. Вирази для визначення середнього наробітку до відмови $\overline{T}_0(t_Р, \tau_Д)$ після відповідальних перетворень приводять до вигляду (9):

для випадку, коли $\tau_Д$ – випадкова величина з функцією розподілу $D(t) = 1 - e^{-\gamma t}$,

$$\overline{T_0}(t_p, \tau_д) = \frac{1}{n\lambda B}\left[(n\lambda + \mu)A(e^{Bt_p} - 1) + B\right], \quad (9)$$

де $B = \mu A - \gamma_П - \gamma$; $A = \frac{\gamma_П}{(n+\alpha)\lambda+\mu}$;

для випадку, коли ($\tau_Д = t_Д$) – невипадкова величина ($t_Д$ = const) (10),

$$\overline{T_0}(t_p, t_д) = n\lambda(A_i + \frac{n\lambda}{\mu})A_{i+1}, \quad (10)$$

де $A_i = \sum_{i=o}^{[t_p/t_д]}(\frac{\mu}{(n+\alpha)\lambda+\mu})^i \sum_{j=0}^{i}(-1)^j\binom{i}{j}e^{-j\gamma_П t_д}I(i, \gamma_П(t_p - jt_д))$;

$$A_{i+1} = \sum_{i=o}^{[t_p/t_д]-1}(\frac{\mu}{(n+\alpha)\lambda+\mu})^{i+1} \sum_{j=0}^{i+1}(-1)^j\binom{i+1}{j}e^{-j\gamma_П t_д}I(i, \gamma_П(t_p - jt_д));$$

$$I(i, \gamma_П(t_p - jt_д)) = 1 - \sum_{k=1}^{i}\frac{[\gamma_П(t_p - jt_д)]^{k-1}}{(k-1)!}e^{-\gamma_П(t_p - jt_д)};$$

$[\tau_Р / t_Д]$ – позначає цілу частину числа.

Для вирішення задачі в загальному випадку ($n \geq 1, m \geq 1$) скористаємось алгоритмом укрупнення станів [8; 9].

Аналіз процесу функціонування і відповідного йому графа станів і переходів системи (рис. 1, *а*) дозволяє побудувати наступну процедуру укрупнення. Всі підмножини працездатних станів розіб'ємо на дві великі підмножини: $\hat{e}_0$ і $\hat{e}_1$ (рис. 1, *б*). Підмножина ергодичних станів $\hat{e}_0 \in E_+$ утворюється за рахунок об'єднання станів e_i, $i = \overline{0, m}$ неукрупненого марківського ланцюга $\xi(n)$ (рис. 1, *а*). Переходи всередині підмножини $\hat{e}_0$

зумовлені процесами відмов резервних і відновлення непрацездатних елементів (рис. 1, *в*). Підмножина станів $\hat{e}_1 \in E_+$ утворюється за рахунок неасимптотичного укрупнення станів e_i, $i = \overline{m + 1,2m}$, тобто вона об'єднує стани, в яких відбувається підключення резервного елементу замість основного, що відмовив. Область непрацездатних станів E_- укрупнюється також до двох станів $\hat{e}_2$ і $\hat{e}_3$. Укрупнений стан $\hat{e}_3$ утворюється за рахунок неасимптотичного об'єднання непрацездатних станів e_i, $i = \overline{2m + 1,3m}$, у яких відбувається підключення резервного елементу після витрачення допустимого часу $\tau_Д$. Укрупнений стан $\hat{e}_2$ складається з одного стану e_{3m+1} початкового графа (рис. 1, *а*), в якому відбувається відновлення працездатності l елементів ($1 \le l \le m + 1$).

Можливість неасимптотичного об'єднання станів e_i, $i = \overline{m + 1,2m}$, у одну підмножину ґрунтується на результатах роботи [9]. Для випадку, що розглядається, виконується необхідна і достатня умова укрупнення процесу: ймовірність переходу між станами укрупненого процесу не залежить від конкретної пари станів початкового процесу, що визначають даний перехід. Значення цих імовірностей приймаються за імовірності переходу укрупненого процесу. Ця незалежність зумовлена природою переходів – підключенням резервного елементу замість основного, що відмовив. Імовірність здійснення підключення за допустимий час $\tau_Д$ або перевищення цього часу визначається тільки співвідношенням часу підключення $t_П$ і допустимого часу $\tau_Д$ (при заданих законах розподілу) і не залежить від конкретних станів укрупнених підмножин.

Для укрупненого графа станів (рис. 1, *б*) одержимо систему рівнянь для визначення перетворень Лапласа – Карсона імовірності безвідмовного функціонування і середнього наробітку до відмови.

Використовуючи загальний вираз (2), одержимо систему рівнянь для визначення $P_i(s,\omega)$, $i \in E_+$ (11):

$$\begin{cases} P_0(s,\omega) = 1 - F_0(s) + P_{01}(s)P_1(s,\omega); \\ P_1(s,\omega) = P_{10}(\omega)P_0(s,\omega), \end{cases} \tag{11}$$

звідти знаходимо (12)

$$P_0(s,\omega) = \frac{1 - F_0(s)}{1 - P_{01}(s)P_{10}(\omega)} \tag{12}$$

Для визначення $\overline{T}_i(\omega)$ використовується наступна система рівнянь:

$$\overline{T_0}(\omega) = a_0 + p_{01}\overline{T_1}(\omega);$$
$$\overline{T_1}(\omega) = P_{10}(\omega)\,\overline{T_0}(\omega),$$

вирішуючи яку відносно $\overline{T}_0(\omega)$, одержуємо (13):

$$\overline{T_0}(\omega) = a_0 / (1 - p_{01}P_{10}(\omega)). \tag{13}$$

Використовуючи співвідношення (3) та (4), визначимо перетворення Лапласа – Карсона перехідної ймовірності і функцій розподілу часу перебування, що входять до виразів (12) та (13), для випадку $D(t) = 1 - e^{-\gamma t}$, $F_П(t) = 1 - e^{-\gamma_П t}$:

$$P_{01}(s) = q_{01}/(s+\Lambda_0); \quad F_0(s) = \Lambda_0/(s+\Lambda_0);$$
$$P_{10}(\omega) = \gamma_П/(\gamma_П + \gamma + \omega); \quad a_0 = 1/\Lambda_0; \quad a_1 = 1/(\gamma_П + \gamma),$$

де q_{01} – укрупнена інтенсивність переходу зі стану $\hat{e}_0$ в $\hat{e}_1$;

Λ_0 – укрупнена інтенсивність виходу зі стану $\hat{e}_0$.

Якщо непоповнювальний резерв часу – невипадкова величина $t_Д$ = const, то $P_{10}(\omega)$ і a_1 слід визначати за формулами:

$$P_{10}(\omega) = \frac{\gamma_П}{\gamma_П+\omega}(1 - e^{-\omega t_Д}); a_1 = \frac{1}{\gamma_П}(1-q).$$

Імовірність p_{ij} визначають шляхом граничного переходу у відповідних виразах для $P_{ij}(s)$ і $P_{ij}(\omega)$; $i, j \in E_+$, тобто

$$P_{ij} = \lim_{s\to 0} P_{ij}(s); \; P_{ij} = \lim_{\omega\to 0} P_{ij}(\omega).$$

Застосовуючи відомі методи обернення до виразів для перетворення Лапласа – Карсона (формули (12) і (13)) [10], одержуємо розрахункові співвідношення для визначення основних показників надійності даних систем:

для випадку, коли $\tau_Д$ – випадкова величина, ($D(t) = 1 - e^{-\gamma t}$) (14), (15):

$$P(t_з, t_p, \tau_д) = e^{-\Lambda_0 t_з}\sum_{i=0}^{\infty}\frac{(q_{01}\gamma_П t_з)^i}{i!(\gamma_П+\gamma)^i}\left\{1 - e^{-(\gamma_П+\gamma)t_p}\sum_{j=1}^{i}\frac{\left[t_p(\gamma_П+\gamma)\right]^{j-1}}{(j-1)!}\right\}; \tag{14}$$

$$\overline{T_0}(t_p, \tau_д) = \frac{1}{\Lambda_0\left[(\gamma_П+\gamma)\Lambda_0 - q_{01}\gamma_П\right]}\left\{(\gamma_П+\gamma)\Lambda_0 - q_{01}\gamma_П e^{-\frac{\left[(\gamma_П+\gamma)\Lambda_0 - q_{01}\gamma_П\right]t_p}{\Lambda_0}}\right\}; \tag{15}$$

для випадку, коли $t_Д$ – невипадкова величина ($t_Д$ = const) (16), (17),

$$P(t_з, t_p, t_д) = e^{-\Lambda_0 t_з}\sum_{i=0}^{\left[t_p/t_з\right]}(q_{01}t_з)^i\sum_{j=0}^{i}(-1)^j\frac{e^{-j\gamma_П t_д}}{j!(i-j)!}I(i,\gamma_П(t_p - jt_д)); \tag{16}$$

$$\overline{T_0}(t_p, t_д) = \frac{1}{\Lambda_0}\sum_{i=0}^{\left[t_p/t_д\right]}\left(\frac{q_{01}}{\Lambda_0}\right)^i\sum_{j=0}^{i}(-1)^j C_i^j e^{-j\gamma_П t_Д} I(i,\gamma_П(t_p - Jt_Д)), \tag{17}$$

де $I(i,\gamma_П(t_P - jt_Д)) = 1 - \sum_{k=1}^{i}\frac{\left[\gamma_П(t_P - jt_Д)\right]^{k-1}}{(k-1)!}e^{-\gamma_П(t_P - jt_Д)}$.

Використовуючи загальний підхід і розрахункові співвідношення, наведені в [8], визначимо укрупнення інтенсивності переходів q_{01} та Λ_0 (18):

$$q_{01} = \frac{\sum_{i=0}^{m-1}\rho_i^{(0)}b_{i1}}{\sum_{i=0}^{m}\rho_i^{(0)}a_i}; \qquad \Lambda_0 = \frac{\sum_{i=0}^{m-1}\rho_i^{(0)}b_{i1} + \rho_m^{(0)}b_{m2}}{\sum_{i=0}^{m}\rho_i^{(0)}a_i}, \tag{18}$$

де a_i – середній час перебування в i-му стані $i \in \hat{e}_0$;

$\rho_i^{(0)}$ – стаціонарна ймовірність перебування незбуреного вкладеного марківського ланцюга $\xi(n)$ у станах підмножини $\hat{e}_0$;

b_{ij} – елементи матриці збурень, $i \in \hat{e}_0, j \overline{\in} \hat{e}_0$.

Таким чином, визначення значень параметрів q_0 і Λ_0 зводиться до оцінки стаціонарної імовірності $\rho_i^{(0)}$, середнього часу перебування a_i і елементів матриці збурень b_{ij}, $i \in \hat{e}_0, j \overline{\in} \hat{e}_0$.

Для підмножини ергодичних станів $\hat{e}_0$, переходи всередині якого утворюють процес загибелі і розмноження, стаціонарна ймовірність визначається за формулою (19):

$$\rho_i^{(0)} = \frac{\Theta_i}{\sum_{S=0}^{m} \Theta_S}, \qquad i \in \hat{e}_0, \qquad i = \overline{0, m}, \tag{19}$$

де $\Theta_i = \frac{\lambda_0 \lambda_1 \dots \lambda_{i-1}}{\mu_1 \mu_2 \dots \mu_i}$, $i = \overline{1, m}$, $\Theta_0 = 1$; λ_i – визначається (20) з виразу (1);

$$\mu_i = \begin{cases} 0, i = 0; \\ i\mu, i \le l; \\ l\mu, i > l. \end{cases} \tag{20}$$

Використовуючи початковий граф станів (рис. 1, *а*), визначимо середній час перебування системи в *i*-му стані (21):

$$a_i = \frac{1}{\lambda_i + \mu_i}, \; i = \overline{0, m}. \tag{21}$$

З представлення матриці ймовірності переходів **P** реальної системи у вигляді **P** = **P**$_0$ – **B** [8] випливає, що елементи матриці збурень b_{ij}, $i \in \hat{e}_0, j \overline{\in} \hat{e}_0$, можуть бути визначені як:

$$b_{ij} = p_{ij}^{(0)} - p_{ij}.$$

Отже, для оцінки елементів матриці збурень **B** необхідно набути значення імовірності переходів ідеальної і реальної систем. Використовуючи відомий вираз для визначення імовірності переходів p_{ij} і граф станів (рис. 1, *в*), отримаємо:

для ідеальної системи (за відсутності збурення за рахунок відмов основних елементів) (22)

$$\begin{cases} p_{i,i+1}^{(0)} = \frac{\lambda_i}{\lambda_i + \mu_i}, \; i = \overline{0, m-1}; \\ p_{i,i-1}^{(0)} = \frac{\mu_i}{\lambda_i + \mu_i}, \; i = \overline{1, m}; \end{cases} \tag{22}$$

для реальної системи (з урахуванням збурень) (23), (24)

$$\begin{cases} p_{i,i+1} = \frac{\lambda_i^*}{\lambda_i + \mu_i}, \; i = \overline{0, m-1}; \\ p_{i,i-1} = \frac{\mu_i}{\lambda_i + \mu_i}, \; i = \overline{1, m}; \end{cases} \tag{23}$$

де

$$\lambda_i^* = \lambda_i - n\lambda. \tag{24}$$

Звідси можна знайти вирази для елементів матриці збурень (25), що входять у формули (18):

$$\begin{cases} b_{i1} = \frac{n\lambda}{\lambda_i+\mu_i}, i = \overline{0, m-1}; \\ b_{m2} = \frac{n\lambda}{n\lambda+\mu_m}. \end{cases} \quad (25)$$

Розрахунок показників надійності здійснюється в наступній послідовності:

1) обчислення значень елементів матриці збурень b_{ij} і b_{m2}, що входять у формули для q_{01} і Λ_0 (25);

2) визначення стаціонарної імовірності $\rho^{(0)}$ перебування незбуреного марківського ланцюга $\xi(n)$ у станах підмножини $\hat{e}_0$ (формули (1), (19), (20));

3) розрахунок середніх годин перебування системи в станах e_i, $i = \overline{0, m}$ (21);

4) обчислення укрупнених інтенсивностей переходів q_{01} і Λ_0 (18);

5) розрахунок імовірності безвідмовного функціонування $P(t_З, t_Р, \tau_Д)$, $P(t_З, t_Р, t_Д)$ (формули (14) і (16)) і середнього наробітку до відмови (зриву функціонування) $\overline{T}_0(t_Р, \tau_Д)$, $\overline{T}_0(t_Р, t_Д)$ (формули (15), (17)).

Таким чином, з використанням алгоритму укрупнення одержано наближені розрахункові співвідношення для основних показників надійності системи безперервного використання зі структурними, навантажувальними і комбінованими часовими резервами, в якій інтервали часу відновлення включаються в сумарний час простою.

роведено оцінку похибки знайдених наближених аналітичних співвідношень для показників надійності розглянутої системи, використовуючи підхід, який дозволяє оцінити значення похибки зверху, тобто для найгіршого випадку. Таким випадком для алгоритму асимптотичного укрупнення є система з одним резервним елементом ($n \geq 1$, $m = 1$). Це пояснюється тим, що при $m = 1$ матриця збурень має максимальні елементи, а отже, алгоритм асимптотичного укрупнення – мінімальну точність [8]. Таким чином, оцінку похибки розроблених аналітичних моделей будемо проводити шляхом порівняння результатів розрахунків для випадку $m = 1$ за точною (10) і наближеною (17) формулами.

Результати оцінки відносної похибки $\delta_{\overline{T_0}}$ наведено на рисунку 3, де величина похибки $\delta_{\overline{T_0}}$ визначається за формулою:

$$\delta_{\overline{T_0}} = \frac{\left|\overline{T_0}^{(T)}(t_р, t_д) - \overline{T_0}^{(H)}(t_р, t_д)\right|}{\overline{T_0}^{(T)}(t_р, t_д)} \text{ x } 100\%,$$

де $\overline{T_0}^{(T)}(t_р, t_д)$, $\overline{T_0}^{(H)}(t_р, t_д)$ – відповідно точна і наближена формули середнього наробітку до відмови.

Аналіз рисунка 3 дозволяє зробити **наступні висновки.** Одержані в статті розрахункові співвідношення дають можливість визначати основні показники надійності даних системи з достатньою для інженерної практики точністю ($\delta_{\overline{T_0}} < 10$–$12$ %) у широкому діапазоні робочих умов. Зі збільшенням кількості резервних елементів m величина похибки буде зменшуватись. Найбільш суттєвий вплив на точність результатів робить величина відношення μ / λ. Застосування розроблених аналітичних моделей є допустимим для систем при $\mu / \lambda \geq 10$, а при $\rho = t_р / t_д > 5$ – при $\mu / \lambda \geq 10^2$ або $m > 1$.

Напрямком подальшої роботи є проведення дослідження отриманих формул для показників надійності для кількісної оцінки ефективності різних методів резервування і обґрунтування рекомендацій щодо підвищення надійності функціонування розглянутої системи.

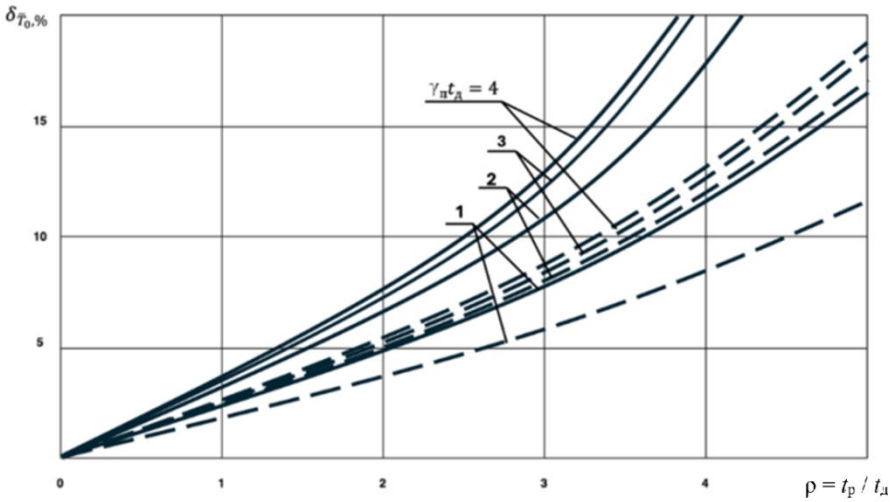


Рис. 3. Графіки залежності відносної похибки відношення між складовими резервами часу $\rho = t_р / t_д$ при різних значеннях $\gamma_п t_д$ та $n = m = \alpha = l = 1$; ── $\mu / \lambda = 10$, ─ ─ ─ $\mu / \lambda = 20$

СПИСОК ВИКОРИСТАНИЙ ДЖЕРЕЛ

1. Креденцер Б. П., Могилевич Д. І., Кононова І. В., Пантаєв Ю. Оцінка надійності телекомунікаційного обладнання мережі спеціального призначення з урахуванням збоїв // Збірник наукових праць ВІТІ. 2019. Вип. 4. С. 44–48.

2. Mogylevych D., Kononova I., Kredentser B., Oksiuk O. Reliability of Redundant Telecommunications Equipment Advanced Model Considering Failures and Refusals of Structure Elements. IEEE International Conference on Advanced Trends in Information Theory (ATIT) 2019. DOI: https://doi.org/10.1109/ATIT49449.2019.9030502. ISBN: 978-1-7281-6144-0 e-ISBN: 978-1-7281-6144-0. P. 238–243.

3. Mogylevych D., Kononova I., Kredentser B., Karadschow I. Comprehensive Reliability Assessment Technique of Telecommunication Networks Equipment with Reducible Structure // Вісник НТУ КПІ. Серія – Радіотехніка Радіоапаратобудування. 2020. Вип. 85. DOI: https://doi.org/10.20535/RADAP.2020.85.39-47. С. 39–47.

4. Kredentser Borys, Mogylevych Dmytro, Kononova Iryna, Mohylevych Vadym. Analytical Model with Interruption of Service of Short-term Objects with Temporary Reservation // Information Technology and Interactions. P. 295–301.

5. Креденцер Б. П., Сидоров Л. А., Бутянов А. Н. Применение операции укрупнения при оценке надежности одного класса резервируемых сетей // Кибернетика. 1990. № 2. С. 26–29.

6. Креденцер Б. П. Техническое обслуживание и надежность сетей с временным резервированием. Киев: Феникс, 2016. 384 с.

7. Креденцер Б. П., Могилевич Д. І., Кононова І. В. Оцінка виграшу в надійності при комплексному використанні надлишковості в об’єктах телекомунікацій // Збірник наукових праць ВІТІ. К., 2017. Вип. 2. С. 48–57.

8. Королюк В. С, Турбин А. Ф. Фазовое укрупнение сетевых систем. К.: Вища школа, 1978. 112 с.

9. Захарян А. М. Об ухудшении состояния микросхем и микропроцессорных приборов и способах их укрепления // Анализ стохастических процессов в приборостроении // Кибернетика. 1991. № 4. С. 56–65.

10. Дей Г. Руководство к практическому решению задач Лапласа и Z-преобразования. М.: Наука, Главная редакция физико-математической литературы, 1971. 288 с.

DOI: 10.58254/viti.7.2025.06.65

УДК 621.3

д-р. техн. наук, професор Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ ім. Героїв Крут)
Ланко А. В. ORCID: 0009-0001-1124-1526 (ВІТІ ім. Героїв Крут)

ЗАСТОСУВАННЯ БЕЗКОНТАКТНОГО ІНДУКЦІЙНОГО МЕТОДУ ПРИ ВИЗНАЧЕННІ ПОКАЗНИКІВ НАДІЙНОСТІ ОБ'ЄКТА КОНТРОЛЮ

У сучасних умовах спостерігається широке застосування технічних систем подвійного призначення іноземного виробництва, зокрема у Збройних Силах. Для таких систем об'єктивно існує обмеження вхідної технічної інформації.

Отже, важливим завданням для інженерно-технічного складу при організації системи обслуговування та експлуатації зазначених систем та об'єктів стає пошук нових та удосконалення існуючих підходів для визначення показників надійності радіоелектронного обладнання, яке отримано та знаходиться в експлуатації.

Один з інструментів, який надає можливість часткового розв'язання цього завдання, є застосування безконтактного індукційного методу.

У статті наведено сутність та опис безконтактного індукційного методу, а також варіант його застосування для визначення одного з параметрів надійності об'єктів радіоелектронного обладнання. У роботі розглядається параметр довговічності радіоелектронного обладнання. Також запропоновано інженерну методику з визначення довговічності об'єкта контролю. Рішення приймається за результатами обробки даних, отриманих безконтактним індукційним датчиком, та методики оцінки ресурсу об'єкта контролю при невідомому напрацюванні від початку експлуатації. Застосування безконтактного індукційного датчика дозволило отримати та оцінити чисельні зміни параметрів найбільш низко надійного радіоелектронного компонента у складі радіоелектронного обладнання.

Запропоновані рішення для визначення довговічності радіоелектронного обладнання з обмеженою вхідною інформацією розглядаються вперше. Поставлена задача набуває особливого значення в сучасних умовах під час використання силами оборони засобів радіоелектронного обладнання від країн-партнерів (здебільшого не нового, з певним ресурсом напрацювання та/або зберігання). Все вищесказане визначило актуальність та важливість науково-технічної задачі створення (розробки) інженерних методик визначення надійності зразків радіоелектронного обладнання за окремими показниками.

Зазначається, що запропонований підхід може бути розвинений шляхом створення інших інженерних методик визначення надійності радіоелектронного обладнання за іншими окремими показниками, їхнього комплексування для прийняття рішення про надійність об'єкта контролю та визначення умов технічного обслуговування.

Ключові слова: *безконтактний індукційний датчик, надійність, діагностична інформація, радіоелектронне обладнання, ресурс напрацювання, довговічність.*

V. Kuzavkov, A. Lanko. Application of non-contact induction method in determining reliability indicators of the control object

In modern conditions, there is a widespread use of dual-purpose technical systems of foreign production, including in the armed forces. For such systems, there is an objective limitation of incoming technical information.

Therefore, an important task for the engineering and technical staff, when organizing the system of maintenance and operation of these systems and facilities, is to find new and improve existing approaches to determine the reliability of radio electronic equipment received and in operation.

One of the tools that makes it possible to partially solve this problem is the use of a non-contact induction method.

The article presents the essence and description of the non-contact induction method and a variant of its application for determining one of the reliability parameters of radio electronic equipment. The paper considers the parameter of radio electronic equipment durability. Also, an engineering methodology for determining the durability of the object under control is proposed. The decision is made based on the results of processing the data obtained by a non-contact induction sensor and the methodology for assessing the life of the controlled object at an unknown operating time from the beginning of operation. The use of a non-contact induction sensor made it possible to obtain and evaluate numerical changes in the parameters of the most unreliable radio-electronic component in the radio-electronic equipment

The proposed solutions for determining the durability of radio-electronic equipment with limited input information are considered for the first time. This task is of particular importance in modern conditions when the defense forces use radio-electronic equipment from partner countries (mostly not new, with a certain resource of

operation and (or) storage). All of the above has determined the relevance and importance of the scientific and technical task of creating (developing) engineering methods for determining the reliability of electronic equipment samples by individual indicatorsIt is noted that the proposed approach can be developed by creating other engineering methods for determining the reliability of radio-electronic equipment by other individual indicators, combining them to make a decision

Keywords: *non-contact induction sensor, reliability, diagnostic information, radio electronic equipment, service life, durability.*

Постановка завдання в загальному вигляді

Реалії бойових дій в Україні спричинили новий виток модернізації та переоснащення Збройних сил України та інших військових формувань, запровадження новітніх зразків озброєння та військової техніки. До Збройних сил надходить все більша кількість радіоелектронного обладнання (РЕО) іноземного виробництва. Значна кількість цих зразків перебувала на базах та складах тривалого зберігання. Ця обставина обумовлює загострення питання визначення надійності отриманих зразків РЕО, організації технічного обслуговування та їх ремонту.

Якість виконання поставлених завдань значною мірою залежить від якості та надійності зразків РЕО, яким укомплектовані бойові підрозділи. Абсолютно всі підрозділи використовують засоби РЕО (засоби зв’язку, планшети, ноутбуки, системи відеоспостереження, комплекси керування БпЛА і т. ін.). Однак, майже для всіх зразків РЕО відсутня повна технічна інформація. Окрім того, в більшості випадків виробник озброєння не дозволяє здійснювати ремонт наданого устаткування на території іншої держави. Тому застосування традиційних (класичних) методів теорії надійності для визначених зразків не можливо або має суттєві обмеження.

Отже, одним зі шляхів вирішення питання визначення надійності та актуальним напрямком наукової роботи є розробка саме інженерних методик визначення та оцінки надійності РЕО, що гарантуватиме обґрунтоване прийняття рішення при організації технічного обслуговування та ремонту РЕО.

Аналіз публікацій за темою дослідження

У спеціальній науковій літературі розглядаються загальні підходи, математичні моделі і методи аналізу надійності РЕО [1–4]. Відповідно до загальної практики, визначення та оцінка кількісних значень показників надійності об’єктів радіоелектронної техніки розпочинається на етапах проєктування та виробництва і продовжується під час її експлуатації шляхом накопичення та узагальнення статистичної інформації.

В окремих роботах [5] розглядаються питання прогнозування технічного стану РЕО як важливої складової частини теорії технічного діагностування.

Особливості застосування безконтактного індукційного методу для отримання діагностичної інформації про об’єкт контролю розглянуто в роботах [6; 7].

Питання визначення надійності РЕО в умовах обмеженої вихідної інформації про об’єкт контролю (ОК) (технічної та статистичної) в літературі розглянуто недостатньо, хоча для їх вирішення є необхідні передумови.

Метою статті є обґрунтування можливості застосування безконтактного індукційного методу для визначення та оцінки довговічності ОК (як окремого показника надійності) при обмеженій вхідній інформації про ОК.

Виклад основного матеріалу

Ефективність функціонування РЕО визначається низкою факторів, серед яких важливу роль відіграє їх надійність.

Надійність – це комплексна властивість, яка залежно від призначення об’єкта і умов його застосування може включати безвідмовність, довговічність, ремонтопридатність і збережуваність або певні комбінації цих властивостей. Однією з найгостріших проблем

у сучасних реаліях залишається визначення безвідмовності РЕО за обмеженою вихідною інформацією про ОК.

Складність проблеми обумовлена низкою специфічних факторів. Такі зазвичай зразки тривалий час зберігалися на складах, а в комплекті постачання відсутня відповідна технічна документація, в якій відображено умови зберігання, час напрацювання, методики перевірки та оцінки фактичного технічного стану. В більшості випадків виробник систем озброєння не дозволяє здійснювати ремонт наданого устаткування на території іншої держави. Тому користувач обладнання (обслуговуючий персонал, інженерно-технічний склад) змушений здійснювати пошук способів оцінки надійності такого устаткування, способів інтеграції отриманого устаткування в існуючу систему технічного обслуговування та ремонту.

Традиційні методи та засоби визначення чисельних значень показників надійності (в тому числі довговічності) РЕО мають низку суттєвих обмежень. У зв'язку з цим ведеться активний пошук нових підходів (методів та методик) визначення надійності РЕО в умовах обмеженої вихідної інформацію.

У статті наведено короткий опис безконтактного індукційного методу та варіант його застосування для визначення одного з параметрів надійності об'єктів РЕО, а саме параметра довговічності. Запропоновано інженерну методику з визначення довговічності об'єкта контролю (ОК) за результатами обробки даних, отриманих безконтактним індукційним датчиком, та методики оцінки ресурсу ОК при невідомому напрацюванні від початку експлуатації. Методика оцінки ресурсу ОК ґрунтується на аналізі зміни параметрів найбільш низко надійного радіоелектронного компонента (РЕК) у складі РЕО.

Сутність безконтактного індукційного методу наведено в низці наукових праць [6; 7]. Діагностичний параметр – сигнал, отриманий з шини живлення цифрового блока, відображує в собі фізико-хімічні процеси старіння елементної бази. Реєстрація чисельних значень діагностичного параметра відбувається в безконтактний спосіб (безконтактним датчиком). Такий спосіб отримання діагностичної інформації мінімізує вплив засобів вимірювання на процеси, які відбуваються в РЕО, та виключає спотворення отриманої інформації.

Зміна параметрів струму (фізичного прояву діагностичного параметра) в шині живлення ОК в умовах виконання цифровим пристроєм спеціально сформованого діагностичного тесту дозволяє отримати еталон (еталонний енергетичний паспорт ОК).

Стохастичні зміни струму спричиняють зміну магнітної складової поля навколо провідника що, у свою чергу, призводить до формування діагностичного сигналу. Сигнал фіксується датчиком діагностичної інформації (ДДІ). Наявність сигналу на виході ДДІ засвідчує не лише факт роботи цифрового блока, але і відображує його фактичний технічний стан.

Наявність еталона (еталонного енергетичного паспорта) або математичної моделі, в якій відображено динаміку зміни діагностичного параметра залежно від часу експлуатації РЕО, дозволяють застосувати методику оцінки ресурсу ОК (визначити показник довговічності). Отже, висновок про довговічність ОК можливо зробити на підставі порівняння чисельних значень діагностичної інформації з графіком динаміки зміни діагностичного параметра.

Розглянемо конструкцію та принцип функціонування датчика діагностичної інформації (ДДІ). ДДІ по своїй фізичній суті є різновидом вимірювальної котушки, яка використовується для отримання діагностичної інформації (рис. 1).

На рисунку 1 позначено: e_1 – джерело змінної напруги; $R_н$ – опір навантаження; n_1 – число витків первинної обмотки; n_2 – число витків вторинної обмотки; u_1 – напруга первинної обмотки; u_2 – напруга вторинної обмотки; Ф – електромагнітна індукція.

Запропонований датчик складається з двох котушок індуктивності, зв'язаних загальним магнітним полем. Довкола провідників, крізь які протікає струм, виникає магнітне поле.

Для отримання параметрів поля і перетворення їх в електричний сигнал, один з проводів протягнутий крізь магнітний сердечник з обмоткою. Пропущений провід виступить в ролі первинної обмотки з одного витка, вторинна обмотка може мати більшу кількість витків. Така конструкція є струмовим трансформатором, напруга та форма сигналу у вторинній обмотці якого пропорційна змінам струму в первинній обмотці.

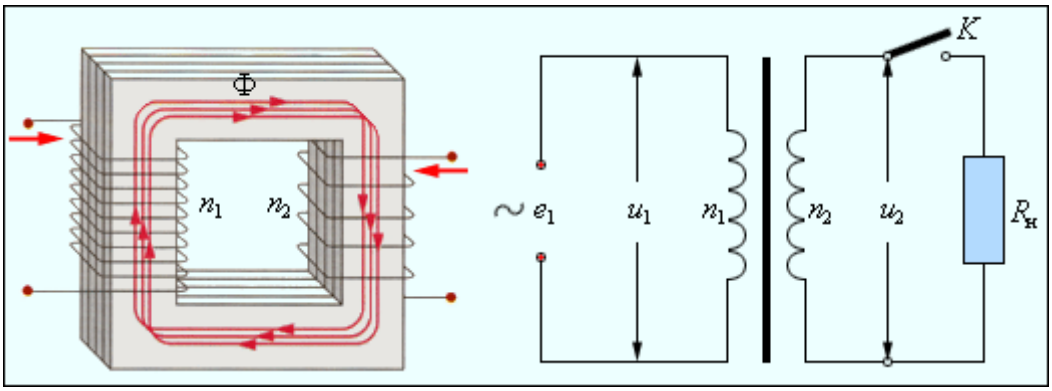


Рис. 1. Датчик діагностичної інформації

Котушка, до якої прикладається джерело змінної напруги e_1, називається первинною обмоткою. Інша обмотка називається вторинною. До вторинної обмотки підключається навантаження $R_н$.

У принцип роботи ДІ покладено закон електромагнітної індукції, або закон Фарадея. Напруга первинної обмотки u_1 (напруга під'єднаного джерела), пов'язана з магнітним потоком Ф, який проходить через кожен виток первинної обмотки, визначається виразом:

$$u_1 = n_1 \frac{d\Phi}{dt},$$

де n_1 – число витків первинної обмотки.

Аналогічно, електрорушійна сила (ЕРС), наведена у вторинній обмотці з числом витків n_2 , визначається виразом:

$$u_2 = n_2 \frac{d\Phi}{dt}.$$

Коефіцієнт передачі напруги, або коефіцієнт трансформації n, визначається співвідношенням кількості витків:

$$n = \frac{u_2}{u_1} = \frac{n_2}{n_1}.$$

Розглянемо процеси, які відбуваються в системі, де дві обмотки мають однакову кількість витків (рис. 2).

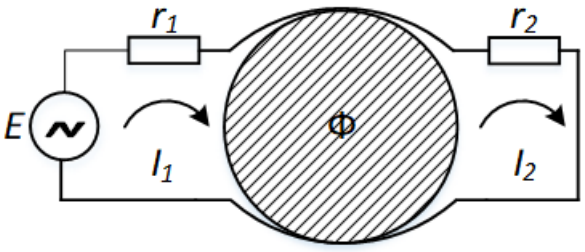


Рис. 2. Трансформатор з повним перекриттям обмоток

Нехай кожна обмотка має індуктивність L. Розташуємо їх так, щоб магнітний потік Ф, який створюється первинною обмоткою, повністю охоплювався вторинною обмоткою. В цьому випадку коефіцієнт зв’язку обмоток дорівнює одиниці. Як відомо, падіння напруги на індуктивності пов’язане з магнітним потоком наступним співвідношенням:

$$U_1 = \frac{d\Phi}{dt} = L\frac{dI}{dt},$$

де I – струм, що протікає через індуктивність.

Застосуємо 2-й закон Кірхгофа та отримаємо:

$$E = I_1 r_1 + L\frac{dI}{dt} - M\frac{dI}{dt} = I_1 r_1 + L\left(\frac{dI_1}{dt} - \frac{dI_2}{dt}\right),$$

для $M = L$

$$E_0 = I_2 r_2 + L\frac{dI_2}{dt} - M\frac{dI_1}{dt} = I_2 r_2 + L\left(\frac{dI_2}{dt} - \frac{dI_1}{dt}\right),$$

де M – це взаємна індуктивність, тобто індуктивність вторинної обмотки, “відчутна” з боку первинної і навпаки;

$M\frac{dI_1}{dt}$ – напруга, яка наводиться вторинною обмоткою в первинному контурі.

Взаємна індуктивність M визначається через коефіцієнт зв’язку k (при $k = 1$ і $L_1 = L_2 = L$ отримуємо $M = L$): $k = \frac{M}{\sqrt{L_1 L_2}}$.

Записані рівняння дають еквівалентну схему датчика діагностичної інформації, представлену на рисунку 3.

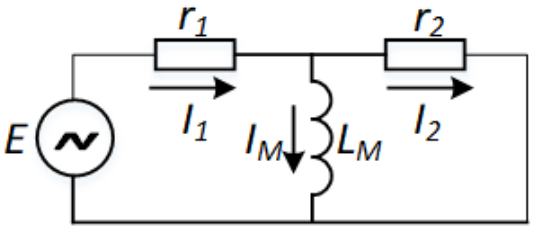


Рис. 3. Еквівалентна схема датчика з повним перекриттям обмоток

До параметра r_1 відносяться: внутрішній опір джерела, опір проводу обмотки, опір контактів і т. д., а до r_2 – опір навантаження разом з опором проводів. Якщо нехтувати величиною r_1, то видно, що напруга джерела повністю виявляється прикладеною до навантаження і збігається за величиною (в разі $w_1 = w_2$) та фазою.

Датчик присутній на схемі у вигляді паралельної індуктивності L_M, яка називається індуктивністю намагнічення і в нашому випадку дорівнює L. Напруга джерела, прикладена до датчика, викликає струм намагнічення, який змінюється. Зміна струму намагнічення в свою чергу створює напругу на вторинній обмотці. Швидкість зміни струму пропорційна величині миттєвої напруги на обмотках.

Отже, використовуючи безконтактний датчик, ми можемо отримати чисельні значення діагностичного параметра найбільш низко надійного РЕК у складі РЕО.

У роботі [8] доведено, що до низьконодійних РЕК відносяться електролітичні конденсатори. Для таких РЕК встановлена динаміка зміни діагностичного параметра. Графічна екстраполяція значень діагностичного параметра (ДП) має вид, представлений на рисунку 4.

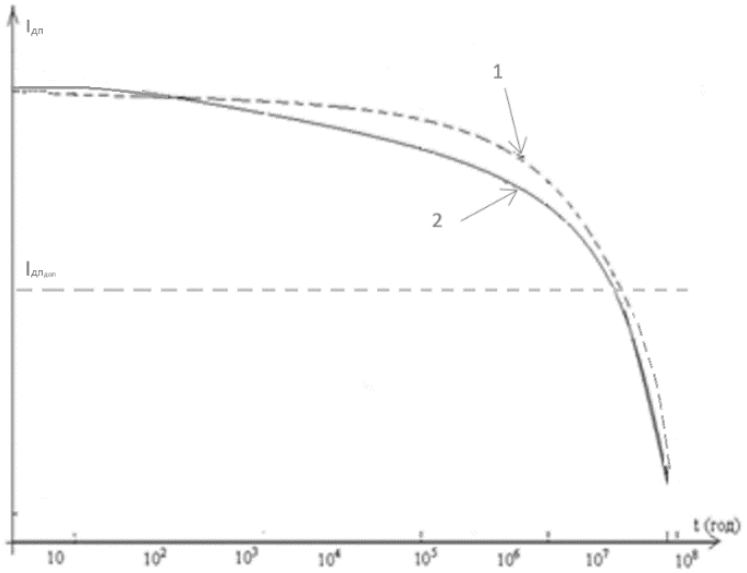


Рис. 4. Динаміка зміни сигналу на ДДІ в часі:
1 – експериментальна крива; *2* – аналітична крива

На рисунку 4 позначено: $I_{\text{дп}}$ – значення діагностичного параметра; $I_{\text{дп}_{\text{доп}}}$ – допустиме значення діагностичного параметра; $I_{\text{дп}_{\text{ном}}}$ – номінальне значення діагностичного параметра; $t_{\text{кр}}$ – критичний час напрацювання РЕК; $t_{\text{доп}}$ – максимально-допустимий час напрацювання РЕК.

Використовуючи методику оцінки ресурсу ОК при невідомому напрацюванні від початку експлуатації, стає можливим визначити термін служби РЕО.

Для вирішення цієї задачі (визначення довговічності ОК) пропонується два підходи, які взяті за основу для інженерної методики оцінки безвідмовності ОК. Маючи відомості про ресурс ОК, можемо визначати довговічність ОК.

Перший підхід – визначення ресурсу ОК, для яких наявна конструкторська та експлуатаційна документація з обліком напрацювання від початку експлуатації в паперовому або електронному вигляді.

Другий підхід – характерний для зразків, які виготовляються за межами держави і перебувають на озброєнні з невідомими параметрами.

В обох випадках оцінка безвідмовності ОК відбувається на підставі порівняння еталонних значень ДП з отриманими при застосуванні активуючої тестової послідовності значеннями. В свою чергу, еталонні енергетичні паспорти можливо отримати:

– від виробника устаткування (як результат проєктної діяльності);

– внаслідок аналітичних розрахунків з урахуванням фізико-хімічних процесів старіння РЕО під час життєвого циклу;

– як результат статистичної обробки репрезентативної вибірки результатів досліджень однотипних пристроїв з однаковими умовами експлуатації (збереження, транспортування, напрацювання);

– внаслідок проведення прискорених випробувань.

В будь-якому випадку дослідник матиме математичне очікування динаміки зміни ДП найбільш низко надійного РЕК (див. рис. 4).

Обидва підходи оцінки ресурсу ОК складають єдину методику, оскільки ґрунтуються на єдиних принципах отримання діагностичної інформації. Сукупність отриманих значень ДП після статистичної обробки дозволяє не лише зробити висновок про безвідмовність ОК, але й передбачити (з певною ймовірністю), як довго цей стан зберігатиметеся.

У межах аналізу ОК першого типу для процесу формування активуючої послідовності оцінки ресурсу, реєстрація ДП, обчислення, порівняння з еталонними значеннями, повинна бути присутня низка спеціальних даних (табл. 1).

Таблиця 1

Дані для визначення ресурсу РЕО

№	Вихідні дані	Позначення	Джерело
1	Номінальне значення діагностичного параметра	P_H	Технічна документація
2	Граничне значення діагностичного параметра	$P_{\text{гр}}$	Технічна документація
3	Показник, який характеризує закономірність змін значення діагностичного параметра	α	Технічна документація
4	Напрацювання від початку експлуатації до моменту контролю	t_H	Технічна документація
5	Значення діагностичного параметра, що вимірюється під час контролю	P_K	Показання засобів вимірювання

Інформаційну модель процесу визначення ресурсу (P) при відомій закономірності зміни ДП представлено на рисунку 5.

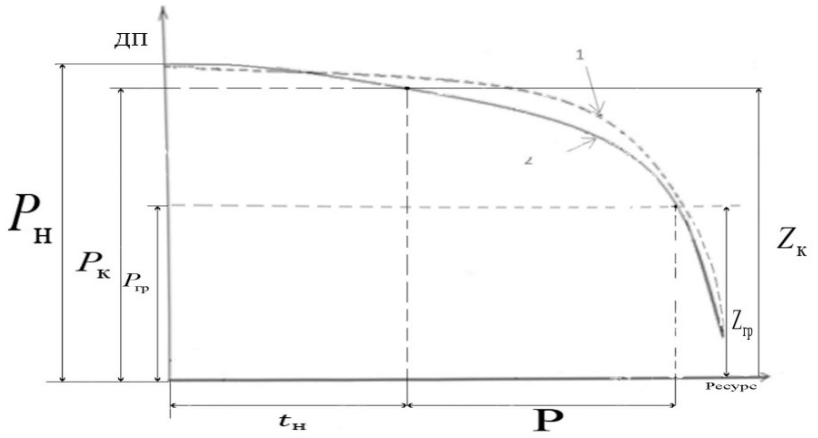


Рис. 5. Інформаційна модель визначення ресурсу об'єкта контролю при відомому напрацюванні

На рисунку 5 позначено: t_H – використаний ресурс до моменту контролю; $Z_K = P_H - P_K$ – зміна значення параметра до моменту контролю (діагностування); $Z_{\text{гр}} = P_H - P_{\text{гр}}$ – гранична зміна значення параметра; P– шуканий ресурс.

Маючи вказані дані, ресурс визначають за формулою (1):

$$P = t_н \left[\left(\frac{Z_к}{Z_{\text{гр}}} \right)^{\frac{1}{\alpha}} - 1 \right]. \quad (1)$$

На практиці значення α знаходиться в межах від 0,8 до 2,0. Значення $Z_{\text{гр}}$, $P_н$, α розраховують заздалегідь і заносять в таблицю.

Таким чином, для визначення ресурсу ОК (1) необхідно провести вимірювання ДП і знати напрацювання до моменту вимірювання ДП. Значення інших показників табличні.

У другому випадку, коли відомості про напрацювання окремих складових частин РЕО військового призначення від початку експлуатації або останнього капремонту відсутні,

ресурс можливо визначити за значеннями параметрів, виміряних при дворазовому контролі (діагностуванні) та напрацюванні між першим і другим вимірюваннями.

Послідовність визначення ресурсу при невідомому напрацюванні від початку експлуатації представлена на рисунку 6.

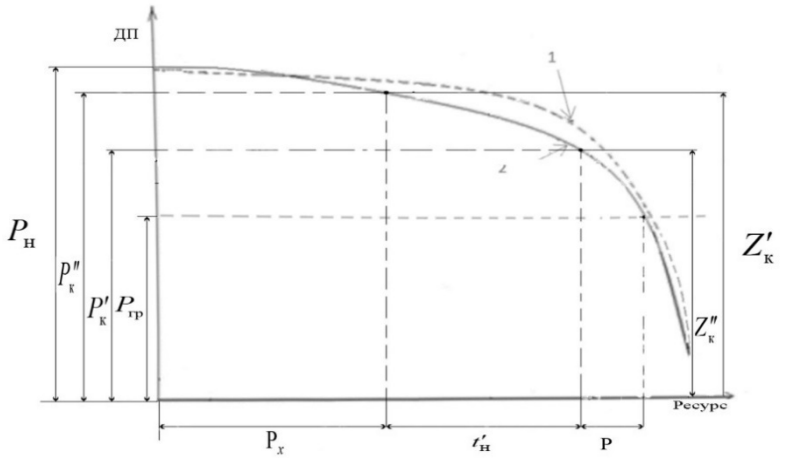


Рис. 6. Інформаційна модель визначення ресурсу об'єкта контролю при невідомому напрацюванні

На рисунку 6 застосовано наступні позначення: $P'_к$– значення параметра при першій перевірці; $P''_к$– значення параметра при повторній перевірці; $Z'_к = P'_н - P_к$ – зміна значення параметра від початку експлуатації до першої перевірки; $Z''_к = P''_н - P_к$ – зміна значення параметра від початку експлуатації до повторної перевірки; $Z_{гр} = P_н - P_{гр}$ – гранична зміна значення параметра; P_x – використаний ресурс (величина невідома); $t'_н$ – ресурс, витрачений за час функціонування між першою і другою перевірками.

Таким чином, для визначення P при невідомому напрацюванні зразку РЕО військового призначення з початку експлуатації необхідно виміряти значення контрольованого параметра не менше двох разів і знати напрацювання за час роботи між цими вимірами (2):

$$P = t'_н \left[\frac{1}{\left(\frac{Z_{к'}}{Z_{к''}}\right)^{\frac{1}{\alpha}} - 1} \left(\frac{Z_к}{Z_{гр}}\right) + 1 \right] \times \left[\left(\frac{Z_{к''}}{Z_{гр}}\right)^{\frac{1}{\alpha}} - 1 \right]. \quad (2)$$

Висновки. Представлену методику оцінки ресурсу ОК при невідомому напрацюванні від початку експлуатації за результатами обробки даних, отриманих безконтактним індукційним датчиком, можна запропонувати як інженерну методику з визначення довговічності об'єкта контролю. Методика ґрунтується на аналізі динаміки зміни параметрів найбільш низко надійного РЕК у складі РЕО.

Напрямком подальших досліджень є розвиток запропонованого підходу створення інженерних методик визначення надійності РЕО за окремими показниками для обґрунтованого прийняття рішення про надійність ОК.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методика комплексної оцінки надійності телекомунікаційного обладнання мереж зв'язку / Д. Могилевич та ін. // Військово-технічний збірник. Експлуатація та відновлення ОВТ. 2020. № 23. С. 50–57. URL: https://doi.org/10.33577/2312-4458.23.2020.50-57.

2. Фізичні основи теорії надійності: підручник / М. К. Жердєв, С. В. Лєнков, Б. П. Креденцер та ін.; за ред. М. К. Жердєва. К.: Видавничо-поліграфічний центр «Київський університет», 1998. С. 19.

3. ДСТУ 3004:95. Надійність техніки. Методи оцінки показників надійності за експериментальними даними. [Чинний від 1995-01-25]. К.: Держстандарт України, 1994. 124 с. (Державний стандарт України).

4. ДСТУ 3433:96. Надійність техніки. Моделі відмов. [Чинний від 1997-12-05]. К.: Держстандарт України, 1996. 46 с. (Державний стандарт України).

5. Kuzavkov V., Khusainov P. Forecasting the technical state of the same type software and hardware equipment // Informatics and mathematical methods in simulation. 2018. Vol. 8, no. 1. P. 57–68. URL: https://doi.org/10.15276/imms.v8.no1.57 (date of access: 13.02.2025).

6. Кузавков В. В. Безконтактний індукційний метод визначення технічного стану цифрового блока: розрахунок потужності випромінювання провідника / В. В. Кузавков, Г. І. Гайдур, С. О. Сєрих, Є. В. Редзюк // Зв’язок. 2016. № 1. С. 32–39. URL: http://nbuv.gov.ua/UJRN/Zvjazok_2016_1_9.

7. Міночкін А., Кузавков В., Погребняк С. Визначення технічного стану складових вторинних джерел живлення за фізико-хімічними процесами в електролітичних конденсаторах під час експлуатації // Сучасні інформаційні технології у сфері безпеки та оборони. 2021. Т. 40, № 1. С. 99–104. URL: https://doi.org/10.33099/2311-7249/2021-40-1-99-104.

8. Кузавков В. В., Погребняк С. В., Михайлюк С. С. Варіант визначення технічного стану електролітичного конденсатора методом безконтактної діагностики // Системи і технології зв’язку, інформатизації та кібербезпеки. 2023. № 3. С. 48–55. DOI: 10.58254/viti.3.2023.06.48.

DOI: 10.58254/viti.7.2025.07.74

УДК 004.056.55

д-р техн. наук, професор Кузавков В. В. ORCID: 0000-0002-0655-9759 (ВІТІ ім. Героїв Крут)
Тлустий А. О. ORCID: 0000-0002-4777-9563 (ВІТІ ім. Героїв Крут)

АНАЛІЗ СТАТИСТИЧНИХ ТЕСТІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У сфері інформаційної безпеки та криптографії оцінка характеристик (статистичної безпеки) згенерованих послідовностей є надзвичайно важливим завданням. Це питання відіграє ключову роль також у таких галузях, як комп'ютерна безпека, моделювання систем, мережева інформаційна безпека, статистика.

Інформаційна безпека в мережах забезпечується випадковістю створених ключів шифрування, токенів ідентифікації та цифрових підписів у мережевих протоколах. Ненадійні генератори можуть значно знижувати рівень захисту мережі.

У статистиці випадкових послідовностей і псевдовипадкових послідовностей для побудови тестових вибірок, перевірки гіпотез та проведення експериментів важливі генератори з низькою якістю можуть спотворити результати аналізу.

Комп'ютерна безпека забезпечується при застосуванні генераторів випадкових чисел і генераторів псевдовипадкових чисел шляхом створення паролів, токенів доступу, ідентифікаторів сесій тощо. Якщо генератор ненадійний, це може стати причиною вразливостей, що ставлять під загрозу безпеку інформації.

У моделюванні та симуляціях генератори використовуються для створення випадкових подій та наборів даних. Недоліки у їхній роботі можуть викликати похибки у моделюванні та призводити до неточних результатів.

У криптографічних системах випадкові послідовності і псевдовипадкові послідовності використовуються для генерації ключів, випадкових чисел та сольових значень. Низька якість генератора може створити вразливості, які дозволяють зловмисникам зламати криптографічні протоколи.

Таким чином, якість генераторів прямо впливає на ефективність і безпеку систем, що робить перевірку їхніх статистичних властивостей ключовим завданням.

Генератори псевдовипадкових чисел формують числові значення (послідовності), які здаються випадковими, хоча фактично мають певну структуру. Це робить їх затребуваними в різних галузях, зокрема для створення ключів, забезпечення конфіденційності, захисту цілісності даних і безпеки транзакцій. Тому надійність та захищеність таких послідовностей є основними характеристиками.

Робота присвячена аналізу інструментів для оцінки статистичних властивостей генераторів випадкових і псевдовипадкових послідовностей.

Ключові слова: *генератор псевдовипадкових послідовностей, криптозахист, статистичні тести, генерація ключів.*

V. Kuzavkov, A. Tlustyi. Analysis of statistical tests of pseudorando sequences

In the field of information security and cryptography, the assessment of the characteristics (statistical security) of generated sequences is an extremely important task. This issue also plays a key role in such areas as computer security, system modeling, network information security and statistics.

Information security in networks is ensured by the randomness of the generated encryption keys, identification tokens, and digital signatures in network protocols. Unreliable generators can significantly reduce the level of network security.

In statistics, random sequences and Pseudo-random sequences are important for constructing test samples, testing hypotheses, and conducting experiments. Low-quality generators can distort the results of the analysis.

Computer security is ensured when using Random Number Generators and Pseudo-Random Number Generators by generating passwords, access tokens, session identifiers, etc. If the generator is unreliable, this can cause vulnerabilities that threaten information security.

In modeling and simulations, generators are used to generate random events and data sets. Deficiencies in their operation can cause errors in the modeling and lead to inaccurate results.

In cryptographic systems, random sequences and Pseudo-random sequences are used to generate keys, random numbers, and salt values. Low quality of the generator can create vulnerabilities that allow attackers to break cryptographic protocols.

Thus, the quality of generators directly affects the efficiency and security of systems, which makes checking their statistical properties a key task.

Pseudo-random number generators generate numerical values (sequences) that appear random, although in fact they have a certain structure. This makes them in demand in various industries, in particular for key generation,

ensuring confidentiality, protecting data integrity, and transaction security. Therefore, the reliability and security of such sequences are the main characteristics.

The work is devoted to the analysis of tools for evaluating the statistical properties of random and pseudorandom sequence generators.

Keywords: *pseudorandom sequence generator, crypto protection, statistical tests, key generation.*

Постановка проблеми

Відомо, що генерація псевдовипадкових чисел (ПВЧ) значною мірою впливає на інформаційні технології у сферах як криптологія, аналітика, моделювання, медицина, симуляції та ін. Якість псевдовипадкових послідовностей (ПВП) безпосередньо впливає на стійкість шифрування, ефективність чисельних методів та надійність різних цифрових систем. Недостатня випадковість або наявність статистичних закономірностей у ПВП може призвести до їх передбачуваності та, як наслідок, до вразливостей у безпекових механізмах.

Тому необхідність дослідження тестових наборів обумовлена зростаючими вимогами до криптографічної стійкості та важливістю адаптації статистичних тестів до сучасних викликів. Основні проблеми, що потребують вирішення, включають: узагальнення критеріїв випадковості, оптимізацію існуючих тестових наборів, автоматизацію тестових процесів та як наслідок розробку нових тестових наборів. Значною мірою на якість ПВП впливають генератори псевдовипадкових чисел (ГПВЧ).

Аналіз публікацій за темою дослідження

Питанням надійності ГПВП займаються чимало вчених та дослідників. Так, у роботах [5; 6; 9] вчені Х. Махалінгам, В. Срірам, С. Поперешняк розглядають питання дослідження та оцінки тестових наборів і характеристик генераторів. Однак питанням порівняння широкої оцінки відомих тестів приділено недостатньо уваги, хоча це питання є достатньо необхідним для визначення надійності ПВП в умовах сучасних викликів.

У роботі [9] запропоновано методи оцінки бітових послідовностей із різноманітними шляхами використання тестових наборів, проте недостатньо формалізовано критерії вибору того чи іншого методу для конкретних випадків застосувань.

Мета статті. Провести порівняльний аналіз основних відомих тестових наборів псевдовипадкових та випадкових послідовностей: TestU01, NIST STS та DieHard як інструментів для оцінки статистичних властивостей генераторів, які формують псевдовипадкові та послідовності.

Виклад основного матеріалу

Тести NIST є стандартом у криптографії, пропонуючи широкий набір підходів для оцінки випадковості послідовностей. DieHard-тести спрямовані на глибокий аналіз складних статистичних характеристик і часто використовуються для виявлення детальних недоліків генераторів ПВП. TestU01 вирізняються більшою чутливістю, що дозволяє їм виявляти ширший спектр можливих недоліків ПВП.

Розглянемо особливості, недоліки і ключові області застосування згаданих механізмів перевірки.

Статистичні тести служать для перевірки того, чи забезпечують ГВП або ГПВП достатній рівень випадковості. Їхня мета полягає у зборі доказів, що генеровані числа мають властивості, притаманні істинно випадковим послідовностям [1].

Під час цих перевірок аналізуються згенеровані послідовності та порівнюються їхні статистичні характеристики з очікуваними властивостями ідеальних випадкових послідовностей. Це дозволяє оцінити якість генератора (наскільки його робота відповідає очікуванням) та виявити вразливості (знайти можливі закономірності чи систематичні відхилення), які можуть зробити генератор ненадійним для певних завдань.

Такі порівняння допомагають оцінити, чи є генератор придатним для криптографічних, аналітичних або застосування в інших галузях, де випадковість є ключовою вимогою.

Вирішення подібних завдань базується на перевірці гіпотез про властивості випадкових процесів (ВП) і випадкових вибірок (ВВ), які створюються генераторами. У ролі статистичної гіпотези може виступати будь-яке припущення щодо розподілу або характеристик випадкової величини. За допомогою методів математичної статистики це припущення перевіряється на істинність чи хибність: якщо результати підтверджують гіпотезу, вона приймається, якщо ні – відхиляється [2] .

Процес створення механізму перевірки статистичних гіпотез ґрунтується на створенні (висуванні) двох гіпотез: нульової (H0) та альтернативної (H1). Якщо нульова гіпотеза доводить, що послідовність дійсно випадкова, то альтернативна випадковість не є випадковою [3; 4; 12].

На сьогодні основна частина тестів сформована як програмне забезпечення. Це дає змогу ефективно та якісно виконувати тестування, заощаджує час і ресурси.

Тести необхідно провести для визначення безпечності генераторів та критеріїв їхньої випадковості. Важливо також звернути увагу на подальше застосування того чи іншого генератора при виборі набору тестів, оскільки це кардинально впливатиме на подальшу оцінку ГПВЧ.

Існує ряд тестів, які використовують різні інструменти та алгоритми. Найбільш відомим є набір тестів NIST Statistical Test Suite (NIST STS), до складу якого входить щонайменше 16 статистичних тестів, метою яких є визначення міри випадковості двійкової системи послідовностей, створених апаратними чи програмними генераторами [7].

Основний пакет тестів DieHard складається з 13 наборів окремих тестових перевірок [8; 9]. Тест DieHard був розроблений математиком Джорджем Магсаглією протягом шести років та вперше опублікований в 1995 році. В основі тесту лежить вимірювання якості множини випадкових чисел [8]. Він став одним із перших широко відомих інструментів для статистичного тестування генераторів випадкових чисел (ГВЧ) та криптографічних алгоритмів. Завдяки своїй новаторській природі та доступності він швидко здобув популярність у наукових та інженерних колах [10].

Всі тести спрямовані на виявлення можливих закономірностей, передбачуваності або структур, що можуть вказувати на слабкості ГВЧ. Результати тестів зазвичай використовуються для оцінки придатності генератора у криптографічних або інших чутливих до випадковості системах.

Однак, незважаючи на його історичну роль, набір тестів DieHard має свої недоліки:

суб'єктивність вибору тестів. Набір включає тести, які не завжди охоплюють усі аспекти випадковості, а їх добір вважається дещо неоднозначним;

складність інтерпретації. Результати деяких тестів можуть бути важкими для розуміння та аналізу, що ускладнює використання DieHard для неспеціалістів [11];

помилки в реалізації. Початкова програмна версія набору страждала від технічних недоліків, що могли впливати на точність тестів і знижувати їхню надійність.

Незважаючи на ці недоліки, DieHard послужив основою для створення більш сучасних і вдосконалених наборів тестів, таких як DieHarder і TestU01, які враховують недоліки оригінальної версії [13].

Test U01 – пакет статистичних тестів, реалізований на мові ZNSI C, який використовує набір утиліт для тестування ПВП. Остання версія тесту була представлена П'єром Л'Екуйе та Річардом Сімарде з Монреальского університету в 2007 році [2].

Перевагою TestU01 є:

− наявність трьох рівнів тестування: SmallCrush, Crush та BigCrush. Це дозволяє гнучко підходити до перевірки ГВЧ, починаючи з базових тестів і закінчуючи глибоким статистичним аналізом;

− висока чутливість до дефектів. Тести в TestU01 ґрунтуються на передових статистичних методах, що дозволяє виявити навіть незначні відхилення від ідеальної випадковості, які можуть бути критичними у криптографічних і симуляційних застосуваннях.

TestU01 дозволяє перевіряти як класичні ГВЧ (наприклад, лінійні конгруентні генератори), так і складніші криптографічні генератори. Він також підтримує різні параметри конфігурації для адаптації тестування до конкретних потреб [15];

− наявність вихідного коду дає змогу дослідникам аналізувати методи тестування, модифікувати алгоритми та інтегрувати TestU01 у власні проєкти.

Багато наукових публікацій і досліджень використовують TestU01 як стандартний інструмент для перевірки ГВЧ, що підтверджує його ефективність і надійність. При цьому відомі наступні недоліки TestU01:

− testU01 не є ідеальним для оцінки криптографічних ГВЧ, оскільки він не враховує деякі специфічні атаки та вимоги, що використовуються у криптографії;

− виконання повного набору потребує значного обсягу пам’яті та обчислювальної потужності, що може бути проблематичним для деяких застосувань [16];

− для ефективного застосування TestU01 необхідно мати глибокі знання в галузі статистики та теорії випадкових чисел, що може бути складним для дослідників, які не мають відповідної підготовки;

− обмежена підтримка багатьох мов програмування. TestU01 розроблений на мові C++ і може бути складним для інтеграції у середовища, що базуються на інших мовах програмування без додаткової адаптації.

Таким чином, TestU01 є потужним інструментом для оцінки псевдовипадкових генераторів, що широко використовується в наукових дослідженнях і практичних застосуваннях. Його головними перевагами є широка база тестів, відкритий код і висока чутливість до статистичних аномалій. Водночас його застосування вимагає значних обчислювальних ресурсів і спеціальних знань, що може бути бар’єром для нових користувачів.

Особливе місце серед інструментів оцінки ПВП займає пакет тестів NIST STS. У роботі проведемо аналіз наборів інструментів, які відсутні в DieHard та Test U01.

Тест перевірки накопичених сум призначений для виявлення довгострокових відхилень у випадковій послідовності. Він перевіряє, чи є загальна тенденція накопичених значень (сума бітів, інтерпретованих як +1 та –1) у послідовності узгодженою з випадковим розподілом.

Переваги тесту в тому що він виявляє довгострокові зміщення в послідовності та аналізує як локальні, так і глобальні аномалії у розподілі.

Обмеження зосереджені на чутливості до тривалих послідовностей, де навіть невеликі відхилення можуть накопичуватися, а також тест не враховує залежності між сусідніми бітами.

Тест перевірки накопичених сум використовується для аналізу якості генераторів випадкових чисел, криптографічних алгоритмів та інших систем, що вимагають високого рівня випадковості. Він є важливою складовою комплексного аналізу в пакеті тестів NIST STS, дозволяючи оцінювати як короткострокові, так і довгострокові характеристики випадковості.

Тест на перевірку серій є важливим етапом аналізу генераторів випадкових чисел (ГВЧ). Цей тест використовується для визначення того, чи кількість послідовних однакових бітів у виході ГВЧ відповідає статистичним очікуванням для випадкової послідовності.

Мета тесту полягає в перевірці частоти повторення однакових бітів (серій) заданої довжини та аналізу розподілу довжин серій 0 і 1, що відповідає теоретично очікуваному.

Тест працює наступним чином: спочатку обчислюється довжина серій (кількість послідовних 0 або 1) у бітах. Далі кількість серій порівнюється зі значеннями, які очікуються для випадкової послідовності. Заключним етапом є використання критерію хі-квадрат (x^2) для оцінки відповідності.

Теоретичні очікування:

− для випадкової послідовності частота серій довжиною *i* повинна зменшуватися експоненційно;

− формула теоретичної ймовірності для серії довжини і $P(i) = (1 – p)^2 \cdot p(i)$, де $p = 0{,}5$;

Результат роботи тесту:

− генерується *p*-значення (*p-value*), яке показує ймовірність того, що відхилення від очікуваного розподілу є випадковим;

− якщо $p \geq 0{,}01$, послідовність вважається випадковою для даного тесту.

Спектральний тест базується на дискретному перетворенні Фур'є (ДПФ). Він призначений для виявлення періодичних компонент у бітовій послідовності, які можуть свідчити про невипадковість.

Мета спектрального тесту полягає у виявленні синусоїдальних або періодичних компонент, що свідчать про наявність регулярності у послідовності.

Особливостями використання спектрального тесту є:

− чутливість до регулярностей та кореляцій у бітовій послідовності, особливо до періодичних компонент;

− необхідність використання достатньо довгих послідовностей, оскільки короткі послідовності можуть давати недостовірні результати.

Застосування універсального тесту Маурера обумовлено необхідністю визначитись, наскільки добре бітова послідовність стискається без втрати інформації. Якщо послідовність добре стискається, це може свідчити про наявність закономірностей, тобто невипадковість.

Тест базується на принципі інформаційної ентропії: чим більше випадковості в послідовності, тим складніше її стискати. Якщо послідовність має низький рівень ентропії, це свідчить про наявність повторюваних структур або передбачуваності [14].

До переваг даного тесту можна віднести: виявлення глобальних закономірностей у довгих послідовностях та якісну роботу для генераторів випадкових чисел, які мають тенденцію до повторюваності.

Тест перевірки шаблонів, які перекриваються, створений для оцінки якості ГВЧ. Він призначений для виявлення повторюваних шаблонів у послідовності бітів, які можуть свідчити про відхилення від випадковості.

Тест перевіряє, чи виявляються у бітовій послідовності повторювані шаблони заданої довжини *m*. Якщо таких повторень занадто багато або занадто мало порівняно з очікуваним рівнем випадковості, це може свідчити про невипадковість послідовності [14].

Основні етапи застосування тесту:

− вибір шаблону *m*: зазвичай вибирається короткий бітовий шаблон, наприклад, 111, 101 тощо;

− розбиття послідовності: бітова послідовність розбивається на блоки однакової довжини *N*, щоб аналізувати частоту появи шаблону в кожному блоці;

− обчислення частот: підраховується кількість повторень шаблону *m* в кожному блоці;

− порівняння з теоретичною моделлю: частоти повторення шаблону порівнюються з теоретичним розподілом Пуассона;

− обчислення *p*-значення: розраховується значення *p*, яке показує ймовірність того, що послідовність випадкова. Якщо *p*-значення менше порогового рівня (наприклад, 0,01 або 0,05), то послідовність вважається невипадковою.

Результат тесту наступний:

- якщо *p*-значення вище порогу, то послідовність вважається випадковою;
- якщо *p*-значення нижче порогу, то є ознаки невипадковості.

Тест на перевірку випадкових відхилень (Random Excursions Test) призначений для оцінювання, чи випадкова бітова послідовність поводиться як випадковий процес у термінах проходження через нуль (так звані «випадкові блукання»). Основна мета цього тесту – перевірити, наскільки часто певні стани (відхилення) виникають під час проходження послідовності.

Тест дозволяє проаналізувати, як часто послідовність повертається до стану 0, і перевіряє розподіл відхилень для певних значень. Якщо бітова послідовність є випадковою, частота появи станів повинна відповідати теоретично очікуваній для випадкового процесу.

Переваги тесту:

- наявність готової реалізації тесту, яка враховує його особливості;
- можлива реалізація на інших мовах (наприклад, MATLAB чи C++).

Перевірка випадкових відхилень (варіантний тест) є розширенням основного тесту випадкових відхилень. Цей тест аналізує кумулятивну суму випадкового блукання, але зосереджується на тому, як часто конкретні стани (від –9 до +9, крім 0) досягаються в послідовності. Метою є перевірка щодо відповідності частоти цих станів очікуваному розподілу для випадкового процесу.

Призначений для перевірки випадкових відхилень та визначає, чи є частоти появи певних станів (наприклад, −9, −8, …, 8, 9) у послідовності такими, що відповідають моделі випадкового блукання.

Перевірка шаблонів, які не перекриваються, використовується для виявлення конкретних бітових підпослідовностей (шаблонів) у випадковій послідовності. На відміну від тесту Overlapping Template Matching Test, тут шаблони не можуть перекриватися.

Тест перевіряє, чи з'являється заданий бітовий шаблон із частотою, яка відповідає очікуваній для випадкової послідовності, а також якщо шаблон з'являється занадто часто або занадто рідко, це може вказувати на наявність закономірностей у даних.

Загальні висновки

Набір тестів NIST STS (стандарт NIST SP 800-22) має низку переваг порівняно з TestU01 та DieHard. Цей набір використовується як загальноприйнятий стандарт для оцінки криптографічних генераторів випадкових чисел. Випробування спеціально підібрані для слабких місць, які можуть бути вставлені на безпеку системи. Для криптографічних продуктів NIST STS є оптимальним вибором завдяки спеціалізації на криптографічну стійкість та стандартизацію.

Слід зауважити, що комплексне використання згаданих тестів дає змогу досягти більш точної оцінки якості генераторів ПВП. Це є корисним для розробників, дослідників та інших спеціалістів, які працюють у цій галузі, а також сприятиме створенню більш надійних генераторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Almaraz Luengo E., Román Villaizán J. Cryptographically Secured Pseudo-Random Number Generators: Analysis and Testing with NIST Statistical Test Suite // Mathematics. 2023. № 11 (23). P. 4812. URL: https://doi.org/10.3390/math11234812.

2. Araki S., Wu J.-H., Yan J.-J. A Novel Design of Random Number Generators Using ChaosBased Extremum Coding // IEEE Access. 2024. № 12. P. 24039–24047. URL: https://doi.org/10.1109/ ACCESS.2024.3365638.

3. Нємкова О., Кіх М. Порівняльне дослідження тестів для оцінки статистичних характеристик генераторів випадкових та псевдовипадкових послідовностей // Електронне фахове наукове видання

«Кібербезпека: освіта, наука, техніка». 2024. № 4 (24). P. 115–132. URL: https://doi.org/10.28925/2663-4023.2024.24.115132.

4. Левин Б. Р. Теоретичні основи статистичної радіотехніки. Книга друга. Видавництво «Радянське радіо», 1968. С. 25–30.

5. Mahalingam H., Rethinam S., Janakiraman S., Rengarajan A. Non-Identical Inverter Rings as an Entropy Source: NIST-90B-Verified TRNG Architecture on FPGAs for IoT Device Integrity // Mathematics. 2023. № 11 (4). P. 1049. URL: https://doi.org/10.3390/math11041049.

6. Sriram V., Srikamakshi M., Jegadish Kumar K. J., Nagarajan K. K. Randomness Analysis of YUGAM-128 Using Diehard Test Suite // Innovative Data Communication Technologies and Application. 2020. № 46. P. 600–607. URL: https://doi.org/10.1007/978-3-030-38040-3_68.

7. Kim Y., Yeom Y. Accelerated implementation for testing IID assumption of NIST SP 800-90B using GPU // PeerJ Computer Science. 2021. № 7, e404. https://doi.org/10.7717/peerj-cs.404

8. Al-Daraiseh A., Sanjalawe Y., Al-E’mari S., Fraihat S., Bany Taha M., Al-Muhammed M. Cryptographic Grade Chaotic Random Number Generator Based on Tent-Map // Journal of Sensor and Actuator Networks. 2023. № 12 (5). P. 73. URL: https://doi.org/10.3390/jsan12050073.

9. Поперешняк С. В. Засіб для тестування бітової послідовності на випадковість // Вчені записки ТНУ ім. В. І. Вернадського. Серія: технічні науки. 2020. Том 31 (70). № 4. DOI: https://doi.org/10.32838/2663-5941/2020.4/16.

10. Abdulhameed H. A., Abdalmaaen H. F., Mohammed A. T., Mosleh M. F., Abdulhameed A. A. A Lightweight Hybrid Cryptographic Algorithm for WSNs Tested by the Diehard Tests and the Raspberry Pi. 2022 International Conference on Computer Science and Software Engineering (CSASE), P. 271–276. URL: https://doi.org/10.1109/CSASE51777.2022.9759589.

11. Ryan C., Kshirsagar M., Vaidya G., Cunningham A., Sivaraman R. Design of a cryptographically secure pseudo random number generator with grammatical evolution // Scientific Reports. 2022. № 12 (1). P. 8602. URL: https://doi.org/10.1038/s41598-022-11613-x.

12. Hussein S. N., Al-Alak S. M. Secret Keys Extraction Using Light Weight Schemes for Data Ciphering // Journal of Physics: Conference Series. 2021. № 1999 (1). 012114. URL: https://doi.org/ 10.1088/1742- 6596/1999/1/012114.

13. Semankiv M. Assessment of statistical properties random numbers // Bulletin of the National Technical University ‘KhPI’. A Series of «Information and Modeling». 2016. № 21. URL: https://doi.org/ 10.20998/2411-0558.2016.21.12.

14. NIST SP 800-22. A Statistic Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application. April 2000. URL: http://csrc.nist.gov./publications/niatpubs//SP800-22rev1a.pdf.

15. L’Ecuyer P., Simard R. TestU01: A C Library for Empirical Testing of Random Number Generators // ACM Transactions on Mathematical Software. 2007. № 33 (4). P. 1–40.

16. Knuth D. E. The Art of Computer Programming, Volume 2: Seminumerical Algorithms. Addison-Wesley, 1997.

DOI: 10.58254/viti.7.2025.08.81

УДК 004.05

канд. техн. наук, доцент Любарський С. В. ORCID: 0000-0001-8068-1106 (ВІТІ ім. Героїв Крут)
Кондратюк А. Г. ORCID: 0000-0002-8485-3160 (ВІТІ ім. Героїв Крут)
Шарнін С. А. ORCID: 0000-0002-5856-3995 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Здоренко Ю. М. ORCID: 0000-0002-5649-771X (НУ «Полтавська політехніка ім. Ю. Кондратюка»)

ФУНКЦІОНАЛЬНА МОДЕЛЬ РЕФАКТОРИНГУ ОБ'ЄКТНО-ОРІЄНТОВАНОГО КОДУ НА ОСНОВІ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАВДАННЯ БЕЗПЕКИ ПРОГРАМНОГО КОДУ

Сучасне програмне забезпечення задає високі вимоги до безпеки та якості коду. Одним із важливих завдань безпечного використання сучасних інформаційних систем є запровадження заходів, що унеможливлюють спроби через існуючи вразливості програмного забезпечення впливати на функціональність цих систем. Особливо важлива інтеграція механізмів дотримання безпеки та якості програмного коду у всі фази життєвого циклу проєктування інформаційної системи. Найбільш перспективним напрямом у вирішенні цього завдання виступає застосування процесу рефакторингу програмного коду.

Існуючі підходи до рефакторингу мають чисельні обмеження. Методи штучного інтелекту можуть значно допомогти подолати ці обмеження, надаючи автоматизовані, об'єктивні та адаптивні рішення для покращення якості, безпеки та підтримуваності програмного коду.

Використання методів штучного інтелекту дозволяє автоматизувати процес статичного та динамічного аналізу програмного коду, виявити проблеми і вирішити їх шляхом пропозиції оптимізовано-безпечного та ефективного варіанту.

Пропонується до розгляду модель рефакторингу об'єктно-орієнтованого коду на основі методів штучного інтелекту з метою підвищення рівня його якості та безпеки.

Ключові слова: *функціональна модель, програмне забезпечення, статичний і динамічний аналіз, рефакторинг, технології штучного інтелекту, вразливості безпеки, якість коду.*

S. Liubarskyi, A. Kondratiuk, S. Sharnin, Y. Zdorenko. Functional model of object-oriented code refactoring based on artificial intelligence methods to provide security tasks of software code

Modern software sets high requirements for code security and quality. One of the important tasks of safe use of modern information systems is to implement measures that make it impossible to attempt to influence the functionality of these systems through existing software vulnerabilities. Integration of mechanisms for maintaining security and quality of program code into all phases of the information system design life cycle is especially important. The most promising direction in solving this problem is the use of the program code refactoring process.

Existing approaches to refactoring have numerous limitations. Artificial intelligence methods can significantly help overcome these limitations by providing automated, objective and adaptive solutions to improve the quality, security and maintainability of program code.

The use of artificial intelligence methods allows you to automate the process of static and dynamic analysis of program code, identify problems and solve them by offering an optimized, safe and effective option.

A model for refactoring object-oriented code based on artificial intelligence methods is proposed for consideration in order to improve its quality and security.

Keywords: *functional model, software, static and dynamic analysis, refactoring, artificial intelligence technologies, security vulnerabilities, code quality.*

Постановка завдання. Сучасне програмне забезпечення стикається з дедалі більшими вимогами до безпеки та якості програмного коду через зростаючий рівень кібернетичних загроз, збільшення обсягу даних, що підлягають обробці, і високі очікування користувачів від програмного забезпечення, особливо в контурах підтримки прийняття рішень.

Безпека – це ключовий аспект сучасного програмного забезпечення, оскільки вразливості можуть призвести до серйозних наслідків, таких як витік даних, фінансові збитки або порушення конфіденційності. Якість коду забезпечує надійність, підтримуваність і масштабованість програмного забезпечення. Це також допомагає мінімізувати кількість

помилок і полегшити співпрацю команди розробників по досягненню цільової настанови програмної розробки.

Головними важелями, що потенційно впливають на безпеку та якість коду, є:

– передбачення найбільш документованих вразливостей, виявлення потенційних загроз у програмному об'єктно-орієнтованому коді за допомогою методів статичного та динамічного аналізу;

– інтеграція у вихідний код механізмів обробки виняткових ситуацій без переривання роботи програми, використання механізмів відкату;

– забезпечення читабельності та структурованості коду;

– розбиття коду на маленькі, незалежні модулі або функції, використання принципу *Don't Repeat Yourself*;

– використання ефективних алгоритмів і структур даних, уникнення надмірного споживання ресурсів (*CPU*, *RAM*, мережевої пропускної здатності);

– використання систем контролю версій (наприклад, *Git*) для управління змінами програмного коду, дотримання практик *Code Review* для забезпечення якості;

– дотримання рекомендацій *OWASP* для безпечного програмування, використання сучасних методологій розробки (*Agile*, *DevOps*);

– написання модульних тестів (*unit tests*), інтеграційних тестів і тестів регресії, використання інструментів автоматизації тестування (наприклад, *JUnit*, *pytest*).

Для забезпечення високих стандартів безпеки та якості, особливо для завдань проєктування, розробки і супроводження інформаційних систем спеціального призначення, важливо інтегрувати механізми їхньої реалізації у всі етапи життєвого циклу програмного забезпечення.

Найбільш перспективним напрямом у вирішенні цього завдання виступає застосування процесу рефакторингу програмного коду.

Рефакторинг програмного коду – це процес внесення змін у існуючий програмний код з метою покращення його структури, читабельності та підтримуваності без зміни його зовнішньої поведінки. Рефакторинг є невід'ємною частиною розробки програмного забезпечення, оскільки він допомагає підтримувати якість програмного коду на високому рівні і може значно впливати на його безпеку. У контексті безпеки рефакторинг часто стає превентивною мірою, яка запобігає потенційним атакам та зменшує ризики.

Існуючі підходи до рефакторингу мають чисельні обмеження, такі як трудомісткість, суб'єктивність, відсутність глибокого розуміння контексту, недостатня масштабованість та адаптивність. Методи штучного інтелекту можуть значно допомогти подолати ці обмеження, надаючи автоматизовані, об'єктивні та адаптивні рішення для покращення якості, безпеки та підтримуваності програмного коду.

Використання методів штучного інтелекту (ШІ) дозволить автоматизувати процес аналізу, виявлення проблем та їх усунення [1]. Пропонується для розгляду модель рефакторингу об'єктно-орієнтованого програмного коду на основі методів ШІ для підвищення рівня його безпеки та якості.

Аналіз останніх досліджень і публікацій. Основні вразливості, що потенційно впливають на безпеку та якість програмного коду, представлено на рисунку 1 [2].

SQL-ін'єкції є однією з найнебезпечніших вразливостей. Окрім компрометуючих впливів (доступ до критично важливих даних, зміна структури даних або навіть руйнація їх вмісту), зниження продуктивності інформаційної системи шляхом виконання неконтрольованих запитів, *SQL*-ін'єкції можуть впливати на якість коду. Використання некоректних або незахищених запитів у коді ускладнює його підтримку, підвищує ризик появи нових помилок і вразливостей.

Методи запобігання *SQL*-ін’єкціям включають використання підготовлених запитів (*prepared statements*), *ORM* (*Object-Relational Mapping*) для взаємодії з базами даних, а також застосування механізмів валідації та фільтрації введених даних.

XSS-атаки (*Cross-Site Scripting*) можуть викликати маніпуляції з контентом вебдодатка шляхом уведення дезінформації або підробки елементів інтерфейсу. Це призводить до зниження довіри до додатка, погіршення завдання підтримуваності коду. Недостатня перевірка введених даних, невикористання механізмів фільтрації сприяє накопиченню вразливостей у коді [3; 4].

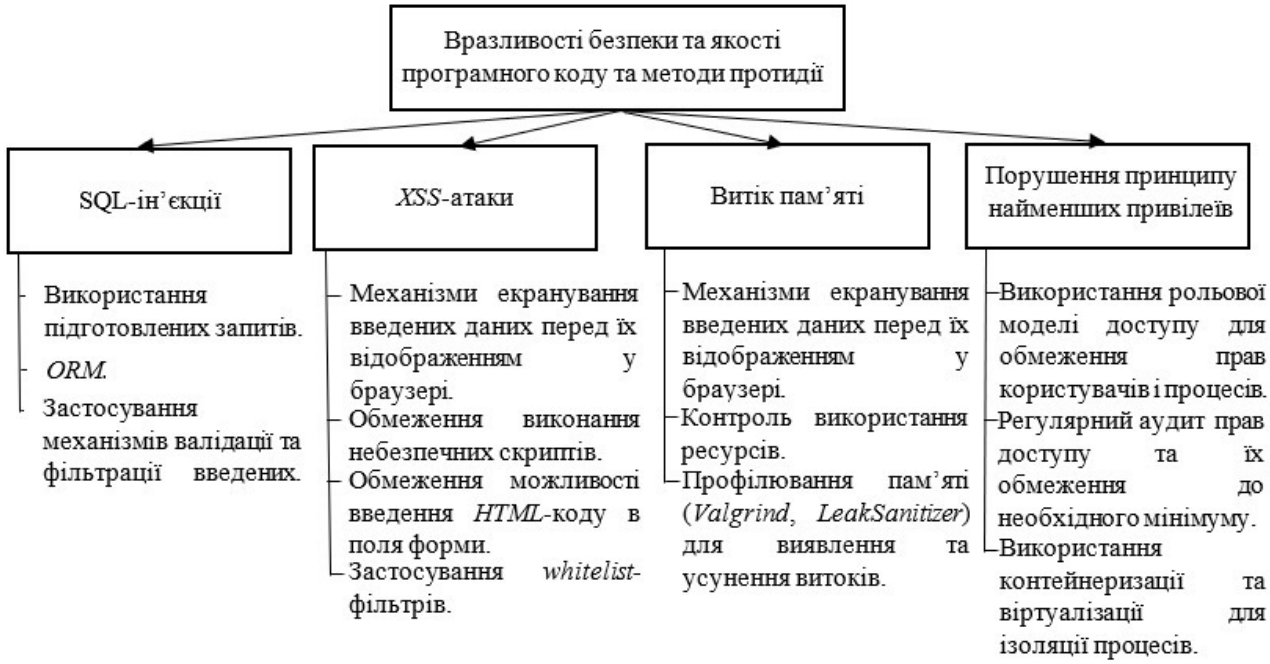


Рис. 1. Основні вразливості безпеки та якості програмного коду та методи їхньому запобіганню

Запобігти у цьому можуть механізми екранування (*escaping*) введених даних перед їх відображенням у браузері, впровадження *CSP* (*Content Security Policy*) для обмеження виконання небезпечних скриптів, обмеження можливості введення *HTML*-коду в поля форми, застосування *whitelist*-фільтрів.

Витік пам’яті (*memory leak*) виникає, коли програмна система неправильно звільняє використані ресурси, що може призвести до поступового зростання споживання пам’яті та збою програмної системи.

Основними наслідками цього може бути: зниження продуктивності програмного коду (неефективне використання пам’яті призводить до уповільнення роботи додатка через збільшене навантаження на оперативну пам’ять); підвищений ризик відмови програмної системи (у критичних системах витік пам’яті може призвести до повного вичерпання доступних ресурсів і аварійного завершення роботи програмної системи); уразливість до *DoS*-атак (зловмисники можуть свідомо спричиняти витоки пам’яті для виснаження ресурсів сервера); погіршення якості програмного коду (код, схильний до витоків пам’яті, є складним у підтримці та модернізації).

Методами, що можуть запобігати цій загрозі, є: використання автоматичного керування пам’яттю (*garbage collection*) у мовах програмування, які це підтримують; контроль використання ресурсів, зокрема явне звільнення пам’яті у мовах без автоматичного

управління пам'яттю (наприклад, *C#*, *C++*); використання інструментів для профілювання пам'яті (*Valgrind, LeakSanitizer*), виявлення та усунення витоків.

Порушення принципу найменших привілеїв відбувається, коли користувачі або процеси отримують доступ до ресурсів або функцій, які їм не потрібні для виконання своїх завдань. Насамперед це впливає на несанкціонований доступ до критичних даних. Надання надмірних привілеїв у коді ускладнює аудит безпеки та підвищує ризик появи несанкціонованих змін.

Методи запобігання порушенню принципу найменших привілеїв включають: використання рольової моделі доступу (*RBAC*) для обмеження прав користувачів і процесів; регулярний аудит прав доступу та їх обмеження до необхідного мінімуму; використання контейнеризації та віртуалізації для ізоляції процесів.

Виявлення потенційних загроз у програмному об'єктно-орієнтованому коді здійснюється за допомогою статичного та динамічного аналізу програмного коду.

Методи статичного аналізу (*Static Code Analysis*) спрямовані на дослідження програмного коду без його виконання. Основна мета статичного аналізу – виявлення вразливостей, помилок програмування, порушень стилю кодування та недоліків архітектури. Методи цієї групи найбільш оптимальні для виявлення вразливостей на ранніх етапах розробки (наприклад, *SQL*-ін'єкції, *XSS*, неправильне управління пам'яттю), перевірки дотримання стандартів кодування, аналізу залежностей та складності коду, автоматизованого рефакторингу та пошуку дублікатів коду.

Методи статичного аналізу покладаються на: використання інструментів аналізу коду (*SonarQube, ESLint, Pylint, Checkmarx*); використання процедур символічного виконання (*Symbolic Execution*); аналіз потоку даних (*Data Flow Analysis*).

На противагу статичному аналізу, динамічний аналіз (*Dynamic Code Analysis*) – це метод перевірки програмного коду під час його виконання. Він дозволяє виявити потенційні вразливості, що виникають лише під час реальної роботи програмної системи. Серед основних аспектів динамічного аналізу можна визначити: тестування безпеки під час виконання (*Runtime Security Testing*); виявлення витоків пам'яті, переповнення буфера, некоректного використання ресурсів; функціональне та навантажувальне тестування для оцінки продуктивності; аналіз поведінки програми за допомогою інструментів профілювання (*Valgrind, Dynatrace*, *AppDynamics*).

Динамічний аналіз дозволяє знаходити помилки, які не можуть бути виявлені за допомогою статичного аналізу, наприклад: вразливості, що виникають під певними умовами виконання програмного коду; атаки типу *race condition*; проблеми з конкурентним доступом до пам'яті.

Обидва методи аналізу є взаємодоповнюючими: статичний аналіз ефективний для раннього виявлення проблем, а динамічний – для тестування реальної поведінки програмного коду.

Статичний і динамічний методи аналізу програмного коду є основою для використання методів ШІ у рефакторингу. Вони дозволяють зібрати необхідні дані для навчання моделей машинного навчання та створення ефективних алгоритмів автоматизованого покращення коду.

Статичний аналіз надає інформацію про синтаксичні, стилістичні та структурні проблеми об'єктно-орієнтованого програмного коду, що використовується для навчання моделей ШІ та створення рекомендацій щодо рефакторингу [5].

Динамічний аналіз виявляє поведінкові проблеми програмного коду, такі як витоки пам'яті та проблеми продуктивності, що дозволяє адаптивно застосовувати методи оптимізації.

Метою статті є проведення порівняльного аналізу методів машинного та глибокого навчання технологій ШІ для автоматизації процесу рефакторингу програмного об'єктно-орієнтованого коду і на їх основі пропозиції функціональної моделі цього процесу в завданнях розробки надійного та якісного програмного коду інформаційних систем спеціального призначення.

Виклад основного матеріалу дослідження. Найбільшого застосування для автоматизації процесу рефакторингу програмного об'єктно-орієнтованого коду набули методи машинного та глибокого навчання технологій ШІ (рис. 2).

Як найбільш перспективні підходи слід розглядати:

1. *Використання нейронних мереж для аналізу коду та пошуку патернів "поганого" коду* (*code smells*). Нейронні мережі можуть ефективно аналізувати великі обсяги програмного коду та виявляти шаблони, що можуть свідчити про проблеми з безпекою та якістю.

Рис. 2. Методи машинного та глибокого навчання технологій ШІ для автоматизації процесу рефакторингу програмного коду

Основними напрямками їхнього застосування можна вважати: глибинне навчання для розпізнавання патернів коду (наприклад, навчання на великих наборах даних коду для виявлення поганих практик програмування, використання рекурентних нейронних мереж та трансформерів для аналізу послідовності коду); визначення "антипатернів" програмування (виявлення надмірної складності коду, дублікатів, порушень принципів *SOLID*, ідентифікація небезпечних конструкцій (наприклад, використання *eval*() або неконтрольованих введень користувача); автоматизований рефакторинг за допомогою ШІ (наприклад, генерація виправленого коду на основі аналізу існуючих помилок, використання *GAN* (*Generative Adversarial Networks*) або *RL* (*Reinforcement Learning*) для оптимізації структури коду).

Перевагами застосування нейронних мереж для аналізу програмного коду є*:*

– здатність апарату нейронних мереж до аналізу величезних обсягів даних і виявлення складних, неочевидних залежностей між різними частинами коду. Особливо це корисно для виявлення *code smells*, які можуть бути результатом комбінації кількох факторів;

– нейронні мережі можуть одночасно аналізувати велику кількість рядків коду, що робить їх ефективними для великих проєктів чи систем, де людський аналіз займе надто багато часу;

– нейронні мережі можуть бути навчені на значних наборах даних, які містять приклади "гарного" та "поганого" коду. Це дозволяє їм виявляти специфічні для певного проєкту чи команди *code smells*;

– нейронні мережі можуть враховувати контекст коду, такий як стиль програмування, доменна логіка або специфічні правила проєкту. Це робить їх гнучкішими порівняно з жорсткими правилами статичного аналізу;

– сучасні нейронні моделі можуть інтегруватися в інструменти розробки (*IDE*), надаючи розробникам моментальний зворотній зв’язок щодо потенційних проблем у коді;

– за допомогою механізмів онлайн-навчання нейронні мережі можуть покращувати свою продуктивність, адаптуючись до нових патернів або змін у проєкті.

Недоліками виступають: потреба значних обчислювальних потужностей для навчання та використання нейронних мереж, особливо для аналізу великих баз коду; рішення нейронних мереж можуть бути важкими для інтерпретації, оскільки вони часто працюють як “чорна скринька”; нейронні мережі можуть страждати від перенавчання, коли вони дуже точно вивчають тренувальні дані та починають давати неточні прогнози на нових даних. Це може призвести до помилкових спрацьовувань чи пропусків реальних проблем; якість роботи нейронної мережі залежить від якості тренувального набору даних. Якщо тренувальні дані містять помилки або не повністю відображають реальні ситуації, то модель може давати некоректні результати.

2. *Глибоке навчання для автоматичної генерації рефакторингових пропозицій*.

Глибоке навчання відкриває можливості для автоматизованого покращення якості коду, зокрема через:

– використання трансформерних моделей (*GPT*, *CodeBERT*, *Codex*) для прогнозування покращень у коді на основі виявлених недоліків;

– автоматичне формування рекомендацій щодо рефакторингу, наприклад, пропозиції замінити складні або дубльовані конструкції більш ефективними;

– навчання на великих наборах кодових баз для знаходження оптимальних рефакторингових рішень з урахуванням контексту та стилю кодування;

– поєднання технік *Natural Language Processing* (*NLP*) та *Computer Vision* для розуміння семантики та структури коду, що дозволяє виявляти складні зв’язки між компонентами програми.

Переваги: ефективне виявлення проблем у програмному коді (автоматична рефакторизація) і, відповідно, зменшення ручних операцій його аналізу; адаптація до різних мов програмування та платформ розробки, врахування контексту програмного коду (наприклад, стиль програмування, доменна логіка або специфічні правила проєкту); можливість навчатися на великих базах даних; глибокі моделі можуть постійно вчитися на нових даних, що дозволяє їм покращувати свою продуктивність і точність у міру отримання додаткових даних.

Недоліки: в деяких випадках ускладнене розуміння того, як саме модель прийшла до конкретної рекомендації рефакторингу; імовірність появи помилкових рекомендацій, особливо якщо тренувальні дані містять помилки або не повністю відображають реальні ситуації; потреба значних обчислювальних ресурсів; обмеження у розумінні семантики коду; потреба у спеціалізованих (експертних) знаннях із машинного навчання та обробки даних; обмеження у генерації оригінальних рішень.

3. *Алгоритми природної мови для аналізу коментарів і документації з метою покращення читабельності коду*.

Алгоритми обробки природної мови (*NLP*) можуть значно покращити читабельність і підтримку коду, аналізуючи коментарі та документацію.

Зазначені алгоритми здатні:

– автоматично оцінити якість коментарів програмного коду (а саме: виявити застарілі, суперечливі або нечіткі коментарі, оцінити відповідності коментарів до коду (наприклад,

наскільки вони описують актуальну функціональність), класифікувати текст для виявлення поганої документації);

– автоматично згенерувати коментарі та документацію до програмного коду. Тут може бути застосовано використання трансформерних моделей (*BERT*, *CodeBERT*, *GPT*) для генерації коментарів на основі коду, створення коротких пояснень до функцій, класів і методів, що спрощує роботу з великими кодовими базами, рефакторинг документації, щоб вона була більш структурованою та лаконічною;

– виявити невідповідності між кодом та документацією. Це забезпечується аналізом семантики коду та описів для знаходження розбіжностей, визначення змін у коді, що потребують оновлення документації;

– покращити стиль написання документації шляхом автоматичного виправлення граматичних і стилістичних помилок у коментарях, переформулювання надто складних або розпливчастих пояснень у більш зрозумілі.

Недоліки: алгоритми *NLP* часто мають труднощі з розумінням глибинного контексту та семантичної значимості тексту. Вони можуть неправильно інтерпретувати спеціалізовані терміни, абревіатури або доменну логіку, можуть не виявити суперечливість між описом у коментарях і реальним функціоналом коду; моделі *NLP* не зможуть покращити читабельність коду, якщо вхідні дані самі собою є некоректними; якщо модель навчена на обмеженому наборі даних, вона може генерувати рекомендації, які добре працюють лише для певного типу текстів. Це може призвести до некоректних пропозицій у нових або нетипових ситуаціях.

Отже, для ефективного використання нейронних мереж у цій задачі важливо:

– правильно налаштовувати моделі;

– забезпечити якість тренувальних даних;

– інтегрувати їх у процеси розробки так, щоб розробники могли довіряти рекомендаціям моделі.

Використання нейронних мереж значно покращує можливості статичного та динамічного аналізу, автоматизує процес виявлення проблем та сприяє ефективному рефакторингу коду.

Для успішного впровадження глибокого навчання у рефакторинг коду важливо:

– використовувати якісні тренувальні дані;

– забезпечувати прозорість і пояснення рекомендацій;

– інтегрувати систему у процеси розробки так, щоб розробники могли довіряти її пропозиціям.

Глибоке навчання має великий потенціал для автоматичної генерації рефакторингових пропозицій, оскільки воно може автоматизувати процес виявлення проблем і запропонувати покращення, які враховують контекст коду.

Для успішного застосування алгоритмів *NLP* важливо враховувати контекст, якість вхідних даних і специфіку проєкту. Ключовий фактор успіху – комбінація автоматичного аналізу з людським контролем, що забезпечує максимальну ефективність і точність рекомендацій.

Побудова моделі. Пропонується застосовувати рефакторинг програмного коду на основі ШІ із застосуванням механізмів статичного та динамічного аналізу не тільки для завдання виявлення вразливостей, помилок програмування, порушень стилю кодування, недоліків архітектури, але і для автоматизованого покращення коду, отримання безпечного та оптимізованого коду на основі виявлених проблем.

Функціональна модель рефакторингу об’єктно-орієнтованого коду на основі методів штучного інтелекту для забезпечення завдання безпеки програмного коду передбачає собою реалізацію наступних етапів (рис. 3):

1. *Збір даних за цільовий об’єктно-орієнтований програмний код як об’єкт аналізу*.

Цей функціональний модуль використовує вбудовані інструменти статичного та динамічного аналізу програмного об’єктно-орієнтованого коду. Інструменти статичного аналізу надають інформацію про помилки синтаксису, порушення стилю коду та потенційні вразливості.

Інструменти динамічного аналізу дають змогу виявити реальні загрози безпеці під час виконання коду.

Процеси статичного та динамічного аналізу програмного коду можуть виконуватися як паралельно, так і послідовно, залежно від контексту, мети аналізу та архітектури програмної системи.

Якщо процеси статичного і динамічного аналізів працюють паралельно, їхні результати потрібно об’єднати для подальшого використання (наприклад, для рефакторингу). У цьому випадку може знадобитися додаткова логіка для синхронізації та обробки цих даних. Це обмеження обумовило першочерговість у застосуванні інструментів статичного аналізу з передачею результатів як вхідних даних для динамічного аналізу.

Це дозволить отримати наступні переваги:

– динамічний аналіз може зосередитися лише на тих частинах коду, які були позначені як потенційно небезпечні під час статичного аналізу. Це економить час і ресурси;

– зменшується ймовірність “шуму” (помилкових сигналів) під час динамічного аналізу, оскільки він базується на надійних даних зі статичного аналізу;

– результати обох аналізів легше інтегрувати, оскільки вони мають чітку послідовність;

– можна сфокусуватися на найкритичніших областях програмного коду.

На цьому етапі формується набір даних, що містить інформацію про потенційні проблеми та вразливості.

2. *Навчання моделей ШІ*.

На даному етапі використовуються методи машинного навчання (*ML*) та глибинного навчання (*DL*) для створення моделей, що прогнозують наявність вразливостей.

У межах підготовчої фази цього етапу здійснюється попередня обробка даних, що отримані на попередньому етапі. Також передбачається створення набору ознак (*features*), таких як частота використання певних операторів, наявність небезпечних функцій тощо.

Виконавча фаза етапу навчання моделей використовує алгоритми *ML* (наприклад, *Random Forest*, *SVM*) для класифікації коду.

Застосування нейронних мереж (наприклад, рекурентних нейронних мереж *RNN* або трансформерів *Transformer*) передбачає виявлення складних шаблонів, які призводять до помилок або вразливостей.

Результатом цього етапу є навчені моделі, які можуть передбачати наявність проблем у коді.

3. *Автоматизований рефакторинг*.

Цей етап передбачає автоматичне виправлення виявлених проблем і також наявність двох фаз реалізації.

Спочатку здійснюється аналіз прогнозів, що передбачає використання навчених моделей для ідентифікації конкретних ділянок програмного коду, які потребують рефакторингу.

Далі здійснюється генерація безпечного коду:

– алгоритми ШІ (наприклад, генеративні моделі, такі як *GPT* або *CodeBERT*) створюють оптимізований та безпечний код;

– вносяться зміни у структуру класів, методів та інтерфейсів для покращення безпеки та продуктивності.

Результатом цього етапу є рефакторний код, який потенційно вважається безпечним і оптимізованим.

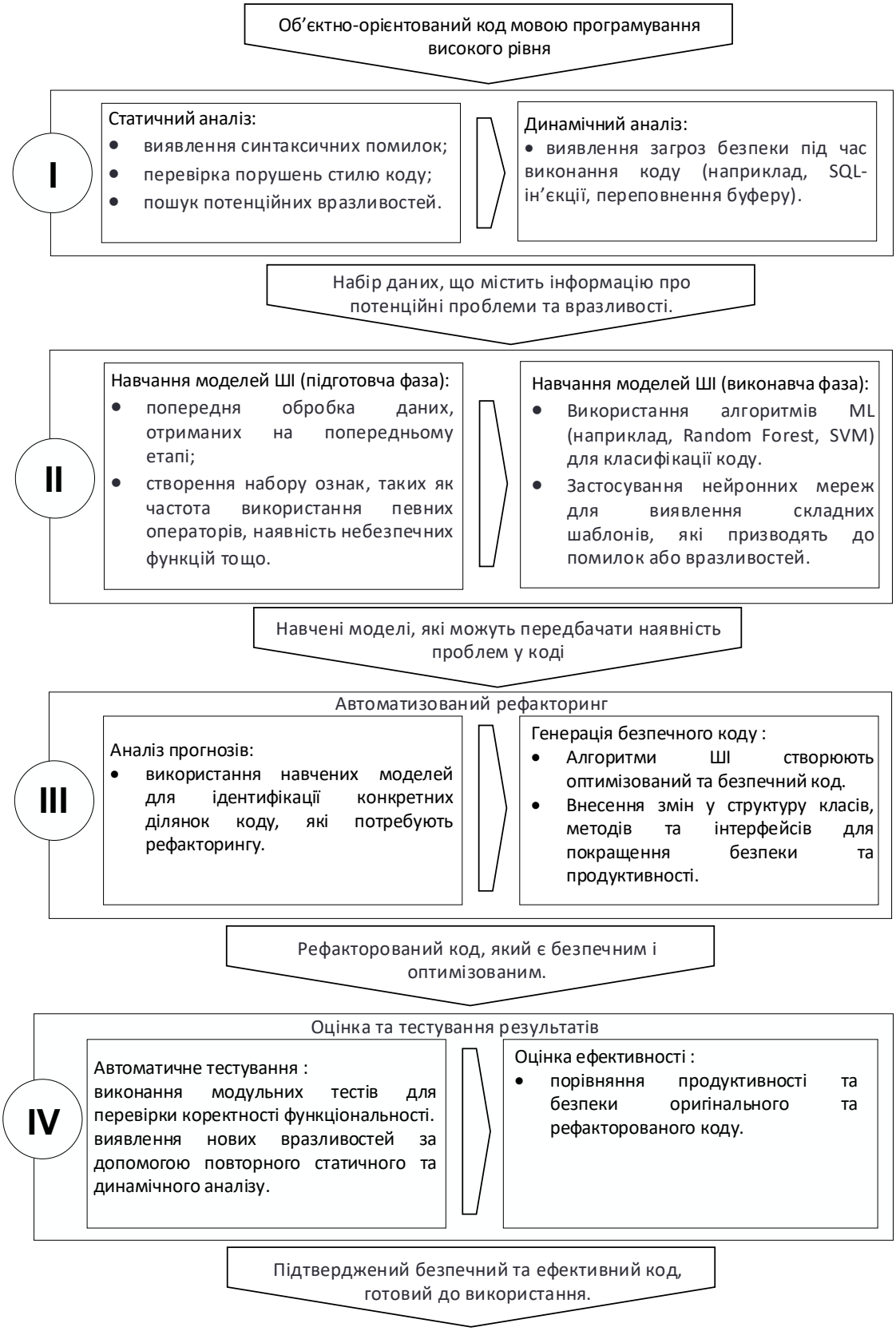


Рис. 3. Функціональна модель рефакторингу об'єктно-орієнтованого коду на основі методів штучного інтелекту

4. *Оцінка та тестування результатів.*

Останній етап функціональної моделі передбачає перевірку якості рефакторного коду.

Автоматичне тестування буде спрямоване на виконання модульних тестів для перевірки коректності функціональності.

Поява нових вразливостей може ініціалізувати собою повторну роботу інструментів статичного та динамічного аналізу.

Оцінка ефективності укладає собою завдання у порівнянні продуктивності та безпеки оригінального та рефакторного коду.

Табличне представлення функціональної моделі рефакторингу об'єктно-орієнтованого коду на основі методів штучного інтелекту за специфікацією *IDEF*0 (*Integration Definition for Function Modeling*) представлено у таблиці 1.

Таблиця 1

Модель рефакторингу об'єктно-орієнтованого коду на основі методів штучного інтелекту за специфікацією *IDEF*0

Процес	**КОНТРОЛЬ (*CONTROL*)**	**ВХІДНІ ДАНІ (*INPUTS*)**	**ВИХІДНІ ДАНІ (*OUTPUTS*)**	**МЕХАНІЗМ (*MECHANISM*)**
I	Процес аналізу коду	Набір даних, що містить інформацію про потенційні проблеми та ризики	Результати аналізу (статичні та динамічні помилки, порушення стилю коду тощо)	Алгоритми статичного та динамічного аналізу
II	Процес навчання моделей ML	Попередньо оброблені дані з результатами аналізу коду	Навчені моделі, які можуть передбачати наявність проблем у коді	Алгоритми машинного навчання (*Random Forest*, *SVM*, нейронні мережі тощо)
III	Процес автоматичного рефакторингу	Навчені моделі та аналізовані дані коду	Рефакторований код, який є безпечним і оптимізованим	Алгоритми генерації безпечного коду та оптимізації
IV	Процес оцінки ефективності та тестування	Рефакторований код	Підтверджений безпечний та ефективний код, готовий до використання	Модулі для тестування та оцінки продуктивності

За результатами етапів функціональної моделі рефакторингу об'єктно-орієнтованого коду на основі методів штучного інтелекту отримується підтверджений безпечний та ефективний код, готовий до використання за призначенням.

Таким чином, використання ШІ у рефакторингу об'єктно-орієнтованого коду дозволяє автоматизувати процеси покращення якості та безпеки, що робить програмне забезпечення більш захищеним та ефективним.

Висновки. Для забезпечення високих стандартів безпеки та якості в завданнях проєктування, розробки і супроводження інформаційних систем спеціального призначення важливо інтегрувати механізми їхньої реалізації у всі етапи життєвого циклу програмного забезпечення. Найбільш перспективним напрямом у вирішенні цього завдання виступає застосування процесу рефакторингу програмного коду. Цей процес постає превентивною мірою, яка запобігає потенційним атакам та зменшує ризики.

Рефакторинг програмного коду має чисельні обмеження, подолання яких покладається на долучення методів штучного інтелекту, особливо в завданнях статичного та динамічного аналізу, виявлення вразливостей, помилок програмування, порушень стилю кодування,

недоліків архітектури, автоматизованого покращення коду, отримання безпечного та оптимізованого коду на основі виявлених проблем.

Запропонована функціональна модель рефакторингу об’єктно-орієнтованого програмного коду на основі методів ШІ дозволяє автоматизувати процес покращення рівня безпеки та якості коду. Результати досліджень демонструють ефективність використання ШІ для виявлення вразливостей та автоматичного покращення структури коду.

Подальші дослідження можуть бути спрямовані на розширення можливостей моделі та її інтеграцію із сучасними інструментами розробки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
2. OWASP Foundation. OWASP Top Ten Security Risks. URL: https://owasp.org/www-project-top-ten/.
3. McConnell S. Code Complete. Microsoft Press, 2004.
4. Martin R. Clean Code: A Handbook of Agile Software Craftsmanship. Prentice Hall, 2008.
5. Fowler M. Refactoring: Improving the Design of Existing Code. Addison-Wesley, 2018.
6. Vasilescu B., Filkov V., Serebrenik A. Perceptions of Diversity on GitHub: A User Survey. Proceedings of CHI 2015.
7. Fields Jay, Harvie Shane, Fowler Martin. Refactoring Ruby Edition. Addison-Wesley, 2009
8. William C. Wake. Refactoring Workbook. Addison-Wesley, 2003. ISBN: 0321109295.
9. Feathers Michael. Working Effectively with Legacy Code. Prentice Hall, 2004.
10. Kerievsky Joshua. Refactoring to Patterns. Addison-Wesley, 2004.
11. Wagner Effective C#:5 Specific Ways to Improve Your C#/ 2015, 224 p.
12. Albahari Joseph, Albahari Ben. C# 7.0 in a Nutshell: The Definitive Reference, 2018. 1070 p.
13. Head First Design Patterns: A Brain-Friendly Guide: Building Extensible and Maintainable Object-Oriented Software Paperback – 5 Jan. 2021.
14. Refactoring: Improving the Design of Existing Code (Addison-Wesley Signature Series (Fowler)) Hardcover – Illustrated, 2 Jan. 2019.

DOI: 10.58254/viti.7.2025.09.92

УДК 621.391.372

канд. техн. наук, ст. наук. співр. Масесов М. О. ORCID: 0000-0003-4537-4295 (ВІТІ ім. Героїв Крут)

КОНЦЕПТУАЛЬНА МОДЕЛЬ ПРЕДМЕТНОЇ ОБЛАСТІ СИСТЕМИ ЗВ’ЯЗКУ

Із початку повномасштабної збройної агресії російської федерації значно зросла актуальність впровадження та використання сучасних інформаційних і комунікаційних технологій у сфері оборони нашої Держави. Завдяки впровадженню сучасних інформаційних (автоматизованих) систем і систем ситуаційної обізнаності, новітнього озброєння іноземного виробництва та масштабного застосування безпілотних систем постійно зростає об’єм інформації, що передається, підвищується рівень вимог до швидкості передачі даних, достовірності передачі інформації та її безпеки. Вищезазначені фактори стимулюють впровадження в комунікаційні системи нових мережевих та інформаційних технологій, що, в свою чергу, призводить до значного ускладнення системи зв’язку ЗС України, планування, побудови, розгортання та управління.

Нинішні підходи до побудови систем та мереж зв’язку військового призначення, що ґрунтуються на традиційних технологіях і орієнтовані в основному на суб’єктивному позадачному підході, не можуть задовольнити сучасні вимоги щодо швидкості та якості процесу побудови системи зв’язку в повному обсязі. Таким чином, однією з актуальних проблем, що виникає при плануванні зв’язку, є вирішення протиріччя між складністю процесів планування та побудови системи зв’язку, вимогами системи управління, що висуваються, і можливостями посадових осіб. Одним із найбільш оптимальних шляхів виходу з існуючого стану є розробка єдиної методології побудови системи зв’язку, що враховує досвід застосування існуючих (раніше побудованих) систем зв’язку та їх гетерогенність, охоплює сукупність моделей системи, її елементів і процесів їх функціонування, моделей процесу планування і побудови, документів по зв’язку, методів, моделей і алгоритмів, що реалізують обробку, передачу, зберігання і відображення інформації на всіх етапах роботи посадових осіб.

У свою чергу, для розв’язання зазначеної проблеми слід отримати наукові результати, які включають концептуальні основи побудови гетерогенної системи зв’язку, а також теоретичні основи, які визначатимуть єдину конструктивну формальну систему, що описує процес побудови системи зв’язку і вимоги до неї. В рамках вирішення наукової проблеми автором статті запропонована концептуальна модель предметної області системи зв’язку, що призначена для узагальненого опису предметної області і формування часткових моделей об’єктів побудови системи зв’язку, що представляється через множину об’єктів предметної області системи зв’язку, їх властивості, характеристики властивостей, процеси функціонування об’єктів, відносини між об’єктами, стани і ситуації функціонування об’єктів. Наведений матеріал статті стане підґрунтям для подальшого розвитку основ теорії побудови системи зв’язку.

Ключові слова: *система зв’язку, теоретичні основи, предметна область, концептуальна модель, побудова, планування.*

M. Masesov. Conceptual model of the subject area of communication systems

Since the beginning of the full-scale armed aggression of the russian federation, the relevance of the introduction and use of modern information and communication technologies in the defense of our State has significantly increased. Due to the introduction of modern information (automated) systems and situational awareness systems, the latest foreign-made weapons and the large-scale use of unmanned systems, the volume of information transmitted is constantly increasing, the level of requirements for data transmission speed, reliability of information transmission and its security is increasing. The above-mentioned factors stimulate the introduction of new network and information technologies into communication systems, which in turn leads to a significant complication of the communication system of the Armed Forces of Ukraine, planning, construction, deployment and management.

Existing approaches to building military communication systems and networks, based on traditional technologies and focused mainly on a subjective task-based approach, cannot fully meet modern requirements for the speed and quality of the communication system construction process. Thus, one of the current problems that arise in communication planning is to resolve the contradiction between the complexity of the communication system planning and construction processes, the requirements of the management system, and the capabilities of officials. One of the most optimal ways out of the current situation is to develop a single methodology for construction a communication system, which takes into account the experience of using existing (previously built) communication systems and their heterogeneity, covers a set of system models, its elements and their functioning processes, models of the planning and construction process, communication documents, methods, models and algorithms that implement the processing, transmission, storage and display of information at all stages of the work of officials.

In turn, to solve the specified problem, it is necessary to obtain scientific results that include the conceptual foundations of construction a heterogeneous communication system, as well as theoretical foundations that will determine a single constructive formal system that describes the process of building a communication system and the

requirements for it. Within the framework of solving the scientific problem, the author of the article proposed a conceptual model of the subject area of the communication system, which is intended for a generalized description of the subject area and the formation of partial models of objects of building a communication system, which is represented through a set of objects of the subject area of the communication system, their properties, characteristics of properties, processes of functioning of objects, relationships between objects, states and situations of functioning of objects. The presented material of the article will become the basis for further development of the foundations of the theory of building a communication system.

Keywords: *communication system, theoretical foundations, subject area, conceptual model, construction, planning.*

Постановка проблеми

За результатами аналізу бойового досвіду в ході відбиття повномасштабної збройної агресії російської федерації можна зробити висновок про постійну зміну противником характеру, форм і способів ведення операцій (бойових дій), а також наявність і застосування сучасних систем і комплексів радіоелектронної боротьби, які особливо успішно функціонують у тактичній ланці управління. З іншого боку, у ЗС України значно збільшилась кількість і номенклатура наявних засобів зв’язку (особливо радіозв’язку), що включає також складні системи і комплекси зв’язку закордонного виробництва, надані різними країнами-партнерами за останні роки.

Із урахуванням вище зазначеного, у сучасних умовах ведення бойових дій постійно зростають об’єм і складність інформації, необхідної для вирішення задач побудови системи зв’язку та планування зв’язку в цілому. Значно підвищились вимоги до своєчасності планування та обґрунтованості рішень, що приймаються. Існуюча технологія реалізації процесів планування зв’язку та побудови системи зв’язку є “ручною”, характеризується високою трудомісткістю, незадовільно обґрунтованістю рішень з організації та забезпечення зв’язку, не завжди враховує можливості нових інформаційних і комунікаційних технологій.

Таким чином, однією з актуальних проблем, що виникає при плануванні зв’язку, є вирішення протиріччя між складністю процесів планування та побудовою системи зв’язку, вимогами системи управління, що висуваються, і можливостями посадових осіб. Складність вирішення проблеми збільшується з розвитком комунікаційних технологій та складністю обладнання, яке використовується Силами оборони України, постійною й активною протидією противника, зміною системи управління ЗС України, яка переходить на корпусну систему, а також змінами керівних документів з організації зв’язку.

Аналіз останніх досліджень і публікацій

Для побудови системи зв’язку на сьогодні використовуються різноманітні моделі (методики та алгоритми), а також програмне забезпечення для побудови і планування окремих інтервалів (ліній) зв’язку та зон радіопокриття [1–5]. Водночас, продовжується процес оснащення підрозділів зв’язку різноманітним сучасним обладнанням різних виробників, що дозволяє забезпечувати передачу даних у тактичній ланці управління [6]. Впроваджуються інноваційні технологічні рішення як вітчизняного, так і закордонного виробництва [7–10], які значно розширюють функціональні можливості військової техніки і озброєння. Але виконання завдань значно ускладнюють зростаюча гетерогенність системи зв’язку, постійний розвиток комунікаційних технологій, суттєва активна протидія противника засобами радіоелектронної боротьби та радіотехнічної розвідки, а також складність обладнання зв’язку, яке отримується від різних країн-партнерів. З іншого боку, система зв’язку як складова системи управління Збройними Силами України знаходиться в стані постійної трансформації, пов’язаної з переходом до корпусної системи.

Зазначені фактори не повною мірою знаходять своє відображення у керівних документах з організації зв’язку [11; 12]. За результатами проведеного аналізу публікацій з питань теоретичних і практичних основ побудови системи зв’язку зроблено висновок, що загальними недоліками зазначених робіт є використання методів (моделей, алгоритмів)

вузького застосування для вирішення часткових задач, які виникають у процесі побудови системи зв’язку. Відомі онлайн-сервіси для розрахунків окремих складових елементів системи зв’язку часто мають спрощені моделі і не враховують усіх факторів (наприклад, погодні умови, типи антен чи завади).

Недостатній рівень розвитку існуючих наукових теоретичних та практичних методологічних основ побудови системи зв’язку дозволяють зробити висновок про актуальність обраної тематики досліджень.

Одним із найбільш оптимальних шляхів виходу з існуючого стану є розробка єдиної методології побудови системи зв’язку, що враховує досвід застосування існуючих (раніше побудованих) систем зв’язку та їх гетерогенність, охоплює сукупність моделей системи, її елементів і процесів їх функціонування, моделей процесу планування і побудови, документів з організації зв’язку, методів, моделей і алгоритмів, що реалізують обробку, передачу, зберігання і відображення інформації на всіх етапах роботи посадових осіб. У свою чергу, зазначена методологія повинна ґрунтуватися на відповідних концептуальних і теоретичних основах, що формують єдину конструктивну формальну систему та описує процес побудови системи зв’язку і вимоги до неї.

Мета статті

Метою статті є розроблення концептуальної моделі предметної області системи зв’язку, яка призначена для узагальненого опису предметної області та формування часткових моделей об’єктів побудови системи зв’язку, що представляється через множину об’єктів предметної області системи зв’язку, їх властивості, характеристики властивостей, процеси функціонування об’єктів, відносини між об’єктами, стани і ситуації функціонування об’єктів.

Виклад основного матеріалу дослідження

Як було зазначено, побудова системи зв’язку є невід’ємною складовою планування зв’язку, яке здійснюється відповідно до вимог керівних документів на всіх етапах оперативного планування. В свою чергу, побудова системи зв’язку являє собою складний, багатовимірний процес, що здійснюється посадовими особами, відповідно до ділення системи зв’язку на функціональні підсистеми (елементи системи), що включає множину етапів, на яких виконуються різноманітні дії щодо визначення способів побудови системи зв’язку, бойових задач підрозділам зв’язку та розподілу сил і засобів зв’язку для створення системи зв’язку й забезпечення її розгортання і функціонування як в мирний час, так і під час операцій (бойових дій). Умовний розподіл на елементи системи, етапи прийняття рішення та дії (завдання), які виконуються під час побудови системи зв’язку, наведено на рисунку 1.

Для якісної реалізації та опису процесів побудови системи зв’язку слід використовувати глибинні та онтологічні знання про предметну область системи військового зв’язку, що враховують принципи організації зв’язку, правила організаційно-технічної побудови системи зв’язку та фундаментальні фізичні закони функціонування елементів системи зв’язку. Можливість маніпулювання такими знаннями представляється запропонованою *теорією об’єктів побудови системи зв’язку*, *яка призначена* для задання та використання моделей об’єктів побудови (у вигляді множини відношень між змінними, що відображають структуру, параметри і функціонування елементів системи зв’язку, факторів, які на них впливають, показники ефективності та ін.).

Основу зазначеної теорії складають сімейство моделей, що описують об’єкти побудови для реалізації процесів побудови системи зв’язку, в тому числі – концептуальна модель предметної області.

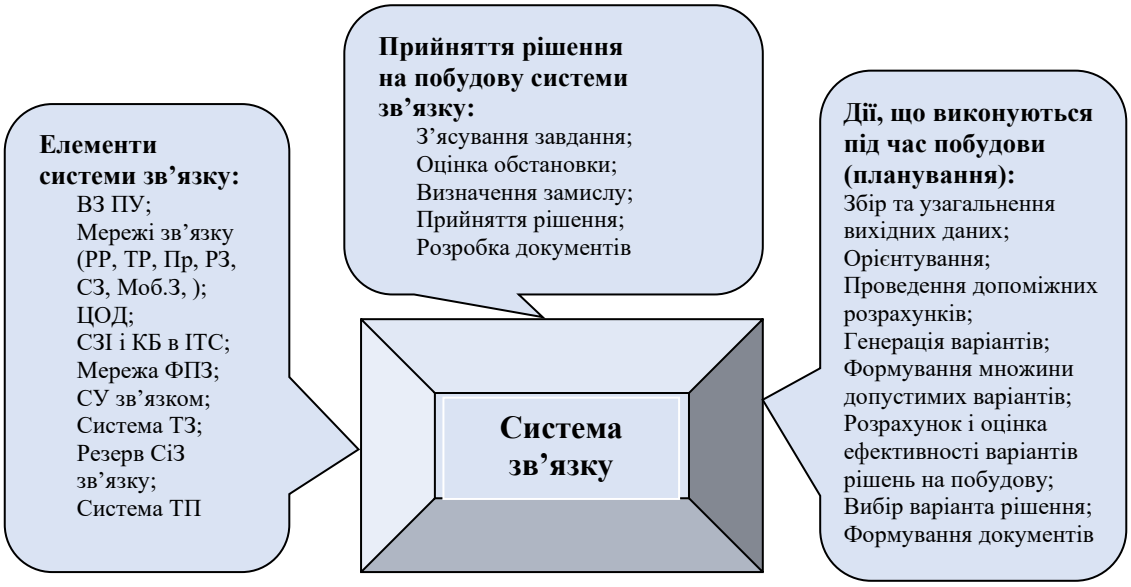


Рис. 1. Побудова системи зв’язку як багатовимірний процес

Нижче викладено основні поняття теорії об’єктів побудови системи зв’язку.

Концептуальна модель предметної області системи зв’язку ($M_{ПрО}$) відображає класифікаційну схему об’єктів, фіксує склад основних понять систем військового зв’язку та стійкі взаємозв’язки між ними, а також визначає побудову часткових моделей об’єктів побудови:

$$M_{ПрО} = <O, P, C, F, R, S, U>,$$

де O – множина об’єктів предметної області системи зв’язку;
P – множина властивостей об’єктів;
C – множина характеристик (атрибутів) властивостей;
F – множина процесів функціонування об’єктів;
R – множина відносин між об’єктами;
S і U – множини станів та ситуацій функціонування об’єктів.

Об’єкти являють собою деякі матеріальні або абстрактні сутності предметної області системи зв’язку, яким можуть відповідати як власне об’єкти побудови (система зв’язку, елементи системи зв’язку, в т. ч. засоби та комплекси зв’язку), так і об’єкти, що впливають на них (фізико-географічні умови, сили і засоби противника та ін.): $O = \{o_i\} = \{o_{i1}\} \cup \{o_{i2}\}$, $i = 1,\ldots, I$, де I – потужність множини об’єктів; $\{o_{i1}\}$ – множина об’єктів побудови; $\{o_{i2}\}$ – множина об’єктів, що впливають на об’єкти побудови. Формування безлічі об’єктів предметної області системи зв’язку для реалізації процесу побудови має полягати у фіксації всіх понять-об’єктів, якими оперують посадові особи органів управління зв’язком у процесі побудови системи зв’язку. Об’єкти можуть бути простими та складними, що включають прості об’єкти.

Властивість – деяка сторона сутності предметної області: $P = \{p_j\}$, $j = 1,\ldots, J$, де J – потужність множини властивостей. Приклади властивостей: бойова готовність системи зв’язку, пропускна спроможність лінії зв’язку та ін.

Характеристика – міра наявності властивості в сутності предметної області: $C = \{c_k\}$, $k = 1,\ldots, K$, де K – потужність множини характеристик. Приклади характеристик – вид зв’язку, тип кабелю і т. п.

Під *процесом* слід визначити взаємодію об'єктів предметної області, що полягає у зміні їх характеристик: $F = <\{o_t\}, \{c_{ot}\}>$, де $\{o_t\}$, $t \subseteq \{1,...,I\}$ – множина об'єктів, що беруть участь у процесі, $\{c_{ot}\}$ – множина їх характеристик. При цьому розглядаються як процеси власне функціонування елементів системи зв'язку (наприклад, передачі інформації по каналу зв'язку, обробки інформації в апаратній тощо), так і процеси керування ними (наприклад, розгортання кабельної лінії, налаштування каналу, налаштування передавача тощо).

Відношення – форма прояву взаємозв'язку об'єктів предметної області: $R = R_S \cup R_A \cup R_F$, де:

$R_S = \{r_{РВ}, r_{ЦЧ}, r_{УО}, r_{РС}, r_{ДМ}, r_С\}$ – *відношення структурного опису* (класу "об'єкт – об'єкт" і "процес – процес"); $r_{РВ}$ – відношення типу "рід – вид" (для структуризації об'єктів і процесів); $r_{ЦЧ}$ – "ціле – частина" (для опису складних об'єктів або процесів через прості із зазначенням послідовного або паралельного з'єднання частин, що дозволяє розчленувати процес над об'єктом на сукупність процесів над кожною з його частин); $r_{УО}$ – "умова – обмеження" (для опису умовних структур об'єктів та процесів); $r_{РС}$ – "ресурс – споживач" (для опису логічного взаємозв'язку об'єктів і процесів); $r_{ДМ}$ – "джерело впливу – мета впливу" (для опису впливу об'єктів на процес); $r_С$ – "синонімія" (для задання зав'язків між синонімами понять об'єктів і процесів);

$R_A = \{r_{ОВ}, r_{ВХ}, r_{ОХ}, r_{ХЗ}\}$ – *відношення подання атрибутів* (класу "об'єкт – характеристика" або "процес – характеристика"); $r_{ОВ}$ – (або $r_{ПВ}$) відношення типу "об'єкт – властивість" ("процес – властивість"); $r_{ВХ}$ – "властивість – характеристика"; $r_{ОХ}$ (або $r_{ПХ}$) "об'єкт – характеристика" ("процес – характеристика"); $r_{ХЗ}$ – "характеристика – значення";

$R_F = \{r_{ВП}, r_{ПВ}, r_{ПЕ}, r_{ПН}, r_{ПС}, r_О, r_{ОВ}, r_{ПР}, r_{ПІ}, r_{ОС}\}$ – *відношення опису функціонування об'єктів* (класу "об'єкт – процес" і "процес – процес"); $r_{ВП}$ – відношення типу "виконувати процес" (для опису процесу функціонування об'єктів); $r_{ПВ}$ – "процес – варіант реалізації" (для задання різних варіантів виконання процесів); $r_{ПЕ}$ – "процес – етапи процесу" (для задання часової послідовності реалізації процесу шляхом перерахування складових його етапів); $r_{ПН}$ – "причина – наслідок" (для задання причини виконання процесів); $r_{ПС}$ – "передує – слідує" (для задання послідовності виконання процесів); $r_О$ – "одночасно" (для задання одночасності виконання процесів); $r_{ОВ}$ – "процес – об'єкт впливу" (для опису об'єкта побудови, на який впливає процес); $r_{ПР}$ – "процес – ресурс" (для опису використовуваного процесом ресурсу); $r_{ПІ}$ – "процес – інструмент" (для завдання об'єкта, що реалізує процес); $r_{ОС}$ (або $r_{ПСс}$) – "об'єкт – стан" (або "процес – стан") та ін.

Приклади типів відносин між процесами, що задають відновлення та розгортання об'єктів побудови, наведено на рисунку 2.

Стани об'єктів побудови фіксують значення характеристик властивостей об'єктів $S = \{s_{oi}\}$, де s_{oi} – стан i-го об'єкта, $i = 1,\ldots, I$. Зміна станів об'єктів побудови визначається процесами і відбувається внаслідок змін значень характеристик властивостей об'єктів через як внутрішні, так і зовнішні причини. Зміна станів об'єктів побудови призводить до зміни стану об'єктів, що взаємодіють. Внутрішні причини зміни стану об'єктів побудови пов'язані з процесами, що протікають в елементах об'єктів (наприклад, з відмовами або пошкодженнями засобів зв'язку), зовнішніми причинами є вплив зовнішніх факторів.

Стани об'єктів побудови характеризують ситуації, у яких перебувають об'єкти. *Ситуація* – сукупність об'єктів, їх станів і відносин між ними, зафіксована в певний момент часу: $U = \{ \{o_t\}, \{s_{ot}\}, \{r(o_1,...,o_m)\} \}$, де $\{o_t\}$, $t \subseteq \{1,...,I\}$ – залучений у ситуацію об'єкт; m – кількість задіяних об'єктів; s_{ot} – стан t-го об'єкта; $r(o_1,...,o_m)$ – екземпляр відносин на об'єктах $1 \div m$.

Рис. 2. Відношення між процесами на прикладі процесу розгортання ділянки радіорелейної лінії (РРС – радіорелейна станція)

У процесі побудови системи зв’язку повинні використовуватися різні моделі об’єктів побудови, що задають їх на різних рівнях деталізації, в різних аспектах, з використанням різних способів подання. Атрибути об’єктів побудови у різних моделях можуть відображати у ряді випадків аналогічні параметри, хоча їх значення можуть бути несумісними (наприклад, виражатися якісно чи кількісно). Для комплексування різних моделей та їх уявлень пропонується використовувати *поняття метамоделі* як інтегральної базової моделі об’єктів побудови, за допомогою якої можна уникнути проблему комбінаторного зростання складності реалізації відображень і підтримання узгодженості між різними моделями. Коли одна модель модифікується внаслідок, наприклад, результатів аналізу варіантів рішень, механізмами метамоделі здійснюється перевірка виконання заданих вимог та обмежень і поширення змін на інші моделі відповідно до знань про відносини між поняттями предметної області. Для визначення відносин між різними моделями необхідні знання, що належать до рівня базової теорії предметної області системи зв’язку. Це онтологічні знання про середовище моделювання, способи створення моделей на основі використання понять, визначених у базовій теорії.

На основі запропонованої концептуальної моделі $M_{ПрО}$ слід визначити *послідовність формування часткових моделей* об’єктів побудови. Ступінь деталізації моделей об’єктів планування визначається сутністю завдань планування та побудови зв’язку, які вирішуються з використанням даних моделей. Після формування безлічі об’єктів O, їх властивостей P і характеристик C на зазначених множинах задаються відносини R_S структурного опису і R_A подання атрибутів. Далі знаходяться обмеження на значення C та виявляються відповідні стани S об’єктів побудови. Потім за допомогою визначення взаємодіючих об’єктів, а для кожного об’єкта його початкового та кінцевого стану, визначаються процеси F

функціонування об’єктів побудови. На отриманій множині об’єктів і процесів задаються відносини R_F опису функціонування об’єктів. Наступним кроком є декомпозиція процесів – вся множина процесів за рахунок визначення відносин R_S структурного опису представляється у вигляді дерева, що відповідає дереву об’єктів. Оскільки властивості об’єктів побудови можна розглядати як прояв взаємодії їх елементів, то будь-який процес можна уявити через процеси, у яких беруть участь прості об’єкти. Моделі складних об’єктів будуються як з урахуванням комплексування моделей простих об’єктів, так і на основі незалежних абстрагованих від нижніх рівнів моделей. Нарешті за допомогою відстеження ланцюжків взаємодіючих процесів додатково визначаються відносини R_F опису функціонування об’єктів – пари залежних процесів, виявлених під час аналізу, що утворюють допоміжні підмножини, у яких встановлюються співвідношення “причина – наслідок” та ін.

Висновки та перспективи подальших досліджень

Розроблена концептуальна модель предметної області системи зв’язку призначена для узагальненого опису предметної області і формування часткових моделей об’єктів побудови системи зв’язку, що представляється через множину об’єктів предметної області системи зв’язку, їх властивості, характеристики властивостей, процеси функціонування об’єктів, відносини між об’єктами, стани і ситуації функціонування об’єктів.

Представлені в роботі результати будуть корисними для фахівців з питань обґрунтування технологічних рішень при побудові мереж (систем) зв’язку спеціального призначення. Крім того, матеріал буде корисним науковцям та здобувачам, які здійснюють наукові дослідження в галузі зв’язку та електронних комунікацій.

Напрямками подальших досліджень є:

розвиток методології побудови системи зв’язку тактичної (оперативної, стратегічної) ланки управління;

розширення і деталізація основ теорії побудови системи зв’язку, в тому числі удосконалення розроблених моделей елементів системи зв’язку, процесів побудови системи зв’язку, прийняття рішень при побудові системи зв’язку;

розроблення (удосконалення) методологічного апарату оцінки ефективності функціонування системи зв’язку;

практична реалізація наукових досліджень для побудови інтелектуальних (інтегрованих, інтерактивних) систем військового призначення, в т. ч. програмного і математичного забезпечення існуючих та перспективних інформаційних (автоматизованих) систем управління військами і зв’язком.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Коваленко І. Г., Масесов М. О., Драглюк О. В., Ткаченко А. Л. Методика побудови радіорелейних ліній на основі використання геопросторової інформації. *Системи і технології зв’язку, інформатизації та кібербезпеки*. 2023. Вип. 3. С. 31–40. DOI: https://doi.org/10.58254/viti.3.2023.04.31. ISSN 2786-6610.

2. Бондаренко Л. О., Масесов М. О., Коваленко І. Г., Руденко В. І., Шугалій О. О. Узагальнена методика оцінки застосування супутникових ретрансляторів зв’язку за цільовим призначенням. *Системи і технології зв’язку, інформатизації та кібербезпеки*. 2024. Вип. 5. С. 52–63. DOI: 10.58254/viti.5.2024.04.52. ISSN 2786-6610.

3. A free tool for amateur Radio. URL: http://www.ve2dbe.com/rmonline_s.asp.

4. EverythingRF Link Budget Calculator. URL: https://www.everythingrf.com/rf-calculators/link-budget-calculator.

5. Онлайн-інструмент для аналізу зон видимості та базового радіопокриття на основі даних SRTM (Shuttle Radar Topography Mission). URL: http://www.heywhatsthat.com/.

6. Остапчук В. М. Масесов М. О. Зінченко М. О. Думітраш В. О. Перспективи розвитку системи та засобів зв’язку спеціального призначення з урахуванням впровадження мереж LTE. *Системи і технології зв’язку, інформатизації та кібербезпеки*. 2024. № 6. С. 153–160. DOI: https://doi.org/10.58254/viti.6.2024.12.153. ISSN 2786-6610.

7. Лаврут О. О., Лаврут Т. В., Климович О. К., Здоренко Ю. М. Новітні технології та засоби зв’язку у Збройних Силах України: шлях трансформації та перспективи розвитку. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. № 1 (34). С. 91–101. URL: https://doi.org/10.30748/nitps.2019.34.13.

8. Масесов М. О. Перспективи побудови гетерогенної системи зв’язку тактичної ланки управління. *Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку:* зб. матеріалів IV Міжнар. науково-техн. конф. (Київ, 28 листоп. 2024 р.) Київ, 2024. С. 96.

9. Лазута Р. Р. та ін. Військова навчально-методична публікація щодо застосування технології LTE (4G) системи зв’язку у військових частинах Збройних Сил України. *Матеріали вивчення бойового досвіду застосування Збройних Сил України*. Київ: НЦЗІ ВІТІ. 20 с.

10. Радзівілов Г. Д., Масесов М. О, Дєгтяр О. А. Світові тенденції зі створення та розвитку військової техніки. *Комп’ютерно-інтегровані технології: освіта, наука, виробництво*. 2024. Вип. 56. С. 381–385. DOI: https://doi.org/10.36910/6775-2524-0560-2024-56-45.

11. ДДП 6-26.22. Настанова “Зі зв’язку Збройних Сил України”. Київ: Головне управління зв’язку та кібербезпеки Генерального штабу (J6) Збройних Сил України, 2025. 256 с. (Для службового користування).

12. Шолудько В. Г., Єсаулов М. Ю., Вакуленко О. В. та ін. Організація військового зв’язку: навч. пос. Київ: Вид. дім “Скіф”, 2023. 280 с. ISBN 978-966-570-839-8.

DOI: 10.58254/viti.7.2025.10.100

УДК.621.396

канд. техн. наук Нестеренко І. К. ORCID: 0009-0003-9423-8203 (ВІТІ ім. Героїв Крут)

СПРОЩЕНИЙ МЕТОД РОЗРАХУНКУ КОЕФІЦІЄНТА ЧАСТОТНОЇ ВИБІРКОВОСТІ ПРИЙМАЧА

Через збільшення кількості діючих радіоелектронних засобів загостюється проблема забезпечення електромагнітної сумісності. Особливо ця проблема актуальна для систем радіозв'язку у найбільш небезпечних завадових ситуаціях, в яких по основному каналу приймача приймається основне випромінювання передавача завади. У таких випадках для розрахунку рівня завади потрібно враховувати коефіцієнт частотної вибірковості приймача (частотно залежне продавлення – frequency dependent rejection, FDR). Для розрахунку коефіцієнта частотної вибірковості приймача використовують аналітичні або спрощені графічні методи, які передбачають наявність вихідних даних стосовно спектральної маски сигналу передавача завади та форми амплітудно-частотної характеристики приймача [1–4; 7–9], але зазвичай необхідних для розрахунку даних стосовно спектральних властивостей даного випромінювання та амплітудно-частотної характеристики приймача недостатньо.

У роботі запропонований спрощений інженерний метод розрахунку коефіцієнта частотної вибірковості приймача, у якому вихідними даними, відносно спектра передавача, є лише ширина необхідної смуги випромінювання та ширина займаної смуги частот, а спектральну маску передавача та амплітудно-частотної характеристики приймача представлено у вигляді трапеції.

Застосування пропонованого інженерного методу дозволить в умовах нестачі вихідних даних, стосовно спектральних масок випромінювання передавача та амплітудно-частотної характеристики фільтра проміжної частоти приймача розраховувати коефіцієнт частотної вибірковості приймача та визначати забезпечення електромагнітної сумісності з достатньою для практичних застосувань точністю.

Ключові слова: *електромагнітна сумісність, основний канал прийому приймача, основне випромінювання передавача, завада, спектральна маска сигналу передавача завади, амплітудно-частотна характеристика приймача, коефіцієнт частотної вибірковості приймача.*

I. Nesterenko. Simplified method of calculation coefficient of frequency selectivity of the receiver

In connection with the increase in the number of active radio-electronic means, the problem of ensuring electromagnetic compatibility is increasing. This problem is especially relevant for radio communication systems in the most dangerous interference situations, in which the main radiation of the interfering transmitter is received on the main channel of the receiver. In such cases, the frequency selectivity coefficient of the receiver (frequency dependent rejection) must be taken into account to calculate the interference level. To calculate the frequency selectivity coefficient of the receiver, analytical or simplified graphical methods are used, which require the availability of initial data regarding the spectral mask of the interference transmitter signal and the shape of the amplitude-frequency characteristic of the receiver [1–4; 7–9]. But usually, the data required for calculating the spectral properties of this radiation and the amplitude-frequency characteristic of the receiver are not enough.

The paper proposes a simplified engineering method for calculating the frequency selectivity coefficient of the receiver, in which the output data relative to the spectrum of the transmitter are only the width of the necessary radiation band and the width of the occupied frequency band, and the spectral mask of the transmitter and the amplitude-frequency characteristic of the receiver is presented in the form of a trapezoid.

The application of the proposed engineering method will make it possible to calculate the coefficient of frequency selectivity of the receiver and determine the provision of electromagnetic compatibility with sufficient accuracy for practical applications, in the absence of initial data regarding the spectral masks of the transmitter radiation and the amplitude-frequency characteristic of the intermediate frequency filter of the receiver.

Keywords: *electromagnetic compatibility, the main receiving channel of the receiver, the main radiation of the transmitter, interference, the spectral mask of the interference transmitter signal, the amplitude-frequency characteristic of the receiver, the coefficient of frequency dependent rejection.*

Постановка завдання. Задача забезпечення електромагнітної сумісності (ЕМС) в умовах дії ненавмисних завад з часом загострюється. Для визначення електромагнітної сумісності потрібно розрахувати рівні корисного сигналу, завад та шумів і перевірити виконання критерію ЕМС. При врахуванні впливу завад, найбільш небезпечніша ситуація виникає при прийомі по основному каналу приймача основного випромінювання передавача завади. У такому випадку для розрахунку потужності завади на вході приймача потрібно

визначити частину потужності завади, що попадає в смугу пропускання приймача, яка зазначається як коефіцієнт частотної вибірковості *FDR*.

Аналіз останніх досліджень. Вихідними даними для розрахунку *FDR* є спектральні маски сигналу, що задають максимально допустимі значення позасмугових випромінювань передавача завади, які не мають бути перевищені у реальному передавачі радіоелектронного засобу (РЕЗ) та дані (маски) за характеристикою вибірковості приймача. Значення коефіцієнта частотної вибірковості приймача визначається шляхом розрахунку площі перекриття спектральної маски випромінювань передавача-джерела завади і амплітудно-частотної характеристики (АЧХ) фільтра (вхідного або проміжної частоти) приймача-рецептора цієї завади та заданому частотному рознесенні несучих частот сигналу завади і корисного сигналу. Для розрахунку площі перекриття застосовують чисельні методи інтегрування. Для спрощення розрахунків використовують графічний метод, для застосування якого спектральні маски задаються у виді кусочно-лінійної функції частоти. Така маска може бути поділена на кілька ділянок, причому, площа під кривою кожної ділянки являє собою його "внесок" у спектр сигналу.

Через нестачу вихідних даних, стосовно спектральних масок випромінювання передавача і АЧХ фільтра проміжної частоти (ПЧ) приймача та враховуючи те, що вихідними даними відносно спектра передавача у більшості випадків є лише ширина необхідної смуги випромінювання (necessary bandwidth) та ширина займаної смуги (occupied bandwidth – OCW), спектральну маску передавача та АЧХ приймача для розрахунку співканальної частотної вибірковості можна представити у вигляді трапеції [4]. У методиці розрахунків **е**лектромагнітної сумісності для присвоєння радіочастот радіоелектронним засобам рухомої служби [4] наведений приклад розрахунку *FDR* для двох найпростіших випадків перекриття спектра випромінювання передавача та АЧХ приймача: а) ширина смуги частот випромінювань передавача, який створює завади, менша за ширину смуги пропускання приймача, який відчуває вплив цієї завади, а весь спектр випромінювань передавача потрапляє у смугу пропускання приймача; б) ширина смуги частот випромінювань передавача, що створює завади, більша за ширину смуги частот приймача, яка відчуває влив цієї завади, а частина спектра випромінювань передавача потрапляє у смугу частот приймача.

Недоліком вищерозглянутої методики є те, що в них не запропонований порядок розрахунку FDR у випадках, коли спектри завади та АЧХ приймача перекриваються частково (не все випромінювання передавача знаходиться у межах смуги пропускання приймача, а лише його частина).

Метою статті є вирішення наукового завдання щодо розробки спрощеного інженерного методу розрахунку коефіцієнта частотної вибірковості приймача для усіх можливих випадків перекриття спектральної маски завади та АЧХ приймача за умови нестачі вихідних даних стосовно частотних властивостей завади та приймача.

Виклад основного матеріалу

Рівень радіозавад у приймачі є функцією посилень і втрат, яким піддається сигнал завади на шляху від джерела завади до приймача, може бути представлений наступними формулами [2]:

$$P_I = P_{Tx} + G_{Tx} + G_{Rx} - L_{prop} - FDR(\Delta f), \quad \text{дБВт}, \tag{1}$$

де P_I – потужність завади у приймачі, *дБВт*;

P_{Tx} – потужність передавача завади, *дБВт*;

G_{Tx} – коефіцієнт підсилення антени джерела завади у напрямку приймача, *дБі*;

G_{Rx} – коефіцієнт підсилення антени приймача у напрямі джерела завади, *дБі*;

L_{prop} – основні втрати сигналу при поширенні радіохвиль на трасі між джерелом завади та приймачем, *дБ*;

$$FDR(\Delta f) = 10 \times \lg \frac{\int_0^\infty P(f)\,\mathrm{d}f}{\int_0^\infty P(f)|H(f+\Delta f)|^2\,\mathrm{d}f}, \quad \text{дБ}, \tag{2}$$

де $FDR(\Delta f)$ – коефіцієнт частотної вибірковості приймача;

$P(f)$ – еквівалентна спектральна щільність потужності сигналу завади на проміжній частоті (ПЧ), спектральна маска передавача;

$H(f)$ – частотна характеристика тракту ПЧ (вибірковість приймача);

Δf – рознесення частот між передавачем, що заважає, і приймачем, що зазнає заваду:

$$\Delta f = f_{Tx} - f_{Rx}, \tag{3}$$

де f_{Tx} – частота налаштування передавача завади;

f_{Rx} – частота налаштування приймача.

Фізичний зміст коефіцієнта частотної вибірковості приймача (*FDR*) полягає у визначенні частини потужності завади, яка попадає в смугу пропускання приймача (рис. 1). На рисунку наведена АЧХ приймача (по центру) та спектральна маска сигналу завади (крива справа).

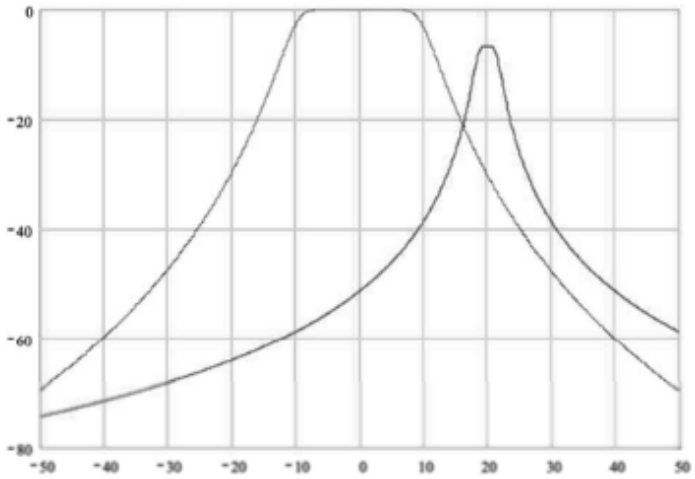


Рис. 1. Фізичний зміст коефіцієнта частотної вибірковості приймача (*FDR*)

Значення коефіцієнта частотної вибірковості приймача визначається шляхом розрахунку площі перекриття спектральної маски випромінювань передавача-джерела завади і АЧХ фільтра (вхідної або проміжної частоти), приймача-рецептора цієї завади та заданому частотному рознесенні несучих частот сигналу завади і корисного сигналу.

У свою чергу, *FDR* може бути розбитий на два члени: – *коефіцієнт співканальної вибірковості (on- tune rejection – OTR) і коефіцієнт позаканальної вибірковості (off-frequency rejection – OFR):*

$$FDR(\Delta f) = OTR + OFR(\Delta f), \quad \text{дБ}. \tag{4}$$

Коефіцієнт позаканальної вибірковості (*OFR*) являє собою ослаблення сигналів у вхідних ланцюгах приймача (преселектора) на відповідній частоті.

Основний канал прийому – смуга частот, що знаходиться в межах смуги пропускання приймача. Завада основним каналом прийому можлива, якщо виконується умова

$$\Delta f \leq (B_{\text{Tx}} + B_{\text{Rx}})/2, \tag{5}$$

де B_{Tx} *і* B_{Rx} – відповідно ширина займаної смуги випромінювання передавача і смуги пропускання приймача.

Для розрахунку *FDR* необхідні спектральні маски сигналу, які задають максимально допустимі значення позасмугових випромінювань, що не мають бути перевищені у реальному передавачі РЕЗ.

Для отримання найбільш реалістичного значення цього коефіцієнта варто використовувати тільки достовірні дані (маски) по характеристиці вибірковості приймача і за спектром сигналу передавача, які отримані безпосередньо від виробника даного устаткування або в результаті його сертифікації (т. зв. маски) [2]. При цьому, інтеграли у формулі (2) доцільно розраховувати на ЕОМ за допомогою одного з числових методів інтегрування функцій, заданих у табличному вигляді. У ряді випадків цей інтеграл можна також обчислити й аналітично, але для цього необхідно попередньо апроксимувати спектр передавача і вибірковість приймача функціями, які легко інтегруються.

Найчастіше замість реального спектра сигналу передавача, що заважає, на практиці використовується його огинаюча (маска), яка задається у виді кусочно-лінійної функції частоти. Це обумовлено відносною простотою усіх розрахунків із використанням лінійних функцій. Така маска може бути поділена на кілька ділянок, причому площа під кривою кожної ділянки являє собою його "внесок" у спектр сигналу.

Аналогічним чином задається маска амплітудно-частотної характеристики приймача.

Очевидно, що чим більше число плоских і похилих (що чергуються між собою) ділянок буде містити огинаюча, тим точніше вона буде описувати реальний спектр сигналу передавача або АЧХ приймача.

У нормативних документах [4; 7–9] рекомендовано проводити розрахунок коефіцієнта частотної вибірковості приймача графічним методом.

Метод графічного розрахунку коефіцієнта частотної вибірковості приймача використовується лише в тому випадку, коли відомі характеристики стандартизованих спектральної маски випромінювань передавача-джерела завади і АЧХ приймача-рецептора завади.

Відповідно до цього методу значення коефіцієнта частотної вибірковості приймача визначається шляхом розрахунку площі перекриття спектральної маски випромінювань передавача-джерела завади (амплітудно-частотного спектра АЧС) і АЧХ фільтра приймача-рецептора цієї завади та заданому частотному рознесенні несучих частот сигналу завади і корисного сигналу шляхом перемноження спектральних масок (рис. 2).

Для визначення площі області перекриття пропоновано її розділити на елементи, які відповідають прямокутним ділянкам області перекриття і ділянкам з нахилом [8].

При цьому, для розрахунку площі області перекриття на спектральній масці випромінювань передавача і АЧХ фільтра приймача визначається щонайменше шість точок, кожна з яких характеризується відповідним ослабленням і частотним розстроєнням.

Далі пропонується розрахувати площу кожного елемента, який відповідає різним ділянкам області перекриття, а потім ці площі підсумувати.

В окремих випадках, а саме за відсутності АЧХ фільтра приймача, що досліджується, в розрахунках може використовуватися спектральна маска випромінювань передавача, яка для цього приймача є джерелом корисного сигналу.

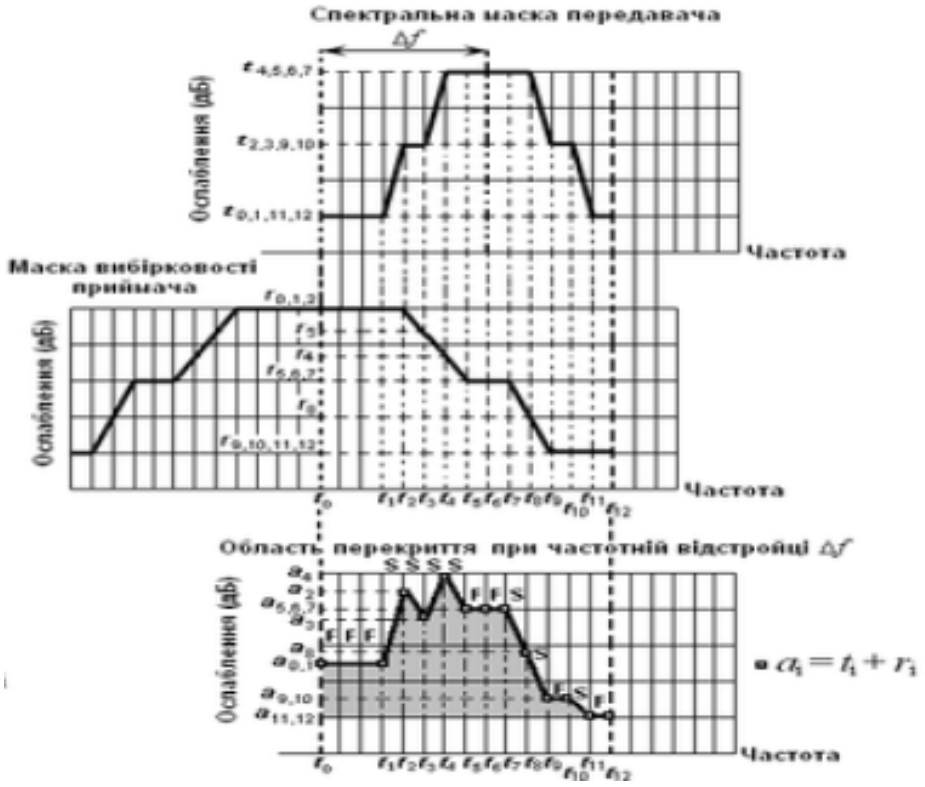


Рис. 2. До визначення області перекриття спектральної маски випромінювань передавача-джерела завади та АЧХ фільтра приймача-рецептора завади

У більшості випадків характеристики спектральної маски випромінювань передавача-джерела завади і АЧХ фільтра приймача-рецептора завади невідомі. Наприклад, у картці тактико-технічних даних радіоелектронного засобу наведені лише необхідна смуга частот і займана смуга частот [5]. Відповідно до пп. 1.152 і 1.153 Регламенту радіозв’язку (РР) МСЕ «необхідна смуга частот» (“necessary bandwidth”) і «займана смуга частот» (“occupied bandwidth”) є основою для визначення спектральних властивостей даного випромінювання або класу випромінювання у найпростіший спосіб [6].

Здебільшого дані стосовно АЧХ фільтра преселектора (ВЧ фільтра) відсутні. Тому зазвичай розрахунок *FDR* виконується у разі наявності джерел завад основним каналом прийому від основного випромінювання передавача, тобто розраховується коефіцієнт співканальної вибірковості на проміжній частоті.

У зв’язку з нестачею вихідних даних, стосовно спектральних масок випромінювання передавача та АЧХ фільтра ПЧ приймача та враховуючи те, що вихідними даними, відносно спектра передавача, у більшості випадків є лише ширина необхідної смуги випромінювання $B_{\text{нТх}}$ та ширина займаної смуги – $B_{\text{Тх}}$ спектральну маску передавача та АЧХ приймача для розрахунку співканальної частотної вибірковості можна представити у вигляді трапеції (рис. 3) [4].

Іноді для спрощення розрахунків *FDR* замість використання формули (2), яка передбачає множення спектральної маски завади та АЧХ приймача, використовують спрощену апроксимацію [2]. Пропонується для спрощення розрахунку замість операції множення спектрів та їх інтегрування визначати загальний (співканальний) *FDR* так:

$$FDR = 10 \times \lg(S_{\text{Тх}}/S_{\text{i}}) + 10 \times \lg(S_{\text{Rx}}/S_{\text{i}}), \quad \text{дБ}, \tag{6}$$

де S_i – площа спектра випромінювання передавача завади, яка потрапляє у смугу пропускання приймача (область перекриття спектральної маски випромінювань передавача-джерела завади та АЧХ фільтра ПЧ приймача-рецептора завади, індекс "i" – interference);

S_{Tx} – площа спектра випромінювання передавача завади;

S_{Rx} – площа АЧХ фільтра ПЧ приймача.

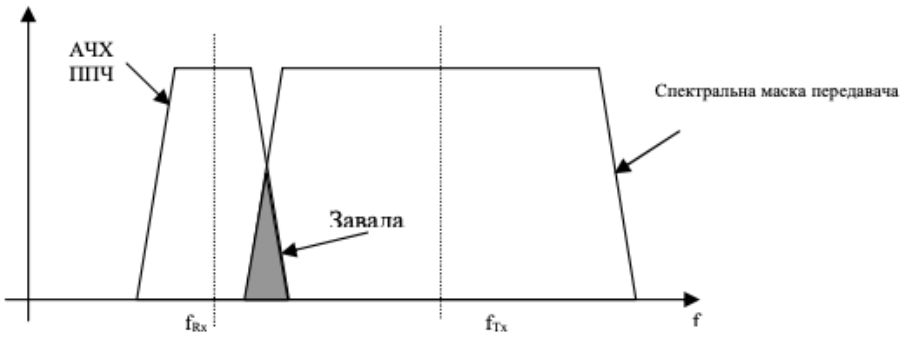


Рис. 3. До визначення області перекриття спектральної маски випромінювань передавача-джерела завади та АЧХ фільтра ПЧ приймача-рецептора завади

Як відомо, площа трапеції S визначається за формулою:

$$S = \frac{1}{2}(a + b)h, \tag{7}$$

де a, b – довжини відрізків (основ) трапеції;

h – висота трапеції.

Для сигналів усіх класів випромінювання, окрім спеціально обумовлених, ширина займаної смуги B_{Tx} не повинна перевищувати ширину необхідної смуги $B_{нTx}$ більш ніж на 20 % ($B_{Tx} \leq 1{,}2 \cdot B_{нTx}$). Враховуючи, що висота трапеції нормована ($h = 1$), а займана смуга частот пов'язана у більшості випадків з необхідною смугою частот коефіцієнтом *1,2*, площа АЧХ приймача становить:

$$S_{Tx} = 1{,}1 \times B_{нTx}, \tag{8}$$

$$S_{Rx} = 1{,}1 \times B_{нRx}. \tag{9}$$

Якщо припустити, що ширина смуги частот випромінювань передавача, який створює завади, менша за ширину смуги пропускання приймача, який відчуває вплив цієї завади ($S_i = S_{Tx}$), а *весь спектр випромінювань передавача потрапляє у смугу пропускання приймача* (рис. 4), тобто виконуються наступні умови:

$$B_{нTx} \leq B_{нRx} \quad \text{і} \quad \Delta f \leq (B_{Rx}/2 - B_{Tx}/2), \tag{10}$$

де $B_{нTx}$ та $B_{нRx}$ (на рисунку – $B_{пр}$) – необхідна ширина смуги частот передавача (АЧХ приймача);

B_{Tx} та B_{Rx} – ширина займаної смуги частот передавача і приймача.

Формула (6) для розрахунку коефіцієнта частотної вибірковості *FDR* спрощується та має наступний вигляд:

$$FDR = 10 \times \lg(B_{нRx}/B_{нTx}), \quad \text{дБ}. \tag{11}$$

Пояснення наведено на рисунку 4.

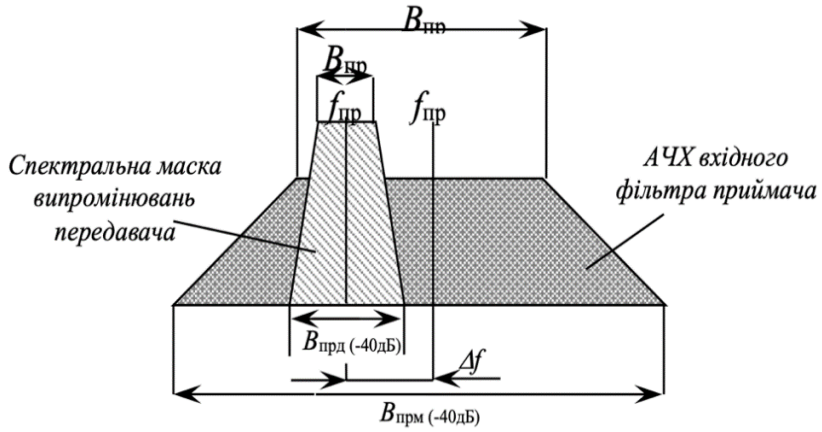


Рис. 4. До визначення коефіцієнта частотної вибірковості при $B_{нRx} > B_{нTx}$

Якщо ширина смуги частот випромінювань передавача, що створює завади, більша за ширину смуги частот приймача ($S_i = S_{Rx}$), що відчуває влив цієї завади, а частина спектра випромінювань передавача потрапляє у смугу частот приймача (рис. 5), тобто одночасно виконуються умови:

$$B_{нTx} > B_{нRx} \quad \text{і} \quad \Delta f \le (B_{Tx}/2 - B_{Rx}/2), \tag{12}$$

коефіцієнт частотної вибірковості розраховується за спрощеною формулою [2; 4]:

$$FDR = 10 \times \lg (B_{нTx}/B_{нRx}), \quad \text{дБ}. \tag{13}$$

Пояснення наведено на рисунку 5.

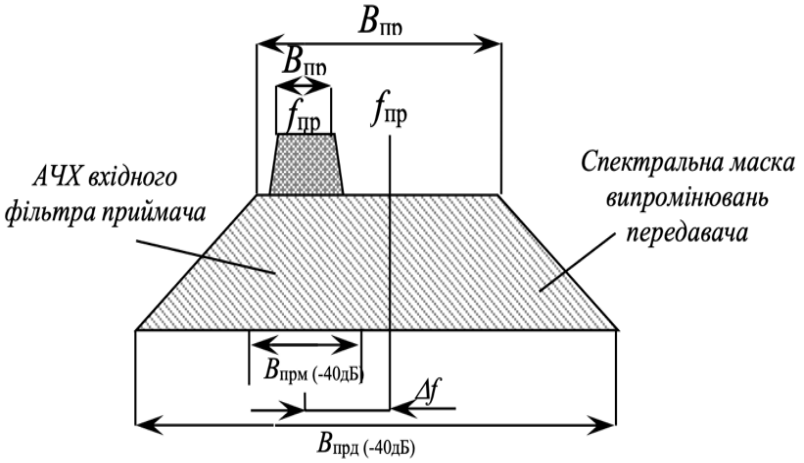


Рис. 5. До визначення коефіцієнта частотної вибірковості приймача при $B_{Rx} < B_{Tx}$

Якщо спектри завади та АЧХ приймача перекриваються частково (не все випромінювання передавача знаходиться у межах смуги припускання приймача, а лише його частина), потрібно розрахувати площу перекриття спектрів та визначити її долю у площі АЧХ приймача.

Спектральні маски можуть перекриватися тільки на рівні займаних смуг частот (як це показано на рис. 3). У такому випадку площа перекриття має вигляд трикутника. Якщо спектральні маски перекриваються так як показано на рисунку 6, площа перекриття має вигляд нерівнобедреної трапеції та складається з прямокутника (перекриття на рівні необхідних смуг частот) та двох прямокутних трикутників для T_x та R_x.

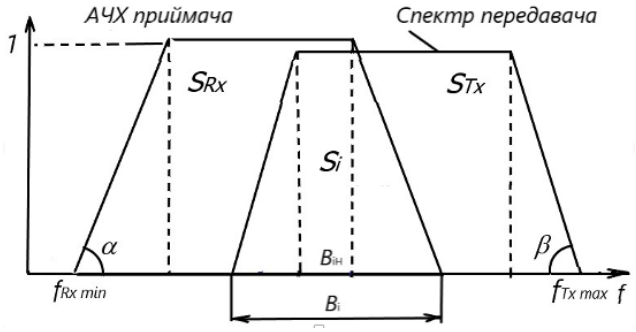


Рис. 6. До визначення області перекриття спектральної маски

У такому випадку умовою прийому завади основним каналом прийому приймача від основного випромінювання передавача завади для необхідної смуги частот буде нерівність:

$$\Delta f \leq (B_{нTx} + B_{нRx})/2. \tag{14}$$

Якщо умова (14) виконується площа перекриття розраховується за формулою:

$$S_i = S_{ПР.ВН.} + S_{ТР.Rx} + S_{ТР.Tx}, \tag{15}$$

де $S_{ПР.ВН}$ – площа прямокутника (ПР) на рівні перекриття необхідних смуг частот);

$S_{ТР.Rx}$ та $S_{ТР.Tx}$ – площі прямокутних трикутників у спектральних масках сигналів R_x та T_x.

$$S_{ПР.ВН} = f_{нRxmax} - f_{нTxmin} = (f_{Rx} + B_{нRx}/2) - (f_{Tx} - B_{нTx}/2) = (B_{нRx} + B_{нTx})/2 - |\Delta f|, \tag{16}$$
$$S_{ТР.Rx} = (B_{Rx} - B_{нRx})/4,$$
$$S_{ТР.Tx} = (B_{Tx} - B_{нTx})/4.$$

Коефіцієнт частотної вибірковості *FDR* при виконанні умови (14) можна розрахувати за формулою (6) з урахуванням розмірів площі, які отримані у виразах (8), (9) та (15).

Якщо виконується умова (5), але не виконуються ні одна з умов (10), (12), та (14), тобто площа перекриття спектральних масок має від нерівностороннього трикутника, як показано на рисунку 3 та рисунку 7, умовою прийому завади основним каналом прийому приймача від основного випромінювання передавача завади для займаної смуги частот буде нерівність:

$$\Delta f > (B_{нTx} + B_{нRx})/2. \tag{17}$$

Для визначення площі трикутника зручно скористатися виразом для розрахунку його площі по відомому боці та двох прилеглих кутах:

$$Si = \frac{a^2 \cdot \sin\alpha \cdot \sin\beta}{2 \cdot \sin(180 - (\alpha + \beta))}, \tag{18}$$

де a = $(f_{Rxmax} - f_{Txmin} = (f_{Rx} + B_{Rx}/2) - (f_{Tx} - B_{Tx}/2) = (B_{Rx} + B_{Tx})/2 - |\Delta f|$;

$\alpha_{Rx} = \arctan(2/(B_{Rx} - B_{нRx}))$, з урахуванням $B_{Rx} = 1{,}2 \times B_{нRx}$, $\alpha_{Rx} = \arctan(10/B_{нRx})$;
$\beta_{Tx} = \arctan(2/(B_{Tx} - B_{нTx}))$, з урахуванням $B_{Tx} = 1{,}2 \times B_{нTx}$, $\beta_{Tx} = \arctan(10/B_{нTx})$.

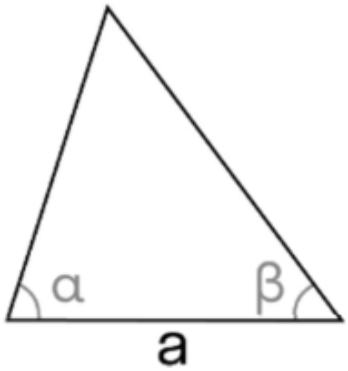


Рис. 7. Для пояснення розрахунку площі трикутника

За вказаних умов (при виконанні умови (5) та невиконанні ні однієї з умов (10), (12) або (14) і виконанні умови (17) коефіцієнт частотної вибірковості *FDR* визначається з урахуванням розмірів площі, які наведені у виразах (8), (9) та (18).

Висновки. Запропонований спрощений інженерний метод розрахунку співканальної частотної вибірковості може бути застосований для приблизного розрахунку потужності завади на вході приймача за умови можливості створення завади основним каналом прийому від основного випромінювання передавача завади та у разі відсутності достатніх даних, стосовно спектральної маски випромінювання передавача завади та АЧХ приймача.

Подальші напрямки досліджень передбачають вивчення можливості практичного застосування пропонованого спрощеного інженерного методу розрахунку коефіцієнта частотної вибірковості приймача шляхом визначення його точності порівняно з результатами розрахунків іншими методами, які передбачають наявність достатньої вихідної інформації для більш точних розрахунків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Spectra and bandwidth of emissions. RECOMMENDATION ITU-R SM.328-11. URL: https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.328-11-200605-I!!PDF-E.pdf.

2. Frequency and distance separations. RECOMMENDATION ITU-R SM.337-6. URL: https://www.itu.int/dms_pubrec/itu-r/rec/sm/R-REC-SM.337-6-200810-I!!PDF-E.pdf.

3. Іванов В. О., Габрусенко Є. І., Ільницький Л. Я., Щербина О. А. Електромагнітна сумісність радіоелектронної апаратури: навч. посіб. Київ: Національний авіаційний університет, 2014. 309 с. URL: http://er.nau.edu.ua/handle/NAU/28232.

4. Методика розрахунків електромагнітної сумісності для присвоєння радіочастот радіоелектронним засобам рухомої служби. Додаток 4. Методи розрахунків коефіцієнта частотної вибірковості приймача. Затверджено Наказом Адміністрації Держспецзв’язку від 13.08.2021 № 500. URL: https://ips.ligazakon.net/document/FN070350.

5. Положення про реєстр радіообладнання та випромінювальних пристроїв, яке затверджено Постановою Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку 29 червня 2022 року № 87. Додаток 3 «Форма картки технічних даних радіоелектронного засобу». URL: https://zakon.rada.gov.ua/laws/show/z0788-22#Text.

6. Регламент радіозв’язку ITU. URL: https://www.itu.int/pub/R-REGCУ.

7. Методика розрахунків електромагнітної сумісності для присвоєння радіочастот радіоелектронним засобам радіомовної служби. Затверджено Наказом Адміністрації Держспецзв’язку від 20.10.2021 № 619. URL: https://zakon.rada.gov.ua/rada/show/v0619519-21#Text.

8. Методика розрахунків електромагнітної сумісності для присвоєння радіочастот радіоелектронним засобам фіксованої служби. Затверджено Наказом Адміністрації Держспецзв’язку від 26.10.2021 № 634. URL: https://zakon.rada.gov.ua/rada/show/v0634519-21#Text.

9. Методика розрахунку електромагнітної сумісності для присвоєння радіочастот радіоелектронним засобам супутникових служб радіозв’язку. Затверджено Наказом Адміністрації Держспецзв’язку від 20.10.2021 № 635. URL: https://zakon.rada.gov.ua/rada/show/v0635519-21#Text.

DOI: 10.58254/viti.7.2025.11.110

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.О RCID: 0000-0002-8317-4131(ДержНДІ технологій кібербезпеки)
Ушаков В. Д. ORCID: 0009-0009-0787-6607 (ФОП «Ушаков Віктор Дмитрович»)

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ РАДІОЛІНІЙ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ БПЛА

На поточний час захист від придушення радіоліній спеціального зв'язку засобами РЕБ складає серйозну проблему при тактичному використанні БпЛА.

Метою статті є викладення основних підходів до створення перспективних радіоліній спеціального зв'язку БпЛА, стійких до впливу засобів РЕБ, результатів розрахунку потенціалу макетного зразка інформаційної радіолінії БпЛА, а також результатів її натурних випробувань.

Наразі, до основних недоліків наявних радіоліній спеціального зв'язку БпЛА відносять недостатній рівень захисту від впливу засобів РЕБ, слабку захищеність від перехоплення управління та схильність до взаємних завад. Для послаблення цих недоліків, окрім реалізації заходів щодо криптозахисту інформації, обґрунтовано використання перспективного діапазону міліметрових хвиль електромагнітного спектра.

Наведено оцінку потенціалу радіолінії низькочастотного відтинку міліметрового діапазону із обґрунтуванням необхідних запасів (20 дБ). При розрахунках розглядалися антени наземного сегмента діаметром 300 мм та 600 мм, а у якості бортової антени – антена у вигляді відкритого фланця хвилевода з орієнтовною діаграмою спрямованості 159°× 96.

Розглянуто функціональні схеми перспективних наземного та бортового сегментів радіолінії БпЛА, а також основні технічні характеристики макетного зразка інформаційної радіолінії (борт – земля) і результати його попередніх натурних випробувань (зокрема, досягнута відстань зв'язку склала 14 км).

Зроблено висновок, що запропоноване перенесення робочих частот радіоліній спеціального зв'язку БпЛА у міліметровий діапазон електромагнітного спектра дасть можливість оперативно змінювати їх робочі частоти, що може стати суттєвою тактичною перевагою в умовах масованого застосування засобів РЕБ.

Ключові слова: *безпілотні літальні апарати (БпЛА), радіолінії спеціального зв'язку БпЛА, засоби РЕБ для боротьби з БпЛА, міліметровий діапазон електромагнітного спектра.*

I. Panchenko, D. Bondarenko, O. Lypskyi, Ya. Stefanyshyn, V. Ushakov. Increasing the security of UAV special communication radio lines

Currently, protection against suppression of special communication radio lines by electronic warfare (EW) is a serious problem in the tactical use of UAVs.

The purpose of the article is to present the main approaches to creating promising UAV special communication radio lines resistant to the influence of electronic warfare (EW), the results of calculating the potential of a prototype UAV information radio line, as well as the results of its full-scale tests.

Currently, the main disadvantages of existing UAV special communication radio lines include an insufficient level of protection against the influence of electronic warfare (EW), weak protection against interception of control, and a tendency to mutual interference. To mitigate these disadvantages, in addition to implementing measures for cryptographic protection of information, the use of the promising millimeter wave range of the electromagnetic spectrum is justified.

An assessment of the potential of a radio line of the low-frequency section of the millimeter range is presented with a justification of the necessary reserves (20 dB). The calculations considered ground segment antennas with a diameter of 300 mm and 600 mm, and as an onboard antenna - an antenna in the form of an open waveguide flange with an approximate directivity pattern of 159°×96°.

Functional diagrams of promising ground and onboard segments of the UAV radio line were considered, as well as the main technical characteristics of the prototype of the information radio line (board - ground) and the results of its preliminary field tests (in particular, the achieved communication distance was 14 km).

It was concluded that the proposed transfer of the operating frequencies of the UAV special communication radio lines to the millimeter range of the electromagnetic spectrum will make it possible to quickly change their operating frequencies, which can become a significant tactical advantage in conditions of massive use of electronic warfare equipment.

Keywords: *unmanned aerial vehicles (UAVs), UAV special communication radio lines, EW means for combating UAVs, millimeter range of the electromagnetic spectrum.*

Постановка проблеми

Безпілотні літальні апарати (БпЛА, дрони) будь-якого типу обладнані командно-телеметричною та інформаційною радіолініями спеціального зв’язку.

За допомогою командно-телеметричної радіолінії БпЛА забезпечується передавання команд управління на борт БпЛА та отримання сигналів зворотного зв’язку (які, зокрема, підтверджують виконання команд і сигналізують про роботоспроможність окремих вузлів та блоків). Обсяги інформації, які передаються цією радіолінією, – порівняно невеликі (швидкість передавання інформації не перевищує декількох сотень кбіт/с). Зазвичай, командно-телеметрична радіолінія складається із двох незалежних радіоліній земля – борт та борт – земля. У багатьох випадках радіолінія борт – земля відсутня, а зворотна інформація передається інформаційною радіолінією. Для уникнення несанкціонованого перехоплення управління БпЛА (spoofing) у командно-телеметричній радіолінії часто застосовується криптозахист інформації. Крім того, командно-телеметрична радіолінія, з цією самою метою, часто будується за технологією псевдовипадкового переналаштування робочої частоти (ППРЧ). При цьому смуга робочих частот розширюється (до декількох десятків МГц). Тим не менше, командно-телеметрична радіолінія, у загальному випадку, слабо захищена від впливу засобів РЕБ, внаслідок дії яких забезпечується її придушення (jamming) завадою, що генерується у смузі робочих частот. Зважаючи на те, що системи РЕБ забезпечують, переважно, нерівномірну щільність перекриття смуги робочих частот радіолінії сигналами завади, існує певна можливість неповного придушення функціонування радіолінії з ППРЧ. Однак цей факт не дає підстави говорити про повну захищеність цієї радіолінії від впливу засобів РЕБ.

Інформаційна радіолінія БпЛА призначена для передавання у реальному масштабі часу відеоінформації від бортової відеокамери чи інших високоінформаційних давачів. Швидкість передавання сигналу (наприклад, відеопотоку) сягає 10 Мбіт/с, тому запас потенціалу радіолінії реалізувати значно важче і, відповідно, забезпечення якісних показників передавання інформації становить певну проблему. Для усунення можливості перехоплення інформаційного потоку доцільно також застосовувати криптозахист інформації. Саме застосування криптозахисту може стати одним із чинників, що визначає певні тактичні переваги БпЛА. Разом із тим, інформаційна радіолінія загалом також не захищена від придушення засобами РЕБ.

Таким чином, захист від придушення радіоліній спеціального зв’язку БпЛА ворожими засобами РЕБ складає серйозну проблему. Причому придушення інформаційної радіолінії так званих FPV-дронів можна визнати більш дошкульним, бо, фактично, це означає фізичну втрату БпЛА (зважаючи на переважну відсутність у FPV-дронів іншої навігації, окрім візуального орієнтування оператора).

Аналіз останніх досліджень і публікацій

Основні вимоги до частотних діапазонів, перспективних видів модуляції, швидкостей передавання інформації, методів боротьби з багатопроменевістю розповсюдження радіохвиль. а також конструктивного виконання антенних пристроїв цифрових радіоліній спеціального зв’язку БпЛА наведені у роботі [1].

Загальні характеристики інформаційних радіоліній FPV-дронів із робочими частотами у діапазонах 2,4 ГГц та 5,8 ГГц розглянуто у роботі [2]. Зроблено висновок про перспективність використання у складі цих БпЛА аналогових радіоліній спеціального зв’язку діапазону 5,8 ГГц. Приклад реалізації радіоліній у діапазоні 900 МГц наведено у роботі [3].

Робота [4] присвячена розгляду особливостей побудови радіоліній зв’язку для БпЛА малого (до 30 км) та середнього і великого радіусу дії (до та більше 100 км). Наголошено на перспективності використання частотних діапазонів 2,4 ГГц та 5,8 ГГц, а також більш

високочастотних (зокрема, діапазон міліметрових хвиль). Серед факторів, які обмежують використання високочастотних діапазонів електромагнітного спектра, названа сильна залежність умов розповсюдження радіохвиль від погодних умов, необхідність забезпечення прямої видимості між передавачем та приймачем, а також багатопроменевість розповсюдження радіохвиль. Наголошено, що висота підйому наземної антени слабо впливає на дальність зв’язку з БпЛА, тому на практиці висота наземної щогли вибирається з міркувань зниження впливу багатопроменевості, яка виникає у результаті наявності завад на шляху поширення сигналу (рельєф місцевості, будівлі, дерева, лісопосадки тощо).

У роботах [5; 6] наведено типові основні тактико-технічні характеристики засобів РЕБ противника, аналіз яких дозволяє зробити висновок про обмеженість їх робочого частотного діапазону приблизно на рівні 20 ГГц.

Нормативно-правовим документом [7] регламентується розподіл смуг радіочастот між радіослужбами в Україні та визначаються смуги радіочастот для спеціального та загального користування.

У роботі [8] наведено відомості про принципи розрахунку радіоліній зв’язку з БпЛА за двома методиками (класичною – для вільного простору, та експериментально вивіреною – згідно з рекомендаціями, викладеними у документі [9]). Сформульовано рекомендації щодо підвищення запасу потенціалу радіоліній спеціального зв’язку з БпЛА.

Фізичні розміри параболічних антен, у загальному випадку, розраховуються відповідно до загальновідомої залежності, яка, наприклад, наведена у роботі [10]. Розрахунки з такими самими результатами також можна виконати за допомогою online-калькулятора, розміщеного за посиланням [11].

Технічні характеристики бортового передавача діапазону 5,8 ГГц AKK Race Ranger FPV VTX, відомості щодо діаграми спрямованості антени у вигляді відкритого фланця хвилеводу та технічні характеристики дисплея FPV 7″ Readytosky 800×480 DVR Diversity 5,8 GHz, які використано як складові для макетування перспективної інформаційної радіолінії БпЛА, розміщено на вебресурсах [12–14] відповідно.

Незважаючи на те, що більшість загальнодоступних джерел як захист БпЛА від впливу засобів РЕБ пропонують використання ППРЧ, видається, що ця технологія, забезпечуючи стійкість радіолінії до перехоплення інформації (РЕР), не гарантує стовідсотковий її захист від негативного впливу засобів придушення (РЕБ).

Метою цієї статті є викладення основних підходів до створення перспективних радіоліній спеціального зв’язку БпЛА, стійких до впливу засобів РЕБ, результатів розрахунку потенціалу макетного зразка інформаційної радіолінії БпЛА, а також результатів її випробувань.

Викладення основного матеріалу

Основні вимоги до побудови радіоліній спеціального зв’язку БпЛА. Типовим підходом до побудови радіоліній спеціального зв’язку БпЛА є технологія цифрової передачі інформації. Це дає можливість забезпечити високу якість передавання інформації шляхом корекції спотворень та помилок, які виникли при розповсюдженні сигналу уздовж траси. Зокрема, у роботі [1] пропонується для цього використовувати модуляцію виду OFDM (мультиплексування з ортогональним частотним розділенням сигналів) або C-OFDM (мультиплексування з ортогональним частотним розділенням сигналів та кодуванням). Видається, що модуляція C-OFDM, яка дає можливість забезпечити корегування помилок, що виникли при розповсюдженні сигналу уздовж траси, у багатьох випадках при створенні радіолінії для БпЛА (наприклад, на протяжних трасах) є більш перспективною. Ці види модуляції забезпечують зниження символьної швидкості передавання інформації завдяки розділенню інформації на декілька менш швидкісних потоків та передаванню кожного з них на своїй частоті-субносії, ортогональній до інших частот-субносіїв.

Крім того, пропонується використання типового методу боротьби з багатопроменевістю розповсюдження радіохвиль – технології MIMO (зокрема, найпростішої схеми з двохантенною передачею інформації з борту БпЛА на одну наземну антену), що дозволяє вирішити проблему забезпечення надійного зв’язку при маневрах дрона у просторі.

На сьогодні робочий частотний діапазон розглянутих радіоліній спеціального зв’язку БпЛА, у переважній більшості випадків, не перевищує 5,825 ГГц. Це дає можливість використовувати однотипні всеспрямовані бортові антени, а різноманітність конструктивного виконання наземних антен звести до двох типів: всеспрямовані – для зв’язку на невеликих відстанях і вузькоспрямовані – для зв’язку з віддаленими БпЛА. Як один із варіантів спрощеної реалізації наземної вузькоспрямованої антени пропонується використання направлених секторіальних антен (зазвичай, у кількості 6 одиниць), які перемикаються, створюючи псевдокругову діаграму спрямованості. Видається, що у якості бортової антени може бути використана також patch (мікросмужкова) антена. Крім того, наземна вузькоспрямована антена може бути виконана також у вигляді більш складної активної або пасивної фазованої антенної решітки.

На думку авторів, реалізація бортової чи наземної секторіальної антенної системи, незважаючи на її певну громіздкість є достатньо перспективною ідеєю, бо дає можливість позбутися енерговитратних механічних пристроїв повороту антени.

Загалом, можна сказати, що цифрові радіолінії спеціального зв’язку БпЛА мають переваги перед аналоговими, зважаючи на можливості забезпечення:

значно кращої якості передавання інформації (завдяки використанню спеціального кодування інформації, яке дозволяє проводити автоматичну корекцію прийнятого сигналу для усунення похибок, що виникли при розповсюдженні сигналу уздовж траси);

криптозахисту інформації (підвищує стійкість до несанкціонованого перехоплення);

часткового захисту від впливу штучно створених (засобами РЕБ) чи природних завад (завдяки автоматичному переходу на інші робочі частоти, або використанню технології ППРЧ у межах певного робочого діапазону частот);

передавання додаткової інформації;

менших габаритно-масових показників (завдяки більшій пристосованості до мініатюризації).

Таким чином, при створенні радіоліній спеціального зв’язку БпЛА в умовах мирного часу для загального використання альтернативу цифровим лініям знайти важко.

Якщо мова йде про БпЛА спеціального використання (особливо FPV-дрони), то переваги цифрових радіоліній зв’язку не такі однозначні. Як не дивно, позитивні властивості цифрових радіоліній (наявність сигналу визначеної якості, або його відсутність взагалі при значних спотвореннях чи помилках) тут відіграють негативну роль. Ситуація з повною відсутністю сигналу на виході приймального пристрою радіолінії при управлінні FPV-дроном видається у багатьох випадках вкрай небажаною, бо може призвести до втрати управління, що, зазвичай, означає фізичну втрату БпЛА.

Натомість, в аналогових радіолініях спеціального зв’язку БпЛА при наявності завад суттєво втрачається якість сигналу (значно знижується його контрастність та інтенсивність), але зображення певний час не зникає повністю і це дає змогу досвідченому оператору, у багатьох випадках, вчасно оцінити ситуацію, не втратити геопросторову орієнтацію і, тим самим, попередити фізичну втрату FPV-дрона. Тобто, у ситуації впливу засобів РЕБ в аналогових радіолініях спеціального зв’язку БпЛА важливу роль відіграє кваліфікація оператора (людський фактор). Як бачимо, незважаючи на те, що, зазвичай, у людино-машинних системах людський фактор намагаються всіляко зменшити, для конкретного

випадку керування FPV-дроном саме людський фактор суттєво підвищує живучість всієї людино-машинної системи.

Що відноситься до частотних діапазонів радіоліній спеціального зв’язку БпЛА, то, загалом, у переважній більшості наразі використовують 3 діапазони частот: 900 МГц, 2,4 ГГц та 5,8 ГГц. При цьому, діапазон 900 МГц в основному використовується для командно-телеметричних, діапазон 5,8 ГГц – інформаційних радіоліній, а у діапазоні 2,4 ГГц можуть працювати як командно-телеметричні, так й інформаційні радіолінії.

Кожний із вищеозначених діапазонів частот має свої особливості. Наприклад, у роботі [2] розглянуто загальні характеристики інформаційних радіоліній FPV-дронів з робочими частотами у діапазонах 2,4 ГГц та 5,8 ГГц (представлено у таблиці 1) і сформульовано висновки щодо доцільності переважного використання при створенні FPV-дронів аналогових радіоліній спеціального зв’язку діапазону 5,8 ГГц.

Таблиця 1

Характеристики радіоліній FPV-дронів із різними робочими частотами

Діапазон, ГГц	**Характеристики радіолінії**		**Характеристики інформації**		**Інтенсивність використання**
	завантаженість	**спосіб передавання інформації**	**якість**	**затримка передавання**	
2,4	Висока	Аналогова	Низька	-	Невелика
		Цифрова (Wi-Fi)	Середня	Велика	Середня
5,8	Середня	Аналогова	Висока	-	Велика
		Цифрова (Wi-Fi)		Прийнятна	Середня

Як вже наголошувалося, більш низькочастотний частотний діапазон 900 МГц також широко використовується. Наприклад, командна радіолінія БпЛА «Ланцет» частотного діапазону 900 МГц працює саме у цьому робочому діапазоні (зокрема, 868–870 МГц та 902–928 МГц [3]).

Основні недоліки радіоліній БпЛА. Наразі бойове застосування БпЛА, особливо, FPV-дронів, виявило їх суттєві недоліки, які обумовлені недоліками радіоліній:

1) недостатній рівень захисту від впливу засобів РЕБ;

2) слабка захищеність від несанкціонованого перехоплення управління внаслідок ідентичності обладнання, яке використовується ворогом, та переважної відсутності криптозахисту командної інформації;

3) схильність до взаємних завад при використанні декількох БпЛА внаслідок обмеженості кількості робочих частот.

Зважаючи на це, широке застосування ворожих купольних (окопних) засобів РЕБ створило умови для суттєвого зниження ефективності використання БпЛА за цільовим призначенням.

Підходи до зменшення впливу засобів РЕБ на БпЛА. Одним із класичних методів часткового зменшення впливу засобів РЕБ на ефективність використання БпЛА, як вже наголошувалося, є застосування криптозахисту інформації, що циркулює радіолініями спеціального зв’язку. При цьому такий захід може покращити ситуацію з несанкціонованим перехопленням управління, але не усунути можливість придушення сигналу засобами РЕБ.

Більш кардинальним методом боротьби з негативним впливом засобів РЕБ (який тим не менше не відкидає криптозахист інформації) видається перенесення робочих частот засобів спеціального зв’язку БпЛА у більш високочастотні діапазони електромагнітного спектра, як рекомендовано в [4]. На думку авторів, у конкретному випадку протистояння на лінії зіткнення, це могло б забезпечити (протягом певного часу) усунення вищеозначених недоліків ліній спеціального зв’язку БпЛА, а також дало б можливість оперативно реагувати на зміну ситуації щодо появи нових засобів РЕБ (шляхом переходу на інші робочі частоти)

і, тим самим, отримати суттєву тактичну короткострокову та й у багатьох випадках довгострокову переваги.

Вибір робочого діапазону частот радіолінії. Для вибору робочої частоти радіоліній спеціальної інформації БпЛА доцільно врахувати наступні фактори:

максимальні робочі частоти засобів РЕБ противника, які потенційно можуть бути використані для боротьби з БпЛА;

рекомендації Міжнародного комітету з радіочастот (МКРЧ) щодо вибору робочих частот для забезпечення рухомого зв’язку (частоти, на використання яких потенційно можна буде отримати дозвіл в установленому порядку).

Аналіз відкритих джерел інформації свідчить, що наразі діапазон робочих частот ворожих засобів РЕБ не перевищує 20 ГГц. Наприклад, у [5] повідомляється про робочі частоти станції РЕБ РФ «Свет-КУ», які лежать у діапазоні від 25 МГц до 18 ГГц. У [6] наведено згадку про відсутність у противника засобів РЕБ із робочими частотами у міліметровому (ММ) діапазоні електромагнітних хвиль (30–300 ГГц). Таким чином, видається, що, зважаючи на значно меншу інтенсивність використання діапазону ММ хвиль, саме перенесення спектра робочих частот у цей діапазон дасть можливість упродовж певного часу отримати на лінії зіткнення тактичні переваги.

Особливістю ММ-діапазону електромагнітного спектра є те, що він освоєний значно менше, а, відповідно, елементна база цього діапазону – менш розповсюджена, ціна її значно вища, ніж елементної бази сантиметрового діапазону і, крім того, вона суттєво зростає пропорційно підвищенню частоти.

Що відноситься до дотримання вимог МКРЧ, на думку авторів, неуважне відношення до вибору частот, яке, зазвичай широким загалом мотивується воєнним станом, може призвести до невиправданих втрат часу на створення нероботоспроможного засобу зв’язку (при випадковому потраплянні на робочі діапазони інших радіоелектронних засобів) та у подальшому до втрати для цього засобу комерційної перспективи при спробі його постачання на світовий ринок (після настання мирного часу).

Аналіз [7] дає можливість зробити висновок про наявність широкої номенклатури смуг радіочастот, на які загальним користувачам в установленому порядку, потенційно, можна отримати дозвіл на використання (присвоєння номіналів радіочастот) для рухомої служби (служба радіозв’язку між рухомою і сухопутною станціями або між рухомими станціями). Не завжди ці частоти передбачають спеціальне використання, але, видається, що це не може бути причиною відмови, особливо в умовах воєнного стану.

Оцінка потенціалу радіолінії ММ-діапазону. Орієнтовний розрахунок потенціалу аналогової інформаційної радіолінії (борт – земля) проведемо для довільно вибраної частоти ММ-діапазону, наприклад, $\boldsymbol{F} = 30$ ГГц і інтервалів зв’язку $\boldsymbol{R} = 10$ км та $\boldsymbol{R} = 30$ км у припущенні, що потужність бортового передавача складає $\boldsymbol{P_{Tx}} = 30$ дБм (1 Вт), коефіцієнт підсилення бортової всеспрямованої антени $\boldsymbol{G_{Tx}} = 5$ дБі, коефіцієнт підсилення приймальної антени $\boldsymbol{G_{Rx}} = 36$ дБі, температура шуму наземного приймального пристрою $\boldsymbol{T_{NRx}} = 2{,}5$ дБ (≈ 250 К), смуга його робочих частот – $\boldsymbol{B_{Rx}} = 10$ МГц та необхідне відношення сигнал/шум на виході приймача – $\boldsymbol{SNR_{Rx}} = 10$ дБ.

Загальне затухання сигналу $\boldsymbol{L}$, при розповсюдженні його у вільному просторі уздовж траси, розраховуємо за загальновідомою формулою, наведеною, наприклад, в [4].

У результаті розрахунку визначаємо, що величина затухання сигналу при розповсюдженні його у вільному просторі уздовж вибраної траси протяжністю $\boldsymbol{R} = 10$ км складає $\boldsymbol{L_{10км}} = -142$ дБ, а для траси протяжністю $\boldsymbol{R} = 30$ км – $\boldsymbol{L_{10км}} = -152$ дБ.

При цьому чутливість приймального пристрою, розрахована для вищеозначених вихідних даних за формулою, яка, зокрема, також наведена у цій роботі, становить:

$$\boldsymbol{P_{s\,min}} = -95{,}0 \text{ дБм}.$$

Сигнал на вході приймального пристрою P_{Rx} визначимо за формулою:

$$P_{Rx} = L + P_{Tx} + G_{Tx} + G_{Rx},$$

де P_{Rx} – потужність сигналу на виході приймального пристрою, *дБм*;
L – затухання на трасі, *дБ*;
P_{Tx} – потужність передавача, *дБм*;
G_{Tx} – коефіцієнт підсилення передавальної антени, *дБі*;
G_{Rx} – коефіцієнт підсилення приймальної антени, *дБі*.

Підставивши числові величини складових у вищенаведену формулу, отримаємо реальний рівень сигналу на вході приймального пристрою для траси R = 10 км $P_{Rx(10\ км)}$ = = –71 дБм, а для траси R = 30 км $P_{Rx(30\ км)}$ = –81 дБм.

Різниця між реальним рівнем сигналу на вході приймача та його чутливістю (запас потенціалу радіолінії) $P_{Rx} - P_{s\ min}$ складає 24,0 дБм (для R = 10 км) та 14 дБм (для R = 30 км).

На перший погляд такий запас можна вважати завеликим для R = 10 км та прийнятним для R = 30 км. Разом з тим, у роботі [8] наведено відомості про принципи розрахунку радіоліній за двома методиками. Зокрема, розрахунки, які базуються на класичних залежностях для вільного простору (як і було розраховано вище), та розрахунки, які рекомендовано використовувати при організації радіозв’язку у повітряних службах (згідно з рекомендаціями Міжнародного Союзу електрозв’язку [9]), тобто у нашому випадку, для БпЛА. Вищеозначені рекомендації базуються на експериментально вивіреній моделі розповсюдження радіохвиль в атмосфері, але вони наведені для максимальної частоти 15 500 МГц (рис. 1). Тому величину затухання сигналу на трасі для вибраної нами частоти ММ-діапазону можна спрогнозувати тільки приблизно.

Аналіз графіку свідчить про наявність для авіаційних систем суттєвої відмінності між втратами сигналу, розрахованими для вільного простору, та визначеними за експериментально вивіреною моделлю. Зокрема, ці втрати суттєво залежать від відстані між антенами та висотами їх підняття. Наприклад, для частоти 15,5 ГГц на відстані 400 км при висоті підняття антен 1000 м додаткові втрати сигналу сягають величини 90–100 дБ. Компенсація таких втрат – завдання, загалом, проблематичне, що свідчить про суттєву обмеженість інтервалів зв’язку радіоліній ММ-діапазону. На відстанях до 100 км для 95 % часу ці додаткові втрати становлять більш прийнятну величину (орієнтовно 15–20 дБ), яка може бути достатньо легко компенсована. Таким чином, оснащення FPV-дронів (на відстані передавання інформації не більше 20–30 км) радіолініями ММ-діапазону можливе.

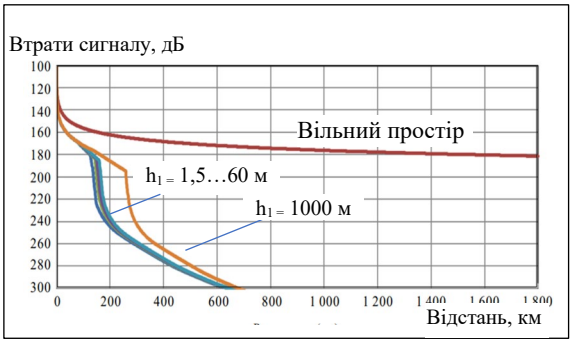


Рис. 1. Залежність основних втрат сигналу частоти 15 500 МГц для 95 % часу та висоти h_2 = 1000 м (h_1 – висота як наземної антени так і БПЛА, h_2 – висота БПЛА)

На думку авторів, попередньо для вибраної частоти $F = 30$ ГГц та відстані $R = 10$ км запас потенціалу радіолінії доцільно також встановити не менше 20 дБ. Тобто, розрахованого запасу потенціалу (24 дБ) для забезпечення гарантованої роботи радіолінії спеціального зв'язку БпЛА цілком достатньо.

На жаль, цього не можна сказати про потенціал траси $R = 30$ км. Для досягнення запасу потенціалу більше 20 дБ (зокрема 24 дБ, як і для $R = 10$ км), тут доцільно підвищити на 3 дБ потужність випромінювання передавача (до $P_{Rx} = 2$ Вт) та збільшити на 7 дБі коефіцієнт підсилення приймальної антени (до $G_{Rx} = 43$ дБі). Незважаючи на певне збільшення енергоспоживання бортового передавача, такий шлях у багатьох випадках може виявитися прийнятним.

Для визначення можливості практичної реалізації приймальної антени розрахованої радіолінії діаметр її рефлектора D_{Rx} визначимо з використанням загальновідомої залежності, наведеної, наприклад, в [10]:

$$G = (0{,}4…0{,}6) \times 4\pi \times S/\lambda^2,$$

де G – коефіцієнт підсилення параболічної антени, одиниць;

S – геометрична площа рефлектора параболічної антени, $м^2$;

λ – довжина робочої хвилі антени, *м*.

Розрахована величина діаметру рефлектора параболічної антени (при орієнтовно вибраному коефіцієнті у формулі близько 0,5) складає $D_{Rx} \approx 0{,}3$ м (для $R = 10$ км) та $D_{Rx} \approx 0{,}6$ м (для $R = 30$ км). Такі самі результати можна отримати у результаті машинного розрахунку, наприклад, згідно з програмою, наведеною на вебресурсі [11]. Загалом, визначені розміри рефлекторів антен цілком прийнятні, зважаючи на невелику парусність та масу, що цілком допускає комфортну експлуатацію наземного приймального пристрою.

Альтернативним (або взагалі доповнювальним) рішенням до цих пропозицій можна вважати використання повітряного ретранслятора. Встановлення на борт БпЛА антени з діаметром рефлектора $D_{Rx} \approx 0{,}3$ м взагалі великих труднощів не складе. При цьому, видається, що із тактичних міркувань (необхідність забезпечення надійного маскування наземного сегмента) доцільно використовувати повітряний ретранслятор штатно. Це дасть можливість зробити габарити наземного приймального пристрою достатньо малими, що спростить проблему його надійного маскування.

Побудова приймально-передавальних пристроїв радіоліній БпЛА. Як вже згадувалося, практично масове виробництво БпЛА обумовило ситуацію, за якої на світовому ринку широко представлені комплектувальні вироби високого ступеню інтеграції для побудови радіоліній спеціального зв'язку БпЛА, уже згаданих частотних діапазонів 900 МГц, 2,4 ГГц та 5,8 ГГц, які, крім того, мають достатньо демократичні ціни.

Таким чином, для скорочення термінів та зменшення трудовитрат, при побудові перспективних радіоліній ММ-діапазону доцільно використовувати наявні штатні складові сантиметрового діапазону. Тобто найоптимальнішим варіантом запропонованого доопрацювання є включення до складу штатного передавального пристрою БпЛА передавача ММ-діапазону (Up-конвертор із підсилювачем потужності вихідного сигналу та антеною), а до складу штатного приймального пристрою – приймача ММ-діапазону (антени, малошумливого підсилювача та Down-конвертора). При цьому, бортові антени передавачів та приймачів ММ-діапазону, очевидно, повинні бути всеспрямовані, а наземні – вузькоспрямовані.

Разом із тим, це не відноситься до бортового ретранслятора, зважаючи на необхідність підтримання потенціалу радіолінії. Тому на борту ретранслятора необхідно буде розміщувати як всеспрямовані, так і вузькоспрямовані антени.

Структурна схема радіолінії спеціального зв’язку БпЛА. У загальному випадку структурна схема побудови передавального та приймального пристроїв як інформаційної, так і командно-телеметричної радіоліній спеціального зв’язку БпЛА однакова. Тільки, зазвичай командно-телеметрична радіолінія побудована за принципом часового дуплексу, а інформаційна радіолінія – завжди односпрямована (або, у окремих випадках, симплексна).

Для прикладу на рисунку 2 представлена структурна схема бортового передавача інформаційної радіолінії спеціального зв’язку БпЛА.

Рис. 2. Структурна схема бортового аналогового передавального пристрою інформаційної радіолінії БпЛА

У наведеній схемі як штатний передавач відеосигналу, до антенного виходу якого підключено передавач ММ-діапазону, використано передавач відеосигналу AKK Race Ranger FPV VTX [12], який функціонує у діапазоні $(5{,}8 \pm 0{,}15)$ ГГц із регульованою потужністю випромінювання від 200 мВт до 1,6 Вт. При цьому, для узгодження зі створюваним передавачем ММ-діапазону потужність передавача необхідно зменшити до мінімальної та додатково встановити атенюатор відповідного номіналу. До складу Up-конвертора включається фільтр дзеркального каналу, який забезпечує виділення необхідної бокової смуги змішувача, а також, за необхідності, вихідний фільтр (на виході підсилювача потужності), який формує смугу робочих частот у ММ-діапазоні.

Як всеспрямована (більш конкретно, слабоспрямована) антена у ММ-діапазоні, загалом, може бути використано, наприклад, антена у вигляді відкритого фланця хвилеводу. Як показано в [13], для відкритих фланців хвилеводів стандартних розмірів ширина діаграми спрямованості на рівні 3 дБ складає 159° у площині вузької стінки та близько 96° у площині широкої стінки. До недоліків такої антени відноситься погане узгодження хвилевода (хвильовий опір 480–590 Ом) із вільним простором (хвильовий опір 377 Ом), наслідком чого коефіцієнт стоячої хвилі сягає 1,6–1,9 (що для антен, загалом, можна вважати прийнятним). Зауважимо, що із тактичних міркувань при розташуванні антени у вигляді відкритого фланця хвилевода на борту БпЛА, зважаючи на різницю у формі діаграми спрямованості, доцільно відкритий фланець хвилеводу розташовувати широкою стінкою вертикально до землі.

Загальновідомо, що для боротьби з нестійкою роботою радіолінії в умовах перевідбиття сигналу від завад часто використовується метод передавання сигналу одночасно двома каналами з різною поляризацією. Для цього до антенного виходу підключається подільник потужності на 3 дБ, виходи якого з’єднуються, наприклад, з відкритими фланцями хвилеводів, розташованими ортогонально один до другого. Для вирівнювання форми діаграми спрямованості у двох площинах можна запропонувати використання секторіальних рупорів.

Крім того, при створенні передавального пристрою за запропонованою схемою доцільно приділити увагу його екрануванню. Це дасть можливість запобігти виявленню роботи передавача засобами радіоелектронної розвідки шляхом фіксації випромінювання на штатних робочих частотах (у діапазонах 900 МГц, 2,4 ГГц та 5,8 ГГц), які використовуються як проміжні. Відсутність належного екранування може звести нанівець всі переваги перенесення спектра у ММ-діапазон, особливо на невеликих відстанях від засобу РЕБ.

Структурна схема наземного приймача інформаційної радіолінії спеціального зв’язку БпЛА представлена на рисунку 3.

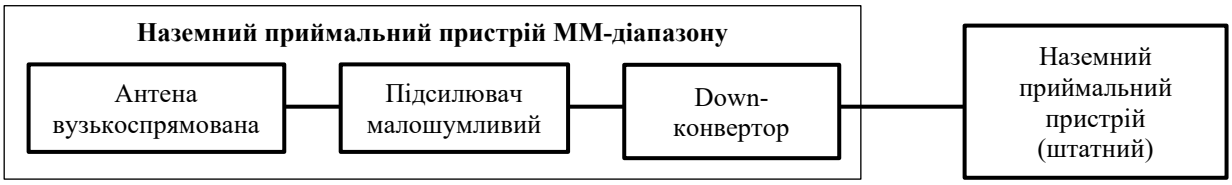


Рис. 3. Структурна схема наземного аналогового приймального пристрою інформаційної радіолінії БпЛА

Сигнал, прийнятий приймачем ММ-діапазону, подається на антенний вхід штатного приймального пристрою з робочою частотою 5,8 ГГц та монітором (дисплей FPV 7″ Readytosky 800×480 DVR Diversity 5,8 GHz [14]). Як вузькоспрямована антена використовується параболічна антена (наприклад, антена offset з діаметром рефлектора 0,3 м).

Для забезпечення можливості приймання сигналу двома каналами, як передбачено у штатному приймальному пристрої (дисплей FPV 7″ Readytosky 800×480 DVR Diversity 5,8 GHz), необхідно використати 2 приймальні пристрої ММ-діапазону, які мають ортогональне розташування фланців хвилеводів, що опромінюють спільний рефлектор.

Формування робочої смуги частот у ММ-діапазоні, а також зменшення шумової складової на виході приймача ММ-сигналу забезпечується включенням до складу приймального пристрою вхідного фільтра. Крім того, до складу Down-конвертора включено фільтр дзеркального каналу, який призначений для виділення необхідної бокової смуги частот змішувача, яка відповідає смузі робочих частот штатного наземного приймача інформаційного сигналу БпЛА. Застереження щодо екранування приймального пристрою такі ж суворі, як і для передавального, бо потужний сигнал РЕБ, при відсутності екранування, спроможний придушити його роботу каналами проміжних частот.

При цьому, приймальний пристрій ММ-діапазону доцільно розміщувати на поворотному штативі. Для зручності експлуатації радіолінії доцільно використати поворотний штатив з автоматичним регулюванням та підтриманням напряму на передавач.

З’єднання приймача ММ-діапазону з дисплеєм виконується коаксіальним кабелем. Із тактичних міркувань кабель повинен допускати розміщення оператора на певній відстані від поворотного пристрою, тому використання кабелю невеликих перерізів – проблематичне. Крім того, для електричного з’єднання доцільно використовувати найбільш надійні в експлуатації радіочастотні роз’єми N-типу.

Створення та випробування макетного зразка. Макетний зразок інформаційної радіолінії з робочою частотою у нижній частині ММ-діапазону представлено на рисунку 4.

Макетний зразок передавального пристрою інформаційної радіолінії для забезпечення його автономності включає до свого складу повний комплект штатного обладнання БпЛА (у тому числі джерело живлення), що значно збільшує його габаритні розміри. У якості антен передавального пристрою використано відкритий фланець хвилеводу. Антена наземного приймального пристрою – офсетна з діаметром рефлектора 300 мм. Опромінювач антени не оптимізувався. Макетний зразок виготовлено тільки для одного поляризаційного каналу. Передавальний пристрій, разом з електронними елементами FPV-дрона, поміщено у кожух, який закріплено на борту квадрокоптера DJI Matric. Наведення наземної антени на БпЛА забезпечувалося у ручному режимі.

У процесі випробувань передавальний пристрій піднімався на висоту до 200 м, а приймальний пристрій розташовувався на висоті не більше 1,5 м. Випробувальна траса вибиралася за умови відсутності на ній природних завад.

а) *б)*

Рис. 4. Загальний вигляд макетного зразка радіолінії ММ-діапазону:
а – бортовий сегмент; *б* – наземний сегмент

При цьому, за потужності передавача 27 дБм відстань зв’язку склала близько 15 км. За експертними оцінками якість відеосигналу, що передавався, – задовільна.

Висновки і перспективи подальших досліджень

Перенесення робочих частот радіоліній спеціального зв’язку БпЛА у ММ-діапазон електромагнітного спектра видається перспективним напрямом їх подальшого розвитку. При цьому, наразі, для скорочення термінів і трудовитрат створення таких радіоліній доцільно використовувати штатні радіолінії сантиметрового діапазону, підключаючи до них конвертори ММ-діапазону.

Розрахункові гарантовані відстані зв’язку радіоліній ММ-діапазону (із запасом потенціалу відносно розповсюдження сигналу у вільному просторі не менше 20 дБ), для нижніх частот ММ-діапазону складають: при габаритах наземної приймальної системи не більше 300 мм – 10 км, а при габаритах антени 600 мм – близько 30 км.

Використання ретрансляторів дасть можливість не тільки використовувати наземні антени з меншим діаметром рефлектора, але й досягнути більш якісного передавання відеосигналу при еволюціях БпЛА на мінімальних висотах.

Для зменшення спотворень/втрат сигналу від завад на трасі розповсюдження при його перевідбиттях дієвим заходом залишається одночасне передавання сигналу двома каналами (зокрема, з різною поляризацією чи різними частотами).

Створення вітчизняних конверторів ММ-діапазону дасть можливість оперативно змінювати робочі частоти БпЛА, що може забезпечити певні тактичні переваги при застосуванні ворожих засобів РЕБ.

У перспективі передбачається розроблення ретранслятора, а також вжиття заходів щодо освоєння високочастотних ділянок діапазону ММ-хвиль з метою їх використання на всіх видах дронів (повітряних, морських, наземних), що дасть можливість, завдяки оперативному маневруванню робочими частотами, підвищити ефективність боротьби із ворожими засобами РЕБ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Слюсар В. Радиолинии связи с БпЛА. Примеры реализации // ЭЛЕКТРОНИКА. НТБ, 2010. № 5. С. 56–60. URL: https://www.slysar.kiev.ua.

2. Що таке FPV і в чому різниця 2,4 ГГц та 5,8 ГГц аналог або Wi-Fi. URL: https://maroder.com.ua/uk/obzor/chto-takoe-fpv-i-v-chem-raznitsa.

3. Радіоелектронна протидія безпілотним літальним апаратам «Ланцет» // G7 – сайт ТрО ЗСУ. URL: https://sprotyvg7.com.ua/lesson/radioelektronna-protidii-bezpilotnim-lital[]nim-aparatam-lancet.

4. Дмитрук Р. І., Коротєєв І. М., Думанський М. В. // Аналіз радіоліній зв’язку з безпілотними літальними апаратами // Сучасна спеціальна техніка. 2014. № 3 (38). Електронний репозитарій НАВС. URL: http://www.elar.naiau.kiev.ua/server/api/core/bitstreams/efcc7b78-8d44-4184-8e15-9667b0645b83/content.

5. Сили оборони вперше знищили російську РЕБ «Свет-КУ». URL: https://bagnet.org/news/accidents/1353595/cili-oboroni-vperche-znishchili-rsiysku-reb-svet-ku-video/.

6. Радіоелектронна боротьба: аналіз арсеналу Росії. Сильні та слабкі сторони російських засобів РЕБ. URL: https://defens-ua.com/weapon_and_tech/radioelectronna_borotba_jak_i_chim_rosija_vojue_proti_ukrajini-708.html.

7. Про затвердження Національної таблиці розподілу смуг радіочастот: постанова Каб. Міністрів України від 15.12.2005 № 1208 // Офіційний вісник України. 2005. № 51. С. 54. Ст. 3196.

8. Снісаренко А. Г. Особливості розрахунку радіоканалів командних радіоліній крилатих ракет // Системи озброєння і військова техніка. 2018. № 1 (53). С. 49–53. URL: http://www.reaseachgate.net/publication/324974422_Osoblivosti_rozrahunku_radiokanaliv_komandnih_radioliniy_krilatih_raket.

9. Кривые распространения радиоволн для подвижной и радионавигационной служб, работающих в диапазонах ОВЧ, УВЧ и СВЧ: Рекомендации МСЭ-R P.528-3 (02/2012). URL: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.528-3-201202-S!!PDF-R.pdf.

10. Методичні вказівки до курсової роботи з дисципліни “Проектування антенно-фідерних пристроїв НВЧ” для студентів спеціальності “Радіотехніка” всіх форм навчання // Запорізький національний технічний університет. URL: https://studfile.net/preview/9875374/page4.

11. Расчет зеркальной параболической антенны. URL: https://www.3g-aerial/biz/onlijn-raschety/raschety-antenn/raschet-parabolicheskoj-antenny.

12. URL: https://www.akktek.com/akk-race-ranger-n-a-for-customer.html.

13. Долбик А. И. Устройства сверхвысоких частот и антенны. Часть 2. Антенные системы РЭС РТВ. Казань, 2004. 104 с.

14. URL: https://www.droua.com.ua/ua/p1847976773-monitor-fpv-readytosky.html.

DOI: 10.58254/viti.7.2025.12.122

УДК 621.396

канд. техн. наук, професор Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
Думітраш О. В. ORCID: 0009-0003-9550-5377 (ВІТІ ім. Героїв Крут)

ХАРАКТЕРИСТИКА СПРОМОЖНОСТІ ІСНУЮЧИХ РІШЕНЬ УПРАВЛІННЯ РАДІОЗВ'ЯЗНІСТЮ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

У статті представлено комплексний огляд сучасних підходів і рішень щодо управління радіозв'язністю у бездротових сенсорних мережах тактичної ланки управління, що функціонують в умовах бойових дій. Проведено систематизацію результатів наукових досліджень українських і зарубіжних учених, проаналізовано стан і перспективи розвитку методів забезпечення надійного зв'язку в умовах високої мобільності, впливу завад, змінної топології та обмежених ресурсів. Обґрунтовано актуальність розгляду цієї тематики у контексті положень Стратегічного оборонного бюлетеня України та стандартів НАТО, які вимагають впровадження сучасних технологічних рішень у системи військового управління.

Наведено класифікацію сенсорних мереж, архітектуру бездротових сенсорних мереж тактичної ланки управління, а також детально описано основні вимоги до мереж у тактичному середовищі. Розглянуто сучасні технології управління зв'язком, серед яких особливо виділено когнітивне радіо, MANET, гетерогенні мережі, мобільні агентні системи, самоорганізовані мережі та рішення з використанням штучного інтелекту.

У статті також проаналізовано низку прикладних систем (наприклад, ITN, Bittium Tactical Wireless IP, Thales + Persistent MANET), що використовуються у Збройних Силах провідних країн світу. Розкрито переваги та обмеження кожного з підходів і рішень, з урахуванням їх стійкості до радіоелектронної боротьби, складності впровадження, вартості, енерговитрат та ефективності функціонування в умовах бойових дій.

Узагальнення результатів дозволило визначити найбільш ефективні напрями розвитку систем управління радіозв'язністю бездротових сенсорних мереж тактичної ланки управління. Зокрема, зроблено висновок про перспективність використання інтегрованих гібридних рішень, що поєднують інтелектуальні алгоритми, адаптивну маршрутизацію та гнучкі радіотехнології. Запропоновано напрями подальших досліджень, пов'язані з розробкою математичної моделі, яка враховує стохастичний характер середовища функціонування, а також вдосконаленням алгоритмів адаптивного управління з використанням методів машинного навчання.

Ключові слова: *сенсорні системи, бездротові (безпроводові) сенсорні мережі, тактична ланка управління, топологія, мобільна радіомережа, радіозв'язність, Стратегічний оборонний бюлетень, C4ISR.*

H. Radzivilov, O. Dumitrash. Assessment of the capabilities of existing radio connectivity management solutions for tactical-level wireless sensor networks

The article presents a comprehensive review of modern approaches and solutions for managing radio connectivity in wireless sensor networks at the tactical level, operating under combat conditions. The results of scientific studies by Ukrainian and foreign researchers have been systematized, and the current state and development prospects of methods for ensuring reliable communication under conditions of high mobility, interference, dynamic topology, and limited resources have been analyzed. The relevance of the topic is substantiated in the context of the Strategic Defense Bulletin of Ukraine and NATO standards, which require the integration of advanced technological solutions into military command and control systems.

The article provides a classification of sensor networks, the architecture of tactical-level wireless sensor networks, and a detailed description of the core requirements for such networks in a tactical environment. Modern communication management technologies are examined, with particular attention given to cognitive radio, MANETs, heterogeneous networks, mobile agent systems, self-organizing networks, and artificial intelligence-based solutions.

The study also analyzes a number of applied systems (e.g., ITN, Bittium Tactical Wireless IP, Thales + Persistent MANET) currently deployed in the armed forces of leading countries. The advantages and limitations of each approach and solution are outlined, considering their resilience to electronic warfare, deployment complexity, cost, energy consumption, and operational effectiveness in combat environments.

The synthesis of research findings has made it possible to identify the most effective directions for the development of radio connectivity management systems in tactical-level wireless sensor networks. Specifically, the article highlights the potential of integrated hybrid solutions combining intelligent algorithms, adaptive routing, and flexible radio technologies. Future research directions are proposed, including the development of a mathematical model that accounts for the stochastic nature of the operational environment, as well as the enhancement of adaptive management algorithms using machine learning techniques.

Keywords: *sensor networks, wireless sensor networks, tactical command level, topology, mobile radio network, radio connectivity, Strategic Defense Bulletin, C4ISR.*

Актуальність та постановка завдання в загальному вигляді

Відповідно до Стратегічного оборонного бюлетеня України, затвердженого Указом Президента України від 17 вересня 2021 року № 473/2021, схвалено, що одним із першочергових напрямів реалізації воєнної політики в Україні є побудова системи об’єднаного керівництва силами оборони та військового управління у Збройних Силах України, яка має здійснюватися відповідно до передового досвіду, принципів і стандартів держав-членів НАТО [1–3]. Досвід російсько-української війни свідчить про те, що використання передових технологій держав-членів НАТО сприяє покращенню процесу прийняття оперативних рішень, гарантує миттєве та ефективне їх доведення до виконавців, забезпечує контроль і здатність до супроводу під час виконання поставлених бойових завдань. Прикладом однієї з таких передових технологій можна вважати гнучкі автоматизовані системи управління військами, які налаштовані за нормами концепції C4ISR (модифікації C5ISR, C6ISR, C7ISR), що означає «Command and Control, Computers, Communications, Intelligence – Surveillance – Reconnaissance» (Командування і контроль, Зв’язок, Комп’ютеризація, Розвідка – Спостереження – Рекогносцировка) і являє собою інтегрований підхід до керування й координації військових операцій у сучасних гібридних війнах [4].

Ключовим інструментом для збору, обробки та передачі даних, що забезпечують належне функціонування систем C4ISR, ситуаційну обізнаність та ефективне управління військами, є бездротові сенсорні мережі (Wireless Sensor Networks, далі – БСМ), де вирішальну роль відіграє забезпечення радіозв’язності. Під радіозв’язністю в БСМ варто розуміти можливість доступності сенсорного вузла щодо інших з метою передачі інформації. БСМ мають ряд переваг для ефективного виконання оперативних завдань: здатні до швидкого розгортання та самоорганізації, адаптивні, енергоефективні, відмовостійкі, своєчасно реагують на вплив різноманітних зовнішніх факторів.

У зв’язку з цим виникає завдання дослідження існуючих рішень управління радіозв’язністю БСМ тактичної ланки управління (далі – ТЛУ), формування узагальненої характеристики сучасних підходів управління радіозв’язністю БСМ тактичного рівня та аналіз їх спроможності.

Аналіз попередніх досліджень

Упродовж 2015–2025 років спостерігається значний розвиток бездротових технологій передачі інформації, зокрема БСМ як одних із ключових складових Інтернету речей, що все більше поширюються у цивільних і військово-оборонних сферах. Огляд наукових досліджень у сфері БСМ свідчить про активну участь як українських (В. А. Романюк, О. В. Жук, О. Я. Сова, А. І. Міночкін, Р. О. Бєляков, А. В. Романюк та ін.), так й іноземних (Akyildiz, Lee, Gerla, Kumaraswamy, Dohler, Prakash, Bessani та ін.) вчених у розвитку цієї галузі. Велику кількість досліджень було присвячено критеріям вибору вузлів, спрямованим на поліпшення ефективності процесу інформаційного обміну в БСМ [5–9], оскільки від цього залежатиме ефективність мережі. Проведений аналіз наукових публікацій [10–21] свідчить про те, що вчені розглядали різні підходи для підвищення ефективності використання БСМ: відновлення зв’язності між сенсорами шляхом введення додаткових вузлів, застосування функції ретрансляції, управління топологією, використання різних методів маршрутизації, збору даних чи контролю доступу тощо. Незважаючи на значний прогрес у дослідженнях, деякі аспекти управління радіозв’язністю в БСМ залишаються недостатньо вивченими: зазначені підходи не враховують динамічні зміни умов середовища функціонування БСМ (наприклад, зона ведення бойових дій), не розглядалося забезпечення надійного та стійкого зв’язку в умовах передачі великих обсягів даних, високої мобільності, впливу завад, високої щільності вузлів та змінних радіоумов, що впливають на радіозв’язність мережі та стабільність роботи мережі.

Метою статті є дослідження спроможності існуючих рішень управління радіозв’язністю БСМ в умовах стохастичного середовища та динамічної зміни топології під час проведення військових операцій.

Виклад основного матеріалу

Залежно від безлічі факторів (поставлених задач, способу організації, середовища функціонування, типу сенсорів (датчиків) тощо) сенсорні мережі класифікують за різними ознаками. На рисунку 1 наведено узагальнену класифікацію сенсорних мереж.

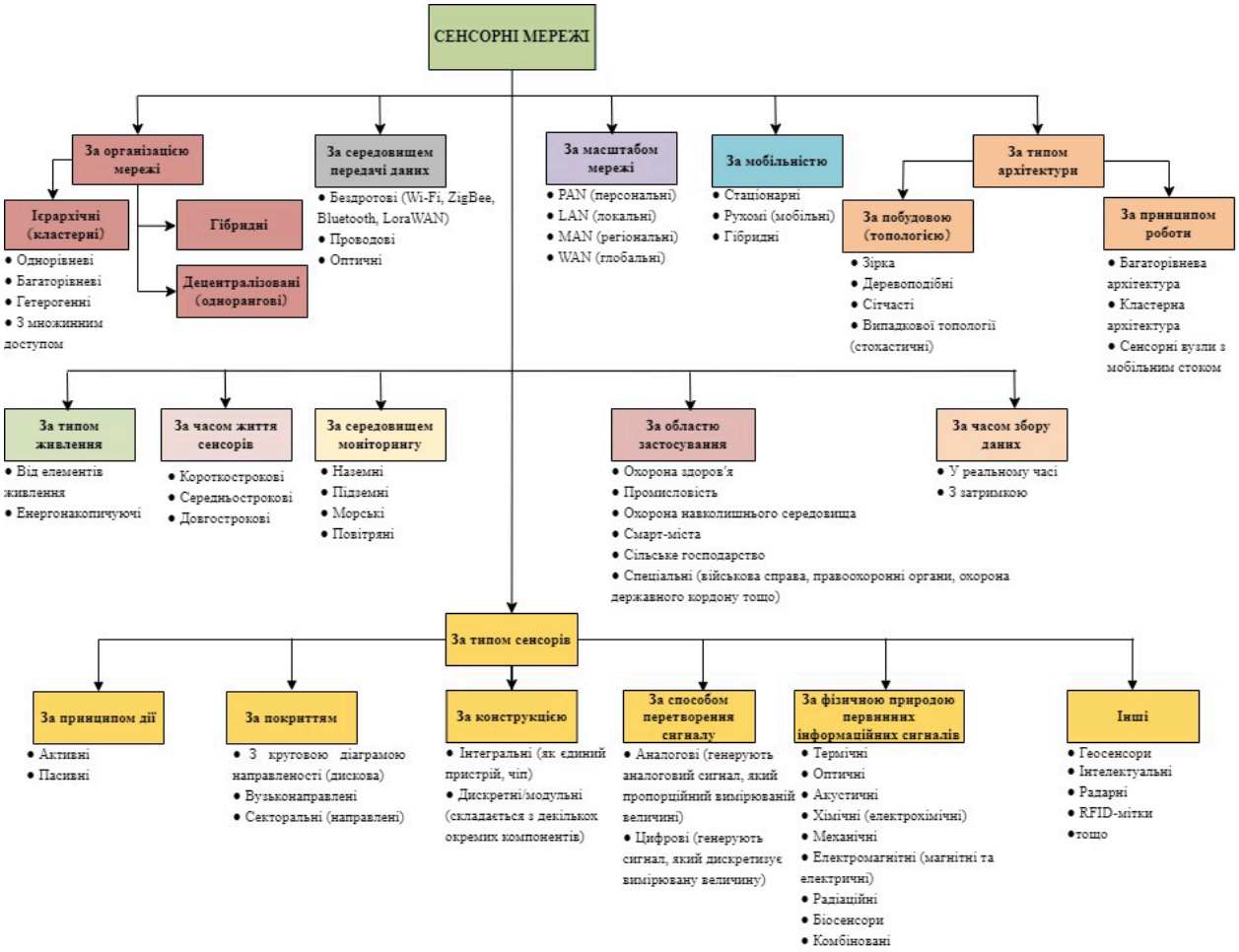


Рис. 1. Узагальнена класифікація сенсорних мереж

Оскільки БСМ можуть функціонувати з різними типами сенсорів (датчиків), при розгортанні таких мереж необхідно враховувати архітектуру побудови, яка у подальшому забезпечить стійкий та надійний зв’язок між підрозділами, високу ситуаційну обізнаність і моніторинг.

На рисунку 2 наведена архітектура БСМ ТЛУ на базі чотирирівневої моделі, яка складається з рівня сенсорів, рівня каналів передачі даних, рівня обробки даних і рівня додатків. Це забезпечує універсальний та ефективний набір інструментів для вирішення різноманітних задач спеціального призначення для військових цілей, а кожен із рівнів може бути незалежним і характеризується відносною простотою та гнучкістю оперативного розгортання або оптимізації безпосередньо на лінії зіткнення [22; 23].

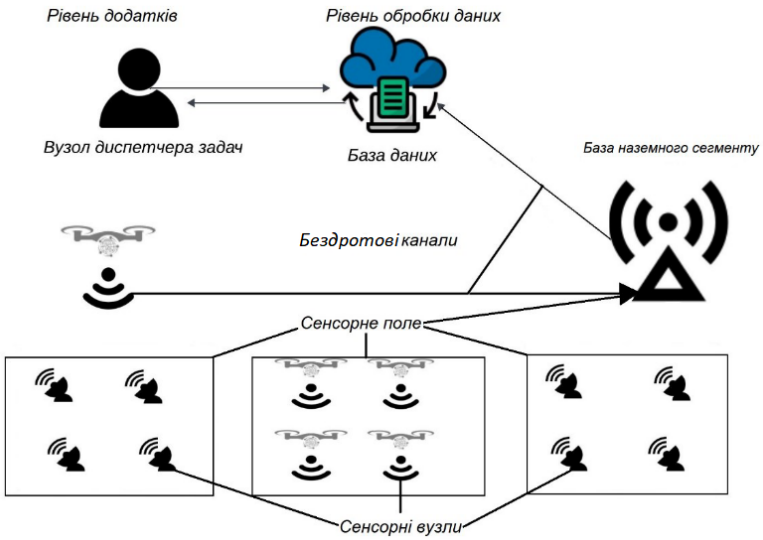


Рис. 2. Архітектура бездротової сенсорної мережі тактичної ланки управління

Окрім того, при розгортанні БСМ варто врахувати вимоги до мережі з огляду на характеристики БСМ ТЛУ, які визначено у таблиці 1.

Таблиця 1

Основні вимоги до БСМ ТЛУ

№	Характеристика	Опис
1	Динамічна топологія	Топологія мережі постійно змінюється через переміщення вузлів, що потребує адаптивних протоколів маршрутизації
2	Обмежені енергетичні ресурси	Сенсори та комунікаційні модулі працюють від автономних джерел живлення, тому важливо оптимізувати споживання енергії
3	Обмежені обчислювальні ресурси	Обробка даних, криптографія та зберігання інформації обмежені через малі обсяги оперативної пам’яті та потужності процесорів вузлів
4	Вимога до безперервності зв’язку	Тактичне середовище вимагає безперервного зв’язку для забезпечення командування і контролю, у тому числі при збої окремих вузлів
5	Стійкість до дій противника	Мережа повинна функціонувати в умовах електромагнітного протиборства (РЕБ), зазнавати атак (DoS, перехоплення, підміна вузлів) та бути стійкою до них
6	Низька затримка передачі даних	Час доставки критичних даних (наприклад, сигналів тривоги) має бути мінімальним, особливо в мережах реального часу
7	Масштабованість	Мережа повинна ефективно працювати як при малій, так і при великій кількості вузлів та їх щільності, з урахуванням ієрархічної організації (рій, група, мережа тощо)
8	Автономність та самовідновлення	Мережа повинна самостійно відновлювати структуру після втрати вузлів або порушення зв’язку, без централізованого керування
9	Адаптивність до умов середовища	Повинна змінювати параметри роботи відповідно до навколишніх умов – завади, зміни висоти, швидкості руху, погодних умов тощо
10	Синхронізація часових процесів	Для коректної передачі даних і координації дій важливо забезпечити синхронізацію між вузлами в реальному часі

З огляду на вищезазначене варто зазначити, що саме забезпечення радіозв’язності є однією з ключових цільових функцій задач управління вузлами БСМ ТЛУ [24; 25]. Враховуючи високий рівень мобільності, радіоелектронної протидії та потребу в оперативній координації, виникає необхідність у надійних системах управління радіозв’язністю, здатних до адаптації в реальному часі. З цією метою застосовуються програмні методи (нечітка логіка, нейронні мережі, когнітивне радіо), апаратні рішення (MANET, COTS IoT радіо,

інтегровані IP-мережі), інтегровані підходи (ITN, системи з розподіленим управлінням топологією). У таблиці 2 наведено основні підходи управління радіозв'язністю БСМ ТЛУ.

Таблиця 2

Основні підходи управління радіозв'язністю БСМ ТЛУ

№	Тип підходу	Основна ідея	Переваги	Обмеження
1	Управління топологією	Оптимізація структури мережі для підвищення її ефективності	Економія енергії, адаптивність	Складність обчислень у реальному часі
2	Кластеризація	Поділ мережі на кластери з головними вузлами	Масштабованість, зниження трафіку	Вразливість головного вузла
3	Гетерогенні мережі	Поєднання вузлів з різними можливостями	Гнучкість, баланс навантаження	Ускладнення маршрутизації
4	Ієрархічне управління	Багаторівнева організація з координаційними вузлами	Керованість, логічна структура	Вразливість командного рівня
5	Контекстно-адаптивні	Адаптація до змін середовища (перешкоди, мобільність)	Гнучкість, висока ефективність	Потреба в сенсорній обізнаності
6	На основі штучного інтелекту / машинного навчання	Інтелектуальна маршрутизація, виявлення загроз	Самонавчання, прогнозування	Вимоги до ресурсів
7	Мобільні агентні системи	Застосування БпЛА або мобільних вузлів	Гнучкість покриття, реле	Енерговитрати, безпека
8	Самоорганізовані мережі (SON)	Автономне формування топології, маршрутизація	Висока автономність, надійність	Нестабільність при сильних змінах
9	Безпека і криптозахист	Шифрування, аутентифікація, виявлення атак	Захист інформації, довіра	Обмеженість обчислень у вузлах

Відповідно до основних підходів управління радіозв'язністю БСМ ТЛУ, наведених у таблиці 2, визначено основні технології управління радіозв'язністю, які наведено у таблиці 3 та виділено найперспективніші [26–29].

Таблиця 3

Основні рішення управління радіозв'язністю БСМ ТЛУ

№	Технологія	Протидія РЕБ	Складність розгортання	Складність функціонування	Вартість	Примітка
1	MANET	Висока	Середня	Середня	Висока	Універсальне, вже активно застосовується
2	Когнітивне радіо (CR)	Дуже висока	Висока	Висока	Дуже висока	Найперспективніше для умов РЕБ
3	Thales + Persistent MANET	Дуже висока	Дуже висока	Середня	Дуже висока	Сучасне бойове рішення НАТО
4	Bittium Tactical Wireless IP	Висока	Висока	Середня	Дуже висока	Готове комерційне рішення
5	Нечітка логіка (ретранслятори)	Середня	Низька	Висока	Низька	Ефективне для невеликих мереж
6	ANFIS (нейро-нечітка система)	Середня	Середня	Висока	Середня	Підходить для прогнозування та розподілу
7	DSA (динамічний доступ до спектра)	Дуже висока	Висока	Висока	Висока	Оптимально для зміни середовища

№	Технологія	Протидія РЕБ	Складність розгортання	Складність функціонування	Вартість	Примітка
8	Туманні обчислення	Середня	Висока	Висока	Середня	Потребує складної інфраструктури
9	IoT + COTS рішення	Низька	Дуже низька	Низька	Дуже низька	Застосування поза межами бойових дій
10	Біоінспіровані алгоритми	Середня	Середня	Середня	Низька	Перспективні в динамічних MANET
11	Self-Organizing Networks (SON)	Висока	Середня	Висока	Висока	Автономне та адаптивне середовище
12	QoS із нечіткою логікою	Середня	Низька	Середня	Низька	Добре для регулювання навантажень
13	ITN (Інтегрована тактична мережа)	Дуже висока	Дуже висока	Середня	Дуже висока	Стандартизоване військове рішення США

Висновки

У результаті проведеного аналізу встановлено, що забезпечення надійної та стабільної радіозв’язності у БСМ ТЛУ є критично важливим чинником для ефективного функціонування систем командування та контролю в умовах сучасних бойових дій. Найбільш ефективними у таких умовах виявилися рішення, що базуються на концепціях когнітивного радіо, мобільних самоконфігурованих мереж (MANET), а також інтегрованих тактичних мереж (ITN). Зазначені технології забезпечують високий рівень адаптивності до змін середовища, стійкість до дій радіоелектронної боротьби та масштабованість у складних динамічних умовах.

Водночас їх впровадження потребує значних ресурсів, що обумовлює необхідність пошуку компромісних варіантів для конкретних сценаріїв застосування. Перспективними для завдань оптимізації ресурсів і підвищення гнучкості управління є також рішення на основі методів нечіткої логіки, біоінспірованих алгоритмів і нейро-нечітких систем (ANFIS), які доцільно використовувати для інтелектуального управління трафіком, маршрутизації та контролю доступу.

Перспективним напрямком подальших наукових досліджень є розробка математичної моделі управління радіозв’язністю в умовах стохастичного середовища функціонування БСМ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 06.06.2016 № 240/2016. URL: http://www.president.gov.ua/documents/2402016-20137 (дата звернення: 03.03.2025).

2. Про Стратегічний оборонний бюлетень України: Рішення Ради нац. безпеки і оборони України від 20.08.2021: станом на 21 верес. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0063525-21#Text (дата звернення: 03.03.2025).

3. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 17 вересня 2021 року № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/ 473/2021#n17 (дата звернення: 03.03.2025).

4. Концептуальні підходи застосування бездротових сенсорних мереж арміями передових країн світу / В. Машталір та ін. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. Т. 47, № 2. С. 96–112. URL: https://doi.org/10.33099/2311-7249/2023-47-2-96-112 (дата звернення: 13.03.2025).

5. Optimization of Wireless Sensor Network and UAV Data Acquisition / D.-T. Ho et al. *Journal of Intelligent & Robotic Systems*. 2015. Vol. 78, no. 1. P. 159–179. URL: https://doi.org/10.1007/s10846-015-0175-5 (date of access: 13.03.2025).

6. Okcu H., Soyturk M. Distributed clustering approach for UAV integrated wireless sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing*. 2014. Vol. 15, no. 1/2/3. P. 106. URL: https://doi.org/10.1504/ijahuc.2014.059912 (date of access: 13.03.2025).

7. Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey / B. Jan et al. *Wireless Communications and Mobile Computing*. 2017. Vol. 2017. P. 1–14. URL: https://doi.org/10.1155/2017/6457942 (date of access: 13.03.2025).

8. Zhan C., Zeng Y., Zhang R. Energy-Efficient Data Collection in UAV Enabled Wireless Sensor Network. *IEEE Wireless Communications Letters*. 2018. Vol. 7, no. 3. P. 328–331. URL: https://doi.org/10.1109/lwc.2017.2776922 (date of access: 13.03.2025).

9. Романюк А. В. Алгоритм временной кластеризации узлов беспроводных сенсорных сетей для сбора информации мониторинга с использованием БпЛА. *Адаптивні системи автоматичного управління*. 2018. Т. 2, № 33. С. 106–117. URL: https://doi.org/10.20535/1560-8956.33.2018.164680 (дата звернення: 13.03.2025).

10. Алгоритм пошуку топології в неоднорідній безпроводовій сенсорній мережі. / Сова О. Я. та ін. *Проблеми телекомунікацій*: Матеріали IX Міжнар. науково-техн. конф. «Проблеми телекомунікацій – 2015», м. Київ, 20–24 квітня 2015 р. URL: https://conferenc-journal.its.kpi.ua/article/view/104314 (дата звернення: 20.03.2025).

11. Методика управління топологією наземно-повітряних радіомереж / В. А. Романюк, Є. О. Степаненко Проблеми телекомунікацій: Матеріали XIII Міжнар. науково-техн. конф. «Перспективи телекомунікацій – 2019», м. Київ, 15–19 квітня 2019 р. URL: https://conferenc-journal.its.kpi.ua/article/view/169014 (дата звернення: 20.03.2025).

12. Управління топологією в безпроводних сенсорних мережах / О. В. Жук та ін. *Проблеми телекомунікацій*: Матеріали XI Міжнар. науково-техн. конф. «Проблеми телекомунікацій – 2017», м. Київ, 18–21 квітня 2017 р. URL: https://conferenc-journal.its.kpi.ua/article/view/101432?utm_source=chatgpt.com (дата звернення: 20.03.2025).

13. Романюк А. В. Методи збору даних з безпроводових сенсорних мереж телекомунікаційними аероплатформами: дис. ... канд. техн. наук: 05.12.02 Телекомунікаційні системи та мережі. Київ, 2021. 185 с. URL: https://ela.kpi.ua/handle/123456789/40572 (дата звернення: 23.03.2025).

14. Міночкін А. І., Романюк В. А., Сова О. Я. Інтелектуальний метод маршрутизації в мобільних радіомережах (MANET). *Збірник наукових праць* ВІТІ НТУУ „КПІ". 2009. № 1. С. 74–87.

15. Романюк А. В. Метод доступу до радіоканалу вузлами безпровідної сенсорної мережі при зборі даних моніторингу телекомунікаційними аероплатформами. *Збірник наукових праць ВІТІ*. 2018. № 4. С. 84–91.

16. Wireless sensor networks: a survey / I. F. Akyildiz et al. *Computer Networks*. 2002. Vol. 38, no. 4. P. 393–422. URL: https://doi.org/10.1016/s1389-1286(01)00302-4 (date of access: 27.03.2025).

17. A survey on wireless multimedia sensor networks/ I. F. Akyildiz et al. *Computer Networks*. 2006. Vol. 51, no. 4. P. 921–960. URL: https://doi.org/10.1016/j.comnet.2006.10.002 (date of access: 27.03.2025).

18. Gerla M. Vehicular urban sensing. *the 11th international symposium*, Vancouver, British Columbia, Canada, 27–31 October 2008. New York, New York, USA. URL: https://doi.org/10.1145/1454503.1454504 (date of access: 27.03.2025).

19. Internet of Things/ M. Dohler et al. *IEEE COMMUNICATIONS MAGAZINE*. 2024. Vol. 62, no. 1. P. 24–25. URL: https://doi.org/10.1109/MCOM.2024.10401870 (date of access: 23.03.2025).

20. Mahana C. B., Carvalho M. M., Prakash R. Minimal Latency and Buffer-Constrained Gathering of Data in Sensor Networks. *2024 19th International Symposium on Wireless Communication Systems (ISWCS)*, Rio de Janeiro, 14–17 July 2024. URL: https://doi.org/10.1109/ISWCS61526.2024.10639050 (date of access: 18.03.2025).

21. Alysson Bessani. The Power of Simplicity on Dependable Distributed Systems (Invited Talk). In 28th International Conference on Principles of Distributed Systems (OPODIS 2024). Leibniz International Proceedings in Informatics (LIPIcs), Volume 324, p. 1:1, Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 2024. URL: https://doi.org/10.4230/LIPIcs.OPODIS.2024.1.

22. Проблематика використання безпровідних сенсорних мереж у військових цілях / Д. Михалевський та ін. *Herald of Khmelnytskyi National University. Technical sciences*. 2024. Т. 331, № 1. С. 97–100. URL: https://doi.org/10.31891/2307-5732-2024-331-16 (дата звернення: 27.03.2025).

23. Mykhalevskiy D. Development of a method for assessing the effective information transfer rate based on an empirical model of statistical relationship between basic parameters of the Standard 802.11 wireless channel. *Eastern-European Journal of Enterprise Technologies*. 2020. Vol. 5, no. 9 (107). P. 26–35. URL: https://doi.org/10.15587/1729-4061.2020.213834 (date of access: 27.03.2025).

24. Романюк А. В. Цільові функції управління вузлами безпровідних сенсорних мереж для моніторингу об’єктів критичної інфраструктури. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки.* 2017. Т. 28 (67). № 2. С. 49–54.

25. Objective control functions of mobile AD-HOC networks by means of UAVs / O. I. Lisenko et al. *2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, Kyiv, Ukraine, 13–15 October 2015. URL: https://doi.org/10.1109/apuavd.2015.7346610 (date of access: 30.03.2025).

26. Akyildiz I. F., Lee W.-Y., Chowdhury K. R. CRAHNs: Cognitive radio ad hoc networks. *Ad Hoc Networks*. 2009. Vol. 7, no. 5. P. 810–836. URL: https://doi.org/10.1016/j.adhoc.2009.01.001 (date of access: 26.03.2025).

27. Maj. Matthew S. Blumberg, U.S. Army. The Integrated Tactical Network. Pivoting Back to Communications Superiority. MILITARY REVIEW. May-June 2020. P. 104–115. URL: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-20/Blumberg-Int-Tactical-Network.pdf (date of access: 26.03.2025).

28. Mitola III J. Cognitive Radio Architecture. *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems*. Dordrecht. P. 43–107. URL: https://doi.org/10.1007/978-1-4020-5542-3_3 (date of access: 30.04.2025).

29. Fog Computing: A Platform for Internet of Things and Analytics / F. Bonomi et al. *Big Data and Internet of Things: A Roadmap for Smart Environments*. Cham, 2014. P. 169–186. URL: https://doi.org/10.1007/978-3-319-05029-4_7 (date of access: 30.04.2025).

DOI: 10.58254/viti.7.2025.13.130

УДК 621.391

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)
Плугова О. Б. ORCID 0000-0001-7848-7806 (ВІТІ ім. Героїв Крут)

КОНЦЕПТУАЛЬНІ АСПЕКТИ ЩОДО РОЗРОБКИ ПЕРСПЕКТИВНОЇ МОДЕЛІ СИСТЕМИ СУПУТНИКОВОГО ЗВ’ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ В УМОВАХ ВПЛИВУ ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

На підставі проведеного аналізу ефективності функціонування основних підсистем супутникового зв’язку Збройних Сил України під час відсічі збройної агресії російської федерації, впливу засобів радіоелектронної боротьби противника на дані системи визначаються напрямки розвитку військової системи супутникового зв’язку на ближню та подальшу перспективи. У статті розглядаються концептуальні аспекти щодо розробки нової моделі перспективної системи супутникового зв’язку ЗС України, яка базується на оренді потоків (каналів) або частотно-орбітального ресурсу в операторів супутникового зв’язку. Дані системи супутникового зв’язку спеціального призначення повинні забезпечувати високий і стабільний рівень сигналу над Україною, необхідну якість, швидкість передачі, розвід- та завадозахищений супутниковий зв’язок із використанням новітніх інформаційно-комунікаційних технологій. Для протидії засобам радіоелектронної боротьби противника використовуються супутники на низьких навколоземних орбітах, бортова обробка сигналів та вузькі промені бортових діаграм направленості. Поряд з даними способами захисту від радіоелектронного придушення науково обґрунтовуються та пропонуються до застосування адаптивні антенні решітки. Принцип роботи даних антен характеризується її діаграмою направленості. Придушення завади досягається завдяки управлінню положеннями нулів діаграми направленості і зменшенню рівня бічних пелюсток у напрямку джерела завади. Адаптивні антени здатні також визначати напрямок впливу завад і зменшувати їх вплив в умовах відсутності апріорної інформації про сигнально-завадову обстановку.

Запропонована модель перспективної системи супутникового зв’язку ЗС України збільшить швидкість передачі, стійкість до засобів радіоелектронної боротьби противника та зменшить затримку сигналу на різних рівнях управління ЗС України.

Майбутній розвиток моделі перспективної системи буде полягати в застосуванні адаптивного формування променю антенної решітки на базі SDR технології, що дозволить формувати більш вузьку діаграму направленості та надасть можливість доступу більшій кількості користувачів.

Ключові слова: *система супутникового зв’язку, супутники, термінали, перспективна система супутникового зв’язку, радіоелектронна боротьба, адаптивні антенні решітки.*

V. Rudenko, M. Zinchenko, O. Yakovchuk, O. Plugova. Conceptual aspects of developing a promising model of a special-purpose satellite communication system under the influence of electronic warfare means

Based on the analysis of the effectiveness of the functioning of the main satellite communication subsystems of the Armed Forces of Ukraine during the repulsion of the armed aggression of the Russian Federation, the impact of enemy electronic warfare on these systems, the directions of development of the military satellite communication system for the near and long term are determined. The article considers conceptual aspects of developing a new model of a promising satellite communication system for the Armed Forces of Ukraine, which is based on leasing streams (channels) or frequency-orbital resources from satellite communication operators. These special-purpose satellite communication systems must provide a high and stable signal level over Ukraine, the necessary quality, transmission speed, intelligence- and jamming-protected satellite communication using the latest information and communication technologies. Particular attention is paid to the use of satellites in low Earth orbits, on-board signal processing, narrow beams of on-board directional diagrams to counter enemy electronic warfare. Along with these methods for protection against electronic jamming, adaptive antenna arrays are scientifically substantiated and proposed for use. The principle of operation of these antennas is characterized by its directivity diagram. Suppression of interference is achieved by controlling the positions of the zeros of the directivity diagram and reducing the level of side lobes in the direction of the interference source. Adaptive antennas are also able to determine the direction of interference and reduce their impact in the absence of a priori information about the signal-interference situation.

The proposed model of a promising satellite communication system for the Armed Forces of Ukraine will increase transmission speed, resistance to enemy electronic warfare equipment, and reduce signal delay at various levels of command of the Armed Forces of Ukraine.

Future development of the promising system model will involve the use of adaptive beamforming of the antenna array based on SDR technology, which will allow for the formation of a narrower directivity pattern and provide access to a larger number of users.

Keywords: *satellite communication system, satellites, terminals, promising satellite communication system, electronic warfare, adaptive antenna arrays.*

Вступ. Досвід ведення війни з російською федерацією показав, що противник активно застосовує засоби радіоелектронної боротьби (далі – РЕБ) з метою виведення з ладу системи зв’язку ЗС України [1], в тому числі і системи супутникового зв’язку (далі – ССЗ) [2], для порушення надійного управління військами (силами). Через це ситуація, яка склалася, показала, що відсутність надійного супутникового зв’язку є суттєвим недоліком існуючої системи зв’язку ЗС України. Тому було прийнято рішення щодо оренди потоків (каналів) або частотно-орбітального ресурсу у міжнародних операторів супутникового зв’язку провідних держав світу та/або у військових ССЗ країн-членів НАТО для забезпечення зв’язку військовим користувачам.

Постановка задачі. На підставі аналізу ефективності функціонування основних підсистем супутникового зв’язку ЗС України під час застосування російською федерацією засобів РЕБ можна зробити висновки, що діючі підсистеми не завжди відповідають покладеним на них функціям та потребують модернізації і перебудови. Тому ставиться задача розробити нову модель перспективної системи супутникового зв’язку (далі – ПССЗ) ЗС України на основі оренди потоків (каналів) або частотно-орбітального ресурсу. Дана система повинна забезпечувати стійкий і безперебійний зв’язок між пунктами управління об’єднань, з’єднань, частин і підрозділів в умовах активного застосування противником засобів РЕБ.

Аналіз останніх публікацій та досліджень

Доктрина [1] забезпечує загальне стратегічне керівництво із застосування зв’язку та інформаційних систем у ЗС України. Вводить термінологію в галузі зв’язку та інформаційних систем, сумісну із прийнятою термінологією в НАТО. Даний документ відповідає положенням і структурі викладення та понятійному апарату, який використовується в союзній публікації НАТО AJP-06.

Настанова [2] є регламентуючим документом, який визначає основні теоретичні положення та принципи функціонування існуючих ССЗ. Здійснює опис складових частин

і технічних характеристик кінцевого обладнання супутникового зв’язку, що перебуває на озброєнні в ЗС України.

У статті [3] розроблена модель ПССЗ та передачі даних ЗС України на підставі аналізу існуючих ССЗ армій провідних країн світу та країн-членів НАТО, новітніх досягнень інформаційних технологій у галузі зв’язку і тенденцій розвитку електронних комунікаційних мереж ЗС України. До складу даної моделі входить одна система з використанням супутника на геостаціонарній орбіті та дві системи на низьких і середніх навколоземних орбітах, які повною мірою не забезпечують захист від впливу засобів РЕБ противника.

У роботі [4] розглянутий стан ССЗ збройних сил США та країн-членів НАТО. На підставі даного аналізу були розроблені пропозиції щодо побудови ПССЗ ЗС України, але дана система будувалась на використанні супутників на геостаціонарній орбіті, які мають низьку швидкість передачі та не забезпечують надійний захист від засобів РЕБ противника.

Концепція [5] забезпечує формування економічно стійкої, конкурентоспроможної, диверсифікованої ракетно-космічної галузі та передбачає розвиток сучасних космічних технологій в Україні. Документ дозволить створити потужну систему дистанційного зондування Землі та Національну систему космічного зв’язку з використанням наукового та промислового потенціалу України.

Настанова [6] дає визначення, що таке РЕБ та регламентує порядок виконання заходів радіо-, радіотехнічного контролю у процесі виконання завдань за призначенням військовими частинами (підрозділами) радіоелектронного захисту.

У виданні [7] розглядаються основні положення систем адаптивних матриць. З кожним роком кількість застосувань даних систем зростає, розширюються принципи та фундаментальні методи, які мають вирішальне значення для цих систем. Задача подавлення завад досить складна, може вирішуватись із застосуванням різних способів і методів.

У статті [8] проводиться аналіз ефективності застосування адаптивних антенних решіток у системах радіозв’язку в умовах активної РЕБ. Показано, що перспективними напрямками підвищення захисту військових систем радіозв’язку від завад є використання багатоантенних систем, що працюють з використанням адаптивних антенних решіток, але в роботі не розглядається ефект застосування антенних решіток в ССЗ.

Таким чином, проведений аналіз основних публікацій та досліджень показав, що на сьогодні існує багато статей і матеріалів стану та розвитку ССЗ спеціального призначення, але дані системи здебільшого використовують геостаціонарні орбіти, які не тільки мають низьку швидкість передачі, але й не здатні забезпечувати надійний зв’язок в умовах активної РЕБ.

Метою статті є розкриття концептуальних поглядів щодо розробки перспективної моделі ССЗ спеціального призначення в умовах впливу засобів РЕБ.

Виклад основного матеріалу дослідження

1. Дослідження ефективності функціонування основних систем супутникового зв’язку Збройних Сил України

Супутниковий зв’язок посідає особливе місце в системі військового зв’язку та відіграє важливу роль у забезпеченні надійного управління військами (силами).

Основне призначення ССЗ ЗС України полягає в забезпеченні надійних, захищених каналів зв’язку на усіх рівнях управління. Супутниковий зв’язок відіграє та буде продовжувати відігравати ключову роль у військових системах зв’язку. Найважливішими перевагами супутникового зв’язку щодо інших видів зв’язку є глобальне охоплення, висока стійкість та оперативність – здатність забезпечувати зв’язок з будь-якої точки Землі за дуже короткий час.

Нині ССЗ ЗС України складається з різних систем, станцій та засобів супутникового зв’язку, таких як: Starlink, Tooway, OneWeb, Satcube, KIT 9350, L-TAC Slingshot, Hughes Thuraya XT-PRO, Iridium 9575A, Kymeta Corporation, SatPaq2 та інших. У даному розділі ми проведемо дослідження технічних характеристик та ефективність функціонування трьох основних ССЗ: Starlink, Tooway, OneWeb, і зробимо висновки щодо їх використання.

1.1. Система супутникового зв’язку Starlink

Після повномасштабного вторгнення російської федерації, Україні було надано доступ до ССЗ Starlink – проєкту американської компанії SpaceX.

Комерційна ССЗ Starlink (рис. 1) – перше та найбільше у світі супутникове угруповання, яке використовує низьку навколоземну орбіту для надання широкосмугового Інтернету у будь-якій точці планети. Понад 6 000 супутників знаходяться на орбітах висотою від 336 км до 570 км від поверхні Землі, які рухаються зі швидкістю 27 000 км/год. Очікуваний термін служби даних супутників складає біля 8 років [3].

ССЗ Starlink складається з двох супутникових мереж:

перша мережа – використовує Ku- та Ka-діапазони;

друга мережа – використовує V-діапазон.

Із появою у ЗС України системи Starlink ситуація щодо організації супутникового зв’язку значно покращилась. Система стала невід’ємною складовою військового управління ЗС України та використовується як основний засіб зв’язку на різних рівнях управління.

ССЗ стрімко розвивається, останнім часом на супутниках почали розміщувати додаткове обладнання в інтересах військових користувачів. Обладнання, що встановлюється, збільшує швидкість передачі та підвищує стійкість до протидії засобам РЕБ та радіоелектронної розвідки (далі – РЕР) противника.

Нині близько 3 000 терміналів ЗС України отримали доступ до захищеної мережі американського військового супутникового зв’язку Starlink – Starshield, яка сумісна з цивільними супутниками Starlink.

Таким чином, використовуючи низькі навколоземні орбіти, сучасні супутники та новітнє обладнання, ССЗ Starlink надає надійний високошвидкісний Інтернет з малою затримкою сигналів для користувачів у найвіддаленіших точках світу. Швидкість підключення Інтернету в перспективі становитиме до 1 Гбіт/с із затримкою сигналу до 40 мс. Антена термінала користувача “бачить” один супутник в інтервалі від 3 до 5 хвилин, після чого перемикається на інший низькоорбітальний супутник. Зона покриття навколо наземних хабів знаходиться у радіусі біля 900 км.

Комплекти терміналів Starlink поставляються з усім необхідним для підключення обладнанням, терміни їх розгортання становлять лічені хвилини. Термінали rev1 та rev2 з круглою антеною (V1) знімаються з виробництва, термінали rev3, hp1 та rev4 не завжди придатні для застосування в бойових умовах та потребують доопрацювання. Сучасні модернізовані термінали адаптовані для використання в польових умовах, можуть застосовуватися на безпілотних і транспортних засобах, в яких використовуються стандартні інтегровані елементи живлення, роз’єми, перемикачі, що призводить до скорочення часу на розгортання/згортання комплектів та спрощує їх експлуатацію [9].

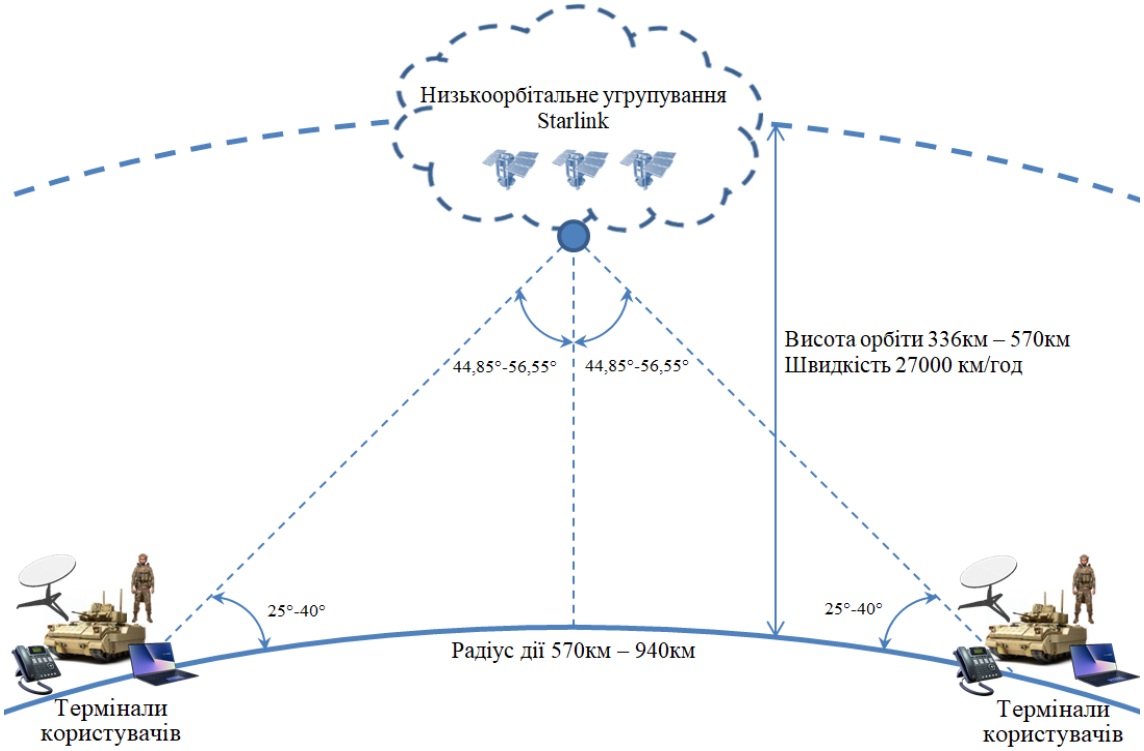


Рис. 1. Система супутникового зв’язку Starlink

Основні тактико-технічні характеристики даної системи наведено у таблиці 1.

Застосування програмних способів відключення модуля GPS в системах Starlink – Starshield та різних організаційно-технічних заходів захисту терміналів супутникового зв’язку забезпечить надійний захист системи від впливу засобів РЕБ противника.

1.2. Система супутникового зв’язку Tooway

Система резервного зв’язку Ka-Sat VSAT eTria (рис. 2) призначена для організації двостороннього супутникового зв’язку в Ka-діапазоні. Супутниковий Інтернет Tooway надається провайдером супутникового зв’язку Eutelsat на території всієї Європи з використанням супутника Ka-Sat 9A, який працює в Ka-діапазоні на геостаціонарній орбіті. Даний супутник обладнується чотирма багатоканальними антенами і транспондером та формує 82 промені, 10 з яких мають доступ та забезпечують 100 % покриття всієї території України. На один промінь виділяється смуга частот 237 МГц транспондера з пропускною здатністю 475 Мбіт/с. Маса корисного навантаження становить близько 1000 кг. Час роботи супутника на орбіті – 16 років. Супутник здатний забезпечити широкосмуговий доступ до мережі Інтернет для більше 1 мільйона користувачів [4].

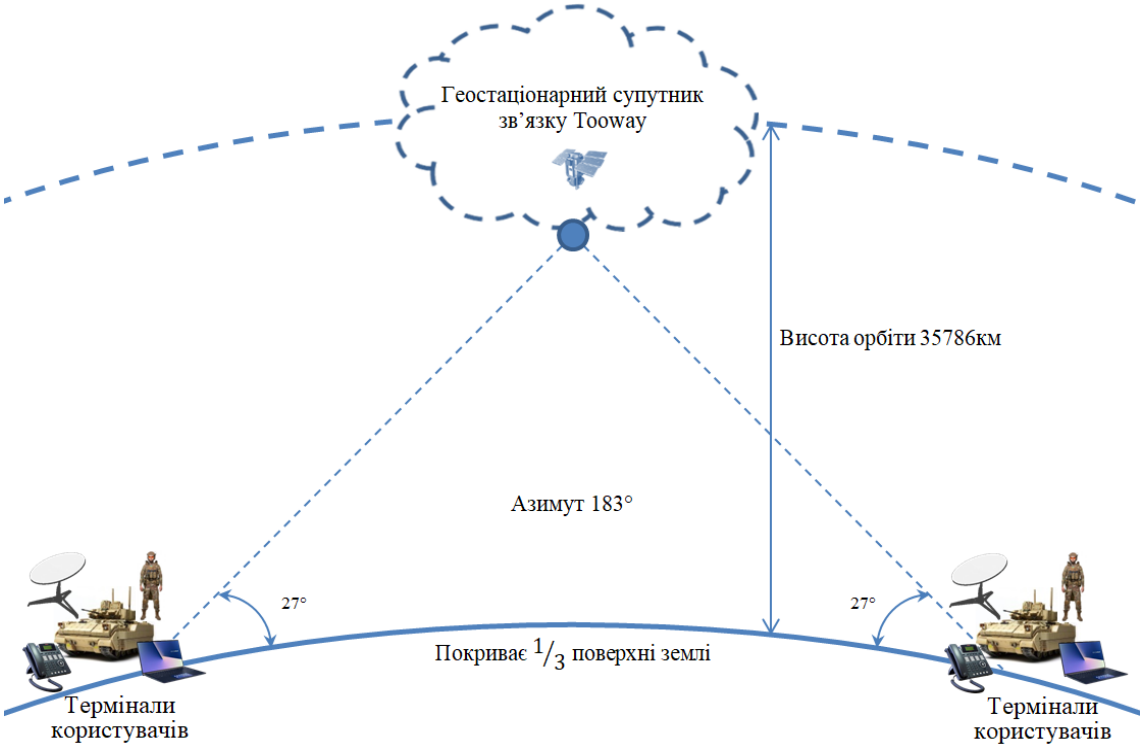


Рис. 2. Система супутникового зв’язку Tooway

ССЗ Tooway забезпечує стійкий зв’язок на усіх рівнях управління ЗС України з можливістю застосування апаратури криптографічного захисту, розширений стандарт шифрування – AES (128, 256 біт).

Основні тактико-технічні характеристики даної системи наведено у таблиці 1.

Після повномасштабного вторгнення російської федерації дана система періодично зазнає впливу зі сторони засобів РЕБ противника, що призводить до зниження швидкості передачі, рівня сигналу та періодичного зникнення сигналу від супутника. В результаті проведеного дослідження встановлено, що перебої зв’язку відбувалися внаслідок встановлення різних видів сторонніх радіозавад на транспондерах геостаціонарних супутників зв’язку у частотному діапазоні (Передача – 29,5–30,0 Ггц; Прийом – 19,7–20,2 Ггц), виділеному для функціонування даної системи.

1.3. Система супутникового зв’язку OneWeb

Система супутникового зв’язку OneWeb (рис. 3) призначена для надання широкосмугового Інтернету через угрупування OneWeb супутників в Ku-діапазоні з використанням технології CDMA (Code Division Multiple Access), що забезпечує роботу мережі за будь-яких погодних умов на низькій навколоземній орбіті (Low Earth Orbit – LEO) [10]. Дана система має гарантовану на 99,5 % доступність мережі, забезпечує підтримку будь-яких IP-додатків, голосового і відеоконференцзв’язку високої якості. ССЗ OneWeb включає в себе технологію оптимізації мультисервісних послуг (MSO), двонаправлене визначення пріоритетів QoS, вбудовані системи керування загрозами та запобігання мережевим вторгненням, антивірусну програму та 256-бітне шифрування AEAD. Система у складі понад 400 супутників на низькій навколоземній орбіті висотою 1200 км являє собою нове покоління послуг супутникового зв’язку, забезпечує в 3–5 разів меншу затримку сигналу, ніж геостаціонарні супутники. Очікуваний термін служби кожного супутника – 5 років, маса становить 147,7 кг. Це перша низькоорбітальна система, яка повністю оптимізована для підтримки онлайн-середовища з використанням сучасних додатків: SaaS/STaaS, Office 365, Google Workspace, SAP, Oracle, IBM та інших. В ССЗ можуть використовуватися термінали, як з параболічними, так і плоскими антенами. Дані термінали користувачів оснащені електронною керованою антеною, яка дозволяє автоматично відстежувати супутники OneWeb, забезпечуючи безперервне підключення сигналу. Модем CNX-WIFI дозволяє отримувати доступ до мережі Інтернет за допомогою технології WiFi.

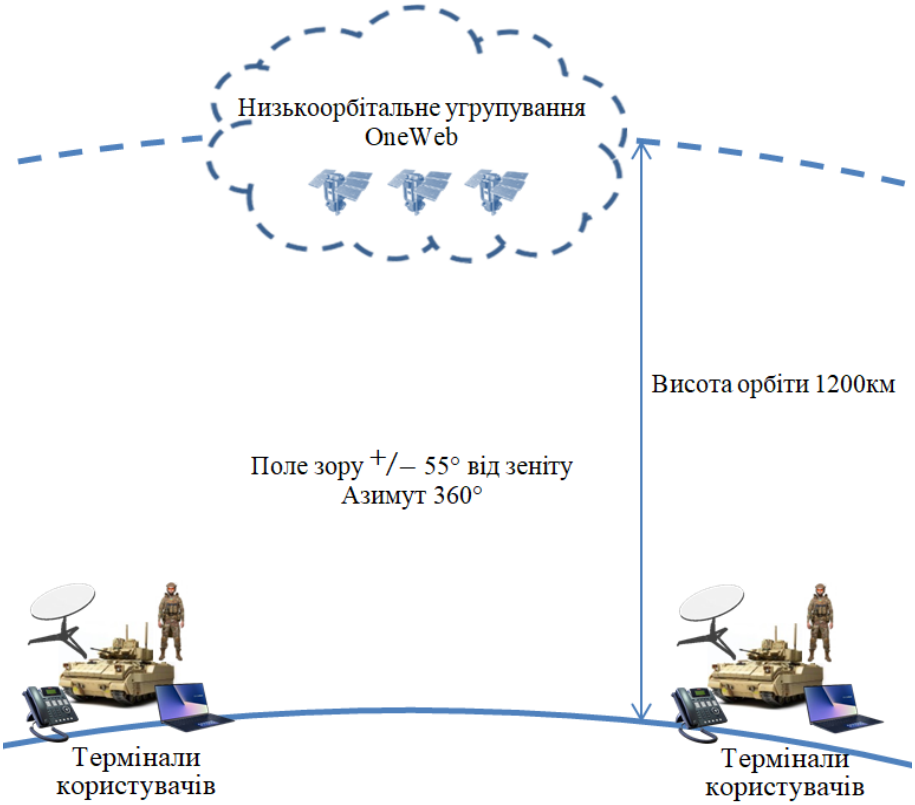


Рис. 3. Система супутникового зв’язку OneWeb

Система OneWeb використовується в наземному та морському транспорті для забезпечення фіксованого та мобільного зв’язку. Тактико-технічні характеристики даної системи наведено у таблиці 1.

ССЗ дозволяє забезпечити надійний зв’язок на всіх рівнях управління ЗС України в умовах активного застосування противником засобів РЕБ.

Тактико-технічні характеристики основних ССЗ ЗС України наведено у таблиці 1.

На підставі проведеного аналізу ефективності функціонування основних ССЗ можна зробити наступні висновки:

1. Система супутникового зв’язку Starlink забезпечує організацію високошвидкісних каналів передачі даних на усіх рівнях управління ЗС України в умовах впливу засобів РЕБ. Застосування програмних способів відключення модуля GPS та різних організаційно-технічних заходів захисту терміналів користувачів забезпечить захист системи від впливу засобів РЕБ противника.

2. Система супутникового зв’язку Tooway дозволяє організувати ефективні, інтерактивні лінії зв’язку високої якості з віддаленими військовими користувачами на різних рівнях управління. Але після повномасштабного вторгнення російської федерації система зазнала суттєвого впливу. На початку повномасштабного вторгнення була здійснена кібернетична атака на ССЗ, внаслідок чого всі станції супутникового зв’язку Ka-діапазону (модеми та прийомо-передавачі) були виведені з ладу. Кібервпливу піддалися також термінали супутникового зв’язку Ku-діапазону, а комерційний супутник, що забезпечував ресурс для ССЗ ЗС України, постійно зазнає впливу зі сторони засобів РЕБ противника, що призводить до зниження швидкості передачі, рівня сигналу або повної відсутності сигналу від супутника.

На наш погляд, перебої зв’язку відбувалися внаслідок того, що супутники на геостаціонарних орбітах постійно знаходяться над однією й тією самою точкою земної кулі, покривають майже одну третину поверхні Землі, тому противник може впливати своїми засобами РЕБ з вказаної території на роботу транспондерів даних супутників.

Таблиця 1

Системи супутникового зв’язку	**Starlink (типу rev3, hp1, rev4)**	**Tooway Ka-діапазону**	**OneWeb**
Основні складові	Wi-Fi роутер, антена	модем, передавач, антена	модем CNX, антена OW10HV
Модуляція	BPSK ... 64QAM	QPSK, 8PSK, 16APSK, 32APSK	
Діапазон частот, *ГГц*	Прд – 14,0–14,5 Прм – 10,7–12,7	Прд – 29,5–30,0 Прм – 19,7–20,2	Ku (10,7–12,7; 14,0–14,5). Ka (17,8–19,3; 27,5–30,0)
Затримка сигналу, *мс*	до 40	біля 239	до 70
Швидкість, *Мбіт*/с	до 300	до 5	до 200
Мережеві стандарти	IPv4, IPv6	VPN тунель, IPSec	IPv4, IPv6
Шифрування	WPA2, WPA3	AES (128, 256 біт)	AEAD (256 біт)
Потужність передавача, *Вт*	2/4	4/6	до 18
Електроживлення	100–240 В змінного струму	110/220 В змінного струму	100–240 В змінного струму, 12–24 В постійного струму
Споживана потужність, *Вт*	до 400	24	до 180
Тип антени	Електронна фазована решітка	Параболічна антена, ФАР	Фазована антенна решітка
Розміри антен, *см*	50 × 30, 57 × 51, 60 × 40	діаметром від 60 до 75	56 × 45 × 12
Поле зору (офсет)	100°, 110°, 140°	(10°)	+/– 55° від зеніту, азимут 360°

Системи супутникового зв’язку	Starlink (типу rev3, hp1, rev4)	Tooway Ka-діапазону	OneWeb
Коефіцієнт підсилення		Антена – 75 $G_{апд}$ = 44,2 дБі $G_{апм}$ = 40,1 дБі	$G_{апд}$ = 36,6 дБВт
Клас виконання	IP56 (IP54)	IP44	IP66
Діапазон робочих температур, °С	–30…+50	–30…+50	–40…+55
Тип орбіти	Низька навколоземна	Геостаціонарна	Низька навколоземна

3. Система супутникового зв’язку OneWeb дозволяє забезпечити надійний зв’язок на усіх рівнях управління ЗС України в умовах складної завадової обстановки. Потребує постійного контролю зі сторони експлуатуючого персоналу за технічними параметрами транспондерів і терміналів супутникового зв’язку в різних режимах роботи з метою визначення необхідності залучення додаткового обладнання, методів і способів захисту терміналів користувачів від засобів РЕБ противника.

Інші ССЗ: Satcube, KIT 9350, L-TAC Slingshot, Hughes Thuraya XT-PRO, Iridium 9575A, Kymeta Corporation, SatPaq2 проходять перевірку, апробацію та дослідну експлуатацію, після чого буде прийняте рішення на їх подальше використання в ССЗ ЗС України.

Український досвід війни з російською федерацією показав, що ворог намагається заблокувати роботу всіх операторів ССЗ ЗС України. Кібернетичній атаці піддалася ССЗ Tooway на геостаціонарній орбіті – системи Ka- та Ku-діапазонів зазнали втручання з боку противника та були виведені з ладу. Через це гостро виникло питання щодо відновлення супутникового зв’язку та застосування інших більш надійних і стійких до впливу засобів РЕБ противника ССЗ в ЗС України.

За результатами проведених досліджень та зроблених висновків щодо ефективності функціонування основних ССЗ можна констатувати, що діюча ССЗ ЗС України потребує модернізації та перебудови.

2. Метод розробки перспективної системи супутникового зв’язку Збройних Сил України

Після суттєвого впливу засобів РЕБ російської федерації на ССЗ ЗС України виникла нагальна потреба в розробці ПССЗ ЗС України.

Перспективна система супутникового зв’язку повинна забезпечувати:

управління військами (силами) ЗС України в умовах впливу засобів РЕБ противника;

доставку прийнятих рішень органам військового управління всіх рівнів шляхом збору, узагальнення та обробки різнорідної інформації;

функціонування з урахуванням бойового досвіду, набутого ЗС України під час відсічі збройної агресії з боку російської федерації, переваг та недоліків існуючих ССЗ збройних сил провідних країн світу та країн-членів НАТО.

На основі проведеного аналізу провідних країн світу по створенню військових ССЗ [4], наукового потенціалу та спроможності вітчизняного оборонно-промислового комплексу України, впливу засобів РЕБ противника на ССЗ під час відсічі збройної агресії російської федерації, розробку ПССЗ ЗС України, на наш погляд, можна розділити на два етапи:

перший етап – оренда потоків (каналів) або частотно-орбітального ресурсу у захищених військових ССЗ країн-членів НАТО та/або у низькоорбітальних комерційних систем провідних країн світу;

другий етап – розроблення сучасної ССЗ ЗС України або Національної системи супутникового зв’язку з використанням новітніх інформаційно-комунікаційних технологій, у якої для військових користувачів виділяються потоки (канали) або частотно-орбітальний ресурс.

2.1. Розробка перспективної системи супутникового зв’язку ЗС України на основі оренди потоків (каналів) або частотно-орбітального ресурсу

На першому етапі розробки ССЗ ЗС України спочатку потрібно правильно вибрати оператора супутникового зв’язку з його навколоземною орбітою, а потім розвивати її наземний потенціал.

Існуючі ССЗ на геостаціонарних орбітах використовують супутники, які постійно знаходяться над однією й тією самою точкою земної кулі, покривають майже одну третину поверхні Землі, тому існує можливість впливу на неї зі сторони засобів РЕБ (РЕР) противника. До повномасштабного вторгнення російської федерації в Україну армії провідних країн світу та країн-членів НАТО здебільшого використовували/орендували ресурс у військових ССЗ на геостаціонарних орбітах, так як більшість комерційних операторів взагалі не досліджували роботу своїх систем у складній радіоелектронній обстановці [4]. Тому для прийняття рішення по оренді потоків (каналів) або частотно-орбітального ресурсу у військових ССЗ країн-членів НАТО на геостаціонарних орбітах необхідно провести випробування та дослідну експлуатацію на предмет захисту систем від засобів РЕБ противника. Водночас дані системи мають відносно низьку пропускну здатність, значну затримку сигналу і не спроможні задовольняти сучасні потреби ЗС України з організації зв’язку в режимі реального часу та тенденцій на постійне збільшення потоку інформації на одного користувача. Через це ССЗ ЗС України, на наш погляд, необхідно будувати з використанням низькоорбітальних супутників.

Уже сьогодні більшість супутників, які знаходяться на орбітах, використовують низькі навколоземні орбіти. Через незначну відстань до поверхні Землі дані системи забезпечують високу швидкість передачі, значну перевагу за енергетичними характеристиками та нижчу вартість розгортання.

Системи з використанням супутників на низьких навколоземних орбітах мають ряд переваг та недоліків щодо супутників на геостаціонарних орбітах [3].

Основні переваги:

значна швидкість передачі даних;

низька затримка розповсюдження сигналу;

можливість організації зв’язку в русі;

забезпечення зв’язку між супутниками;

відносна дешевизна послуг та менші витрати на запуски;

забезпечення швидкісного широкосмугового доступу до Інтернету;

стійкі до засобів РЕБ противника.

Основні недоліки:

необхідність великої кількості супутників на орбіті, захаращення орбіти Землі та короткий термін їх експлуатації.

На підставі проведеного дослідження пропонуємо на конкурсній основі орендувати потоки (канали) або частотно-орбітальний ресурс у декількох низькоорбітальних операторів супутникового зв’язку. Цей ресурс можна використовувати на різних рівнях управління, для окремих видів та родів військ ЗС України.

За результатами проведеного дослідження пропонується нова модель ПССЗ ЗС України, яку наведено на рисунку 4.

Під час вибору/розробки ССЗ особлива увага приділяється її космічному сегменту. ССЗ повинна мати над Україною найбільш високий і стабільний рівень сигналу, забезпечувати необхідну швидкість передачі, низьку затримку сигналу та стійкість до засобів РЕБ (РЕР) противника. Хоча в сучасних військових та деяких комерційних системах вже передбачені ряд методів захисту від завад, а саме: бортова обробка сигналів, використання вузьких променів бортових діаграм направленості та інші, але це не дозволяє повністю забезпечити

надійне функціонування створюваної ПССЗ ЗС України. Водночас Китай та російська федерація вкладають значні кошти в розвиток військових супутникових систем, мають розвинені засоби наземної та космічної розвідки і РЕБ. За такими аспектами розвитку систем, як: РЕБ (РЕР) в космосі, застосування лазерних технологій, виведення з ладу супутників на орбітах різного призначення, – дані країни знаходяться на лідируючих позиціях в світі. Тому під час розроблення ПССЗ ЗС України особливу увагу необхідно приділяти захисту ССЗ від засобів РЕБ (РЕР) противника.

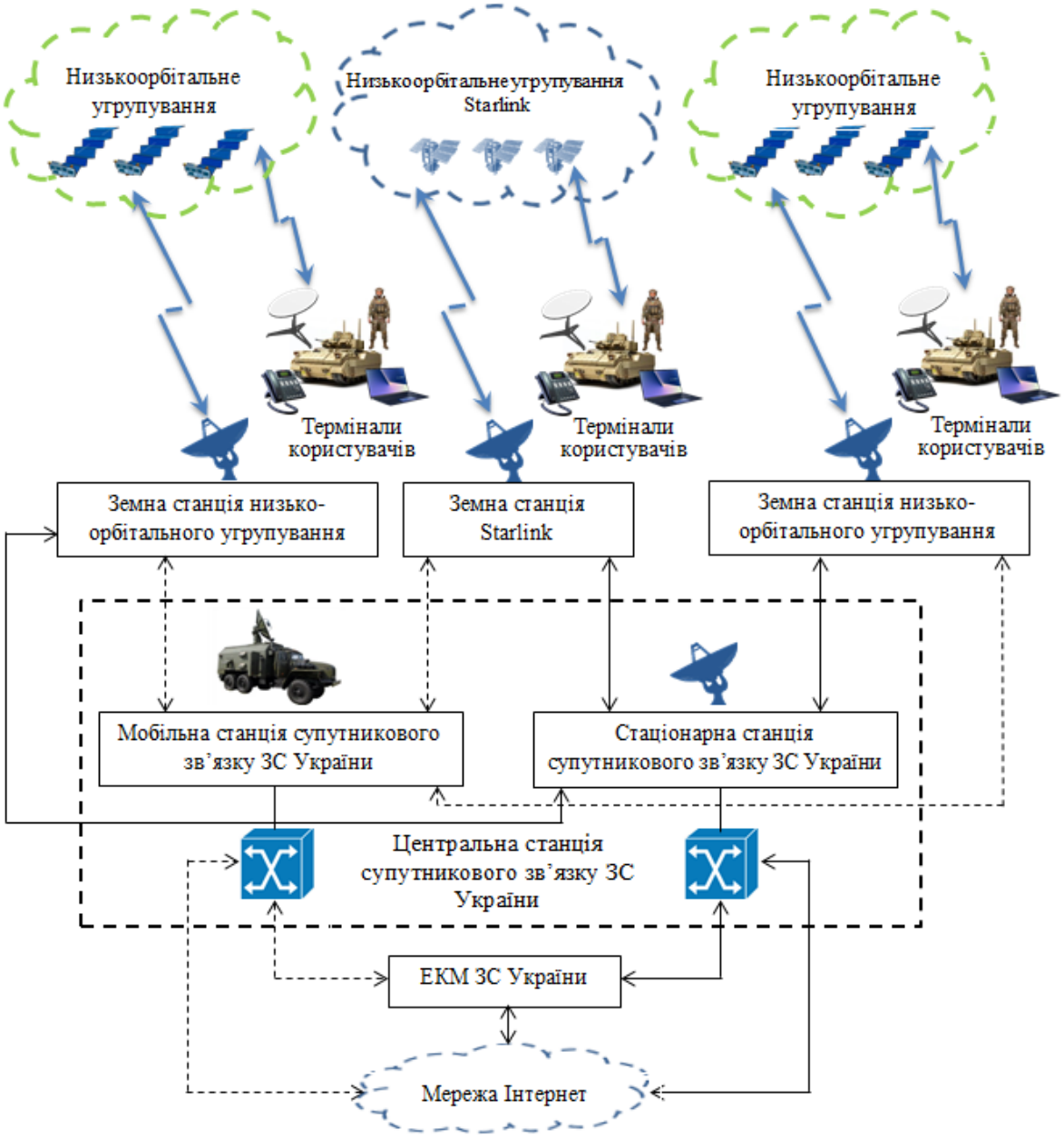


Рис. 4. Нова модель ПССЗ ЗС України з використанням низькоорбітальних супутників

Запропонована модель ПССЗ ЗС України з використанням низькоорбітальних угруповань супутників забезпечить:

збільшення швидкості передачі даних для кожного користувача до 1 Гбіт/с;

зниження затримки сигналу до 70 мс (близьку до наземних ліній зв’язку), що дає змогу передавати інформацію в режимі реального часу;

передачу інформації між супутникам за допомогою лазерного променю, який значно підвищує швидкість та стабільність сигналу;

можливість зв’язку під час руху;

незначну вартість 1 Мбіт/с швидкості передачі даних;

стійкість до засобів РЕБ противника та інші.

Стійкість до засобів РЕБ противника досягається завдяки:

багатошаровості побудови систем;

застосуванню великої кількісті супутників в декількох орбітальних площинах;

використанню орбіт на різних висотах, з різним нахилом, полярних або приполярних;

руху супутників із великою швидкістю по відношенню до наземних станцій;

відносно невеликому радіусу зони покриття супутника;

антені терміналу користувача, яка “бачить” один супутник лічені хвилини з подальшим переключенням на інший;

використанню бортової обробки сигналів;

застосуванню вузьких променів бортових діаграм направленості (гостронаправлених антен);

використанню сучасних типів та видів модуляції;

наявності резерву та інших.

Після вибору низькоорбітальної ССЗ, укладання договору з оператором супутникового зв’язку на оренду потоків (каналів) або частотно-орбітального ресурсу для більш якісного управління та функціонування даної системи створюється її наземний сегмент.

До складу ПССЗ ЗС України увійдуть: орендований ресурс декількох систем на низьких навколоземних орбітах; центральні станції (стаціонарна, мобільна); земні станції; термінали користувачів. Центральна станція супутникового зв’язку виконує функції центрального вузла і забезпечує управління роботою всієї ССЗ ЗС України з використанням низькоорбітальних супутників, перерозподілом її ресурсів, виявлення несправності та з’єднання з електронною комунікаційною мережею ЗС України.

2.2. Розробка перспективної системи супутникового зв’язку ЗС України з використанням наукового та промислового потенціалу України

Діюча Концепція державної політики у сфері космічної діяльності на період до 2032 року [5] застаріла та не відповідає сучасним реаліям розвитку ракетно-космічної галузі в Україні. Тому на другому етапі розробки ССЗ ЗС України, на наш погляд, необхідно прийняти нову Концепцію Загальнодержавної цільової науково-технічної космічної програми зі створення системи космічної підтримки ЗС України, або нову Національну систему супутникового зв’язку, у якої для військових користувачів виділяються потоки (канали) або частотно-орбітальний ресурс.

Прийняття нової концепції є вкрай важливим завданням для забезпечення виконання стратегічних державних завдань у сфері національної безпеки і оборони України та потребує реалізації її на державному рівні з максимальною концентрацією зусиль і ресурсів органів державної влади та промисловості України. На основі виділених потоків (каналів) або частотно-орбітального ресурсу у Національної системи супутникового зв’язку створюється власна Військова система супутникового зв’язку (далі – ВССЗ). Створення ВССЗ, як складової Національної системи супутникового зв’язку на основі національних супутників, – головна задача, яка стоїть перед Україною на ближню перспективу. В подальшому на підставі прийнятої програми, виведення супутників на орбіти – розвивати та удосконалювати діючу ССЗ ЗС України. Під час розроблення нової ПССЗ необхідно використовувати досвід провідних держав світу та країн-членів НАТО, які розробляють й активно використовують

космос в інтересах своїх збройних сил, а також розглядають космічні засоби як найважливіший елемент забезпечення бойових дій із застосуванням новітніх інноваційно-комунікаційних технологій та державно-приватного партнерства.

ВССЗ повинна розроблятися на стадії створення Національної системи супутникового зв’язку на підставі Проєктно-конструкторських та Дослідно-конструкторських робіт відповідно до Загальних вимог та тактико-технічних завдань.

3. Наукове обґрунтування застосування адаптивних антенних решіток в перспективній системі супутникового зв’язку ЗС України

ПССЗ ЗС України на ряду із забезпеченням високого та стабільного рівня сигналу над Україною, необхідної швидкості передачі, низької затримки сигналу повинна також підтримувати радіоелектронний захист від засобів РЕБ (РЕР) противника.

3.1. Основні положення та способи впливу наземних станцій радіоелектронної боротьби на системи супутникового зв’язку

Радіоелектронна боротьба (electronic warfare) – сукупність узгоджених за метою, завданням, місцем і часом дій військ (сил) щодо виявлення систем і засобів управління військами та зброєю противника, їх радіоелектронного подавлення, радіоелектронного захисту своїх систем і засобів управління, а також виконання заходів електронної підтримки радіоелектронної боротьби. РЕБ є одним із видів підтримки операцій (бойових дій) [6].

Основні задачі, які виконують засоби РЕБ:

розкриття (виявлення) радіоелектронної обстановки;

радіоелектронне подавлення систем і засобів управління військами, зброєю, РЕБ і РЕР противника;

дезорганізація систем бойового управління противника у прийнятті оперативних (бойових) рішень з метою підвищення ефективності ведення бойових дій своїми військами;

руйнування, знищення і/чи спотворення програмного забезпечення й інформації в автоматизованих системах управління противника;

зниження ефективності застосування противником засобів РЕБ;

забезпечення електромагнітної сумісності радіоелектронних засобів.

Радіоелектронний захист – комплекс організаційно-технічних заходів і дій, спрямованих на забезпечення стійкої роботи своїх систем управління військами (силами) і зброєю. Радіоелектронний захист організовується та проводиться з метою забезпечення стійкої роботи систем і засобів управління своїми військами (силами) і зброєю в умовах ведення противником РЕБ та взаємного впливу радіоелектронних засобів [6].

Радіоелектронне подавлення ведеться у діапазоні радіохвиль, в якому працюють ССЗ ЗС України, і полягає в порушенні роботи супутників на різних навколоземних орбітах, наземних терміналів (станцій) і засобів радіонавігації шляхом дії на їх приймальні пристрої електромагнітним радіовипромінюванням станцій перешкод (РЕБ).

В умовах активної РЕБ з метою зниження ефективності застосування противником засобів РЕБ в сучасних ССЗ використовуються наступні заходи захисту: бортова обробка сигналів, використання вузьких променів бортових діаграм направленості, технології адаптивних антенних решіток та інші.

На рисунку 5 наведено розроблену схему впливу наземних станцій перешкод (РЕБ) на наземні термінали (станції) супутникового зв’язку та супутники на низьких навколоземних орбітах і GPS.

Як видно зі схеми, станції перешкод (РЕБ) можуть впливати на роботу не тільки наземних терміналів (станцій) супутникового зв’язку, а також на супутники на різних навколоземних орбітах та GPS. Для найпростіших ситуацій якість прийому супутників та терміналів користувачів буде залежати від відношення сигнал/шум [6].

$$P_{прм} = P_с/P_{\sum ш},$$

де $P_{\sum ш} = P_ш + P_з$;

$P_{\sum ш}$ – сумарний рівень шуму;

$P_ш$ – рівень шуму у вільному просторі;

$P_з$ – рівень завади, яка надходить від станції перешкод.

Для збільшення рівня прийому корисного сигналу, тобто зменшення шуму на орбітальних супутниках та наземних станціях, можна застосовувати технології адаптивних антенних решіток.

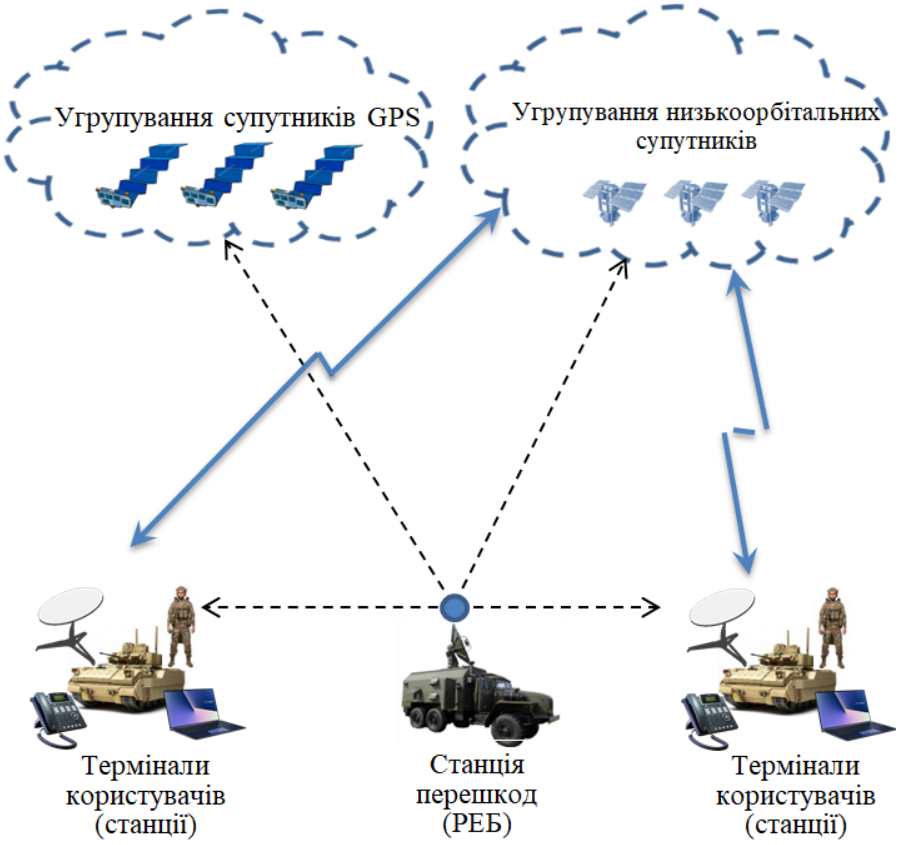


Рис. 5. Схема взаємодії між наземними терміналами супутникового зв’язку, станціями перешкод та супутниками у процесі радіоелектронного впливу

3.2. Принцип роботи адаптивних антенних решіток

Адаптивні антенні решітки здатні визначати напрямок впливу завади і зменшувати її вплив в умовах відсутності апріорної інформації про сигнально-завадову обстановку. Особливістю таких решіток є зміна діаграми направленості антени залежно від розташування терміналу (станції). Дані адаптивні антенні решітки змінюють свою діаграму направленості, зосереджуючи усю випромінювану потужність або найбільш ефективного прийому сигналу в напрям до розміщення терміналу користувача (станції).

Прийом сигналу за допомогою багатоелементних антенних решіток буде одним з основних методів вирішення складних завдань виявлення й оцінювання, оскільки формування діаграм направленості систем із решіткою має переваги перед системами з одноелементними антенними датчиками. Створення систем з антенними решітками, які здійснюють автоматичне підстроювання характеристик відповідно до змінних умов прийому сигналу, стало можливим завдяки появі недорогих міні-ЕОМ (електронно-обчислювальних

машин), що дозволяє реалізувати на їх основі відомі результати теорії виявлення, оцінювання та управління. Здатність до адаптації дає можливість більш гнучкої роботи системи і дозволяє підвищити ефективність прийому, що часто складно реалізувати іншими методами [7].

Звичайні системи чутливі до зменшення відношення сигнал/шум, що обумовлено неминучою присутністю поряд із корисним сигналом небажаних “шумових” сигналів, які надходять на вхід по бічним і/або по головній пелюсткам діаграми направленості антени (рис. 6). Ці сигнали (завади) можуть створюватися засобами РЕБ, передавачами завад, відбиванням від місцевих предметів й іншими джерелами шуму. Зменшення відношення сигнал/шум, крім того, може бути обумовлено рухом антени, невдалою її установкою, ефектами багатопроменевого поширення і змінною завадовою ситуацією.

У зв’язку з цим системи з адаптивними антенними решітками залишаються предметом інтенсивних досліджень, оскільки вони підвищать ефективність прийому корисних сигналів при наявності зазначених завад у системах супутникового зв’язку. Основна причина уваги до адаптивних антенних решіток полягає в здатності таких систем без апріорної інформації про завадову ситуацію автоматично виявляти присутність джерел завад і подавляти їх сигнали на виході, покращуючи тим самим прийом корисного сигналу.

Нижче наводиться приклад роботи адаптивної антенної решітки, яка характеризується її діаграмою направленості (рис. 6). Максимальна потужність діаграми направленості зосереджується у напрямку розміщення корисного сигналу від терміналу (станції), що призводить до найбільш ефективного прийому сигналу. Придушення завадового сигналу досягається за рахунок управління положеннями нулів діаграми направленості і зменшення рівня бічних пелюсток в напрямку джерела завад.

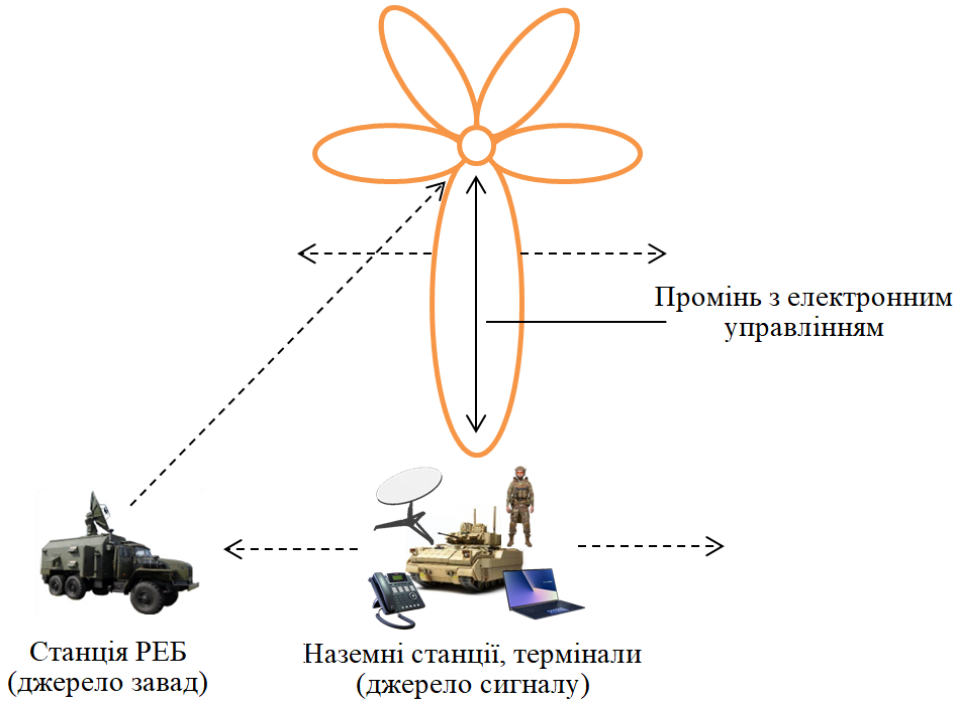


Рис. 6. Принцип роботи адаптивної антенної системи

В адаптивних антенних решітках, які іноді називають “Smart-антенами” (розумними антенами), здійснюється підстроювання характеристик корисного сигналу відповідно до інформації, що надходить про сигнал.

Пояснення роботи адаптивної антени випливає з розгляду наведеної структурної схеми (рис. 7).

Антена виконана у вигляді решітки, яка складається з S_n елементів, і призначена для прийому сигналу у відповідному середовищі поширення. Елементи розміщені так, аби забезпечувалося формування необхідної діаграми направленості в заданій області простору. Характеристики елементів та їх фактичне розташування в решітці накладають основні обмеження на результуючі властивості системи з адаптивною решіткою.

“Серцем” адаптивної антенної системи є цифровий процесор (по суті, це адаптивний фільтр), який відповідає за прийом і обробку сигналів. Основна мета обробки полягає в максимізації відношення сигнал/шум за рахунок автоматичного регулювання вагових коефіцієнтів (w_n), з якими сумуються сигнали, прийняті окремими елементами антенної решітки.

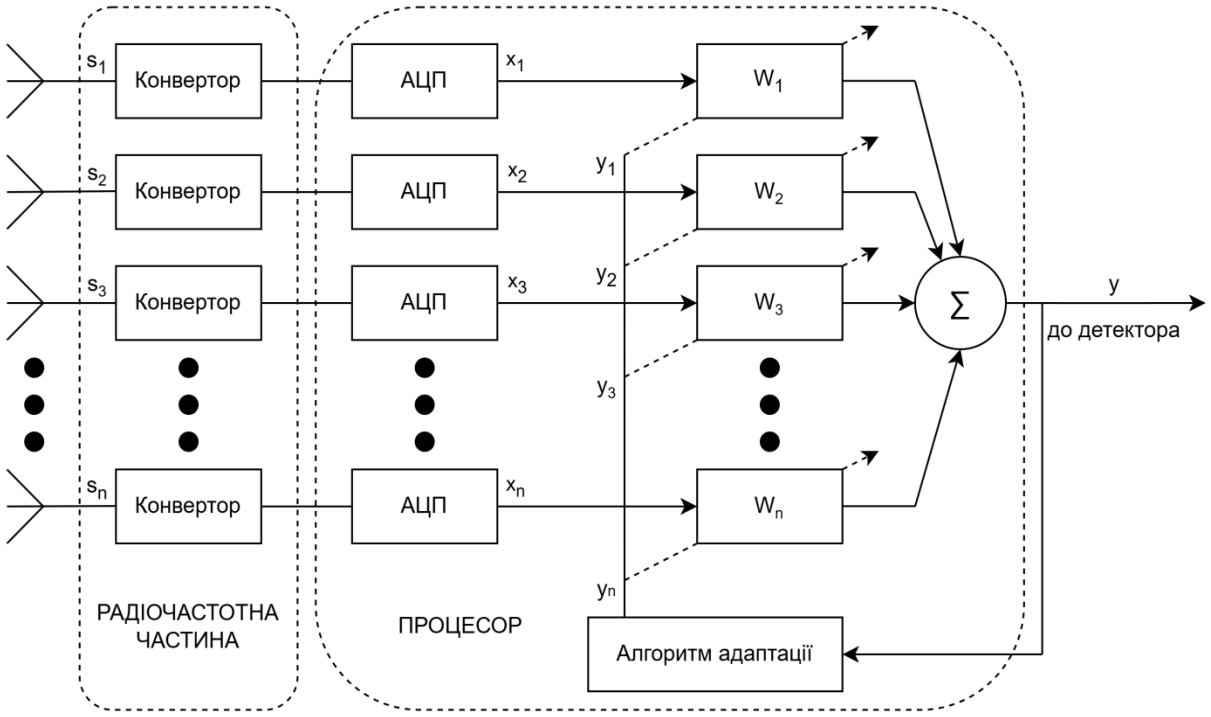


Рис. 7. Структурна схема адаптивної антенної системи

Процес адаптації математично еквівалентний відніманню з вихідної діаграми направленості антенної решітки так званої компенсаційної діаграми, що формується з урахуванням оптимальних (вагових) коефіцієнтів. Внаслідок цього результуюча діаграма направленості антени має “провали” в напрямку завади. Рівень придушення завад і складність процесора визначаються використовуваним методом адаптації.

Сигнали, прийняті елементами антенної решітки S_n, проходять через тракт перетворення частоти в цифровий вид в лінійці АЦП. На виході АЦП формується набір цифрових сигнальних відліків сигналів та завад $x_n(t)$ $(x_1, x_2, \ldots, x_n)$, далі поелементно перемножуються з набором вагових коефіцієнтів $w_n(t)$ $(w_1, w_2, \ldots, w_n)$ і потім поступають на суматор $\sum$. На виході суматора формується вихідний сигнал $y(t)$, який далі використовується в приймальному тракті. Отриманий таким чином сигнал $x_n(t)$ $w_n(t)$ порівнюється з деяким опорним сигналом $y_n(t)$, в результаті чого формується сигнал неузгодженості шляхом порівняння помилки, що підлягає мінімізації [8]:

$$v(t) = x_{\text{n}}(t)\, w_{\text{n}}(t) - y_{\text{n}}(t).$$

У разі повної відповідності $y_{\text{n}}(t) = x_{\text{n}}(\text{t})\, w_{\text{n}}(t)$ величина отриманої неузгодженості $v(t)$ містить всю інформацію про стан завад і шумів в адаптивній антенній системі.

Вагові коефіцієнти у процесі адаптації змінюються відповідно до того чи іншого критерію мінімізації помилки. Наприклад, при використанні алгоритму LMS (мінімізації середнього квадрата помилки – Least Mean Square) оновлені вагові коефіцієнти розраховуються за формулою [7]:

$$\boldsymbol{w}\,(k+1) = \boldsymbol{w}(k) + \mu \cdot \boldsymbol{e}^{*}(k)\, \boldsymbol{x}(k),$$

де $\boldsymbol{w}(k)$, $\boldsymbol{e}(k)$, $\boldsymbol{x}(k)$ – вектори вагової обробки, сигналу помилки і сигналу на вході відповідно;

$*$ – знак комплексного сполучення.

Для генерування сигналу помилки опорний сигнал $y(n)$ вираховується із сигналу на виході фільтра. Далі сигнал помилки використовується для підстроювання коефіцієнтів цифрового фільтра, що мінімізує сигнал помилки на наступному такті обробки. Таким чином, суть адаптивної фільтрації полягає в мінімізації неузгодженості між вхідним сигналом $x(n)$ і опорним сигналом $y(n)$.

Початкові значення коефіцієнтів фільтра, як правило, визначаються при передачі деякого еталонного сигналу, що являє собою відомий зразок даних. При цьому роль алгоритму адаптації полягає в коригуванні коефіцієнтів фільтра для встановлення відповідності між оцінкою отриманих даних і їх еталоном [7].

Перевагами "Smart-антен" є: можливість адаптації до завадової обстановки; підвищення якості передачі даних; зменшення споживання енергії терміналом користувача; мала ймовірність виявлення та перехоплення. Недоліками – складність в реалізації та висока вартість.

Висновки. Використання адаптивних антенних решіток у наземних станціях та супутниках ССЗ ЗС України дозволяє без апріорної інформації про завадову ситуацію автоматично виявляти присутність джерел завад і подавляти їх сигнали на виході, покращуючи тим самим прийом корисного сигналу. В супутникових системах з адаптивними решітками можуть додатково застосовуватися інші методи придушення завад, при цьому результуюча ефективність буде набагато вищою, ніж при звичайних широко відомих способах, таких як використання широкосмугових сигналів, гостронаправлених антен та бортової обробки сигналів.

В результаті проведеного дослідження була досягнута поставлена мети, а саме: розроблена нова модель ПССЗ ЗС України на основі оренди потоків (каналів) або частотно-орбітального ресурсу у супутників на низьких навколоземних орбітах. Створена система забезпечить необхідну швидкість передачі, живучість та стійкість до засобів РЕБ противника на різних рівнях управління ЗС України. Дана модель розроблялася з врахуванням досвіду ведення війни з російською федерацією, аналізу існуючих систем супутникового зв'язку армій провідних країн світу і країн-членів НАТО та новітніх досягнень інформаційно-комунікаційних технологій. До складу ПССЗ ЗС України увійдуть: орендований ресурс декількох систем на низьких навколоземних орбітах; центральні станції (стаціонарна, мобільна); земні станції; термінали користувачів. Для окремих видів та родів військ ЗС України можна використовувати інші системи і засоби супутникового зв'язку. Для збільшення захисту від радіоелектронного придушення орбітальних супутників та наземних станцій (терміналів користувачів) рекомендується застосовувати адаптивні антенні решітки.

Подальші напрямки дослідження передбачають у цифрових антенних решітках застосування адаптивного формування променю антенної решітки на базі SDR технології,

що дозволить формувати більш вузьку діаграму направленості, яка призведе до зменшення інтерференції та надання доступу більшій кількості користувачів до одного і того самого елементу решітки одночасно, використовуючи одні й ті самі частоти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ВКП 6-00(01).01. Доктрина «Зв’язок та інформаційні системи», затверджена Головнокомандувачем Збройних Сил України 1 липня 2020 року.

2. СД 7.01.1.057. Настанова «Супутниковий зв’язок Збройних Сил України», затверджена Начальником Генерального штабу Збройних Сил України в липні 2020 року.

3. Руденко В. І., Зінченко М. О., Яковчук О. В., Плугова О. Б. Аналіз ефективності функціонування та перспективи розвитку системи супутникового зв’язку спеціального призначення // Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 1 (49). С. 45–58.

4. Білий О. А., Шолудько В. Г., Малих В. В., Гай Ю. І. Перспективи розвитку системи супутникового зв’язку ЗС України // Збірник наукових праць ВІТІ. 2018. № 2. С. 6–15.

5. Про схвалення Концепції реалізації державної політики у сфері космічної діяльності на період до 2032 року: розпорядження від 30.03.2011 № 238-р. URL: https://zakon.rada.gov.ua/laws/show/238-2011-%D1%80#Text (дата звернення: 14.03.2025).

6. ВКДП 10-27(56).01. Настанова виконання заходів радіо-, радіотехнічного контролю окремим спеціальним центром радіоелектронної боротьби (окремим вузлом радіоелектронної боротьби) у ході застосування військ (сил), затверджена Командувачем Сил підтримки ЗС України від 18.12.2020.

7. Монзінго Р. А., Міллер Т. У. Адаптивні антенні решітки. Введення у теорію.

8. Лебідь Є. В., Лазута Р. Р., Коваль О. М. (НУОУ ім. Черняхівського). Оцінка ефективності застосування адаптивних антенних решіток у системах радіозв’язку в умовах активної радіоелектронної боротьби // Збірник наукових праць ВІТІ. 2020. № 1. С. 46–57.

9. Starlink // Wikipedia. URL: https://en.wikipedia.org/wiki/Starlink (date of access: 24.03.2025).

10. OneWeb // Wikipedia. URL: https://uk.wikipedia.org/wiki/OneWeb (date of access: 31.03.2025).

DOI: 10.58254/viti.7.2025.14.147

УДК 519.876.5:004.056:004.491.42

д-р техн. наук, професор Савченко В. А. ORCID: 0000-0002-3014-131X (ДУІКТ)
Хавер А. В. ORCID: 0009-0003-4731-914X (ДУІКТ)

МЕТОД РОЗРАХУНКУ КІБЕРСТІЙКОСТІ 2-1 РІВНІВ МОДЕЛІ PURDUE ПРОТИ СПЕЦІАЛІЗОВАНОГО ТЕХНОЛОГІЧНОГО ТРОЯНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Забезпечення кіберстійкості об'єкта критичної інформаційної інфраструктури, зокрема його технологічної системи, є одним з основних завдань, яке стоїть перед керівництвом сучасних державних і приватних підприємств як в Україні, так і світі загалом.

Кібератаки на технологічні системи об'єктів критичної інфраструктури зазвичай здійснюються хакерськими групами (суб'єктами кіберзагрози), які спонсоруються зацікавленими державами. Метою такої кібератаки може бути як кібершпигунство, так і здійснення деструктивного кібервпливу на фізичні виробничі системи підприємства, що може загрожувати значними фінансовими збитками, зупинкою технологічного процесу й навіть техногенними катастрофами. Головним інструментом, із використанням якого суб'єктами кіберзагрози здійснюються такі кібератаки, є спеціалізоване технологічне троянське програмне забезпечення.

Інформаційні системи об'єкта критичної інфраструктури поділяються на комунікаційну та технологічну системи (які ще прийнято називати корпоративною та промисловою відповідно), кожна з яких є об'єктом критичної інформаційної інфраструктури. Найбільш небезпечною є кібератака на 2-1 рівні (згідно з моделлю Purdue) технологічної системи об'єкта критичної інфраструктури. Це зумовлено тим фактом, що на 2-1 рівнях моделі розгорнуті та функціонують найбільш важливі інформаційні підсистеми технологічної системи об'єкта критичної інфраструктури – Basic Process Control Systems і Safety Instrumented Systems. Кіберстійкість Safety Instrumented Systems є ключовим елементом кіберстійкості технологічної системи об'єкта критичної інфраструктури.

Ключові слова: *метод, кібербезпека об'єктів критичної інформаційної інфраструктури, кіберстійкість, спеціалізоване технологічне троянське програмне забезпечення, технологічна система, Basic Process Control Systems, Safety Instrumented Systems, Supervisory Control and Data Acquisition, рішення промислового кіберзахисту.*

V. Savchenko, A. Khaver. Method for calculating the cyber resilience of levels 2-1 of the Purdue model against specialized technological trojan software

Ensuring the cyber resilience of a critical information infrastructure facility, particularly its technological system, is among the primary the primary responsibilities of the management of modern public and private enterprises, both in Ukraine and globally.

Cyberattacks targeting the technological systems of critical infrastructure facilities are typically conducted by hacker groups (cyber threat actors) sponsored by state entities. The objectives of such cyberattacks may include both cyber espionage and destructive cyber impacts on an enterprise's physical production systems, potentially leading to substantial financial losses, disruption of technological process and even man-made disasters. The principal tool employed by cyber threat actors to execute such cyberattacks is specialized technological Trojan software.

The information system of a critical infrastructure facility are divided into communication and technological systems (also called corporate and industrial, respectively), each of which is an object of critical information infrastructure. The most dangerous is a cyberattack at level 2-1 (according to the Purdue model) of the technological system of a critical infrastructure facility. This is due to the fact that the most important information subsystems of the technological system of a critical infrastructure facility are deployed and operate at levels 2-1 of the model - Basic Process Control Systems and Safety Instrumented Systems. The cyber resilience of the Safety Instrumented Systems constitutes a critical component of the overall cyber resilience of the technological system of a critical infrastructure facility.

Keywords: *method, cybersecurity of critical information infrastructure facilities, cyber resilience, specialized technological Trojan software, technological system, Basic Process Control Systems, Safety Instrumented Systems, Supervisory Control and Data Acquisition, industrial cybersecurity solutions.*

Постановка завдання. В умовах, коли кіберстійкість об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) є критично необхідною умовою переваги держави як протиборчої одиниці в кіберпросторі, важливим є забезпечення її високого рівня щодо технологічних систем об'єктів критичної інфраструктури держави та забезпечення

належного кіберзахисту проти деструктивного кібервпливу. Деструктивний кібервплив – це кібератака, метою якої є пошкодження або знищення даних, апаратної та/або програмної складової комунікаційної або технологічної системи (зазвичай об’єкта критичної інфраструктури), порушення її сталого функціонування та/або порушення функціонування елементів, що входять до її складу.

Аналізуючи найбільш резонансні та складні кібератаки на ОКІІ впродовж останнього десятиліття, які мали на меті деструктивний кібервплив, можна зробити висновок, що необхідною передумовою до їх успішного проведення було отримання доступу до керування критичними функціями Safety Instrumented Systems. Цей факт підтверджують численні звіти провідних дослідних компаній у галузі кібербезпеки щодо кібератаки “Blackenergy” (2015 р.), “Industroyer”/“Industroyer v2” (2016 р., 2024 р.), “Triton” (2017 р.) та ін. Заразом всі вони були здійснені з використанням спеціалізованого технологічного троянського програмного забезпечення (далі – СТТПЗ). Автором пропонується наступна дефініція терміну СТТПЗ – це вид кіберзброї, що маскується від засобів виявлення та/або імітує легітимне програмне забезпечення, має функції віддаленого управління та призначене для застосування в конкретній технологічній системі/конкретних типах технологічних систем (з урахуванням технологічних особливостей будови інформаційних систем) з метою здійснення кібершпигунства чи/та деструктивного кібервпливу.

Крім того, дотепер у науковому середовищі спостерігається помітний дефіцит досліджень та публікацій щодо підвищення кіберстійкості головних інформаційних підсистем технологічних систем, зокрема Basic Process Control System і Safety Instrumented Systems, та висвітлення ймовірних негативних наслідків впливу на технологічний процес від суб’єктів кіберзагрози на вищезазначені підсистеми.

За даними MITRE ATT&CK for Industrial Control Systems: Design and Philosophy, найчастіше ціллю хакерів у технологічній системі є наступні три основні інформаційні підсистеми рівня 3 і нижче моделі Purdue: Basic Process Control Systems (далі – BPCS), Safety Instrumented Systems (далі – SIS), Engineering and Maintenance Systems (далі – EMS). Модель Purdue (Purdue Enterprise Reference Architecture (“PERA”/”ISA-99”), далі – модель) – еталонна модель сегментації комунікаційної та технологічної систем.У контексті даної публікації здійснюється дослідження на 2-1 рівнях моделі Purdue (Control Systems Zone – Basic controls Zone).

Варто зауважити, що у разі, якщо кібератака здійснюється суб’єктом кіберзагрози з метою кібершпигунства, то найчастіше вона буде поширюватися на рівні моделі не нижче другого. Це обґрунтовано тим фактом, що саме другий рівень моделі є найнижчою ланкою технологічної мережі, на яку може поширитися кібератака з метою отримання технологічних даних, так як нижче дані щодо діяльності підсистем технологічної мережі не є структурованими, отже їх аналіз ускладнюється та не є виправданим. У свою ж чергу деструктивна кібератака з високою долею ймовірності може поширитися на перший рівень моделі (що залежить від кінцевої мети такого деструктивного кібервпливу).

Аналіз літератури. Аналіз останніх наукових досліджень і публікацій щодо кібербезпеки технологічних систем об’єктів критичної інфраструктури та їх складових, зокрема кібербезпеки Safety Instrumented Systems (далі – SIS), вказує на те, що за даним вектором активно проводять свої дослідження як українські, так й іноземні науковці.

Серед українських науковців (за результатами аналізу публікацій на платформах “Scopys” та “Web of Science”) питаннями кіберзахисту технологічних систем, у тому числі на 2-1 рівнях моделі, займаються [1–3] та інші. Спрямування досліджень зазначених авторів пов’язані з підвищенням кібербезпеки технологічних систем, в тому числі в окремих дослідженнях із використанням підходів машинного навчання.

Серед іноземних науковців питання кіберзахисту SIS на об’єктах критичної інфраструктури морських нафтових родовищ (в нафто-, газовидобувному секторі) підіймаються у дослідженнях [4]; із проблематикою ідентифікації кіберризиків для контрольно-вимірювальних систем та SIS пов’язані наукові дослідження [5]; дослідженнями рішень кібербезпеки для цифрових контрольно-вимірювальних приладів і систем керування на об’єктах ядерної енергетики займалися [6]. Серед вищеперерахованих досліджень не було запропоновано конкретного рішення для покращення такого показника кіберстійкості Safety Instrumented System, як стійкість перед СТТПЗ.

Мета та завдання дослідження. Розробка методу розрахунку кіберстійкості 2-1 рівнів моделі проти спеціального технологічного троянського програмного забезпечення.

Основними завданнями дослідження є:

– вибір взаємоархітектури між BPCS і SIS для оптимальної підтримки кібербезпеки технологічного процесу;

– проаналізувати тактики, які можуть бути використані суб’єктом кіберзагрози при експлуатації СТТПЗ для деструктивного кібервпливу на SIS;

– дослідити існуючі методи (підходи) до забезпечення кіберзахисту технологічних систем на основі обраних пропрієтарних програмних рішень промислового кіберзахисту (з використанням інформації з офіційної технічної документації виробника), визначити їх сильні/слабкі сторони та загальні підходи до їх функціонування;

– розрахувати кіберстійкість для 2-1 рівнів моделі.

Основна частина

1. Аналізуючи особливості кіберзахисту технологічної системи на 2-1 рівнях моделі (де розгорнуто основні інформаційні підсистеми BPCS і SIS) важливо розглянути її типову архітектуру та в подальшому, спираючись на неї, виділити окремі вектори кіберзагроз, характерні на цих ланках технологічної системи (рис. 1).

Другий рівень моделі зазвичай починається з фаєрволу (програмного/апаратного його рішення), що розділяє 3 і 2 рівень моделі між собою. Через фаєрвол здійснюється комунікація 2 рівня моделі з вищими рівнями моделі та, можливо, враховуючи конкретну реалізацію, із системами, які розгорнуті в сегменті комунікаційної мережі, наприклад, системою виконання виробництва (MES) і системами планування ресурсів підприємства (ERP) *(в подальшому дослідженні таку взаємодію будемо ідентифікувати як вектор загрози “згори”).*

Безпосередньо на 2-му рівні моделі розгорнуто верхні рівні управління ключовими інформаційними підсистемами технологічної системи (Industrial Control System, далі – ICS) – BPCS і SIS.

BPCS – це інформаційна підсистема ICS, яка функціонує на 2-1 рівнях моделі, має безпосередній вплив на 0 рівень моделі та призначена для здійснення моніторингу стану технологічного (виробничого) процесу та управління ним. SIS – це інформаційна підсистема ICS, яка функціонує на 2-1 рівнях моделі, має вплив на 0 рівень моделі та призначена для забезпечення безпеки експлуатації технологічного об’єкта, контролю аварійних процедур і, у разі виникнення аномалій, приведення технологічного процесу до безпечного стану. Міжнародним стандартом, що визначає вимоги кібербезпеки для систем BPCS і SIS, є IEC 62443.

На 2-му рівні моделі вищезазначені підсистеми можуть бути представлені такими програмно-апаратними засобами:

BPCS: сервер Supervisory Control and Data Acquisition (SCADA)/сервер Distributed Control System (DCS), Human-Machine Interface (HMI), інженерне робоче місце (робоче місце оператора/Engineering Workstation);

SIS: головний контроллер безпеки (Safety Controller), Human-Machine Interface (HMI), інженерне робоче місце (робоче місце оператора/SIS Engineering Workstation).

Враховуючи підходи до політики безпеки ОКІІ, на 2-му рівні моделі може бути реалізовано доступ до мережі Інтернет або він може бути заборонений. Зокрема, доступ до мережі Інтернет може бути здійснено для реалізації можливості віддаленого доступу для адміністратора SCADA/DCS (згідно з рекомендованими практиками в такому разі має бути застосовано багатофакторну автентифікацію).

Окрім того не виключається, що інформаційні підсистеми рівня 2 можуть отримати несанкціоноване з’єднання з мережею Інтернет через неналежне ставлення персоналу до інформаційної безпеки підприємства (*в подальшому дослідженні таку взаємодію будемо ідентифікувати як вектор загрози “з середини”)*. Крім того, при наявності Інтернет-з’єднання з робочою станцією, на якій є застаріле вразливе програмне забезпечення, суб’єкт кіберзагрози потенційно може отримати ще одну точку входу в технологічну систему. Разом з тим, все частіше зустрічаються випадки, коли користувачі інженерної станції через доступ до мережі Інтернет здійснюють доступ до вебсайту постачальника послуг, на якому суб’єкти кіберзагроз реалізують тип кібератаки “перехоплення ланцюжка поставок” через постачальників спеціалізованого програмного забезпечення (*в подальшому дослідженні таку взаємодію будемо ідентифікувати як вектор загрози “ззовні”).*

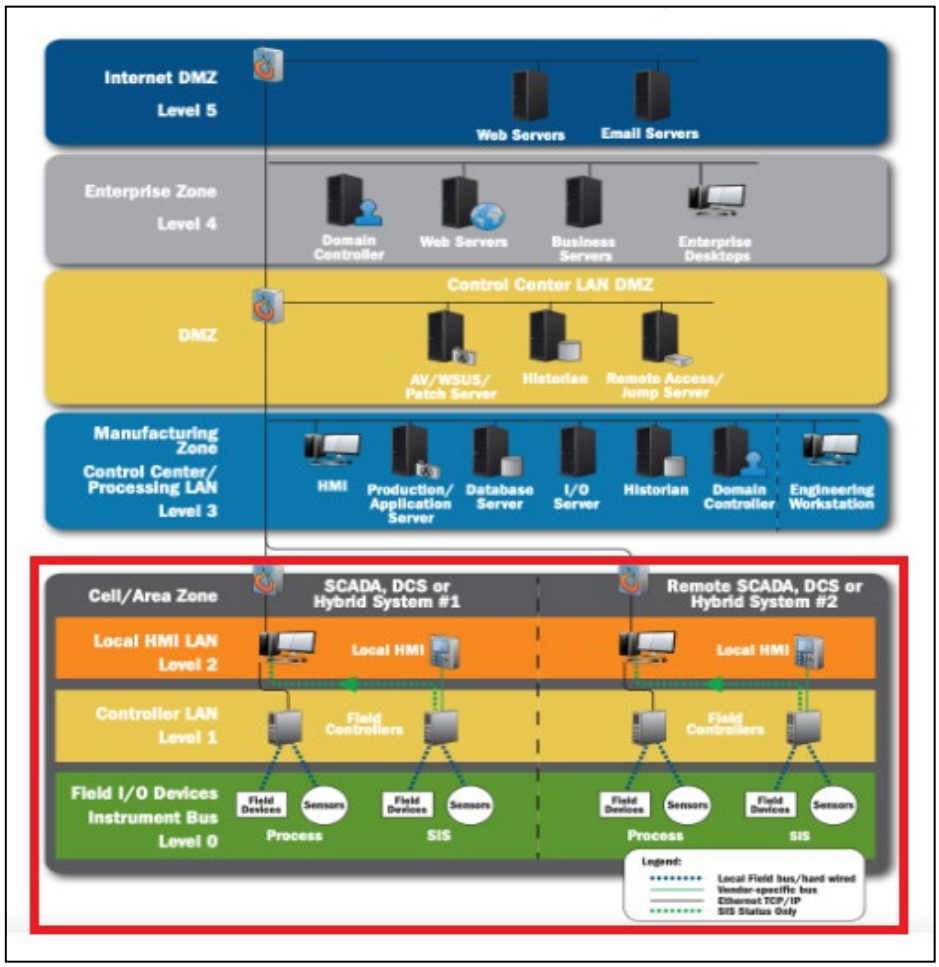


Рис. 1. Структурна схема реалізації моделі Purdue
(червоною рамкою виділено 2-0 рівні моделі Purdue, щодо яких проводиться подальше дослідження)

На 1-му рівні моделі підсистема BPCS представлена рядом контролерів (які мають зв'язок із сервером SCADA/DCS), до яких підключено сенсори, що знаходяться нижче за ієрархією на 0 рівні моделі. До цих же контролерів на другому рівні підключені і виконавчі механізми, які теж знаходяться на рівні 0. Такі підсистеми BPCS, як Support Skids та підсистема розподілу потужності (Power distribution), розгорнуті на 1-0 рівнях моделі.

SIS, зі свого боку, на 1 рівні моделі представлена головним контролером безпеки (Safety Controller), службовими контролерами безпеки, підсистемою розподілу потужності (окремо для роботи SIS, не є обов'язковою, але є рекомендованою), що живить контролери та сенсори, виконавчі механізми (які знаходяться на 0 рівні моделі) та підтримує роботу SIS у разі збоїв у централізованому енергопостачанні.

Згідно з вищерозглянутою архітектурою на рівні 1 моделі, початковою точкою входу в технологічну систему є контролер. Отримати доступ до нього суб'єкт кіберзагрози може у разі, якщо контролер має доступ до мережі Інтернет, або з середини технологічної мережі. З середини технологічної мережі отримати доступ до контролера можна фізично або завдяки використанню ряду технік бокового переміщення.

Не виключається також ризик доступу суб'єктом кіберзагрози з 0 рівня моделі до 2-1 рівнів моделі. Це, зокрема, можливо завдяки компрометації "розумних" сенсорів/виконавчих механізмів, фізичного доступу до фізичних інтерфейсів і бездротових мереж технологічної мережі, а також її пристроїв.

Між інформаційними підсистемами BPCS і SIS на 2-1 рівнях моделі присутній логічний та фізичний взаємозв'язок. Варіант такого зв'язку залежить від обраної архітектури реалізації і може бути виконаний в один із чотирьох способів. Від вибору правильної архітектури залежить рівень кіберстійкості SIS та відповідно вся безпека технологічного процесу, а також успішність ймовірної деструктивної кібератаки з використанням СТТПЗ.

Розглянемо типові можливі архітектури взаємодії BPCS і SIS, які можуть бути практично реалізовані на ОКІІ, та їх надійність з точки зору кібербезпеки.

Перший варіант реалізації архітектури між BPCS і SIS має назву "з повітряним зазором" (англ. "air gap"). Головною характеристикою такого підходу є те, що дві системи функціонують незалежно одна від одної, тобто є фізично й логічно ізольованими. Така архітектура взаємодії застосовується з метою мінімізації впливу кібератак, відмов, збоїв у BPCS на роботу системи безпеки (SIS). В такій реалізації підсистеми BPCS і SIS можуть обмінюватися лише даними про тривоги або сигналами про аварійну ситуацію.

Тобто, реалізація архітектури "з повітряним зазором" дозволяє ізолювати обидві системи одна від одної, проте для обміну критично важливими сигналами про аварійну ситуацію між ними зберігається одна спільна точка перетину (ймовірна точка входу суб'єкта кіберзагрози). Якщо ця точка перетину надійно захищена та враховано всі інші рекомендації до кібербезпеки SIS, така архітектура забезпечує найкращий рівень її кіберстійкості.

Другий варіант реалізації архітектури між BPCS і SIS має назву "інтерфейсний" (англ. "interface"). "Інтерфейсна" архітектура полягає у тому, що між BPCS і SIS використовуються спільні канали зв'язку та спільні протоколи (Modbus, Profibus, Ethernet/IP або HART), при цьому зберігається певний рівень ізоляції для критичних функцій SIS.

Отже, "інтерфейсна" архітектура забезпечує ізоляцію для критичних функцій, проте зберігає дві спільні точки перетину між BPCS і SIS (на рівні фізичного каналу та на рівні використання спільного протоколу), що забезпечує вплив на рівень кіберстійкості та дещо зменшує його порівняно з архітектурою "з повітряним зазором".

Третім підходом до архітектури між BPCS і SIS є "інтегрована" (англ. "integrated") реалізація. За такої архітектури BPCS і SIS є частинами єдиної системи та працюють у тісній взаємодії з використанням спільних фізичних каналів зв'язку, використовують спільні протоколи та дані для управління процесами. Не зважаючи на певні переваги така

архітектура збільшує кількість спільних точок перетину до трьох та не забезпечує достатнього рівня кіберстійкості SIS для ОКІІ.

Четвертим підходом щодо взаємодії між BPCS і SIS є “спільна” (англ. “common”) архітектура. Такий варіант реалізації побудований на використанні спільної платформи для роботи обох інформаційних підсистем. Це, в свою чергу, означає, що BPCS і SIS функціонують на спільних мережах, інтерфейсах, контролерах та, загалом, на спільному апаратному обладнанні. Проте між ними зберігається логічний розподіл функцій керування та безпеки за допомогою налаштованих конфігурацій і програмного забезпечення. Проте кількість спільних точок перетину в цій архітектурі є максимальною (з усіх вищеописаних підходів), що робить її найбільш вразливою до відмов і найменш кіберстійкою.

Варто зауважити, що міжнародні стандарти, такі як IEC 61511 і IEC 61508, не забороняють використання жодної з вищерозглянутих архітектур для BPCS і SIS, але залежно від кожної з реалізацій встановлюють жорсткі вимоги щодо забезпечення належного рівня розділення між цими системами. Проте при виборі архітектури реалізації варто враховувати всі вищезазначені потенційні ризики до збереження кіберстійкості SIS та перш за все враховувати категорію критичності об’єкта критичної інфраструктури, в технологічній системі якого її реалізовано.

Отже, розглянувши основне призначення, структуру, взаємоархітектуру та взаємодію BPCS і SIS можна зробити висновок, що у разі компрометації суб’єктом кіберзагрози елементів/складових BPCS (що у разі успішної деструктивної кібератаки може призвести лише до значних фінансових збитків і простою виробництва) єдиною перешкодою на шляху успішного здійснення масштабної деструктивної кібератаки є SIS (доступ до якої може завдати фізичного пошкодження механізмам та системам і навіть призвести до техногенних катастроф), яка контролює критичні параметри/функції безпеки технологічного процесу. Відтак доступ до SIS є основними пріоритетом суб’єкта кіберзагрози. Крім того, менш пріоритетним, але досить важливим на 2-1 рівнях моделі, є доступ до BPCS, підсистеми розподілу потужності та BPCS Support Skids, що може призвести до значних перебоїв у виробництві та збоїв в енергетичній мережі, хоча й менш серйозних, ніж втрата контролю над системами безпеки (SIS).

Для досягнення деструктивної кібератаки на технологічну мережу на 2-1 рівнях моделі суб’єкт кіберзагрози в якості інструменту кібератаки, майже напевно, буде використовувати СТТПЗ.

2. Розглянута будова 2-1 рівнів моделі описує важливість кіберстійкості підсистем BPCS та особливо SIS, а також окреслює потенційні точки входу суб’єкта кіберзагрози в технологічну систему, які дозволяють йому здійснити спробу деструктивної кібератаки з використанням СТТПЗ. Всі можливі техніки кібертатак, що стосуються ICS описані в методології для систем автоматизації та промислових процесів MITRE ATT&CK for ICS.

Серед усіх розглянутих в методології MITRE ATT&CK for ICS технік, рівнів 2-1 моделі стосуються наступні: T08800, T0830, T0878, T0802, T0895, T0803, T0804, T0805, T0806, T0892, T0807, T0885, T0884, T0879, T0809, T0893, T0813, T0814,T0868, T0816, T0871, T0820, T0890, T0866, T0823, T0874, T0877, T0872, T0826, T0880, T0829, T0835, T0831, T0832, T0849, T0838, T0836, T0839, T0801, T0834, T0840, T0842, T0861, T0845, T0886, T0846, T0888, T0847, T0848, T0851, T0852, T0853, T0881, T0856, T0869, T0862, T0894, T0857, T0863, T0859. Наведені техніки стосуються кібератак на апаратну, програмну та мережеву складові [9].

До найбільш небезпечних технік, що можуть призвести до деструкції/пошкодження компонентів SIS, можна віднести наступні: T0832, T0831, T0880, T0837, T0828, T0879.

Таким чином, потенційно суб’єкт кіберзагрози при виборі тактик і технік, за допомогою яких заплановано здійснення деструктивних кібердій щодо технологічної системи, має

значний арсенал, який дозволяє успішно реалізувати життєвий цикл СТТПЗ з 3 по 8.а етапи, що зображено на умовній схемі життєвого циклу СТТПЗ на рисунку 2 *(штрихпунктирною лінією на схемі рисунка 2 позначено не обов’язкові, проте можливі етапи життєвого циклу СТТПЗ)*.

3. Серед сучасних методів (підходів) до кіберзахисту технологічних систем у пропрієтарних рішеннях промислового кіберзахисту використовуються: сигнатурний аналіз, евристичний і поведінковий аналізи, а також їх комбінація/симбіоз з машинним навчанням, що дає змогу значно покращити захист від СТТПЗ та його виявлення в технологічній системі, починаючи з 3 по 5 етапи життєвого циклу (рис. 2).

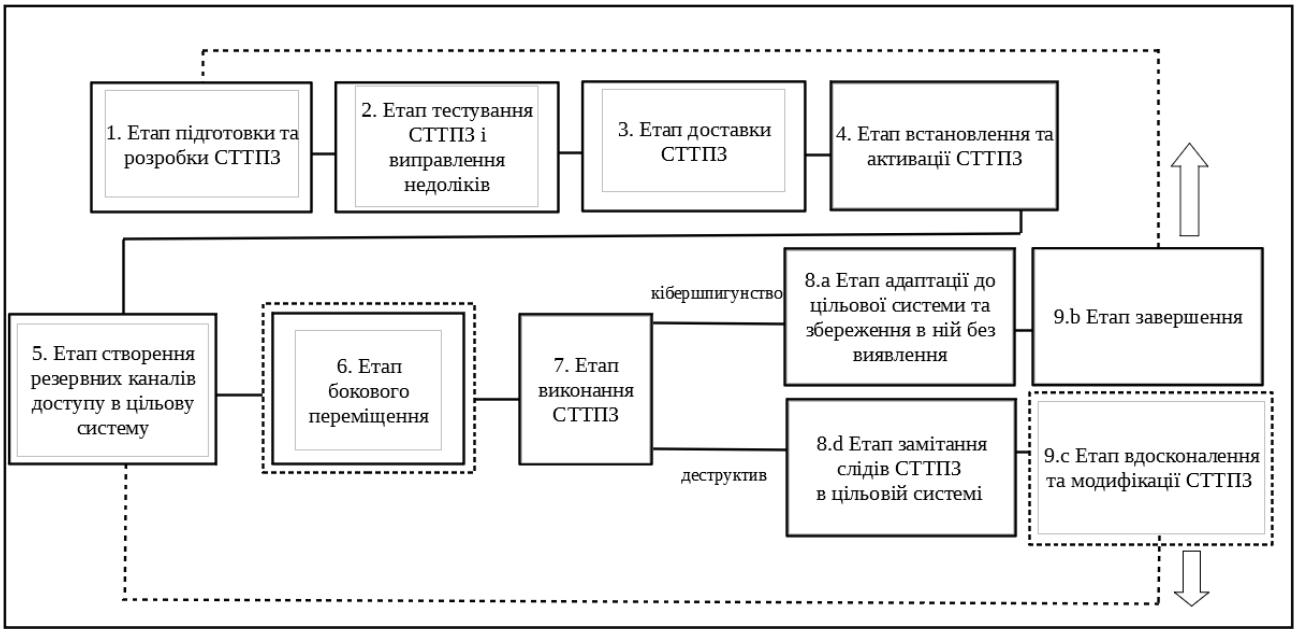


Рис. 2. Схема життєвого циклу СТТПЗ

Для аналізу можливості протидії СТТПЗ в технологічній системі розглянемо існуючі методи (підходи) на основі пропрієтарних рішень промислового кіберзахисту.

У процесі проведення подальшого дослідження було обрано рішення щодо кіберзахисту технологічних систем (в тому числі на 2-1 рівні моделі) Nozomi Networks Guardian (США) та Siemens SCADA and PLC Security (Німеччина). Ці продукти є найбільш популярними в своїй ніші та мають необхідні функціональні можливості, що відповідають завданню дослідження. Крім того, зазначені пропрієтарні рішення обрано з урахуванням їх реального використання на об’єктах критичної інфраструктури в різних географічних регіонах, що передбачає стратегічний підхід.

Nozomi Networks Guardian (далі – NNG). NGG призначене для моніторингу та управління компонентами (активним обладнанням) в технологічній системі.

Тип рішення NNG – NDR, безагентний підхід до збору даних із подальшою можливістю розгортання агентного компонента.

Розгортання NNG може бути здійснено на фізичному, віртуальному чи хмарному сервері. Після чого відповідний компонент NNG підключається до мережі та аналізує трафік, що передається між пристроями. Це дозволяє отримати детальну інформацію про активність і стан систем. З цією метою реалізується підключення до мережевого комутатора через порт віддзеркалення – Switched Port Analyzer (SPAN) або спеціальний пристрій TAP (Test Access Point). Інформацію з хостів (кінцевих пристроїв) NNG може отримувати завдяки режиму “Active Polling” (вимкнений за замовчуванням та потребує додаткової конфігурації), що

дозволяє збирати інформацію безпосередньо з пристроїв через SNMP, WMI, API, Syslog. А у разі, якщо необхідно ще більш детальне отримання інформації про кінцеві пристрої, передбачено додаткове встановлення агентної складової (наприклад, якщо потрібно зчитувати детальні журнали подій Windows-системи). Отже, архітектура рішення NGG передбачає значну гнучкість у питаннях рівня контролю як мережевого, так і хостового трафіку та подій.

На основі аналізу офіційної документації NNG можна зробити висновок, що рішення складається з таких 7 модулів та модуля, що є центральною системою управління: Nozomi Networks Guardian Sensor, Nozomi Networks Asset Intelligence, Nozomi Networks Threat Intelligence, Nozomi Networks Smart Polling, Nozomi Networks vGuardian, Remote Collectors, Guardian Air, Nozomi Networks Central Management Console. Варіант взаємодії елементів NGG по відношенню до моделі зображено на рисунку 3.

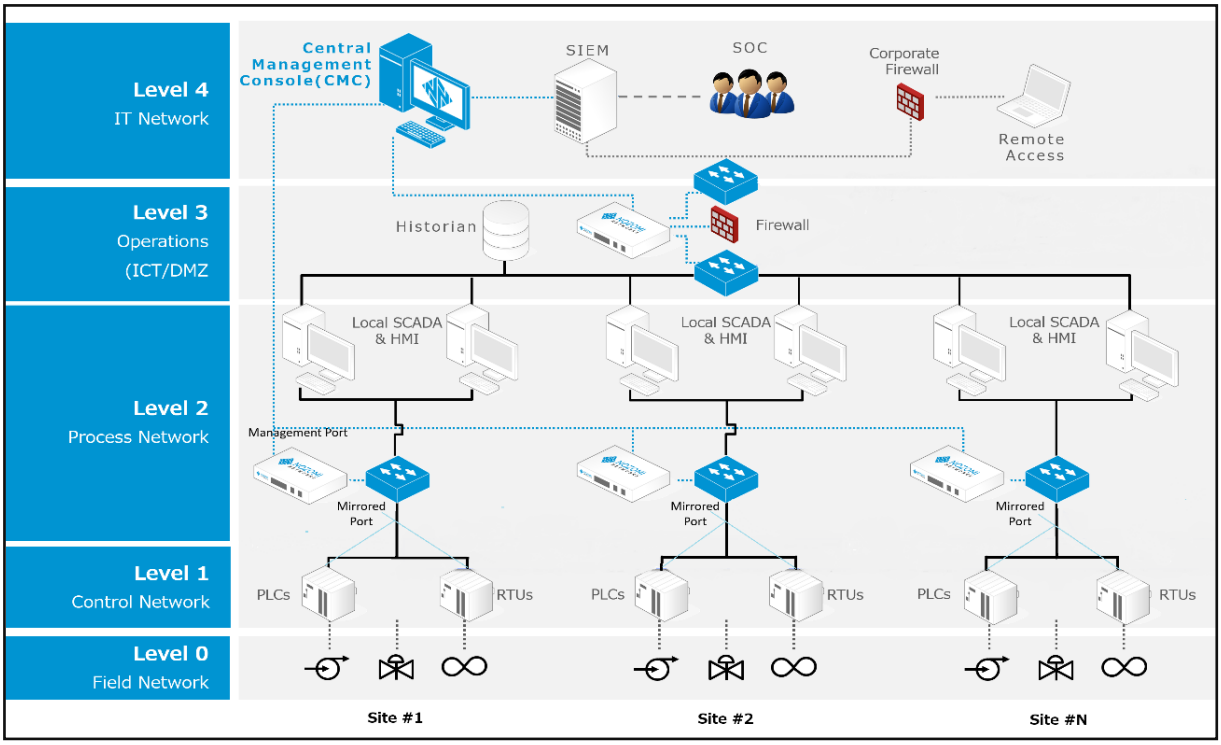


Рис. 3. Варіант взаємодії елементів NGG щодо моделі Purdue

Nozomi Networks Guardian Sensor як модуль відповідає за пасивний моніторинг трафіку через SPAN/TAP для виявлення аномалій, кібератак і вразливостей у технологічній мережі. Модуль автоматично виявляє та класифікує пристрої технологічної автоматизації нижчого рівня, аналізує поведінку пристроїв та створює базову модель нормальної роботи завдяки технології машинного навчання.

Nozomi Networks Asset Intelligence – автоматично виявляє та інвентаризує всі пристрої в мережі, збираючи детальну інформацію про їхні характеристики, конфігурацію, операційну систему, версію прошивки та можливі вразливості.

Nozomi Networks Threat Intelligence, як один із компонентів NGG, допомагає виявити нові типи атак або нестандартну поведінку на основі глобальних даних про загрози, використовуючи статистичні та алгоритмічні підходи.

Nozomi Networks Smart Polling – модуль призначений для опитування мережевих пристроїв і сенсорів для передачі цієї інформації до центральної системи управління, при цьому мінімізуючи навантаження на мережу та пристрої. Крім того, модуль використовує ML

для аналізу тенденцій та виявлення потенційних аномалій в поведінці пристроїв через SNMP, WMI або API.

Nozomi Networks vGuardian – модуль NGG, що призначений для роботи у віртуальному середовищі (наприклад, VMware ESXi, Microsoft Hyper-V) замість фізичного пристрою та розгортається у віртуальній інфраструктурі технологічної системи для моніторингу кібербезпеки технологічної мережі в частині кібербезпеки віртуальних робочих місць;

Remote Collectors – модуль, що відповідає за збір і консолідацію даних із віддалених сегментів мережі (на географічно розподілених локаціях) та передає ці дані до центральної системи управління (CMC).

Guardian Air – модуль NGG, який функціонує як автономний бездротовий сенсор безпеки, розроблений спеціально для технологічних середовищ, які активно використовують IoT. Цей сенсор безперервно моніторить бездротові технології в діапазоні від 800 МГц до 5895 МГц, включаючи Wi-Fi, Bluetooth, IEEE 802.15.4, LoRaWAN, Zwave, стільниковий зв’язок та дрони.

Nozomi Networks Central Management Console (далі – CMC) – є ключовим елементом NGG, його центральною системою управління, з якою взаємодіють усі модулі рішення, що забезпечує єдину, централізовану платформу для моніторингу, аналізу даних і реагування на загрози в технологічній системі [10].

Серед протоколів, які підтримує NNG, налічується близько шестисот варіантів.

Серед підходів до моніторингу мережевого сегмента NNG використовує такі технології як: Deep Packet Inspection (DPI), пасивне спостереження за трафіком (IDS), аналіз мережевих аномалій (Anomaly Detection), моніторинг зв’язків між пристроями (Network Mapping & Asset Discovery), контроль команд і дій у промислових протоколах (Protocol Whitelisting), машинне навчання.

Для моніторингу прикінцевого обладнання в NNG використовується: пасивне спостереження за мережевим трафіком від обладнання та побудова карти кінцевого обладнання, а також оцінка його вразливостей, поведінковий аналіз із застосуванням машинного навчання, аудит промислових протоколів.

Елементи машинного навчання присутні у таких модулях рішення NNG, як: Nozomi Networks Guardian Sensor, Nozomi Networks Asset Intelligence, Nozomi Networks Threat Intelligence. Це покращує характеристики виявлення аномалій і загроз, можливості для класифікації та інвентаризації пристроїв у технологічній мережі, можливості для виявлення досі невідомих загроз та мінімізує хибне спрацьовування (false positive).

Для роботи з віртуалізованою частиною інфраструктури технологічної системи в NGG передбачено використання віртуального образу рішення (наприклад, на віртуальних платформах VMware vSphere, Microsoft Hyper-V, Docker).

Крім того, NNG може інтегруватися з такими платформами та програмними рішеннями: SIEM (“Splunk”, “IBM Qradar”, “ArcSight”, “LogRhythm”), інструментами моніторингу (“Nagios”, “Zabbix”), системами управління подіями та інцидентами (“ServiceNow”, “BMC Remedy”), платформами для управління ризиками (“RSA Archer”, “MetricStream”), засобами виявлення та реагування на кінцевих пристроях (“CrowdStrike Falcon”, “Microsoft Defender for Endpoint”, “SentinelOne”, “Sophos Intercept X”, “Trend Micro Apex One”), платформами управління змінами та конфігураціями (“Ansible”, “SaltStack”), системами управління вразливостями (“Qualys”, “Tenable”, “Rapid7”), мережевими фаєрволами “Fortinet FortiGate”, платформою управління контейнерами “Docker”.

NNG підтримує алгоритми оновлення баз знань у технологічній мережі через центральну систему CMC або через базу вразливостей (наприклад, Національна база даних вразливостей). Причому оновлення через CMC може бути виконано одним із варіантів:

автоматично (як з виходом у мережу Інтернет, так і завдяки знімному носієві), вручну (завдяки вебінтерфейсу чи командному рядку).

NNG відповідає вимогам стандарту IEC 62443 [11].

Серед головних переваг рішення NNG (з точки зору забезпечення кіберстійкості на 2-1 рівнях моделі) – гнучкість у налаштуванні під конкретні потреби щодо моніторингу кібербезпеки, незначне навантаження на мережу та можливість додаткових поглиблених налаштувань моніторингу кінцевих точок у разі необхідності.

Окремої уваги при адмініструванні рішення NNG потребує контроль коректності конфігурацій (**Security Misconfiguration**), так як рішення має велику кількість взаємопов'язаних елементів архітектури. Така особливість може бути використана суб'єктом кіберзагрози у реалізації кібератаки **misconfiguration attack.**

Siemens SCADA and PLC Security (далі — SSPS). SSPS призначене для захисту технологічних систем від кіберзагроз, забезпечуючи безперебійність і безпечність технологічного процесу, акцентуючи свою увагу на кіберзахисті SCADA та PLC, відповідно на 2-1 рівні моделі. Варто зазначити, що перш за все рішення SSPS забезпечує максимальну свою ефективність в технологічній екосистемі "Siemens", завдяки максимальній взаємоінтеграції лінійки продуктів, що передбачає взаємну архітектуру. Проте рішення сумісне і з DCS, SCADA та PLC інших виробників. Крім того, рівень безпеки обладнання стороннього виробника буде залежати від закладених у нього виробником функцій безпеки та можливостей інтеграції з SSPS.

Основою підходу до забезпечення кібербезпеки у рішенні SSPS є класична стратегія "Defense in Depth", яка в технологічному сегменті передбачає комплексний підхід до питання забезпечення кібербезпеки на кожному фізичному/логічному контурі.

Тип рішення SSPS – комплексна система з інтеграцією функцій кіберзахисту в обладнання та програмне забезпечення систем керування.

SSPS складається з таких модулів: модуль безпеки PLC, модуль безпеки SCADA, інтегрований модуль кібербезпеки, модуль аудиту та моніторингу безпеки, модуль управління конфігураціями та оновленнями. Крім того, рішення має два ключових програмні інструменти, які є своєрідними централізованими компонентами "TIA Portal" та "WinCC".

Завдяки програмному компоненту "TIA Portal" інженери інтегрують в PLC модуль безпеки PLC та модуль управління конфігураціями.

"WinCC", в свою чергу, виконує функції SCADA-системи, забезпечуючи візуалізацію, моніторинг та аналіз даних, що надходять із різних модулів, таких як модуль безпеки SCADA, модуль аудиту та моніторингу безпеки. "WinCC" дозволяє операторам відстежувати стан технологічних процесів у режимі реального часу, реагувати на інциденти кібербезпеки та забезпечувати централізоване управління.

Обидва середовища взаємодіють із модулями SSPS через стандартизовані протоколи обміну даними (OPC UA, PROFINET, PROFIBUS та ін.), що дозволяє забезпечити комплексну безпеку, моніторинг та управління всією технологічною інфраструктурою [12].

Рішення SSPS дозволяє реалізувати єдину інтегровану екосистему, де "TIA Portal", "WinCC" та PLC працюють разом із вбудованими функціями кібербезпеки, що включають: сегментацію мережі та ізоляцію рівнів технологічної мережі; шифрування даних, що передаються між SCADA та PLC; контроль доступу та автентифікацію користувачів; захист від шкідливого програмного забезпечення; моніторинг загроз та інцидентів; захист від несанкціонованих змін у PLC та SCADA.

Модуль безпеки PLC працює на 1-му рівні моделі і призначений для: захисту логіки керування та коду PLC (запобігання несанкціонованому доступу до програмного коду контролера, використання технології Know-how Protection для шифрування програми, захист конфігурації контролера від несанкціонованої модифікації); контролю доступу (здійснюється

через багаторівневу систему аутентифікації, авторизації та управління правами користувачів); забезпечення функцій кібербезпеки PLC (програмно-апаратні фаєрволи вбудовані в PLC, шифрування даних та зв’язку), безпечного аварійного відключення (відповідно до вимог міжнародних стандартів ISO 13849-1, IEC 61508).

Модуль безпеки SCADA працює на 2-му рівні моделі, захищаючи взаємодію з вищим і нижчим рівнями та відповідає за: аутентифікацію та авторизацію (на основі використання надійних паролів, двофакторної автентифікації та інтеграції з корпоративними системами, наприклад, LDAP, Active Directory); моніторинг та виявлення загроз (моніторинг мережевих і системних подій на наявність аномалій та потенційних загроз із використанням інтеграції з рішеннями IDS/IPS, SIEM та ін.); шифрування та захист трафіку для безпеки взаємоз’єднань між сервером SCADA, HMI та PLC (на основі використання протоколів TLS, SSL, IPSec VPN), а також між SCADA-сервером і клієнтами (що особливо актуально у розподілених системах); моніторинг та аудит безпеки (логування подій, контроль змін конфігурацій, виявлення несанкціонованих підключень і підозрілих дій); інтеграцію з мережевими рішеннями безпеки (фаєрволами) для обмеження доступу в технологічну мережу.

Інтегрований модуль кібербезпеки у рішенні SSPS відіграє роль централізованої консолі управління. Даний модуль відповідає за: централізоване управління кібербезпекою (виступає централізованою консоллю для моніторингу та управління політиками безпеки для всієї технологічної екосистеми); кореляцію та аналіз даних (збирає інформацію з модулів безпеки PLC та SCADA, модуля аудиту та моніторингу безпеки, модуля управління конфігураціями та оновленням, а також із зовнішніх систем, таких як SIEM, IDS/IPS), що дозволяє оперативно виявляти аномалії та загрози (з використанням підходів машинного навчання); оперативне реагування на кіберінциденти (автоматизує процеси реагування на кіберзагрози, координує дії між різними модулями та допомагає ізолювати потенційні загрози, що здійснюється з використанням підходів машинного навчання); забезпечує інтеграцію й узгодженість політик кібербезпеки.

Модуль аудиту та моніторингу безпеки, зазвичай, розгортається на 2 рівні моделі та відповідає за систематичний збір, аналіз та зберігання інформації про події в системі. До основних функцій модуля належать: збір логів та подій (шляхом фіксування дій користувачів, змін у конфігурації, фіксуванні системних повідомлень та інших важливих подій з усіх компонентів системи); аналіз і кореляція даних (обробка зібраних даних для виявлення аномалій, підозрілих активностей або нетипової поведінки, що може свідчити про потенційні загрози, ймовірно, з цією метою у рішенні використовуються елементи машинного навчання); сповіщення та реагування (автоматичне генерування сповіщень і попереджень при виявленні підозрілої активності); аудит і забезпечення відповідності (проведення аудиту для перевірки на відповідність політикам кібербезпеки, ведення журналів подій).

Модуль управління конфігураціями та оновленнями у рішенні SSPS відповідає за систематичне керування та організацію контролю змін у програмному коді, зокрема: інтеграцію з іншими інформаційно-технологічними системами (забезпечує безпечний взаємообмін інформацією між різними системами); міграцію даних (забезпечує перенесення даних з існуючих систем, необхідних для впровадження та належної роботи системи SCADA та PLC); управління змінами та контроль версій (відслідковування змін у конфігураціях, зберігає початкову конфігурацію та веде історію змін); дозволяє автоматизувати процеси оновлення (централізоване управління оновленнями, в тому числі прошивками PLC).

Умовна схема взаємодії основних компонентів (модулів) рішення Siemens SCADA and PLC Securit зображена на рисунку 4.

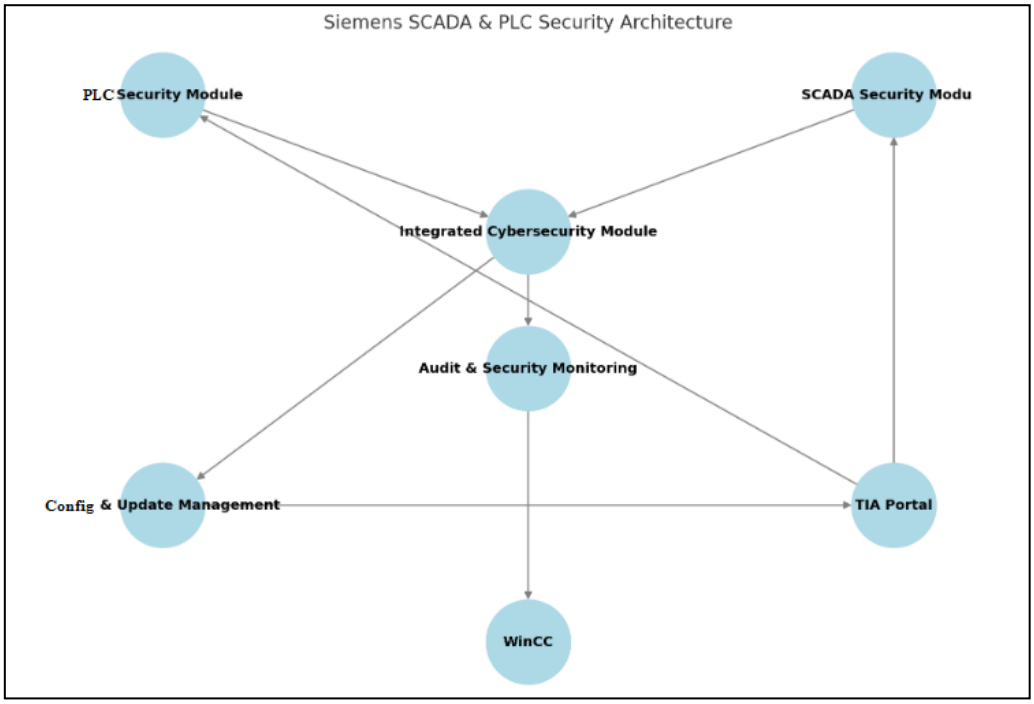


Рис. 4. Умовна схема взаємодії основних компонентів (модулів) рішення Siemens SCADA and PLC Security

Серед підходів до моніторингу мережевого сегмента SSPS використовує: інтеграцію з існуючими засобами кібербезпеки (фаєрволами, IDS/IPS, SIEM та іншими, що дозволяє SSPS ефективно інтегруватися в загальну архітектуру безпеки).

За моніторинг мережевого сегмента SSPS відповідає інтегрований модуль кібербезпеки. Він, зокрема, здійснює:

інтелектуальний моніторинг трафіку (включає DPI для виявлення аномалій на рівні промислових протоколів, сигнатурний аналіз, поведінковий аналіз, виявлення атак типу Man-in-the-Middle, а**втоматизоване реагування на загрози** через інтеграцію з SIEM та рішеннями для управління інцидентами (SOAR), що дозволяє блокувати підозрілу активність у реальному часі);

сегментацію мережі (завдяки використанню VLAN, DMZ, фаєрволів), моніторинг і контроль доступу (здійснюється інтегрованим модулем кібербезпеки та модулем аудиту й моніторингу безпеки);

швидку адаптацію до нових загроз через інтеграцію з програмами оновлення (через модуль управління конфігураціями та оновленнями) [13].

Серед підходів до моніторингу прикінцевого обладнання SSPS використовує: поведінковий аналіз; аудит і контроль доступу до пристроїв; моніторинг стану пристроїв та їх конфігурації; виявлення аномалій за допомогою машинного навчання; інвентаризацію та оцінку вразливостей; виявлення шкідливих програм; автоматизоване реагування та оркестрацію інцидентів (інтеграцію з SOAR для автоматизації процесів реагування на загрози, створення інцидентних маркерів і запуску сценаріїв ізоляції атак у реальному часі), централізоване логування, управління оновленнями, інтеграцію з рішеннями для управління кінцевими точками.

Серед модулів SSPS елементи машинного навчання містять такі: інтегрований модуль кібербезпеки (використовує машинне навчання для аналізу мережевого трафіку, виявлення аномалій і підозрілих патернів у промислових протоколах; допомагає адаптивно реагувати на нові загрози, знижуючи кількість хибного спрацьовування (false positive)); модуль аудиту та

моніторингу безпеки (використовує елементи машинного навчання для виявлення незвичної активності та кореляції подій безпеки; забезпечує аналіз журналів і змін у конфігураціях пристроїв для оперативного реагування на загрози).

Інтегрований модуль кібербезпеки SSPS може розгортатися у віртуалізованому середовищі, зокрема на платформі Microsoft Hyper-V, **VMware vSphere, Citrix Xen, KVM (Kernel-based Virtual Machine).**

Крім того, SSPS може інтегруватися з такими платформами: SIEM, інструментами моніторингу, SOAR, платформами для управління ризиками, засобами виявлення та реагування на кінцевих пристроях – Endpoint detection and response, платформами управління змінами та конфігураціями, системами управління вразливостями (офіційна документація не надає інформації щодо конкретних програмних рішень для інтеграції).

SSPS підтримує такі алгоритми оновлення баз знань у технологічній мережі: автоматичне оновлення через центральний сервер SSPS; оновлення через локальний репозиторій; через API та зовнішні джерела; оновлення в ручному режимі; контекстне (адаптивне) оновлення (відрізняється від традиційного автоматичного оновлення тим, що адаптується до локальних умов і може коригувати свою частоту та обсяг оновлень відповідно до змін у технологічній мережі).

Рішення SSPS відповідає вимогам стандарту IEC 62443.

Серед головних переваг рішення SSPS – надійність у моніторингу стану кібербезпеки на таких підсистемах, як BPCS і SIS, зокрема за критерієм швидкодії реакції. Крім того, однією з переваг є урівноважений розподіл навантаження між програмним і апаратним компонентами даного рішення промислового кіберзахисту, що дозволяє зберегти високий рівень ефективності і водночас не навантажувати мережу і кінцеве обладнання.

До недоліків SSPS можна віднести орієнтованість на технологічну та інформаційну інфраструктуру “Siemens”, отже моногенну інформаційну інфраструктуру.

Таким чином, кожне з розглянутих рішень промислового кіберзахисту (NNG, SSPS) може бути розгорнуто у технологічній системі (щонайменше за критерієм відповідності стандарту IEC 62443). Проте варто зауважити про доцільність вибору конкретного рішення зважаючи на факт закритості вихідного коду та потенційну можливість отримання доступу до критичної технологічної інформації з боку зацікавлених держав, що особливо актуально у світлі сучасної геополітичної нестабільності, в тому числі і для забезпечення кіберзахисту SIS (під час вибору програмних рішень для аналізу не було виявлено у відкритих джерелах окремого рішення кіберзахисту для SIS). Після аналізу архітектури та можливостей кожного з рішень можна сформулювати загальні підходи до їх функціонування:

архітектура системи: багатомодульна, з окремими модулями, що відповідають за кіберзахист прикінцевого обладнання, зокрема за захист пристроїв (PLC, HMI, сенсори, виконавчі механізми) через аналіз їхнього стану, конфігурації та інші) та мережі (забезпечують моніторинг мережевого трафіку, сегментацію мережі та взаємодію з іншими системами (наприклад, SIEM, IDS/IPS та інші). В модулях рішень присутня комбінація сигнатурного, евристичного та поведінкового аналізу. Концептуальний підхід до управління модулями передбачає наявність центральної консолі (доступ до функцій якої суб’єкта кіберзагрози потенційно є одним із найбільш небезпечних явищ для кіберстійкості технологічної системи 2-1 рівнів моделі, як для BPCS, так і для SIS);

елементи машинного навчання присутні в централізованих консолях та модулях, відповідальних за функції поведінкового аналізу та аналізу подій;

для функціонування модуля, який забезпечує моніторинг прикінцевого обладнання, використовуються: агентний підхід (забезпечує більш детальний моніторинг окремих пристроїв, що дозволяє глибокий аналіз та локальний контролю, проте може бути обмежений обчислювальними ресурсами пристроїв); безагентний підхід (є менш інвазивним,

дозволяючи отримувати інформацію через стандартні протоколи без необхідності встановлення додаткового програмного забезпечення на кожному пристрої, що особливо важливо для критичних компонентів SIS. Може здійснюватися, наприклад, через SNMP, WMI, API, Syslog).

Важливо зауважити, що при використанні типового підходу до управління модулями кіберзахисту в рішеннях промислового кіберзахисту, що передбачає наявність центральної консолі, здійснюється централізація управління. Такий підхід у єдиному для BPCS і SIS рішенні промислового кіберзахисту значно підвищує ризик несанкціонованого доступу суб'єкта кіберзагрози до компонентів SIS. З таких міркувань кібербезпеки на найбільш важливих ОКІІ доцільно децентралізувати управління системою промислового кіберзахисту і розгорнути в інфраструктурі SIS альтернативне рішення. Такий підхід підкріплено, зокрема, і рекомендаціями по розподілу або децентралізації архітектури "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security" [14].

4. Враховуючи всі розглянуті особливості забезпечення кіберстійкості від СТТПЗ на 2-1 рівнях моделі (вектори можливих кібератак, взаємоархітектуру між BPCS і SIS, особливості функціонування промислових систем кіберзахисту), можна визначити загальну формулу кіберстійкості для 2-1 рівнів моделі.

Варто зауважити, що кіберстійкість 2-1 рівнів моделі у даному дослідженні як один з головних критеріїв пропонує враховувати сумарний показник кіберстійкості двох основних інформаційних підсистем, які функціонують на цих рівнях, відповідно BPCS і SIS. Крім того, в подальших розрахунках по замовчуванню буде вважатися, що архітектура самої SIS є максимально кіберстійкою.

Врахуємо, що загалом можливі три вектори здійснення кібератаки з використанням СТТПЗ на 2-1 рівні моделі (див. рис. 1):

"згори" – з рівнів комунікаційної системи, DMZ (рівень 3.5 моделі) та Manufacturing zone (рівень 3 моделі);

"ззовні" – через вихід у мережу Інтернет безпосередньо з 2-1 рівнів моделі або через атаку "перехоплення ланцюжка поставок" (коли СТТПЗ вже знаходиться на обладнанні чи програмному забезпеченні, яке встановлюється постачальником);

"з середини" – через інсайдера або некомпетентного оператора/інженера або іншого працівника (який може переносити СТТПЗ на власному пристрої чи накопичувачі, не знаючи цього).

Зазвичай, під час здійснення кібератаки з використанням СТТПЗ для підвищення ефективності заходів суб'єктом кіберзагрози активно буде відпрацьовуватися більш ніж один вектор.

Найменшу загрозу кіберстійкості технологічної системи на 2-1 рівнях моделі несе вектор "згори" (враховуючи кількість засобів захисту, які СТТПЗ необхідно подолати, щоб досягти рівня 2 моделі). Проте цей вектор здійснення кібератаки є найдоступнішим. Вирішити питання нейтралізації цього вектора кібератаки дозволяє використання діодів даних.

Середній рівень загрози кіберстійкості технологічної системи на 2-1 рівнях моделі несе вектор "ззовні", так як зазвичай, всі технічні системи захисту сконцентровані на протидії не типовому/шкідливому трафіку з мережі Інтернет. Проте згідно з останніми дослідженнями все частіше суб'єктами кіберзагрози використовується тактика "перехоплення ланцюжка поставок", яка дозволяє здійснити доступ до технологічної системи під прикриттям "довіреного джерела". Цю тактику можна охарактеризувати як загрозу високого рівня.

Крім того, загрозу високого рівня буде становити вектор "з середини", що насамперед пов'язано з отриманням фізичного доступу суб'єкта кіберзагрози або зацікавленої/некомпетентної особи до технологічної системи.

Запропонований метод розрахунку кіберстійкості 2-1 рівнів моделі проти СТТПЗ ґрунтується на науковому методі експертної оцінки.

Відповідно до робочого документа об'єкта критичної інфраструктури, який визначає модель кіберзагроз технологічній системі підприємства (наприклад, на основі методу Operationally Critical Threat Asset, and Vulnerability Evaluation – OCTAVE), здійснюється визначення критеріїв, які в подальшому будуть враховувати експерти при оцінці кіберстійкості 2-1 рівнів моделі.

Визначення вагового коефіцієнта кожного критерію здійснюється експертами на основі аналізу рівня важливості критерію для збереження кіберстійкості технологічної системи на 2-1 рівнях моделі.

Автор пропонує, що критерії та їх вагові коефіцієнти визначаються на підставі експертних висновків на основі методу Сааті за такою процедурою:

серед працівників, відповідальних за забезпечення кіберзахисту технологічної системи об'єкта критичної інфраструктури, відбираються найбільш кваліфіковані фахівці (експерти);

експертами здійснюється визначення критеріїв та їх вагових коефіцієнтів;

надані експертні оцінки узагальнюються з використанням статистичної медіани або медіани Кеммелі;

здійснюються відповідні розрахунки за запропонованою формулою.

Присвоємо кожній зі взаємоархітектур між BPCS і SIS (завдяки їхнім технічним характеристикам) сталий коефіцієнт кіберстійкості: "з повітряним зазором" – 4; "інтерфейсна" – 3; "інтегрована" – 2; "спільна" – 1.

Визначимо запропоновані автором критерії, які будемо враховувати при оцінці кіберстійкості 2-1 рівнів моделі:

1. Кіберстійкість рішення промислового кіберзахисту. Вважаємо за замовчуванням, що обране рішення є максимально ефективним від СТТПЗ. Його кіберстійкість буде оцінено як суму кіберстійкості кожного з його модулів. Оцінити кіберстійкість кожного з модулів пропрієтарного рішення досить важко (оскільки потрібно аналізувати архітектуру та навіть початковий код рішення, що зазвичай є закритими виробником), проте за необхідності можна здійснити умовну оцінку за відкритою інформацією, враховуючи, що оцінка кіберстійкості буде не точною, а скоріше орієнтовною/наближеною (ваговий коефіцієнт – 0,9).

2. Взаємоархітектура між BPCS і SIS (ваговий коефіцієнт – 0,8).

3. Коректність налаштувань усіх програмно-апаратних вузлів і систем кіберзахисту в рамках BPCS і SIS (ваговий коефіцієнт – 0,7).

4. Ефективність політики усунення вразливостей (ваговий коефіцієнт – 0,6).

5. Ефективність політики розмежування доступу (ваговий коефіцієнт – 0,5).

6. Фактор небезпеки перехоплення ланцюжка поставок (ваговий коефіцієнт – 0,4).

7. Фактор небезпеки зацікавленого у кібератаці користувача/інсайдера (ваговий коефіцієнт – 0,3).

Визначимо й опишемо загальну кіберстійкість для 2-1 рівнів моделі, враховуючи 2 можливі вектори здійснення кібератаки з використанням СТТПЗ ("ззовні", "з середини") та всі можливі варіанти взаємоархітектури між BPCS і SIS. Крім того, під час розрахунку важливо врахувати ваговий коефіцієнт кожного з елементів оцінки:

$$CR_{2\text{-}1} = w_1\left(\frac{Aarch}{4}\right) + w_2\left(\frac{1}{n}\sum_{i=1}^{n} xi\right) + w_3 N + w_4 U + w_5 D + w_6(1 - V_{ext}) + w_7(1 - Vi_{nt}),$$

де $CR_{2\text{-}1}$ – Cyber Resilience, показник кіберстійкості для 2-1 рівнів моделі. Чим вищий цей кінцевий показник, тим стійкіша система до зовнішніх та внутрішніх загроз;

$CR_{2\text{-}1}$ як унормована формула забезпечується відповідною вагою $(w_1 + w_2 + \ldots + w_7) \geqslant 1$, або $CR_{2\text{-}1} = 0{,}99$ для табличного значення;

$\sum w_i = 1$ (наприклад, 0,15 + 0,15 + 0,15 + 0,15 + 0,1 +0,15 + 0,15 = 1),

або $\sum w_i = 0{,}99$ для того, щоб $CR_{2\text{-}1} < 1$ і max 0,99 для табличного порівняння;

$\sum x_i \rightarrow (\frac{1}{n}\sum_{i=1}^{n} xi)$ – середнє значення кіберстійкості для різних модулів є нормованим, що дозволяє отримати об'єктивну оцінку для множинних факторів, що впливають на систему в межах [0,1];

w_n – вагові коефіцієнти, які визначають важливість кожного з факторів у розрахунку кіберстійкості. Вони використовуються для коригування впливу кожного параметра на загальну стійкість системи. Кожен ваговий коефіцієнт (w) задається експертно або на основі аналізу унікальності та важливості кожного фактора для цієї конкретної системи. Наприклад, для фактора, який має критичне значення, ваговий коефіцієнт може бути більшим (для обчислення рекомендується використовувати діапазон в межах від 0,1 до 1 ($w_i \in [0{,}1–1.0]$). Визначити вагу коефіцієнта можна за допомогою: експертної оцінки, емпірично (наприклад, через метод аналізу ієрархій або Analytic Hierarchy Process);

A_{arch} – визначає реалізовану взаємоархітектуру між BPCS і SIS. Так як тип взаємоархітектури впливає на стійкість до кібератак, а ізольовані архітектури можуть бути більш стійкими до них, визначено наступні сталі коефіцієнти: "з повітряним зазором" = 4; "інтерфейсна" = 3; "інтегрована" = 2; "спільна" = 1.

x_i – кількість модулів пропрієтарного рішення промислового кіберзахисту. Для кожного модуля надається певне значення (для обчислення рекомендується використовувати діапазон в межах від 0,1 до 1 ($x_i \in [0{,}1–1{,}0]$), яке оцінює кіберстійкість цього модуля. Загальна кіберстійкість рішення промислового кіберзахисту обчислюється як сума цих значень;

N – визначає рівень коректності налаштувань всіх програмно-апаратних елементів, що використовуються для кіберзахисту на 2-1 рівнях моделі. Значення N обчислюється за допомогою експертного методу чи аудиту налаштувань. Значення N може знаходитися в межах від 0,1 до 1,0 ($N \in [0{,}1–1{,}0]$);

U – визначає ефективність/коректність політики усунення вразливостей в ПЗ на 2-1 рівнях моделі. Значення U може знаходитися в межах від 0,1 до 1,0 ($U \in [0{,}1–1{,}0]$);

D – визначає ефективність/коректність політики контролю доступу та авторизації в системі. Враховує використання мультифакторної автентифікації, рольового контролю доступу (RBAC), обмеження прав доступу. Значення D може знаходитися в межах від 0,1 до 1,0 ($D \in [0{,}1–1{,}0]$);

Z – показник рівня внутрішньої стійкості або адаптивності. Значення Z може знаходитися в межах від 0,1 до 1,0 ($U \in [0{,}1–1{,}0]$);

V_{ext} – визначає оцінку ризику від кібератак на 2-1 рівень моделі "ззовні" (наприклад, кібератаки через мережу Інтернет та з використанням атаки через ланцюг постачання (supply chain attack). Значення V_{ext} може знаходитися в межах від 0,1 до 1,0 ($V_{ext} \in [0{,}1–1{,}0]$);

V_{int} – визначає оцінку ризику від кібератак на 2-1 рівень моделі "з середини" (наприклад, кібератаки, які потенційно можуть бути здійснені інсайдером або ненавмисно некомпетентним співробітником). Значення V_{int} може знаходитися в межах від 0,1 до 1,0 ($V_{int} \in [0{,}1–1{,}0]$).

Кінцевий результат обчислень запропоновано порівняти з наступною умовною шкалою (таблиця 1). Отже, формула $CR_{2\text{-}1}$ дозволяє гнучко адаптуватись до різних систем, одночасно враховуючи технічні та організаційні аспекти кіберзахисту. Для полегшення порівняння між системами або варіантами архітектури використовуємо універсальну шкалу оцінювання в діапазоні [0,1]. Врахування кількості модулів та їхньої кіберстійкості ($\sum x_i$ / n) забезпечує масштабованість формули, яка залишається коректною незалежно від кількості модулів у системі. Формула враховує два вектори атаки (зовнішній і внутрішній), що дозволяє комплексно оцінювати ризики.

Таблиця 1

Умовна шкала оцінювання показника кіберстійкості 2-1 рівнів моделі Purdue

№ з/п	Значення $CR_{2\text{-}1}$	Інтерпретація	Коментар
1	0–0,20	низька кіберстійкість	критичний стан кіберстійкості, відсутність достатнього контролю кібербезпеки, слабка взаємоархітектура, неефективні політики
2	0,21–0,40	середня	окремі елементи захисту працюють ефективно, але високі ризики кіберстійкості
3	0,41–0,60	задовільна (прийнятна)	задовільний рівень, потрібні вдосконалення
4	0,61–0,80	висока	достатній рівень кіберзахисту
5	0,81–0,99	дуже висока	реалізовано повний спектр засобів кіберзахисту

Висновки. Отже, запропонований метод оцінки кіберстійкості 2-1 рівнів моделі, побудований на зваженому аналізі ключових технічних і організаційних факторів, є практичним, адаптивним і орієнтованим на реальні кіберзагрози. Його можна застосовувати як інструмент внутрішнього аудиту, порівняльної оцінки або як підґрунтя для покращення кіберзахисту в технологічній системі ОКІІ.

З огляду на проведений аналіз та враховуючи проміжні **висновки** дослідження, можна підсумувати, що:

найбільшою кіберзагрозою для технологічної системи ОКІ є ураження суб'єктом кіберзагрози SIS (що, зазвичай, здійснюється з використанням СТТПЗ);

оцінка кіберстійкості 2-1 рівнів моделі потребує регулярного перегляду з урахуванням всіх актуальних кіберзагроз (відслідковування тенденцій до застосування нових тактик та технік хакерськими групами з метою здійснення кібершпигунства та деструктивного кібервпливу на ОКІ з метою здійснення превентивних заходів);

поряд із такими традиційними елементами кіберзахисту 2-1 рівнів моделі, як коректність здійснення налаштувань, політика усунення вразливостей та розмежування доступу, одними з найвагоміших чинників кіберстійкості є коректна реалізація взаємоархітектури між BPCS і SIS, а також вибір оптимального (за низкою індивідуальних критеріїв реалізації роботи технологічної системи, наприклад: час реакції/час затримки; збереження балансу між навантаженістю мережі і кінцевого обладнання; достатній рівень гнучкості налаштувань; ефективність захисту від СТТПЗ; можливості розгортання у гетерогенному середовищі; можливості роботи з віртуалізованими середовищами та ін.) рішення промислового кіберзахисту, яке здатне ефективно та своєчасно виявляти кіберзагрози, зокрема СТТПЗ у технологічному середовищі 2-1 рівнів моделі з використанням сучасних підходів (сигнатурний, евристичний та поведінковий аналізи в комбінації/симбіозі з машинним навчанням);

на ОКІ високого рівня критичності при можливості необхідно здійснити децентралізацію рішення промислового кіберзахисту між інформаційними екосистемами BPCS і SIS. Це передбачає розгортання альтернативного (як варіант ізольованого) рішення для SIS.

У випадку коли розгортання альтернативного рішення в SIS обмежується рядом причин (технічного, фінансового характеру та інші), доцільно розглянути варіант реалізації додаткового рівня кіберзахисту (наприклад, із використанням відкритих рішень інтелектуального аналізу даних і машинного навчання).

Майбутні шляхи досліджень. Подальші дослідження автор зосереджує на підвищенні рівня кіберстійкості SIS за допомогою розгортання рішення інтелектуального аналізу даних

і машинного навчання “WEKA” з використанням інструментів поведінкової аналітики та моделі Long Short-Term Memory (LSTM),

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Borychenko Olena, Cherniavskyi Anatolii, Muliarevych Oleksandr, Shelekh Yurii, Sabat Myroslav. Cybersecurity in the energy industry of Ukraine: protection measures and challenges in the context of energy security // Journal of Management & Technology. № 24 (4). P. 67–90.

2. Mnushka O., Savchenko V. Security Model of IOT-based Systems // Conference: 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), February 2020.

3. Kondratenko Yuriy, Atamanyuk Igor, Sidenko Ievgen, Kondratenko Galyna. Machine Learning Techniques for Increasing Efficiency of the Robot’s Sensor and Control Information Processing // MDPI sensors. January 2022.

4. Pengyu Zhu, Jayantha P. Liyanage. Cybersecurity of Safety Instrumented Systems in the Context of Digitalization: Some Issues and Challenges within Oil and Gas Production Assets // The 30th European Safety and Reliability Conference, 1-5 November 2020.

5. Iaiani Matteo, Cozzani Valerio. Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry // Process Safety and Environmental Protection 172. February 2023.

6. Fan Zhang, J. Wesley Hines, Jamie B. Coble. A Robust Cybersecurity Solution Platform Architecture for Digital Instrumentation and Control Systems in Nuclear Power Facilities // Nuclear technology. October 2019. № 206 (1).

7. Лагун Ілона, Яцук Юрій. Супервізорні системи керування та збору даних: навч. посіб. Львів, 2025. 222 с.

8. Ackerman Pascal. Industrial Cybersecurity Second Edition. 2021. 800 p.

9. MITRE ATT&CK Tactics. URL: https://attack.mitre.org/tactics/ics.

10. Documentation Nozomi Networks Guardian. URL: technicaldocs.nozominetworks.com.

11. Nozomi Networks Guardian User Guide. URL: https://technicaldocs.nozominetworks.com/out/pdf-output/Guardian-User%20Guide.pdf.

12. Security guide for SIMATIC WinCC Unified and SIMATIC HMI Unified operator devices. URL: https://manuals.plus/m/eb19631ac50ad569431320d677d4783fa7ba4913e39b74170099b90ff17647c2.

13. WinCC OA Documentation. URL: https://www.winccoa.com/documentation/WinCCOA/latest/en_US/videos/security/security_basics_guideline.htm.

14. NIST. *Guide to Operational Technology (OT) Security (SP 800-82 Rev. 3).* URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pd.

DOI: 10.58254/viti.7.2025.15.165

УДК 621.391

д-р техн. наук Сайко В. Г. ORCID: 0000-0002-3059-6787 (ВІТІ ім. Героїв Крут)
канд. техн. наук, професор Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
канд. техн. наук Комаров В. О. ORCID: 0000-0002-4929-4527 (ВІТІ ім. Героїв Крут)

СПОСІБ ТА ІНТЕГРОВАНИЙ КОМПЛЕКС ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ НАЗЕМНИХ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ НА БАЗІ БПЛА СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Інноваційне рішення належить до галузі електронних комунікацій та радіотехніки, зокрема до способів позиціонування джерела радіовипромінювання (ДРВ), а саме до способів визначення місцезнаходження джерел випромінювання у ворожому середовищі, і може бути використане в навігаційних, пеленгаційних, локаційних засобах під час вирішення задачі прихованого визначення координат джерел радіовипромінювань, зокрема визначення координат ДРВ з борту літального апарата (ЛА). Підвищення ефективності застосування інтеграційного комплексу визначення місцезнаходження наземних ДРВ спеціального призначення порівняно з відомими рішеннями відбувається завдяки додатковому введенню до складу портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента інтелектуального датчика (сенсора) електромагнітної обстановки, системи управління інфраструктурою моніторингу територій угрупованнями ЛА. При цьому інфраструктура моніторингу територій угрупованнями ЛА виконана у вигляді з'єднаних між собою груп безпілотних літальних апаратів (БпЛА), які складають другий рівень літаючого сегмента та є мобільними точками доступу, та з'єднаних між собою груп головних БпЛА, що складають перший рівень літаючого сегмента, що здійснюють ретрансляцію прийнятих/переданих даних до базової станції мобільного зв'язку, яка функціонує у штатному режимі. Інноваційне рішення забезпечує підвищення ефективності функціонування інфраструктури інтегрованого комплексу визначення місцезнаходження наземних ДРВ спеціального призначення в умовах використання противником наземних джерел випромінювання зі спрямованими антенами та які працюють на низьких потужностях, шляхом спільного використання даних масивів первинних вимірювань портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента та вимірювань груп БпЛА другого рівня літаючого сегмента, які є мобільними точками доступу, що дозволяють підвищити точність позиціонування.

Ключові слова: *БпЛА, групи БпЛА, джерела радіовипромінювання спеціального призначення, координати об'єкта, літаючий сегмент, повітряний сегмент..*

V. Saiko, G. Radzivilov, V. Komarov. Method and integrated complex for determining the location of terrestrial sources of radio radiation based on special-purpose UAVs

The innovative solution belongs to the field of electronic communications and radio engineering, in particular, to methods of positioning a radio emission source (REF), namely, to methods of determining the location of radiation sources in a hostile environment and can be used in navigation, direction finding, and location tools when solving the problem of covert determination of the coordinates of radio emission sources, in particular, determining the coordinates of REF from the board of an aircraft (aircraft). Increasing the efficiency of the use of the integration complex for determining the location of ground-based radio emission sources of special purpose in comparison with known solutions occurs due to the additional introduction into the portable multifunctional means of determining the location of a radio emission source of the ground segment of an intelligent sensor (sensor) of the electromagnetic environment, an infrastructure management system for monitoring territories by groups of aircraft. At the same time, the infrastructure for monitoring territories by groups of flying vehicles is made in the form of interconnected groups of UAVs, which constitute the second level of the flying segment and are mobile access points, and interconnected groups of main UAVs, which constitute the first level of the flying segment, which relay received/transmitted data to the mobile communication base station, which operates in the normal mode. The innovative solution ensures increased efficiency of the functioning of the infrastructure of the integrated complex for determining the location of ground-based radio radiation sources of special purpose in conditions where the enemy uses ground-based radiation sources with directional antennas and operating at low power, by jointly using data from the arrays of primary measurements of a portable multifunctional means for determining the location of a ground-based radio radiation source and the changes of groups of UAVs of the second level of the flying segment, which are mobile access points, which allow to increase the accuracy of positioning.

Keywords: *UAVs, UAV groups, special-purpose radio emission sources, object coordinates.*

Постановка завдання у загальному вигляді

В умовах бойових дій ефективність застосування існуючої наземної мобільної техніки радіоконтролю з обмеженою висотою розміщення їх антенних пристроїв суттєво зменшується, а традиційне використання наземних багатопозиційних систем місцезнаходження стає практично непрацездатним, оскільки в умовах використання «малопотужних» наземних ДРВ зі спрямованими антенами та обмеженого часу випромінювання радіосигналів ймовірність одночасної електромагнітної доступності наземних ДРВ до кількох (не менше двох) пунктів прийому багатопозиційних систем визначення місцезнаходження стає вкрай низькою. Через це актуальною є розробка способів визначення джерел випромінювання з використанням БпЛА, які дозволяють істотно збільшити зону покриття з виявленням і визначенням координат ДРВ.

Аналіз публікацій за темою досліджень

Відомий комплекс визначення місцезнаходження наземних ДРВ, який включає прийом сигналів у заданій смузі частот вимірювачем, що переміщується в просторі, вимірювання первинних координатно-інформаційних параметрів виявлених сигналів, в якості яких використовується рівень оцінюваних сигналів, з одночасним вимірюванням і запам’ятовуванням вторинних параметрів [1]. Таке технічне рішення дозволяє скоротити часові витрати на визначення координат ДРВ в умовах, коли накладаються обмеження на габаритні розміри пеленгаторної антени.

Недоліком рішення є відносно низька точність визначення координат ДРВ. Це обумовлено тим, що під час вимірювання параметрів радіосигналу не враховуються його поляризаційні параметри, а для досягнення прийнятної точності визначення координат потрібно додаткове коригування маршруту польоту ЛА, що потребує тривалого електромагнітного контакту з ДРВ.

Відомий також комплекс визначення координат ДРВ при амплітудно-фазовій пеленгації з борту ЛА, який включає прийом радіосигналів бортовою антеною, частотну селекцію, визначення пеленгів, реєстрацію та обробку отриманих даних [2]. Координати ДРВ фіксуються як точка перетину принаймні двох ліній пеленгів. Спосіб дозволяє при його реалізації поєднувати процес визначення координат ДРВ з іншими процесами радіомоніторингу: параметричним та семантичним контролем сигналів.

Недоліком цього рішення є відносно низька точність визначення координат ДРВ. Це пояснюється насамперед виникненням помилок, пов’язаних із випадковими флуктуаціями просторового положення площини пеленгаторної антени під час польоту ЛА. Величину цих помилок можна порівняти із систематичними та експлуатаційними помилками використовуваних при реалізації апаратних засобів.

Відомий також комплекс визначення координат ДРВ при амплітудно-фазовій пеленгації з борту ЛА, який включає прийом радіосигналів бортовою пеленгаторною антеною, частотну селекцію, визначення ліній пеленгів, реєстрацію та вагову обробку отриманих даних [3]. Лінії пеленгів визначають у площині пеленгаторної антени, а за результатами вагової обробки формують допоміжні площини, ортогональні площини пеленгаторної антени і через кожну отриману лінію пеленгу.

Недоліком рішення є відносно невисока точність визначення координат ДРВ, так як під час вимірювання параметрів радіосигналу не враховуються його поляризаційні параметри, а також виникає необхідність використання антенних систем з елементами, що рознесені в просторі, що в більшості випадків неможливо через обмежені габарити ЛА.

Відомий комплекс визначення координат ДРВ, до складу якого входить об’ємна бортова пеленгаторна антенна решітка, що являє собою сукупність двох плоских антенних решіток, розташованих у паралельних або площинах, що перетинаються, що забезпечує можливість підвищення точності радіопеленгування в азимутальній і кутомісній

площинах [4]. Наземна компонента включає наземну апаратуру керування вертольотом та бортовим радіопеленгатором із пристроями керування та відображення у вигляді ноутбуків, а також контейнери для транспортування цільового навантаження.

Недоліком цього комплексу є відносно низька точність визначення координат ДРВ. Це пояснюється насамперед виникненням помилок, пов’язаних із випадковими флуктуаціями просторового положення площини пеленгаторної антени під час польоту ЛА. Крім того, громіскість антенних конструкції на ЛА вертолітного типу обумовлюють низьку експлуатаційну надійність комплексу.

Найбільш близьким технічним рішенням, як по суті, так і за задачею, що вирішується, яке обрано за найближчий аналог (прототип), є портативний багатофункціональний засіб визначення місцезнаходження ДРВ наземного сегмента (як варіант конструктивного виконання), що містить пеленгаційну систему, яка складається з антенної системи для радіомоніторингу та пеленгування, цифрового радіоприймального пристрою, блоку аналого-цифрової обробки сигналів, системи передачі даних, що складається із радіомодема та антени радіомодема, системи картографії і навігації, що складається із пристрою картографії і навігації та антени картографії і навігації, персонального комп’ютера [5].

До недоліків такого інтегрованого комплексу визначення місцезнаходження ДРВ відноситься те, що його функціональні можливості істотно залежать від висоти розміщення антенних пристроїв над земною поверхнею, що визначає дальність їхньої дії та робочу зону. Широкомасштабне використання на сьогодні військовими формуваннями рф завадозахищених наземних радіозасобів для управління силами і засобами під час ведення бойових дій, що функціонують у різних діапазонах частот при знижених потужностях і з використанням спрямованих антен, призводить до істотного зменшення ймовірності їх своєчасного виявлення і просторової локалізації (визначення місця розташування) наземними засобами радіоконтролю. Крім того, в умовах реального рельєфу місцевості робоча зона та ефективність застосування існуючої наземної мобільної техніки радіоконтролю з обмеженою висотою розміщення їх антенних пристроїв суттєво зменшуються.

Постановка завдання

Метою статті є розробка способу та інтегрованого рішення для забезпечення підвищення ефективності функціонування інфраструктури інтеграційного комплексу визначення місцезнаходження наземних ДРВ спеціального призначення в умовах використання противником наземних джерел випромінювання із спрямованими антенами та які працюють на низьких потужностях.

Виклад основного матеріалу

І. Технічні аспекти інноваційного рішення

В основу інноваційного рішення покладено задачу шляхом додаткового введення до складу портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента інтелектуального датчика (сенсора) електромагнітної обстановки, який підключається на вихід персонального комп’ютера та складається із N канальної системи збору даних та узгодження сигналів, драйвера системи збору даних, оперативного запам’ятовуючого пристрою, пристрою обробки сигналів, що складається зі статистичного процесора та нейронної мережі прямої передачі, системи управління інфраструктурою моніторингу територій угрупованнями ЛА. При цьому інфраструктура моніторингу територій угрупованнями ЛА виконана у вигляді з’єднаних між собою груп БпЛА, які складають другий рівень літаючого сегмента та є мобільними точками доступу, та з’єднаних між собою груп головних БпЛА, що складають перший рівень літаючого сегмента та здійснюють ретрансляцію прийнятих/переданих даних до базової станції мобільного зв’язку, яка функціонує в штатному режимі. Таке інноваційне рішення забезпечує підвищення

ефективності функціонування інфраструктури інтегрованого комплексу визначення місцезнаходження наземних ДРВ спеціального призначення в умовах використання противником наземних джерел випромінювання зі спрямованими антенами та які працюють на низьких потужностях, шляхом спільного використання даних масивів первинних вимірювань портативного багатофункціонального засобу визначення місцезнаходження ДРА наземного сегмента та вимірювань груп БпЛА другого рівня літаючого сегмента, які є мобільними точками доступу, що дозволяють підвищити точність позиціонування.

Ключовою відмінністю цього рішення від традиційних сучасних рішень, які використовуються на інтегрованих комплексах визначення місцезнаходження наземних ДРВ спеціального призначення, є використання роїв БпЛА/дронів для підняття сенсорів над землею, що поліпшує ефективність виявлення та контролю за ДРВ. Дрони дозволяють підняти сенсори на висоту, не вдаючись до розгортання важких конструкцій баштового типу, використання яких обмежене легкістю їх виявлення та мобільністю. Висока швидкість розгортання запропонованих радіорозвідувальних комплексів дозволить використовувати їх ближче до лінії зіткнення та матиме краще маскування екіпажів. В умовах, коли ворожі джерела використовують спрямовані антени та працюють на низьких потужностях, ускладнюючи їх виявлення, це стає великою перевагою, адже дозволить виявляти позиції екіпажів ворожих БпЛА під час їх безпосередньої роботи.

Особливість інноваційного рішення в інтегрованому комплексі визначення місцезнаходження наземних ДРВ спеціального призначення полягає у наступному:

по-перше, запропоноване рішення має портативний багатофункціональний засіб визначення місцезнаходження ДРВ наземного сегмента, що містить пеленгаційну систему, яка складається з антенної системи для радіомоніторингу та пеленгування, цифрового радіоприймального пристрою, блоку аналого-цифрової обробки сигналів, системи передачі даних, що в свою чергу складається із радіомодема та антени радіомодема, системи картографії і навігації, що також складається із пристрою картографії і навігації та антени картографії і навігації, персонального комп’ютера, системи живлення;

по-друге, до складу комплексу додатково введено інтелектуальний датчик (сенсор) електромагнітної обстановки, який підключається на вихід персонального комп’ютера та складається із N канальної системи збору даних та узгодження сигналів, драйвера системи збору даних, оперативного запам’ятовуючого пристрою, пристрою обробки сигналів, що складається зі статистичного процесора та нейронної мережі прямої передачі, системи управління інфраструктурою моніторингу територій угрупованнями ЛА;

по-третє, інфраструктура моніторингу територій угрупованнями ЛА літаючого сегмента виконана у вигляді з’єднаних між собою груп БпЛА, які складають другий рівень літаючого сегмента та є мобільними точками доступу, та з’єднаних між собою груп головних БпЛА, що складають перший рівень літаючого сегмента та здійснюють ретрансляцію прийнятих/переданих даних до базової станції мобільного зв’язку, яка функціонує в штатному режимі;

по-четверте, інфраструктура моніторингу територій угрупованнями ЛА літаючого сегмента розділена на два рівні. Перший рівень складається з головних БпЛА, а другий рівень – із членів БпЛА у кожній групі (див. рис. 1).

Зв’язок між членами БпЛА у групі першого рівня та між членами БпЛА та головним БпЛА у групі другого рівня здійснюється на базі стандарту IEEE 802.11p, який був розроблений для бездротової передачі інформації між транспортними засобами з підтримкою самоорганізації. Зв’язок між головними БпЛА у різних групах виконується за допомогою технології IEEE 802.11p* у розширеному режимі, яка може забезпечувати передачу даних на дальність до 740 м [6].

Технічний результат в інтегрованому комплексі визначення місцезнаходження наземних ДРВ спеціального призначення полягає в підвищенні надійності та ефективності в умовах сучасних військових конфліктів, де точність та оперативність грають критичну роль в успішному веденні бойових операцій.

Зазначений результат досягається тим, що у зазначеному комплексі використовується інфраструктура інтегрованого рішення на базі портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента, мережі БпЛА літаючого сегмента, засобів інфраструктури існуючої мобільної мережі.

За цих обставин БпЛА можуть забезпечити більш широкий обхват робочої зони та забезпечити можливість ефективного виявлення ворожих ДРВ в умовах реального рельєфу місцевості. Передбачено об’єднання БпЛА, обладнаних сенсорами, в єдину мережу для отримання точних даних шляхом комплексування даних. Цей спосіб дозволяє взаємодіяти декільком БпЛА, які одночасно піднімають сенсори над землею, та створює можливість визначення точного місцезнаходження ДРВ за допомогою аналізу сигналів із різних точок. Запропоноване рішення покликане розширити можливості систем автоматизованого ведення бою, поліпшуючи виявлення, контроль та ефективність у воєнних умовах. Подальший розвиток таких інновацій може підвищити загальну ефективність та військовий потенціал, забезпечуючи безпеку та захист національних інтересів.

ІІ. Побудова інтегрованого комплексу визначення місцезнаходження наземних ДРВ на базі БпЛА спеціального призначення

Суть інноваційного рішення в інтеграційному комплексі визначення місцезнаходження наземних ДРВ спеціального призначення пояснюється кресленнями, де:

на рисунку 1 зображено інтегровану структуру автоматизованого комплексу визначення місцезнаходження наземних ДРВ для рішення задач силами спеціального призначення;

на рисунку 2 зображено структурну схему портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента;

на рисунку 3 зображено структурну схему інтелектуального сенсора на базі ПЛІС для оцінки електромагнітної обстановки у реальному часі;

на рисунку 4 зображено функціональну схему комплексування вимірювань портативним багатофункціональним засобом визначення місцезнаходження ДРВ наземного сегмента та інфраструктурою моніторингу територій угрупованнями ЛА літаючого сегмента;

на рисунку 5 зображено графіки залежності щільності ймовірності та гістограма помилки визначення місцезнаходження при отриманні 40 сигналів.

Інтегрований комплекс визначення місцезнаходження ДРВ (як варіант конструктивного виконання) містить: наземний сегмент (*1*), до складу якого входить наземний портативний багатофункціональний засіб (*2*) визначення місцезнаходження ДРВ наземного сегмента, інтелектуальний датчик (сенсор) електромагнітної обстановки (*3*), систему управління (*4*) інфраструктурою моніторингу територій угрупованнями ЛА, командний пункт (*5*) керування комплексом, віддалену базову станцію (*6*), джерела радіовипромінювання (*7*), літаючий сегмент (*8*), до складу якого входить інфраструктура (*9*) моніторингу територій угрупованнями ЛА літаючого сегмента, що містить з’єднані між собою групи головних БпЛА (*10*) $_{1...n}$, інфраструктура (*11*) моніторингу територій угрупованнями ЛА літаючого сегмента, що містить також з’єднані між собою окремі групи (*12*) $_{1..n}$ по 3–5 ЛА (див. блок-схему на рис. 1).

ІІІ. Спосіб визначення місцезнаходження наземних ДРВ на базі БпЛА спеціального призначення

В інтегрованому комплексі визначення місцезнаходження наземних ДРВ спеціального призначення здійснюють наступним чином з використанням рисунка 1 та рисунка 4, на яких позначено (див. рис. 1):

1 – наземний сегмент;

2 – наземний портативний багатофункціональний засіб визначення місцезнаходження ДРВ наземного сегмента;

3 – інтелектуальний датчик (сенсор) електромагнітної обстановки;

4 – система управління інфраструктурою моніторингу територій угрупованнями ЛА;

5 – командний пункт керування комплексом;

6 – віддалена базова станція мобільного зв’язку;

7 – джерела радіовипромінювання;

8 – літаючий сегмент;

9 – інфраструктура моніторингу територій угрупованнями ЛА літаючого сегмента першого рівня;

10 $_{1...n}$ – групи головних БпЛА першого рівня;

11 – інфраструктура моніторингу територій угрупованнями ЛА літаючого сегмента другого рівня;

12 $_{1..n}$ – окремі групи по 3–5 ЛА другого рівня.

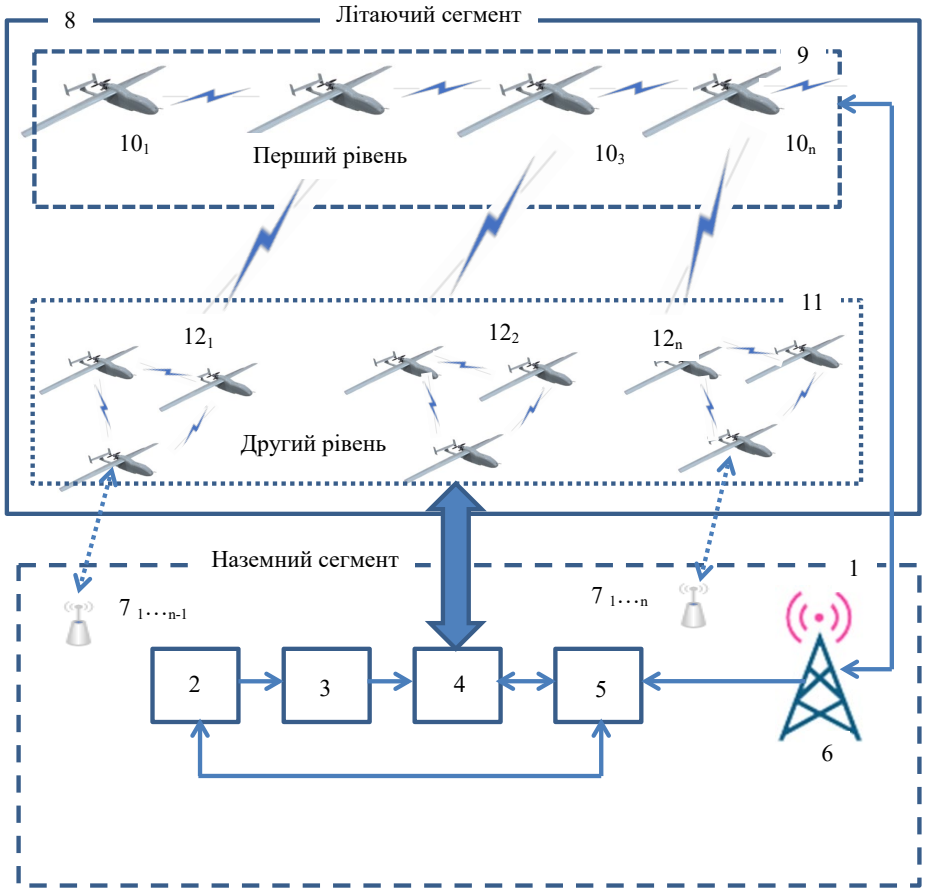


Рис. 1. Інтегрована структура автоматизованого комплексу визначення місцезнаходження наземних ДРВ для рішення задач силами спеціального призначення

На рисунку 2 позначено:

29 – виміряні значення RSSI наземним портативним багатофункціональним засобом визначення місцезнаходження ДРВ наземного сегмента;

30 – фіксовані відліки часу;

31 – виміряні значення RSSI із груп БпЛА інфраструктурою моніторингу територій угрупованнями ЛА літаючого сегмента;

32 – метод найближчих сусідів;
33 – база даних радіокарти;
34 – передача даних до командного пункту;
35 – координати радіоелектронних засобів (РЕЗ) по радіокарті;
36 – фільтр Калмана;
37 – координати РЕЗ по даних груп БпЛА;
38 – визначення місцезнаходження РЕЗ;
39 – підрахунок середньоквадратичної помилки.

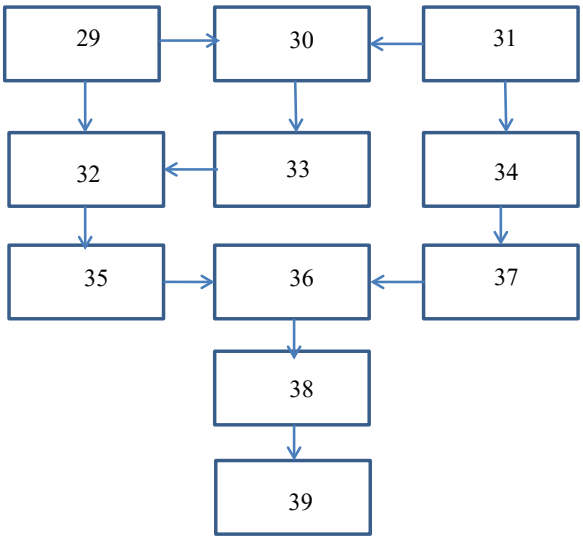


Рис. 2. Функціональна схема комплексування вимірювань портативним багатофункціональним засобом визначення місцезнаходження ДРВ наземного сегмента та інфраструктурою моніторингу територій угрупованнями ЛА літаючого сегмента

На першому етапі при зборі первинних даних формується база даних (БД) радіокарти RSSI (див. блок 33 рис. 2) на базі даних вимірювань місцезнаходження ДРВ наземним портативним багатофункціональним засобом *2* (див. рис. 1) наземного сегмента (див. блок 29 рис. 2) та групи БпЛА 11 другого рівня літаючого сегмента (див. рис. 1 та блок 31 рис. 2). Вимірювання збираються до таблиці БД, яка містить дані рівнів RSSI та звіти часу. Результати першого етапу є БД радіокарти (див. блок 33 рис. 2), що містить набір вимірювань RSSI портативного багатофункціонального засобу *2* (див. рис. 1) наземного сегмента та групи БпЛА другого рівня 11 літаючого сегмента для відповідних координат (див. рис. 1).

При цьому інфраструктура моніторингу територій угрупованнями ЛА літаючого сегмента виконана у вигляді з’єднаних між собою груп БпЛА, які складають другий рівень *11* літаючого сегмента та є мобільними точками доступу для ДРВ *7* $_{1...n}$ (див. рис. 1), та з’єднаних між собою груп головних БпЛА *10* $_{1...n}$, що складають перший рівень *9* літаючого сегмента та здійснюють ретрансляцію прийнятих/переданих даних до базової станції *6* мобільного зв’язку (див. рис. 1), яка функціонує у штатному режимі.

Визначення місцезнаходження ДРВ наземного сегмента портативним багатофункціональним засобом *2* (див. рис. 1) здійснюється класичним методом тріангуляції [8]. Даний процес пояснюється таким чином з використанням рисунка 2, на якому позначено:

13 – пеленгаційна система;

14 – антенна система для радіомоніторингу та пеленгування;
15 – цифровий радіоприймальний пристрій;
16 – блок аналого-цифрової обробки сигналів;
17 – система передачі даних;
18 – антена радіомодема;
19 – радіомодем;
20 – система картографії і навігації;
21 – антена пристрою картографії і навігації;
22 – пристрій картографії і навігації;
23 – персональний комп’ютер;
24 – система живлення.

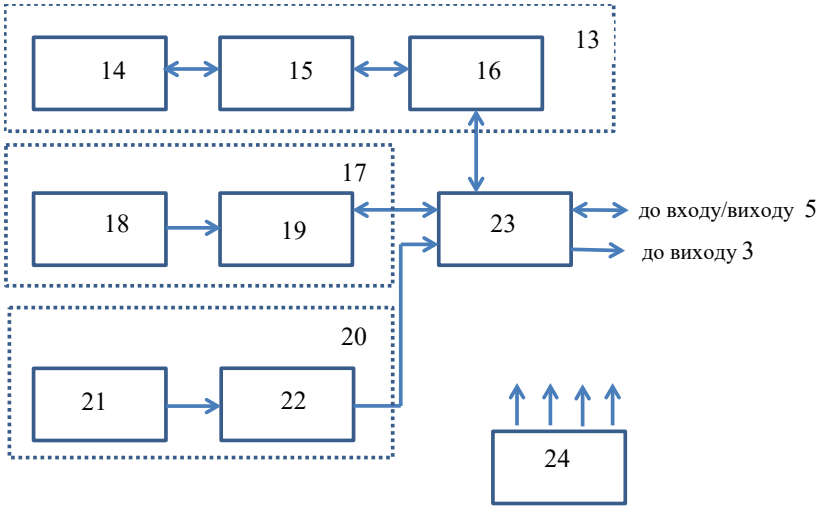


Рис. 2. Структурна схема портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента

Отримані дані визначення координат (див. блок 35 рис. 4) використовуються для формування польотного завдання для груп БпЛА *11* другого рівня літаючого сегмента та одночасно використовуються при комплексуванні вимірювань портативним багатофункціональним засобом визначення місцезнаходження ДРВ наземного сегмента та інфраструктурою моніторингу територій угрупованнями ЛА другого рівня *11* літаючого сегмента (див. рис. 1).

Для оперативного оцінювання змін динамічних параметрів електромагнітної обстановки у реальному часі портативного багатофункціонального засобу *2* застосовується інтелектуальний датчик *3* (див. рис. 1). Структуру інтелектуального датчика *3* показано на рисунку 3, де:

25 – *N* канальна система збору даних та узгодження сигналів;
26 – драйвер системи збору даних;
27 – оперативний запам’ятовуючий пристрій;
28 – пристрій обробки сигналів у складі статистичного процесора та нейронної мережі прямої передачі.

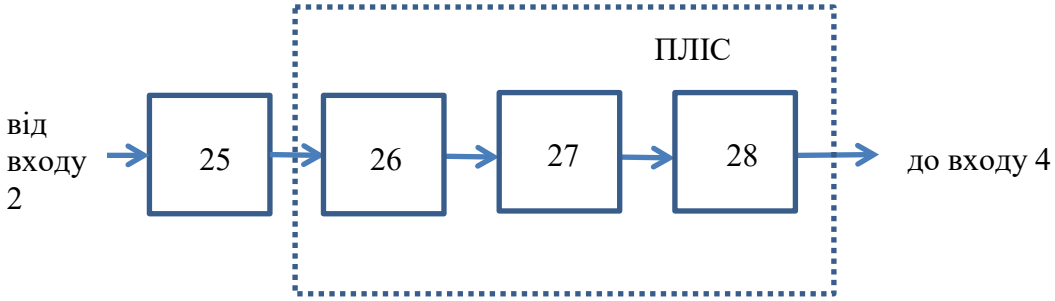


Рис. 3. Структурна схема інтелектуального сенсора на базі ПЛІС для оцінки електромагнітної обстановки у реальному часі

N канальна система *25* збору даних та узгодження сигналів отримує сигнали з виходу персонального комп’ютера *23* (див. рис. 2). Обробка сигналів виконується за допомогою процесора, реалізованого на базі ПЛІС блоками *26*, *27*, *28* (див. рис. 3). Обмін інформацією ведеться через інтерфейс RS232, вбудований у ПЛІС. Дані вимірів відправляються на під’єднану систему управління *4* інфраструктурою моніторингу територій угрупованнями ЛА *11* (див. рис. 1).

Крім того, виміряні значення RSSI даним способом використовуються при комплексуванні вимірювань портативним багатофункціональним засобом визначення місцезнаходження ДРВ наземного сегмента та інфраструктурою моніторингу територій угрупованнями ЛА другого рівня *11* літаючого сегмента (див. рис. 4) для забезпечення збільшення недостатньої частоти вимірювань RSSI і відповідно збільшення точності позиціонування джерел випромінювання $7_{1...n}$ (див. рис. 1).

Група БпЛА другого рівня *11* (див. рис. 1) спочатку здійснює первинну обробку інформації на борту БпЛА, а потім дані про виявлені ДРВ через групи головних БпЛА *9* (див. рис. 1), що складають перший рівень літаючого сегмента, ретранслюються до базової станції *6* мобільного зв’язку (див. рис. 1), яка функціонує у штатному режимі.

Далі дані по швидкодіючим каналам зв’язку передаються на наземний командний пункт *5* керування комплексом, де здійснюються вторинна обробка та відображення даних про розкриту радіоелектронну обстановку на тлі електронної карти місцевості (блок 20 на рис. 2). Для передачі з борту БпЛА більшого обсягу даних (даних про виявлені в широкому діапазоні частот ДРВ) застосовується апаратура передачі даних терагерцового діапазону.

Для цього до складу групи БпЛА першого та другого рівнів додатково введено приймально-передавальний модуль (радарний модуль TRX_024_06 [5]) терагерцового діапазону [7] у вигляді інтегральних мікросхем, що містять повністю прийомопередавач із вбудованою смужковою антенною решіткою, виконаний з можливістю вимірювання відстані та RSSI.

На другому етапі набори даних вимірів БД зіставляються з вимірами RSSI наземного портативного багатофункціонального засобу *2* визначення місцезнаходження ДРВ наземного сегмента та групи БпЛА *11* другого рівня, вибираються відповідні координати методом найближчих сусідів (див. блок 32 рис. 4). Проміжні результати оцінки координат кожним методом окремо комплексуються фільтром Калмана (див. блок 36 рис. 4) для підвищення точності позиціонування і компенсації випадкових викидів.

IV. Модель визначення місцезнаходження об’єкта випромінювання

Процес визначення місцезнаходження об’єкта випромінювання групою БпЛА другого рівня пояснюється таким чином.

Припускаючи, що джерело випромінювання знаходиться на землі ($z_o = 0$), необхідно знайти координату розташування джерела випромінювання (x_i, y_i, 0) та i-ю позицію групи

БпЛА другого рівня (x_i, y_i, z_i) при отриманні сигналу від джерела випромінювання. Якщо група БпЛА другого рівня отримує m сигналів від джерела випромінювання, координати точки визначення місцезнаходження повинні задовольняти рівнянням (1):

$$\begin{cases} (x_1 - x_0) + (y_1 - y_0) + (z_1)^2 = (d_1)^2 \\ \dots\dots\dots \\ (x_i - x_0) + (y_i - y_0) + (z_i)^2 = (d_i)^2 \\ \dots\dots\dots \\ (x_m - x_0) + (y_m - y_0) + (z_m)^2 = (d_m)^2 \end{cases}, \quad (1)$$

де d_i – відстань від групи БпЛА другого рівня до джерела випромінювання.

У бездротовому радіоканалі з урахуванням моделей поширення радіохвиль оцінюють втрати потужності сигналу під час поширення через середовище. Так, потужність сигналу, що приймається, менше потужності переданого. Для прогнозування різниці між сигналами, що передаються і приймаються, потужність кожного прийнятого радіосигналу вимірюють за допомогою показника рівня прийнятого сигналу (Received Signal Strength Indicator, RSSI) [8]. Відстань на базі показників RSSI, як правило, розраховується на основі моделі логарифмічної втрати потужності сигналу при поширенні в середовищі:

$$RSSI = A - 10 * n * log\left({}^{d}/_{d_o}\right) + X_\sigma, \quad (2)$$

де d – відстань від пристрою до передавача (м);

A – потужність сигналу пристрою, виміряна на одиничній відстані d_0 від пристрою (дБм);

n – коефіцієнт втрат потужності сигналу при поширенні в середовищі, показник пов'язаний із конкретною технологією бездротового зв'язку;

X_σ – гаусовий розподіл випадкової змінної з нульовим середнім значенням та дисперсією σ^2.

Оскільки втрата потужності сигналу при поширенні в середовищі залежить від навколишнього середовища, для підвищення точності позиціонування в технічному рішенні необхідно оцінити параметри A, n перед розгортанням операції визначення місцезнаходження.

Отже, у кожній конкретній операції для визначення місцезнаходження джерела випромінювання, група БпЛА другого рівня здійснює попереднє калібрування, тобто показник RSSI розраховується, враховуючи відстань між групою БпЛА другого рівня і початковою точкою, вимірювання проводиться кілька разів.

Потім для знаходження оптимальних параметрів (A, n) використовується нелінійний метод найменших квадратів. При вимірах m ці параметри визначаються як:

$$(A, n) = argmin\left(\sum_{i=1}^{m} 10^{\frac{A-RSSI}{10n}} - d_i\right)^2. \quad (3)$$

Після визначення відстані до джерела випромінювання необхідно обчислити координати цього джерела випромінювання.

Даний процес пояснюється наступним чином.

Припустимо, що позиція джерела випромінювання p (x_i, y_i, 0), а група БпЛА другого рівня отримує сигнал від джерела випромінювання в позиції p_i (x_i, y_i, z_i). Відстань між цими двома точками розраховується з урахуванням похибки вимірювання, що встановлюється під час калібрування. З кожним отриманим сигналом із джерела випромінювання, відстань від нього до групи БпЛА другого рівня дорівнюватиме:

$$d(p_i, p_o) = \sqrt{(x_i - x_0) + (y_i - y_0) + (z_0)^2} + \varepsilon. \quad (4)$$

Таким чином, кількість сигналів, що приймаються, і похибка вимірювання ε впливають на точність процесу позиціонування. Позиція p_k (x_k, y_k) визначається шляхом мінімізації виразу (5):

$$arg\ min\ \sum_{i=1}^{m}(\sqrt{(x_i - x_k) + (y_i - y_k) + (z_i)^2} - d(p_i, p_k)), \quad (5)$$

де m – кількість сигналів, що приймаються від несанкціонованого повітряного об’єкта.

Внаслідок мінімізації стає можливим обчислити координати джерела випромінювання та похибки (див. блоки *38* і *39* на рис. 4).

Таким чином, для оцінки можливості визначення місцезнаходження на основі сигналу, що приймається, в розробленій моделі враховується кількість сигналів, що приймаються, і помилки вимірювання. Результати моделювання показують, що помилка визначення місцезнаходження збільшується, коли збільшується помилка вимірювання відстані (див. рис. 5). Враховуючи отримані залежності, точність визначення місцезнаходження може бути досягнута шляхом підвищення якості вимірювання відстані та забезпечення виявлення більшої кількості сигналів [9–11].

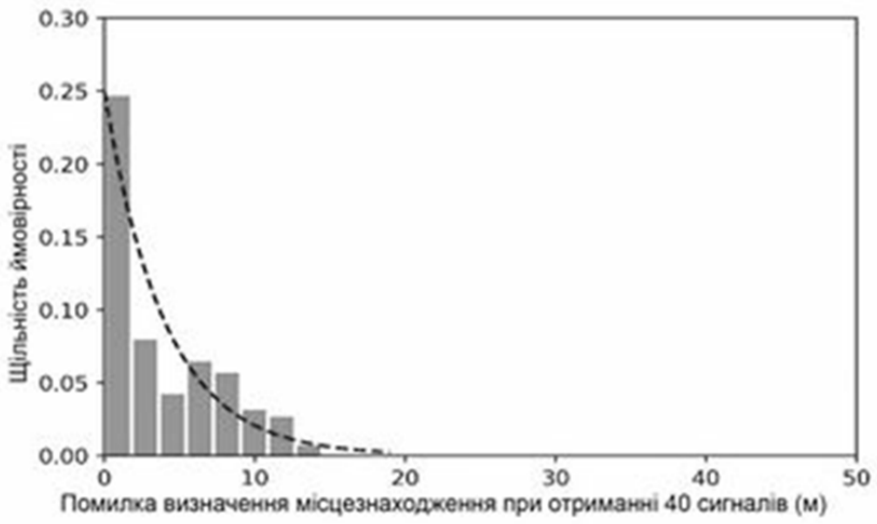


Рис. 5. Щільність імовірності та гістограма помилки визначення місцезнаходження при отриманні 40 сигналів

Напрямки подальшої наукової роботи

Розробка комплексу моделей позиціонування з використанням БпЛА, що дозволяють візуалізувати процес обробки первинних вимірювань та оцінки координат дДРВ для різних топологій стаціонарних приймальних пунктів у складі наземного сегмента та траєкторій рухів приймальних пунктів на борту БпЛА у складі літаючого сегмента.

Висновки

1. Підвищення ефективності застосування інтеграційного комплексу визначення місцезнаходження наземних ДРВ спеціального призначення порівняно з прототипом полягає в тому, що шляхом введення додаткового введення до складу портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента інтелектуального датчика (сенсора) електромагнітної обстановки, системи управління інфраструктурою моніторингу територій угрупованнями ЛА При цьому інфраструктура

моніторингу територій угрупованнями ЛА виконана у вигляді з’єднаних між собою груп БпЛА, які складають другий рівень літаючого сегмента та є мобільними точками доступу, та з’єднаних між собою груп головних БпЛА, що складають перший рівень літаючого сегмента та здійснюють ретрансляцію прийнятих/переданих даних до базової станції мобільного зв’язку, яка функціонує у штатному режимі, забезпечується підвищення надійності та ефективності в умовах сучасних військових конфліктів, де точність та оперативність грають критичну роль в успішному веденні бойових операцій.

2. Зазначений результат досягається тим, що у зазначеному інноваційному рішенні використовується інтегроване рішення на базі портативного багатофункціонального засобу визначення місцезнаходження ДРВ наземного сегмента, мережі БпЛА літаючого сегмента, засобів інфраструктури існуючої мобільної мережі. При цьому БпЛА можуть забезпечити більш широкий обхват робочої зони та забезпечити можливість ефективного виявлення ворожих ДРВ в умовах реального рельєфу місцевості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Патент 2510044 рф. Способ и устройство определения координат источников радиоизлучений. В. А. Заренков, Д. В. Заренков, В. И. Дикарев, А. С. Данилюк. Опубл. 2006.

2. Патент 2275746 рф. Станция радиотехнической разведки. С. М. Вишняков, М. В. Куликов, А. Г. Митянин, П. Л. Смирнов, Д. В. Царик, О. В. Царик, А. М. Шепилов, А. Я. Шишков. Опубл. 2012.

3. Патент 2432580 рф. Способ определения координат источника радиоизлучений при амплитудно-фазовой пеленгации с борта летательного аппарата. А. В. Вассенков, О. Б. Гузенко, А. С. Дикарев, В. А. Скобелкин. Опубл. 2011.

4. Рембовский А. М. Радиомониторинг – задачи, методы, средства. М.: Горячая линия – Телеком, 2010. 624 с.

5. Документація на TRX_024_006. URL: https://siliconradar.com/products/single-product/24-ghz-transceiver-trx_024_046/ (дата звернення: 13.04.2025).

6. Мережі мобільного зв’язку нового покоління 4G/5G/6G: монографія / В. Г. Сайко та ін. К.: ТОВ «Про формат», 2021. 200 с.

7. Безпроводові системи зв’язку терагерцового діапазону: монографія / В. Г. Сайко, Т. М. Наритник. Німеччина. Видавництво «LAP LAMBERT Academic Publishing RU», 2019. 68 с.

8. Слободянюк П. В., Наритник Т. М., Благодарний В. Г., Сайко В. Г., Булгач В. Л Теорія і практика управління використанням радіочастотного ресурсу: навч. посіб. К.: ДУІКТ, 2012. 596 с.

9. Сайко В. Г., Деркач А. П. Комплекс спеціального радіомоніторингу за радіоелектронними засобами з динамічною топологією для силових структур, який швидко розгортається на полі бою («Спеціальний моніторинг»). *Свідоцтво про реєстрацію авторського права на твір № 125830* (УкрНОІВІ), 18 квітня 2024 року.

10. Сайко В. Г., Радзівілов Г. Д., КомаровВ. О., Фомін М. М., Солодовник В. І., Криволапов Я. В., Криволапов Г. Я. Алгоритм визначення місцезнаходження несанкціонованого БПЛА за умов багатопроменевого поширення радіохвиль. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* Серія: технічні науки. Том 35 (74). 2024. № 1. С. 74–80.

11. Сайко В. Г., Романов Д. О., Радзівілов Г. Д., Комаров В. О., Фомін М. М. Метод визначення місцезнаходження низько літаючого повітряного об’єкту за умов багатопроменевого поширення радіохвиль. *Збірник наукових праць ВІТІ. Системи і технології зв’язку, інформатизації та кібербезпеки.* 2024. Вип. 6. С. 204–214.

DOI: 10.58254/viti.7.2025.16.177

УДК 621.396

д-р техн. наук, професор Сайко В. Г. ORCID: 0000-0002-3059-6787 (ВІТІ ім. Героїв Крут)
Станілога О. О. ORCID: 0009-0008-5031-3431 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ ТА МОДЕЛЬ ОЦІНКИ ХАРАКТЕРИСТИК ЕФЕКТИВНОСТІ БЕЗПРОВОДОВИХ МЕРЕЖ СИСТЕМ КОГНІТИВНОГО РАДІО СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У статті представлено комплексний аналіз сучасних тенденцій розвитку та модель оцінки характеристик ефективності безпроводових мереж систем когнітивного радіо спеціального призначення. Дослідження фокусується на ключових напрямах розвитку технологій, їхніх перевагах і недоліках, а також на перспективах застосування в критично важливих галузях. Особливу увагу приділено аналізу сучасних наукових досліджень та розробок у галузі когнітивного радіо, зокрема для військових систем, де надійність та безпека зв'язку є критично важливими.

Стаття розглядає основні принципи когнітивного радіо, такі як динамічний доступ до спектра, адаптивність до змін середовища та інтелектуальне управління ресурсами. Проаналізовано технології, що використовуються в системах когнітивного радіо спеціального призначення, включаючи програмно-визначені радіосистеми (SDR), когнітивні радіомережі (CRN) та технології безпеки зв'язку.

Основні тенденції розвитку, виявлені у процесі дослідження, включають використання штучного інтелекту та машинного навчання для оптимізації роботи мереж, розвиток гетерогенних мереж для забезпечення більшої гнучкості та надійності, а також посилення заходів безпеки для захисту від кібератак і радіоелектронної боротьби.

Специфікою мережевоцентричної системи зв'язку військового призначення є швидкий та гарантований доступ користувачів до її послуг. У представленій роботі розроблено модель вибору оптимальних параметрів когнітивної мережі зв'язку, яка самоорганізується, що забезпечують необхідну доступність його абонентів. Модель дозволяє вибрати оптимальні параметри майданного покриття та канального ресурсу для забезпечення необхідної доступності когнітивної мережі зв'язку.

Стаття також розглядає перспективи практичного застосування когнітивного радіо в спеціальних системах, підкреслюючи його потенціал для забезпечення надійного та ефективного зв'язку в складних і мінливих умовах. Результати дослідження підкреслюють важливість подальших досліджень у цій галузі для розробки більш ефективних і безпечних систем когнітивного радіо.

Ключові слова: *когнітивне радіо, безпроводові мережі, модель, спеціальне призначення, динамічний доступ до спектра, адаптивні системи, безпека зв'язку, штучний інтелект, гетерогенні мережі, військові системи зв'язку.*

V. Sayko, O. Staniloha. Analysis of trends in development and a model for evaluating the performance characteristics of wireless networks used in special purpose cognitive radio systems

The article presents a comprehensive analysis of current trends in the development and a model for evaluating the performance characteristics of wireless networks in cognitive radio systems for special purposes. The study focuses on key directions in the development of these technologies, their advantages and limitations, as well as their potential applications in critical sectors. Particular attention is given to the analysis of contemporary scientific research and developments in the field of cognitive radio, especially for military systems, where communication reliability and security are of paramount importance.

The article examines the fundamental principles of cognitive radio, such as dynamic spectrum access, adaptability to changing environments, and intelligent resource management. It analyzes the technologies used in cognitive radio systems for special purposes, including software-defined radio (SDR), cognitive radio networks (CRNs), and communication security technologies.

The main development trends identified during the study include the use of artificial intelligence and machine learning to optimize network performance, the evolution of heterogeneous networks to ensure greater flexibility and reliability, and the enhancement of security measures to counter cyberattacks and electronic warfare.

A key feature of network-centric military communication systems is the rapid and guaranteed access of users to communication services. This work proposes a model for selecting optimal parameters of a self-organizing cognitive communication network that ensures the required availability for its users. The model enables the selection of optimal coverage and channel resource parameters to achieve the desired accessibility of the cognitive communication network.

The article also explores the prospects of practical application of cognitive radio in specialized systems, highlighting its potential to provide reliable and efficient communication in complex and dynamic environments.

The findings emphasize the importance of continued research in this area to develop more effective and secure cognitive radio systems.

Keywords: *cognitive radio, wireless networks, model, special purpose, dynamic spectrum access, adaptive systems, communication security, artificial intelligence, heterogeneous networks, military communication systems.*

Постановка проблеми

Сучасні безпроводові системи зв’язку стикаються з проблемою обмеженості радіочастотного спектра та необхідністю забезпечення високої надійності та безпеки передачі даних, особливо в умовах спеціального призначення. Когнітивне радіо, з його здатністю до динамічного управління спектром та адаптації до змін середовища, є перспективним рішенням для подолання цих викликів.

Актуальність дослідження полягає в аналізі сучасних тенденцій розвитку когнітивного радіо для спеціальних застосувань, визначенні ключових напрямів досліджень і перспектив їх практичного застосування. Актуальність дослідження безпроводових мереж систем когнітивного радіо спеціального призначення зумовлена низкою факторів, які відображають сучасні виклики та потреби в галузі зв’язку:

Перевантаженість радіочастотного спектра: Зі зростанням кількості безпроводових пристроїв та послуг радіочастотний спектр стає дедалі більш перевантаженим. Це особливо критично для систем спеціального призначення, де надійний зв’язок є життєво необхідним. Когнітивне радіо пропонує рішення цієї проблеми шляхом динамічного доступу до спектра, дозволяючи системам використовувати вільні частоти в реальному часі.

Вимоги до надійності та безпеки: Системи спеціального призначення, такі як військові, аварійно-рятувальні та критично важливі інфраструктурні системи, вимагають високого рівня надійності та безпеки зв’язку. Когнітивне радіо з його здатністю до адаптації та інтелектуального управління ресурсами може забезпечити стійкий та захищений зв’язок у складних умовах.

Необхідність адаптації до мінливих умов: Умови роботи систем спеціального призначення часто є непередбачуваними та мінливими. Це може включати радіоелектронну боротьбу, природні катастрофи або інші надзвичайні ситуації. Когнітивне радіо з його здатністю до адаптації до змін середовища може забезпечити безперебійний зв’язок у будь-яких умовах.

Розвиток технологій штучного інтелекту: Розвиток штучного інтелекту та машинного навчання відкриває нові можливості для оптимізації роботи когнітивного радіо. Алгоритми штучного інтелекту можуть використовуватися для прогнозування змін у радіочастотному середовищі, виявлення завад та прийняття оптимальних рішень щодо використання спектра.

Потреба в інтеграції різнорідних мереж: Сучасні системи спеціального призначення часто використовують різнорідні мережі зв’язку, такі як стільниковий зв’язок, супутниковий зв’язок та спеціалізовані радіосистеми. Когнітивне радіо може забезпечити інтеграцію цих мереж та ефективне використання їхніх ресурсів. Ураховуючи ці фактори, дослідження тенденцій розвитку безпроводових мереж систем когнітивного радіо спеціального призначення є надзвичайно актуальним і має велике значення для забезпечення надійного та ефективного зв’язку в критично важливих сферах.

Аналіз останніх досліджень і публікацій

Фундаментальні роботи Дж. Мітоли III: Впливова робота "Cognitive Radio: Making Software Radios More Personal" (1999) заклала основи концепції когнітивного радіо, виділивши ключові принципи та потенційні застосування. Подальші роботи Мітоли та його колег розвинули ідеї динамічного доступу до спектра та адаптивного управління радіоресурсами [1].

У відповідь на виклики, пов’язані з управлінням радіочастотним спектром у військових мережах, активно ведуться дослідження та розробки в галузі когнітивного радіо для

військового застосування. Основні напрямки цих досліджень включають розробку передових методів зондування спектра, створення ефективних протоколів для когнітивних мереж, посилення безпеки комунікацій та інтеграцію когнітивного радіо з іншими перспективними технологіями, такими як штучний інтелект (AI) та машинне навчання (ML). Важливу роль у цих дослідженнях відіграють оборонні агентства, такі як Агентство передових оборонних дослідницьких проєктів США (DARPA), яке реалізує програми Next Generation та CommEx, а також Європейське оборонне агентство (EDA) з його проєктами SCORED та CORASMA.

Одним із ключових прикладів ініціатив у галузі військового когнітивного радіо є програма Joint Tactical Radio Systems (JTRS), метою якої була розробка сімейства програмно-визначених радіостанцій з когнітивними можливостями для більш ефективного використання спектра та забезпечення сумісності між різними військовими підрозділами. У рамках цієї програми було розроблено концепцію динамічного доступу до спектра (DSA), яка дозволяє радіостанціям автоматично виявляти доступні частоти та використовувати їх для зв’язку, а також метод фрагментації спектра, що передбачає об’єднання невеликих фрагментів невикористаного спектра для створення ширших каналів зв’язку. Іншим прикладом є розробка компанією KNL когнітивних мережевих високочастотних радіостанцій (CNHF), які здатні автоматично сканувати та виявляти доступні смуги спектра, забезпечуючи надійний зв’язок навіть в умовах обмеженого спектра. Хоча концепція когнітивного радіо для військового застосування ще перебуває на етапі становлення, наявні програми та ініціативи становлять практичні кроки у напрямі інтеграції відповідних технологій у військові системи зв’язку.

Метою статті є аналіз сучасних тенденцій розвитку безпроводових мереж систем когнітивного радіо спеціального призначення, визначення ключових напрямів досліджень, перспектив їх практичного застосування та розробка моделі вибору оптимальних параметрів когнітивної мережі зв’язку, яка самоорганізується, що забезпечують необхідну доступність його абонентів.

Виклад основного матеріалу

І. Аналіз тенденцій розвитку безпроводових мереж систем когнітивного радіо спеціального призначення

Когнітивне радіо є однією з ключових технологій сучасних безпроводових мереж, що забезпечує адаптивне використання частотного спектра, підвищує ефективність радіочастотного ресурсу та сприяє розвитку інтелектуальних систем зв’язку. Його поява стала відповіддю на проблему обмеженості доступного спектра, зумовлену зростаючими вимогами до пропускної здатності мереж та щільністю розміщення безпроводових пристроїв.

Основною ідеєю когнітивних радіомереж є можливість забезпечувати високу пропускну здатність для мобільних користувачів за допомогою динамічних методів доступу до спектра і гетерогенної безпровідної архітектури. Однак невизначеність можливого доступного спектра і також змінні вимоги щодо якісних параметрів обслуговування для різних додатків, когнітивні радіомережі створюють унікальні завдання динамічного використання радіочастотного спектра.

Система когнітивного радіо включає наступні особливості [2]:

1. Уміння взаємодії з навколишнім середовищем для отримання інформації про його поточний стан.
2. Здатність інтелектуально аналізувати отриману інформацію про стан радіосередовища.
3. Вміння адаптивно змінювати конфігурацію системи при зміні параметрів радіосередовища.

Рис. 1. Загальні властивості когнітивного радіо

Функціонування когнітивної радіомережі передбачає забезпечення високої пропускної здатності для мобільних користувачів завдяки використанню гетерогенної архітектури бездротового зв’язку та методів динамічного доступу до спектра. Досягнення цієї мети можливе лише шляхом ефективного управління розподілом радіочастотного ресурсу в реальному часі. Однак когнітивні радіомережі стикаються з унікальними викликами, зокрема з постійними змінами доступності спектра та необхідністю задовольняти різні вимоги до якості обслуговування (QoS) залежно від характеристик конкретних застосувань [3]. Типовий цикл роботи когнітивного радіо представлений на рисунку 2.

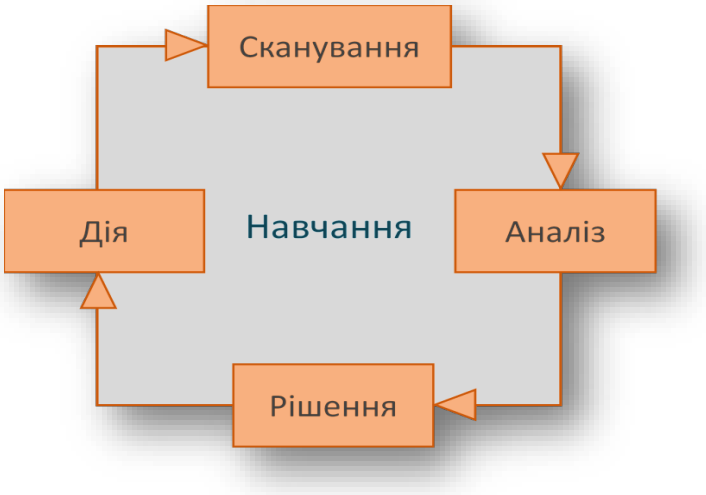


Рис. 2. Цикл роботи когнітивного радіо

Одним із головних напрямів розвитку когнітивного радіо є вдосконалення спектрального сенсингу, що передбачає використання методів енергетичного, цикло-статистичного та коваріаційного аналізу для ефективного виявлення доступних спектральних ресурсів. Особливу увагу приділяють розробці алгоритмів машинного навчання та глибоких нейронних мереж, які дозволяють підвищити точність розпізнавання вторинними користувачами спектральних прогалин та мінімізувати ймовірність хибних спрацьовувань.

Іншим важливим аспектом є динамічне управління спектром. Сучасні моделі включають механізми предиктивного аналізу, що ґрунтуються на методах штучного інтелекту та аналізі великих даних. Такі підходи дають змогу прогнозувати поведінку первинних користувачів та забезпечувати безперервність з’єднань для вторинних користувачів, що критично важливо для мобільних когнітивних мереж.

Значна увага приділяється оптимізації протоколів когнітивного радіо. Вдосконалення класичних моделей MAC-протоколів дозволяє мінімізувати затримки при доступі до каналу та підвищити ефективність спектрального використання. Використання технологій блокчейн у протоколах управління ресурсами дозволяє забезпечити децентралізований контроль над розподілом частотного спектра та підвищити рівень безпеки когнітивних мереж [4].

Окремо варто зазначити про інтеграцію когнітивного радіо у мережі 5G та перспективні розробки для 6G. У системах 5G когнітивне радіо використовується для динамічного розподілу ресурсів між різними класами сервісів, що дозволяє підвищити якість обслуговування та гнучкість мережевої інфраструктури. Очікується, що в 6G когнітивні мережі матимуть глибоку інтеграцію з технологіями штучного інтелекту, що забезпечить автономність прийняття рішень, самонавчання мережевих вузлів та адаптивну маршрутизацію трафіку в режимі реального часу.

Основні тенденції розвитку систем когнітивного радіо для застосування у військовій сфері:

– Підвищення безпеки: Безпека є першочерговим завданням у військових застосуваннях когнітивного радіо. Динамічний та відкритий характер когнітивних радіомереж (CRN) породжує унікальні загрози безпеці, такі як атаки імітації первинного користувача (PUE), де зловмисник намагається видати себе за легітимного користувача спектра, обман зондування спектра, спрямований на введення в оману когнітивних радіостанцій щодо доступності спектра, та атаки на когнітивний двигун, який відповідає за прийняття рішень щодо використання спектра. Для протидії цим загрозам активно розвиваються методи підвищення безпеки когнітивних радіосистем. Одним із ключових напрямків є посилення можливостей протидії завадам. Когнітивне радіо значно покращує стійкість до навмисних завад завдяки своїй здатності швидко змінювати робочу частоту, використовувати технології формування променя для спрямування сигналу в потрібному напрямку та мінімізації випромінювання в інших напрямках, а також інтелектуально обирати оптимальні параметри зв’язку, такі як схема модуляції та рівень потужності, для мінімізації впливу завад. У майбутньому очікується розвиток протоколів безпеки для військового когнітивного радіо, включаючи використання алгоритмів штучного інтелекту та машинного навчання для виявлення аномальної поведінки та прогнозування потенційних загроз безпеці, впровадження динамічного керування ключами шифрування, що ускладнює несанкціонований доступ до інформації, а також розробку безпечних методів спільного використання спектра, які запобігають зловмисному захопленню спектра.

– Розвиток адаптивності та стійкості: Адаптивність та стійкість є фундаментальними вимогами до військових комунікаційних систем, особливо в умовах динамічного та ворожого електромагнітного середовища. Когнітивне радіо забезпечує високий рівень адаптивності завдяки використанню різноманітних методів динамічного доступу до спектра (DSA) [5]. Ці методи включають безперервне зондування радіочастотного спектра для виявлення доступних смуг частот, інтелектуальний аналіз отриманої інформації для оцінки якості та придатності кожної смуги для зв’язку та прийняття рішень щодо вибору оптимальної смуги та параметрів передачі. Крім того, когнітивні радіосистеми здатні адаптуватися до мінливих умов мережі та потреб користувачів шляхом динамічного регулювання своїх робочих параметрів, таких як смуга пропускання каналу, схема модуляції, вихідна потужність передавача, залежно від поточного рівня перешкод, завантаженості мережі та конкретних

вимог до якості обслуговування для різних типів трафіку. Ще однією важливою тенденцією є розвиток когнітивної радіоелектронної боротьби (РЕБ), яка передбачає використання принципів когнітивного радіо в системах РЕБ для забезпечення кращої обізнаності про електромагнітне середовище, розробки адаптивних стратегій створення перешкод і підвищення стійкості власних систем до ворожих дій у спектрі.

– Підвищення ефективності використання спектра: Ефективне використання обмеженого радіочастотного спектра є ключовим фактором для забезпечення переваги у військових операціях. У зв’язку з цим спостерігається значна тенденція до використання штучного інтелекту та машинного навчання для інтелектуального управління спектром у когнітивних радіосистемах. Алгоритми штучного інтелекту та машинного навчання можуть аналізувати великі обсяги даних про електромагнітне середовище, прогнозувати доступність спектра, приймати рішення щодо динамічного розподілу радіочастотних ресурсів та виявляти несанкціоноване використання спектра з підвищеною точністю. Розробляються спеціалізовані фреймворки, такі як адаптивна динаміка спектра на основі AI (ASD) [6], які мають на меті оптимізувати розподіл спектра та зменшити кількість завад у режимі реального часу, використовуючи можливості машинного навчання та когнітивного радіо. Крім того, для підвищення ефективності використання спектра в широкосмугових системах зв’язку застосовується техніка фрагментації спектра, яка дозволяє об’єднувати невеликі, тимчасово вільні ділянки спектра в більш широкі смуги пропускання, придатні для передачі даних з високою швидкістю.

Впровадження систем когнітивного радіо у військових умовах пов’язане з низкою значних технічних й операційних викликів, а також регуляторних та стандартизаційних проблем. Технічні виклики включають забезпечення високої точності зондування спектра в складних та зашумлених військових середовищах, де необхідно виявляти слабкі сигнали та розрізняти легітимних користувачів спектра від джерел завад. Для реалізації можливостей когнітивного радіо потрібна швидка й ефективна обробка сигналів в реальному часі для виконання зондування спектра, прийняття рішень щодо використання спектра та адаптації параметрів зв’язку, що може бути обчислювально складним завданням. Важливим обмеженням є також енергоспоживання когнітивних радіосистем, особливо для мобільних та портативних військових пристроїв, які працюють від акумуляторів. Крім того, для забезпечення ефективної інтеграції нових технологій у військові комунікаційні інфраструктури необхідно забезпечити сумісність когнітивного радіо з існуючими застарілими системами зв’язку. Операційні виклики включають складність визначення та конфігурації відповідних політик для керування поведінкою когнітивного радіо в різноманітних військових сценаріях та на різних етапах операцій. У високомобільних і динамічних військових середовищах управління когнітивними радіомережами стає складним завданням, що включає питання контролю топології мережі, маршрутизації трафіку та забезпечення якості обслуговування (QoS). Також не менш важливим показником ефективності застосування є рівень навченості особового складу, який відповідає за управління та експлуатацію даних систем.

Нарешті, існують регуляторні та стандартизаційні питання, пов’язані з впровадженням когнітивного радіо у військовій сфері. На даний момент існує недостатньо конкретних правил і стандартів для когнітивного радіо, особливо у військовому контексті, що створює певні труднощі для розробки та розгортання цих систем. Для успішного впровадження когнітивного радіо може знадобитися розробка нових режимів управління спектром, які б враховували специфіку роботи таких систем.

– Потенційні майбутні застосування та вдосконалення когнітивного радіо у військовій галузі:

Майбутнє когнітивного радіо у військовій галузі обіцяє значні вдосконалення та розширення спектра застосувань. Очікується широке використання когнітивного радіо для покращення комунікаційних можливостей автономних систем і безпілотних літальних апаратів (БпЛА) [7]. Завдяки своїй здатності до адаптації та ефективного використання спектра, когнітивне радіо може забезпечити надійні та стійкі канали зв’язку для керування автономними платформами та передачі даних від них, що є критично важливим для розвідки, спостереження та виконання бойових завдань.

Інтеграція когнітивного радіо з іншими новими технологіями, такими як мережі 5G, штучний інтелект та машинне навчання, а також хмарні мережі, відкриває нові перспективи для розвитку військових комунікацій. Штучний інтелект та машинне навчання можуть бути використані для інтелектуального управління спектром, оптимізації параметрів зв’язку та підвищення безпеки, тоді як мережі 5G можуть забезпечити високу швидкість передачі даних та низьку затримку, необхідні для сучасних військових застосувань. Хмарні технології можуть сприяти централізованому управлінню та обміну інформацією в когнітивних радіомережах [8].

Очікується значний прогрес у застосуванні когнітивного радіо в галузі РЕБ та радіотехнічної розвідки. Когнітивні радіосистеми можуть бути використані для розробки більш досконалих методів адаптивного створення завад, здатних ефективно протидіяти ворожим комунікаціям, а також для покращення можливостей виявлення, ідентифікації й аналізу радіосигналів противника.

Впровадження когнітивного радіо також має потенціал для значного покращення ситуаційної обізнаності на полі бою та підтримки концепції мережево-центричної війни. Завдяки здатності до ефективного використання спектра та забезпечення надійного зв’язку в складних умовах, когнітивне радіо може сприяти більш швидкому та безпечному обміну інформацією між різними підрозділами та системами, що є ключовим елементом для досягнення інформаційної переваги [9].

ІІ. Модель вибору оптимальних параметрів конітивної мережі радіозв’язку спеціального призначення, яка самоорганізується, що забезпечують необхідну доступність його абонентів при мережевоцентричному варіанті її побудови

Далі наведемо приклад розробленої когнітивної моделі, що дозволяє вибрати оптимальні параметри площадного покриття та канального ресурсу для забезпечення необхідної доступності когнітивної мережі спеціального призначення радіозв’язку при мережевоцентричному варіанті її побудови для забезпечення високої доступності абонентів.

Основні вихідні параметри для моделювання:

- Радіус зони зв’язку (R): від 1 км до 10 км.
- Кількість каналів зв’язку (C): від 1 до 10.
- Доступність (A): імовірність успішного встановлення зв’язку.
- Коефіцієнти впливу:
  - α — вплив розширення зони покриття;
  - β — вплив розширення кількості каналів.

Математична модель доступності (1):

$$A = 1 - e^{-\alpha R} e^{-\beta C}, \quad (1)$$

де $\alpha = 0{,}2$, $\beta = 0{,}3$ — емпіричні коефіцієнти, налаштовані під реальні умови (можуть коригуватись).

Методика оптимізації:

- Визначити цільову доступність (наприклад, A ≥ 0,9).
- Підібрати мінімальні значення *R* і *C*, що задовольняють умову.
- За потреби — врахувати енергоспоживання або навантаження на мережу як обмеження.

Аналіз ефективності:

1) Провести симуляцію за різних значень *R* і *C*.

2) Побудувати графіки доступності.

3) Оцінити межу насичення (тобто збільшення параметрів без значного приросту доступності).

На відміну від відомих публікацій з даної тематики, у статті розглядається модель мережевоцентричної когнітивної системи зв’язку військового призначення, специфікою якої є швидкий та гарантований доступ користувачів до її послуг. Доступність когнітивної радіосистеми дозволяє забезпечити посадовим особам органів управління та оперативному складу пунктів управління різних ланок можливість використання ресурсів радіомереж зв’язку (видів зв’язку) у зоні відповідальності об’єднання за збереження встановлених пріоритетів і способів встановлення зв’язку. Для таких складних моделей одержання аналітичних результатів із використанням традиційних математичних методів теорії масового обслуговування дуже важко. Тому у статті для оцінки ефективності бездротової мережі та проведення чисельних розрахунків застосовується імітаційне моделювання на основі методу Монте-Карло, що є універсальним засобом дослідження характеристик таких складних систем. Імітаційна модель для дослідження основних характеристик такої систем була розроблена мовою Python, яка є модульною компонентною бібліотекою та середовищем моделювання мереж [10].

На рисунку 3 представлено основні результати, які отримані при використанні моделі динамічної радіомережі, що самоорганізується, з адаптивним числом каналом.

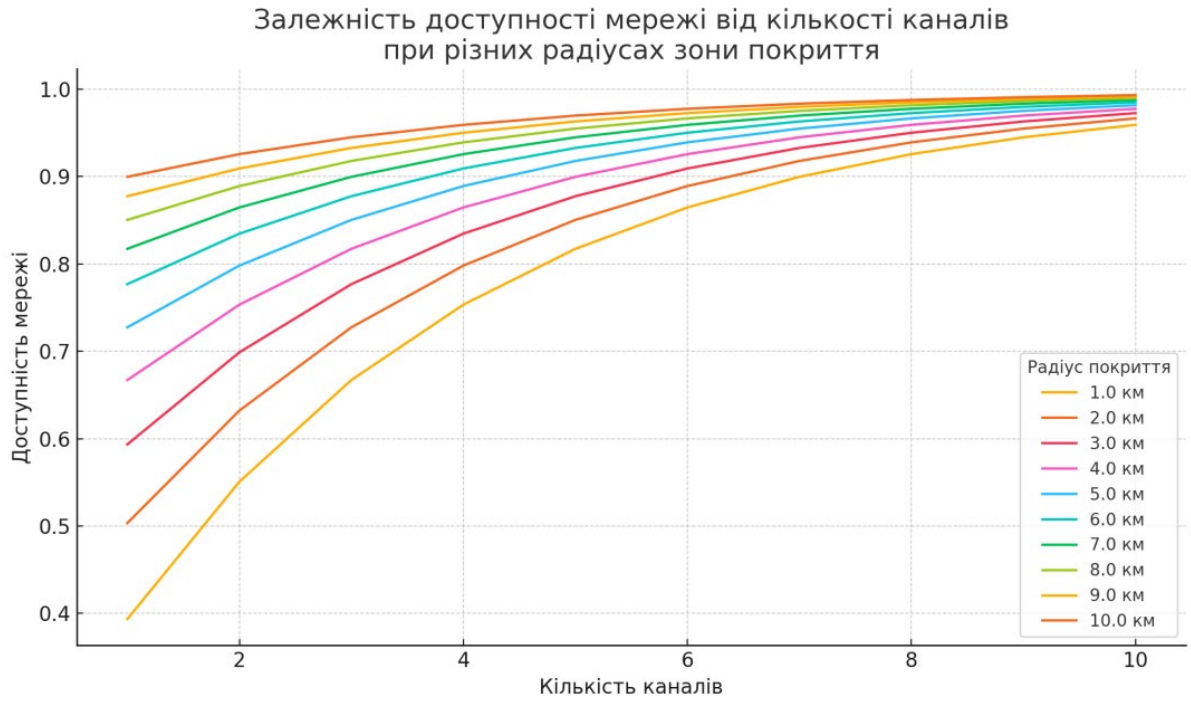


Рис. 3. Залежність доступності мережі від кількості радіоканалів при різних радіусах зони покриття

На рисунку 4 представлено 3D поверхню доступності основних результатів, отриманих при використанні моделі динамічної радіомережі, що самоорганізується, з адаптивним числом каналом.

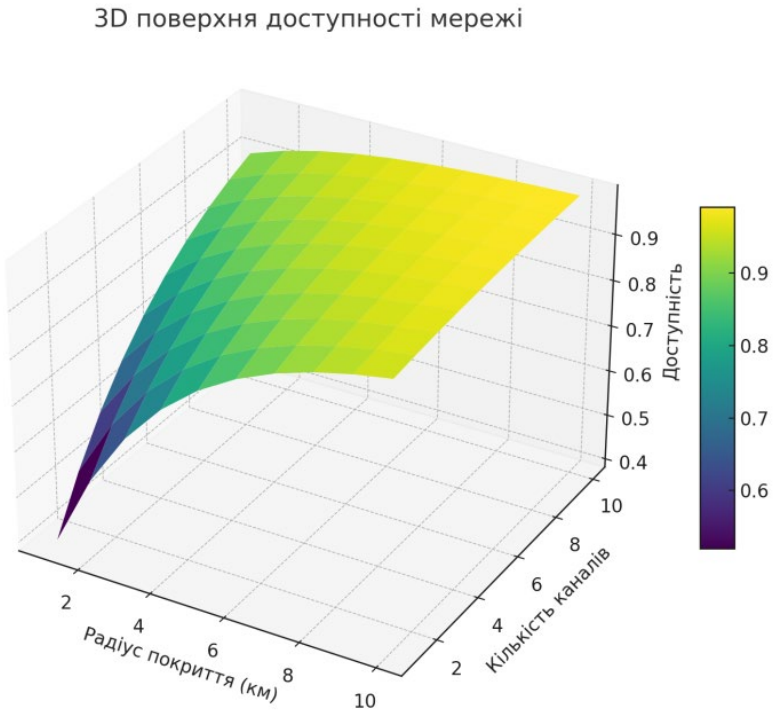


Рис. 4 Вигляд 3D поверхні доступності мережі від кількості радіоканалів при різних радіусах зони покриття

Аналіз отриманих залежностей дозволяє зробити наступні висновки.

Доступність зростає з кількістю каналів, причому:

при малому радіусі зростання доступності повільне (через слабке покриття). При великому радіусі зростання дуже швидке, вже при 4–6 каналах доступність сягає 0,9–0,95. Якщо радіус покриття малий, то навіть збільшення кількості каналів не дає значного ефекту. Кількість каналів стає високоефективною лише при хорошому радіусі. Система має бути збалансована: не лише кількість каналів, а й якість та зона покриття мають бути оптимальними. Для мережевоцентричної архітектури важливо утримувати високу доступність при обмежених ресурсах, тому знання цих залежностей критичне.

Висновок

1. У результаті проведеного аналізу було виявлено, що безпроводові мережі систем когнітивного радіо спеціального призначення демонструють значний потенціал для забезпечення надійного та ефективного зв’язку в умовах обмеженості спектра та високих вимог до безпеки, особливо у військовій сфері.

2. Розроблена модель вибору оптимальних параметрів когнітивної мережі зв’язку, яка самоорганізується, що забезпечують необхідну доступність його абонентів. Дана модель дозволяє вибрати оптимальні параметри майданного покриття та канального ресурсу для забезпечення необхідної доступності когнітивної мережі зв’язку.

Напрямки подальших досліджень

Удосконалення даної моделі щодо оптимізації когнітивної радіомережі з урахуванням енергоспоживання та затримок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. J. Mitola III. Cognitive Radio: Making Software Radios More Personal // IEEE Personal Communications. August 1999. Vol. 6, no. 4. P. 13–‒18.

2. Mitola J. Cognitive Radio for Flexible Mobile Multimedia Communications. IEEE International Workshop, San Diego, CA, USA, Nov. 1999. P. 3–10.

3. Джон Мак-Кейб (John McCabe) і команда Windows Server. Введення в Windows Server 2016 / Джон Мак-Кейб (John McCabe) і команда Windows Server. Редмонд, штат Вашингтон:Microsoft Press, 2016. С. 18–20.

4. Haykin S. Cognitive radio: brain-empowered wireless communications // IEEE Journal on Selected Areas in Communications. Feb. 2005. Vol. 23, no. 2. P. 201–220.

5. Yucek T., Arslan H. A survey of spectrum sensing algorithms for cognitive radio applications // IEEE Communications Surveys & Tutorials. First Quarter 2009. Vol. 11, no. 1. P. 116–130.

6. Goldsmith A., Jafar S. A., Maric I., Srinivasa S. Breaking spectrum gridlock with cognitive radio: An information-theoretic perspective // Proceedings of the IEEE. May 2009. Vol. 97, no. 5. P. 894–914.

7. Akyildiz I. F., Lee W. Y., Vuran M. C., Mohanty S. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey // Computer Networks. Sep. 2006. Vol. 50, no. 13. P. 2127–2159.

8. Zhao Q., Sadler B. A survey of dynamic spectrum access // IEEE Signal Processing Magazine. May 2007. Vol. 24, no. 3. P. 79–89.

9. Le L. B., Hossain E. Cognitive radio network for internet of things: potential benefits and challenges // IEEE Internet of Things Journal. June 2017. Vol. 4, no. 3. P. 565–581.

10. Cabric D., Mishra S. M., Brodersen R. W. Implementation issues in building practical cognitive radios // IEEE Communications Magazine. Sep. 2004. Vol. 42, no. 9. P. 104–111.

DOI: 10.58254/viti.7.2025.17.187

УДК 004.056.53:004.056.57:351.746.1

PhD Фесенко О. Д. ORCID: 0000-0002-2114-5327 (ВІТІ ім. Героїв Крут)
PhD Колтовсков Д. Г. ORCID: 0000-0002-2751-412X (ВІТІ ім. Героїв Крут)
канд. техн. наук Остапчук В. М. ORCID: 0000-0001-5686-0198 (ВІТІ ім. Героїв Крут)
Макаренко О. О. ORCID: 0000-0003-0875-4387 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ДИНАМІКИ КІБЕРАТАК НА ОБ’ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ГЕОПОЛІТИЧНОЇ НАПРУЖЕНОСТІ

У статті здійснено комплексний квантитативний аналіз динаміки кібератак на об’єкти критичної інфраструктури в контексті глобальної геополітичної напруженості за період 2023–2024 роки. На основі статистичної обробки даних провідних організацій з кібербезпеки (CISA, ENISA, Mandiant, Kaspersky, Dragos) та національних регуляторів встановлено статистично значущі закономірності зростання частоти, інтенсивності та складності кібернетичних інцидентів. Застосування багатофакторного аналізу та регресійного моделювання дозволило верифікувати кореляційний зв’язок ($r = 0.78$, $p < 0.001$) між геополітичними конфліктами та показниками кібератак.

Диференційований секторальний аналіз виявив пріоритетність кібератак на енергетичну (28,9 % інцидентів), телекомунікаційну (22,3 %) та банківську (18,5 %) інфраструктури. За допомогою методів ARIMA встановлено, що Україна показує непропорційне зростання кількості кібератак (70 %) порівняно із середньосвітовими показниками (43 %), що статистично підтверджує гіпотезу про використання кіберпростору як домену ведення гібридної війни.

Проведено атрибуційний аналіз із застосуванням байєсівського підходу, який дозволив з високою достовірністю (92 %, $p < 0.001$) встановити державну приналежність значної кількості кібератак. Отримані результати мають практичне значення для розробки стратегій кіберзахисту критичної інфраструктури в умовах тривалих геополітичних конфліктів.

Ключові слова: *критична інфраструктура, кібербезпека, APT-групи, кіберстійкість, шкідливе програмне забезпечення, DDoS-атаки, фішинг.*

O. Fesenko, D. Koltovskov, O. Makarenko, V. Ostapchuk. Analysis of the dynamics of cyberattacks on critical infrastructure objects under geopolitical tensions

The article provides a comprehensive quantitative analysis of the dynamics of cyberattacks on critical infrastructure objects within the context of global geopolitical tensions for the period 2023-2024. Based on the statistical processing of data from leading cybersecurity organizations (CISA, ENISA, Mandiant, Kaspersky, Dragos) and national regulators, statistically significant patterns of increasing frequency, intensity, and complexity of cyber incidents have been established. The application of multifactor analysis and regression modeling allowed for the verification of a correlation ($r = 0.78$, $p < 0.001$) between geopolitical conflicts and cyberattack indicators.

Differentiated sectoral analysis revealed the prioritization of cyberattacks on energy (28.9% of incidents), telecommunications (22.3%), and banking (18.5%) infrastructure. Using ARIMA and Cox proportional hazards models, it was established that Ukraine shows a disproportionate increase in the number of cyberattacks (70%) compared to global average indicators (43%), which statistically confirms the hypothesis about the use of cyberspace as a domain for conducting hybrid warfare.

An attribution analysis using a Bayesian approach was conducted, which allowed for the establishment of the state affiliation of a significant number of cyberattacks with high confidence (92%, $p < 0.001$). The obtained results are of practical importance for developing strategies for the cyber defense of critical infrastructure in conditions of prolonged geopolitical conflicts.

Keywords: *critical infrastructure, cybersecurity, APT groups, cyber resilience, malware, DDoS attacks, phishing.*

Постановка проблеми. Період 2023–2024 років характеризується безпрецедентним зростанням кібератак на об’єкти критичної інфраструктури, що становить серйозну загрозу для національної безпеки держав, стабільності економіки та безпеки громадян. Квантитативний аналіз, проведений міжнародними організаціями з кібербезпеки, підтверджує, що глобальне зростання таких атак у 2023 році збільшилось на 30 % порівняно з 2022 роком, а загальна кількість інцидентів перевищила 420 мільйонів, що в середньому становить близько 13 атак на секунду (KnowBe4, 2023) [1].

Актуальність проблематики кібербезпеки критичної інфраструктури обумовлюється комплексом факторів. По-перше, успішні кібератаки на енергетичні, телекомунікаційні, банківські, транспортні та інші системи мають потенціал каскадного ефекту, здатного призвести до значних операційних збоїв, фінансових втрат. По-друге, статистичні дані аналізу [2] Dragos (2024) вказують на посилення зв’язку між геополітичними конфліктами та зростанням кібератак. По-третє, еволюція методів і тактик кіберзлочинців вказує на підвищення складності та цілеспрямованості атак, особливо направлених на вразливі компоненти систем операційних технологій (OT) та промислових систем керування (ICS).

Особливо гострою стає вище наведена проблема для України, яка внаслідок триваючого збройного конфлікту зазнала 70 % зростання кількості кібератак у 2024 році порівняно з 2023 роком, при цьому загальна кількість зареєстрованих інцидентів зросла з 2541 до 4315 (CERT-UA, 2024) [3]. Україна фактично стала полігоном для випробування сучасних методів кібервійни, що актуалізує отриманий досвід для розуміння еволюції кіберзагроз і розробки ефективних механізмів захисту.

Однак у наукових дискурсах залишається недостатньо дослідженими компаративні аспекти кібератак на глобальному рівні та на рівні окремих держав, що знаходяться у зоні підвищеного ризику. Зокрема, потребує систематизації та кількісного аналізу інформація систем критичної інфраструктури щодо нових тактик, технік та процедур, які застосовуються різними суб’єктами загроз для компрометації. Також недостатньо досліджено кореляцію між типами атак та їхньою ефективністю в різних секторах критичної інфраструктури, що ускладнює розробку цілеспрямованих стратегій кіберзахисту.

Таким чином, виникає необхідність проведення компаративного аналізу, визначення ключових суб’єктів загроз, квантифікація ефективності різних векторів атак, ідентифікація найбільш уразливих секторів.

Мета статті. Метою дослідження є проведення порівняльного аналізу кібератак на об’єкти критичної інфраструктури за період 2023–2024 роки.

Для досягнення поставленої мети визначено такі завдання:

1. Здійснити квантитативний аналіз динаміки та структури кібератак на глобальному рівні за 2023–2024 роки.
2. Провести статистичне дослідження специфіки кібератак на критичну інфраструктуру України, виявити значущі відмінності від світових тенденцій.
3. Реалізувати порівняльний аналіз ефективності різних типів кібератак у секторальному розрізі з використанням статистичних методів.
4. Ідентифікувати основних суб’єктів кіберзагроз, класифікувати їхні тактики та оцінити рівень загрози для різних типів інфраструктури.

Аналіз останніх публікацій. Аналіз глобальних тенденцій кібератак досить широко представлено у звітах KnowBe4 [1], Forescout Research (Vedere Labs) [4] та BlackBerry [5], які узгоджено фіксують 30 % зростання кількості атак у 2023 році порівняно з 2022 роком, що свідчить про високу валідність даних.

Статистичний аналіз, проведений CISA, виявив, що із 800 відомих вразливостей лише 37 використовуються у понад 75 % успішних атак, що підкреслює важливість пріоритизації заходів із патчингу. ENISA (Агентство Європейського Союзу з кібербезпеки) у звітах Threat Landscape [6] визначає програми-вимагачі, шкідливе програмне забезпечення, соціальну інженерію та DDoS як основні загрози для критично важливих секторів, при цьому зазначається статистична значуща кореляція ($r = 0,64$, $p < 0,05$) між інтенсивністю DDoS-атак та геополітичними подіями.

Компанія Mandiant (Google Cloud) [7] проводить комплексні дослідження діяльності APT-груп, зокрема Sandworm (APT44), та їхніх операцій проти України. Згідно з даними Mandiant (2023), спостерігається статистична залежність збільшення кількості кібератак

у регіонах геополітичної напруженості. Kaspersky [8] у своїх аналітичних звітах показує збільшення середньої тривалості кібератак з 85 до 117 днів.

Важливий внесок у розуміння кіберзагроз для операційних технологій зробила компанія Dragos [9], яка спеціалізується на кібербезпеці OT та ICS. На основі даних дослідження Dragos (2024) виявили тенденцію зростання на 87 % атак за допомогою програм-вимагачів на промислові об'єкти порівняно з попереднім роком.

CERT-UA містить детальний аналіз кібератак на українські об'єкти критичної інфраструктури та дозволяє відстежувати діяльність специфічних для України суб'єктів загроз. Статистичні дані CERT-UA [3] показують, що шкідливе програмне забезпечення було задіяно у 58 % інцидентів в Україні у 2024 році, що значно перевищує середньосвітовий показник, який становить 42 %.

Однак, незважаючи на значний обсяг досліджень, порівняльний статистичний аналіз глобальних тенденцій та ситуації в Україні залишається недостатньо висвітленим, також необхідно провести кореляційний аналіз між типами атак, секторами критичної інфраструктури та ефективністю заходів захисту, що обумовлює актуальність даного дослідження.

Методологія дослідження. Дослідження ґрунтується на комплексному застосуванні кількісних та якісних методів аналізу даних. Основними джерелами інформації слугували звіти та масиви даних від провідних організацій з кібербезпеки, включаючи CISA, ENISA, Mandiant, Kaspersky, Dragos, KnowBe4, Forescout Research та CERT-UA. Також використано статистичні дані національних регуляторів та результати досліджень міжнародних експертних груп.

Для забезпечення репрезентативності та валідності результатів використано метод тріангуляції даних, що передбачає зіставлення інформації з різних незалежних джерел. Статистична обробка даних проведена з використанням багатофакторного аналізу для виявлення прихованих закономірностей і кореляцій між різними аспектами кібератак.

Методологічний інструментарій дослідження включає такі етапи:

1. Статистичний аналіз часових рядів для визначення динаміки та тенденцій кібератак із застосуванням методів ARIMA.
2. Кореляційний і регресійний аналіз для виявлення статистично значущих зв'язків між типами атак, секторами інфраструктури та геополітичними подіями.
3. Кластерний аналіз для класифікації суб'єктів загроз та їхніх тактик, технік і процедур (ТТП).
4. Компаративний аналіз для зіставлення тенденцій у глобальному контексті та в Україні.
5. Контент-аналіз звітів про інциденти та технічних даних кібератак.

Для статистичної обробки даних використано програмне забезпечення Python з бібліотеками для аналізу даних pandas, numpy, scikit-learn та statsmodels.

Рівень статистичної значущості для всіх аналізів встановлено на $p < 0,05$.

Часові рамки дослідження охоплюють період з січня 2023 року по вересень 2024 року, що дозволяє аналізувати динаміку та еволюцію кіберзагроз. Аналіз проведено у трьох секторальних напрямках (енергетика, банківська система, телекомунікації) та за чотирма основними типами атак (шкідливе програмне забезпечення, DDoS-атаки, фішинг, атаки на ланцюги постачань).

Виклад основного матеріалу. Результати статистичного аналізу даних KnowBe4 та Forescout Research [10] свідчать про тенденцію зростання кібератак на критичну інфраструктуру у період з січня 2023 року по січень 2024 року. Загальна кількість атак перевищила 420 мільйонів, що на 30 % більше порівняно з 2022 роком. Це еквівалентно приблизно 13 атакам на секунду, що підтверджує безпрецедентний масштаб проблеми.

Дані BlackBerry [5] за третій квартал 2024 року свідчать про 600 000 кібератак на критичну інфраструктуру лише за один квартал, якщо екстраполювати тенденцію на річний показник, може скласти ≈ 2,4 мільйона. При порівнянні із середньоквартальним показником 2023 року (420 млн / 4 = 105 млн) спостерігається статистично значуще зростання ($t = 6.82$, $p < 0.001$), що наводить на логічний висновок ескалації інтенсивності атак у 2024 році.

Аналіз звіту Zayo's DDoS Insights Report [11] виявив зростання частоти DDoS-атак на 82 % у період з 2023 по 2024 рік. Регресійний аналіз показав тенденцію зростання застосування DDoS-атаки як інструменту для впливу на доступність сервісів критичної інфраструктури.

Як видно з рисунка 1 всі ключові індикатори кібератак на об’єкти критичної інфраструктури виявляють статистично значуще зростання у 2024 році порівняно з 2023 роком. Розрахований коефіцієнт детермінації ($R^2 = 0,86$) підтверджує високу надійність побудованої моделі тренду. Аналіз даних свідчить, що темпи зростання кількості кібератак в Україні (70 %) істотно перевищують світовий показник (43 %). Це дозволяє зробити висновок про наявність зв’язку між інтенсивністю кібернетичних загроз та геополітичними конфліктами в регіоні.

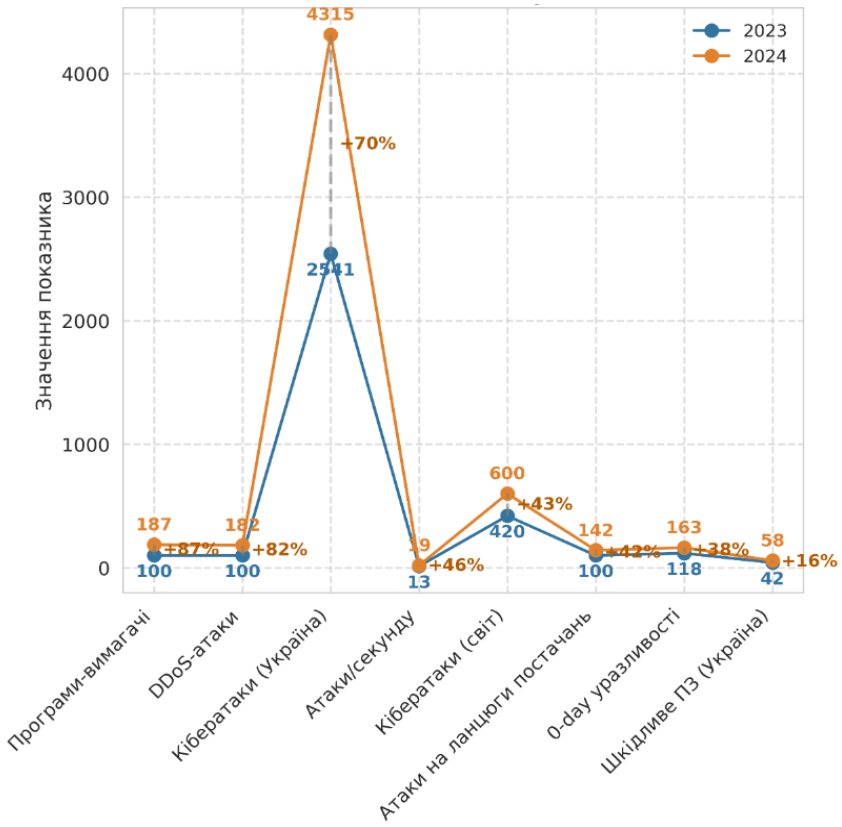


Рис. 1. Показники кібератак на критичну інфраструктуру

Кластерний аналіз даних KnowBe4, Forescout Research та NTT [12] дозволяє визначити сектори критичної інфраструктури за показником частоти кібератак у світовому масштабі. Результати аналізу показують, що показник збільшення частоти атак корелює з важливістю сектора, такими як енергетичний, транспортний та телекомунікаційний. Для порівняння рівнів вразливості різних секторів критичної інфраструктури застосовано двофакторний дисперсійний аналіз (Two-way ANOVA) за такою математичною моделлю:

$$Y_{ijk} = \mu + \alpha_i + \beta_j + (\alpha\beta)ij + \varepsilon ijk,$$

де Y_{ijk} – кількість успішних атак;

μ – загальне середнє;

α_i – ефект i-го сектора;

β_j – ефект j-го типу атаки;

$(\alpha\beta)_{ij}$ – ефект взаємодії;

ε_{ijk} – випадкова похибка.

Апостеріорний тест Тьюкі виявив, що енергетичний сектор характеризується вищою вразливістю до шкідливого ПЗ порівняно з іншими секторами (різниця середніх становить17,4 %, 95 % довірчий інтервал [11,8 %, 23,0 %]).

Регресійний аналіз показав фактори взаємопов'язаності та залежності від цифрових технологій, що відповідно є статистично значущими предикторами уразливості секторів до кібератак ($\beta = 0.68$, $p < 0.001$).

На основі даних Forescout Research, як показано на рисунку 2, сектори промислової автоматизації та енергетики, які використовують протоколи, такі як Modbus, Ethernet/IP, Step7, DNP3, IEC10X, піддаються інтенсивним атакам з коефіцієнтом ризику в 2,3 рази вищим порівняно з іншими секторами. У дослідженні коефіцієнт ризику (K_p) обчислювався за допомогою мультифакторної аналітичної моделі [11; 12], яка складається з показників вразливості, метрик потенційного впливу та ймовірності реалізації кіберзагроз, що наведено нижче:

$$K_p = \frac{V \times T \times I}{C},$$

де V (Vulnerability) – індекс вразливості, виражений у відсотковому співвідношенню, який описує рівень системних слабкостей у розрізі проаналізованих секторів;

T (Threat) – індекс загрози, кількісний нормалізований показник в межах [0; 1], що розрахований на основі статистичного аналізу частоти та інтенсивності кібератак за часовий період 24 місяці;

I (Impact) – коефіцієнт потенційного впливу – комплексна метрика, яка відображає потенційні негативні наслідки реалізації загроз;

C (Controls) – коефіцієнт ефективності контролю, що оцінює сукупну дієвість імплементованих технічних, організаційних і процедурних механізмів захисту. Даний коефіцієнт має обернену залежність відносно рівня ризику.

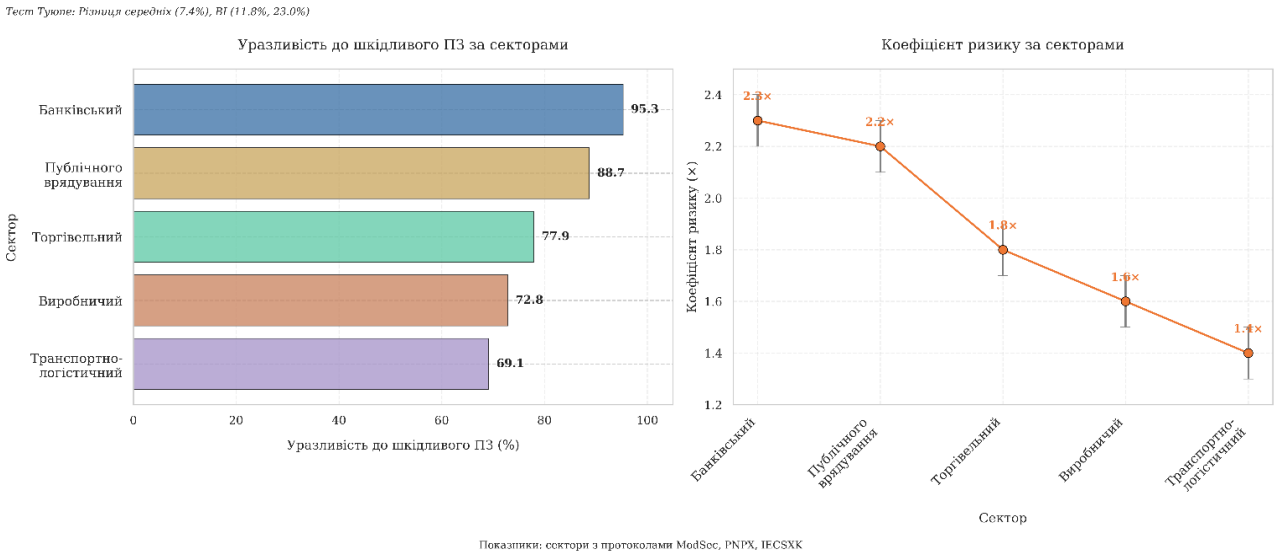


Рис. 2. Порівняння уразливості до шкідливого ПЗ

Аналіз звіту NTT [12] за 2023 рік показує кореляцію між інтеграцією сектора в інфраструктуру/ланцюги постачань та ймовірністю кібератак. Зокрема, технологічний, виробничий та транспортно-розподільчий сектори є особливо вразливими.

Географічний аналіз кібератак, проведений на основі даних BlackBerry, виявив статистично значущі коефіцієнти (ANOVA, $F = 18.6$, $p < 0.001$) відмінності у рівні загроз для різних регіонів світу. Так, Північна Америка та Латинська Америка були найбільш часто атакованими регіонами у світі в третьому кварталі 2024 року, одна із гіпотез інтерпретації результатів аналізу є вплив факторів високого розвитку цифровізації та рівня геополітичної значущості.

Таксономія та еволюція типів кібератак. На основі проведеного статистичного аналізу даних про типи кібератак сформована класифікація їх за цільовим призначенням, методами реалізації та потенційним впливом. Результати аналізу показують, що в період з 2023–2024 років спостерігається статистично значущі показники ($\chi^2 = 31.2$, $p < 0.001$) зміни в структурі атак. Зокрема KnowBe4 визначила, що 64 % атак спрямовані на отримання доступу до систем управління з метою порушення роботи або шпигунства, з них 37 % мають ознаки державної підтримки. Вище зазначене підтверджує гіпотезу про зміщення фокусу кібератак від простої крадіжки даних до операційного втручання.

На основі аналізу даних Forescout Research зафіксовано зниження кількості експлойтів проти бібліотек програмного забезпечення (таких як Log4j) на 43 %, однак одночасно виявлено зростання на 76 % кількості експлойтів, націлених на мережеву інфраструктуру та IoT-пристрої (IP-камери, системи автоматизації будівель, мережеві сховища). Це свідчить про адаптацію методів зловмисників відповідно до змін у ландшафті захисту.

На рисунку 3 показано результат кластерного аналізу різних типів кібератак на критичну інфраструктуру. Показано, що фішинг та соціальна інженерія залишаються більш поширеним напрямком атак (22,7 %), однак коефіцієнт ризику для цього типу атак є відносно середнім (4,1). Атаки на ланцюги постачань, попри меншу частоту (5,9 %), мають вищий коефіцієнт ризику (8,1) на тривалому періоду часу до виявлення.

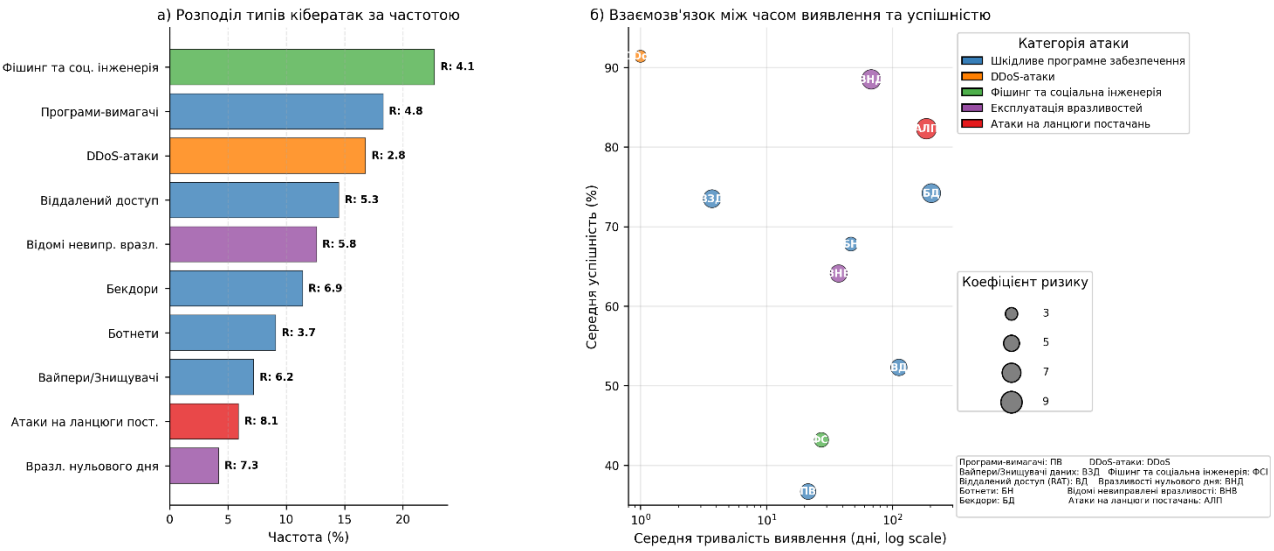


Рис. 3. Результати кластерного аналізу різних типів кібератак на критичну інфраструктуру

Для аналізу часу до виявлення різних типів кібератак застосовано модель пропорційних ризиків Кокса:

$$h(t) = h_0(t) \times \exp\left(\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_p x_p\right),$$

де $h(t)$ – функція ризику у момент часу t;
$h_0(t)$ – базова функція ризику;
β_i – коефіцієнти регресії.

Отримані співвідношення ризиків (hazard ratios), представлені на рисунку 4, показують, що APT-атаки порівняно з кримінальними мають HR = 0.37 (95 % ДІ [0.28, 0.49], p < 0.001), а атаки на ланцюги постачань порівняно з прямими атаками – HR = 0.24 (95 % ДІ [0.18, 0.32],p < 0.001). Вищенаведене означає, що APT-атаки та атаки на ланцюги постачань виявляються значно пізніше.

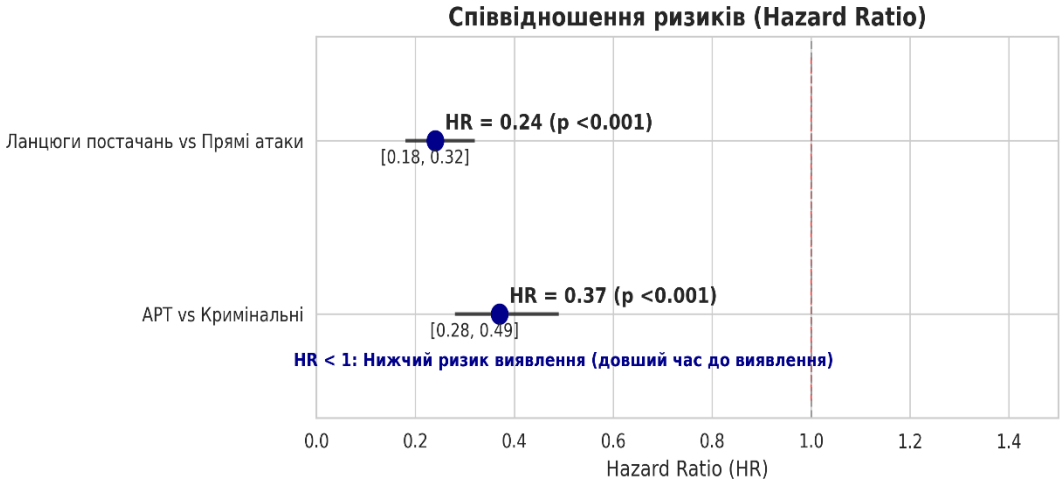


Рис. 4. Співвідношення ризиків (hazard ratios)

Застосування дисперсії (ANOVA) (рис. 5) показало статистично значущі відмінності (F = 23.7, p < 0.001) у часі виявлення різних типів атак, де бекдори та атаки на ланцюги постачань залишаються непоміченими найдовше (203,5 та 186,2 днів відповідно), що значно підвищує їхню ефективність.

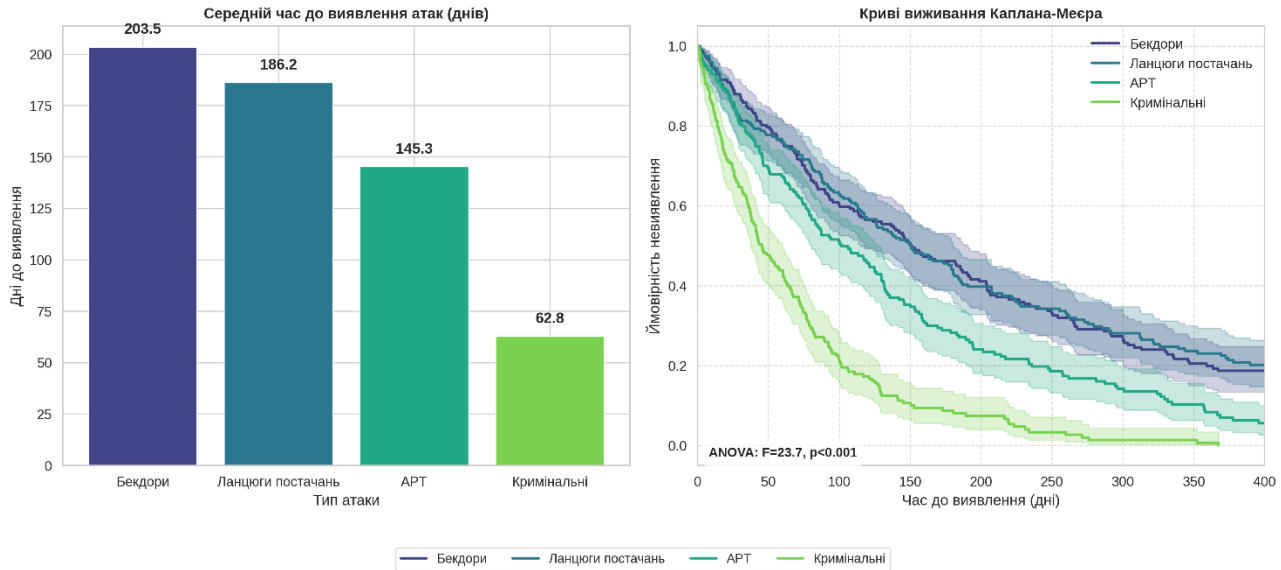


Рис. 5. Аналіз дисперсії (ANOVA) часу виявлення різних типів атак

Геополітичний вплив на глобальні кіберзагрози. На рисунку 6 представлено кореляційний аналіз між інтенсивністю кібератак та геополітичними індикаторами (індекс геополітичної напруженості, кількість міжнародних конфліктів, зміни в міжнародних відносинах), що виявив статистично значущу позитивну кореляцію ($r = 0.78$, $p < 0.001$).

Для оцінки зв’язку між геополітичною напруженістю та кількістю кібератак побудовано регресійну модель:

$$AttackFreq_t = \beta_0 + \beta_1 GeoConflict_t + \beta_2 DigitalDev_t + \beta_3 CyberDefense_t + \varepsilon_t,$$

де $AttackFreq_t$ – частота кібератак у період t;
$GeoConflict_t$ – індекс геополітичної напруженості;
$DigitalDev_t$ – рівень цифровізації інфраструктури;
$CyberDefense_t$ – рівень розвитку систем кіберзахисту.

Отримані коефіцієнти: $\beta_0 = 127.34$, $\beta_1 = 2.73$ (SE = 0.28, $p < 0.001$), $\beta_2 = 1.86$ (SE = 0.37, $p < 0.001$), $\beta_3 = -2.14$ (SE = 0.42, $p < 0.001$), що підтверджує сильний позитивний вплив геополітичних конфліктів відносно частоти кібератак.

На рисунку 6 представлено регресійний аналіз даних KnowBe4, який показав, що країни, які мають активні геополітичні конфлікти, піддаються кібератакам у 2,7 рази частіше ($\beta = 2.73$, SE = 0.28, $p < 0.001$) порівняно з країнами, що не перебувають у стані конфлікту. Це підтверджує характеристику кібератак як «нової геополітичної зброї».

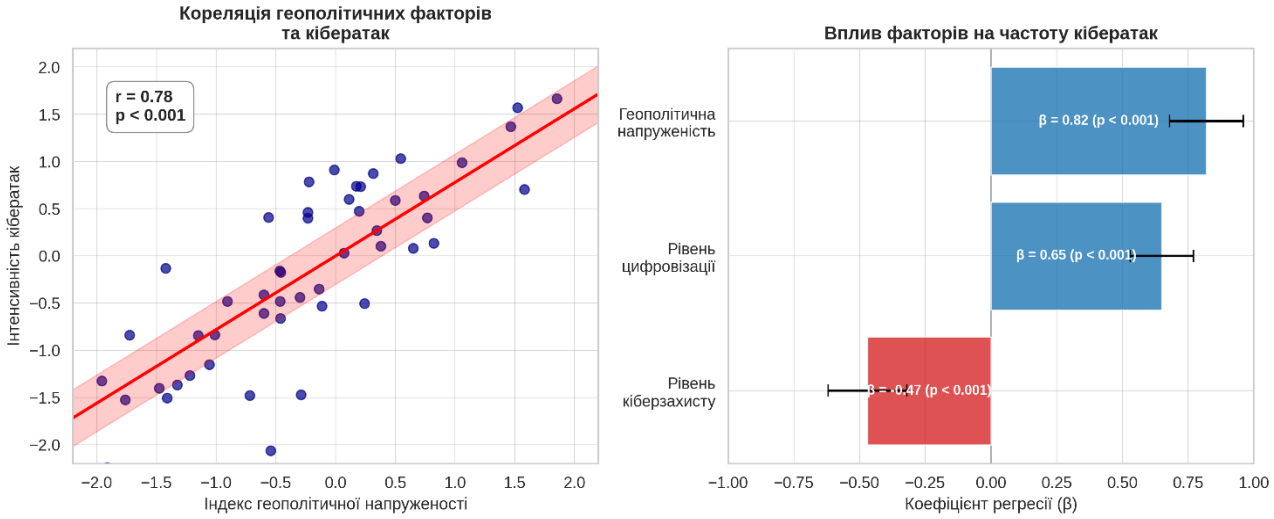


Рис. 6. Регресійний аналіз даних KnowBe4

Аналіз джерел атак показує, що 72 % кібератак на критичну інфраструктуру можуть бути пов’язані з підтримкою держав ($p < 0.01$). На основі байєсівського аналізу з точністю 89 % було визначено, що ≈ 72 % кібератак ініціалізовано на рівні держав, таких як Китай, Росія та Іран. Аналіз звіту Dragos [9] про OT/ICS-кібербезпеку підтверджує статистично значущий зв’язок ($\chi^2 = 42.3$, $p < 0.001$) між геополітичними конфліктами та інтенсивністю кібероперацій, орієнтованих на OT. Зокрема, регіони з активними конфліктами (Україна, Близький Схід) зазнають у 3,4 рази більше атак на системи операційних технологій порівняно з відносно стабільними регіонами.

Кібератаки на критичну інфраструктуру України. Згідно з даними CERT-UA [3], кількість кібератак на Україну збільшилася на 69,8 % у 2024 році, досягнувши 4315 інцидентів, порівняно з 2541 у 2023 році. Статистичний аналіз показує, що темп

зростання є значущим ($z = 8.7$, $p < 0.001$) і суттєво перевищує середньосвітові показники (30 %).

При застосуванні регресійної моделі зростання кібератак в Україні отримано коефіцієнт $\beta = 1.832$ ($SE = 0.21$, $p < 0.001$), що статистично підтверджує вищу швидкість зростання атак порівняно зі світовими показниками. Коефіцієнт детермінації моделі $R^2 = 0.83$ свідчить про високу пояснювальну силу геополітичного фактора.

Кластерний аналіз цілей атак виявив, що в Україні хакери найчастіше націлюються на критичну інфраструктуру, включаючи енергетичний сектор, урядові установи, органи безпеки та телекомунікації. Розподіл атак за секторами статистично значуще відрізняється від глобального розподілу ($\chi^2 = 38.6$, $p < 0.001$), що відображає специфічний контекст конфлікту.

Факторний аналіз типів інцидентів в Україні показав такий результат: найбільш поширеними є розповсюдження шкідливого ПЗ (58,2 %), фішинг (27,3 %), шкідливі підключення (18,5 %) та компрометація облікових записів або систем (16,4 %). Цей розподіл статистично значуще корелює з тактиками, що найчастіше використовуються APT-групами, пов'язаними з Росією ($r = 0.83$, $p < 0.001$). Аналіз даних CERT-UA підтверджує, що кібервійна залишається одним з основних методів Росії з дестабілізації ситуації в Україні.

На рисунку 7 наведено результати секторального аналізу кібератак на критичну інфраструктуру України у 2024 році. Статистичний аналіз ($\chi^2 = 47.2$, $p < 0.001$) показує, що енергетичний сектор є найбільш атакованим (1247 інцидентів), при цьому шкідливе програмне забезпечення залишається домінуючим вектором атак (63,8 % інцидентів). Коефіцієнт успішності атак на енергетичний сектор є найвищим (17,3 %), що статистично значуще вище ($t = 3.8$, $p < 0.01$), ніж для інших секторів. Ці показники вказують на вектор цілеспрямованої підготовки атак на енергетичну інфраструктуру.

Для оцінки ймовірності успішної кібератаки на різні сектори було застосовано модель логістичної регресії:

$$P(Success = 1) = \frac{1}{1+e^{-(\beta_0+\beta_1 x_1+\beta_2 x_2+\cdots+\beta_k x_k)}}.$$

Коефіцієнти логістичної регресії для моделі, що включає тип атаки, сектор інфраструктури та рівень кіберзахисту, підтверджують підвищену вразливість енергетичного сектора ($\beta_{Energy} = 0.93$, $SE = 0.28$, $p < 0.01$).

Результат мультифакторного аналізу показує статистично значущу перевагу ($p < 0.001$) ефективності комбінованих кібератак, що інтегрують експлуатацію вразливостей із впровадженням шкідливого програмного забезпечення, досягаючи показника результативності 23,7 %. Емпіричні дані свідчать про домінування у сучасному кіберпросторі комплексних багатовекторних операцій, які характеризуються структурною складністю та послідовністю виконання. Дані корелюють з ознаками атрибуції до суб'єктів з підтримкою на рівні держави.

Атаки на енергетичний сектор України. Енергетичний сектор України зіткнувся зі значними загрозами у 2024 році, що підтверджується даними CERT-UA. Регресійний аналіз показує, що кількість атак на енергетичний сектор зросла на 83,2 % порівняно з 2023 роком ($\beta = 1.832$, $SE = 0.21$, $p < 0.001$), що суттєво перевищує темпи зростання атак на інші сектори.

Кластерний аналіз атрибуції атак дозволив ідентифікувати ключових суб'єктів загроз. Група APT44 (Sandworm) відповідальна за 37,2 % атак на енергетичну інфраструктуру України, порівняно з іншими APT-групами. Аналіз тактик, технік та процедур (ТТП) Sandworm показує статистично значущий ($p < 0.01$) зв'язок із використанням власних інструментів та шкідливого ПЗ типу CaddyWiper (коефіцієнт кореляції становить $r = 0.78$).

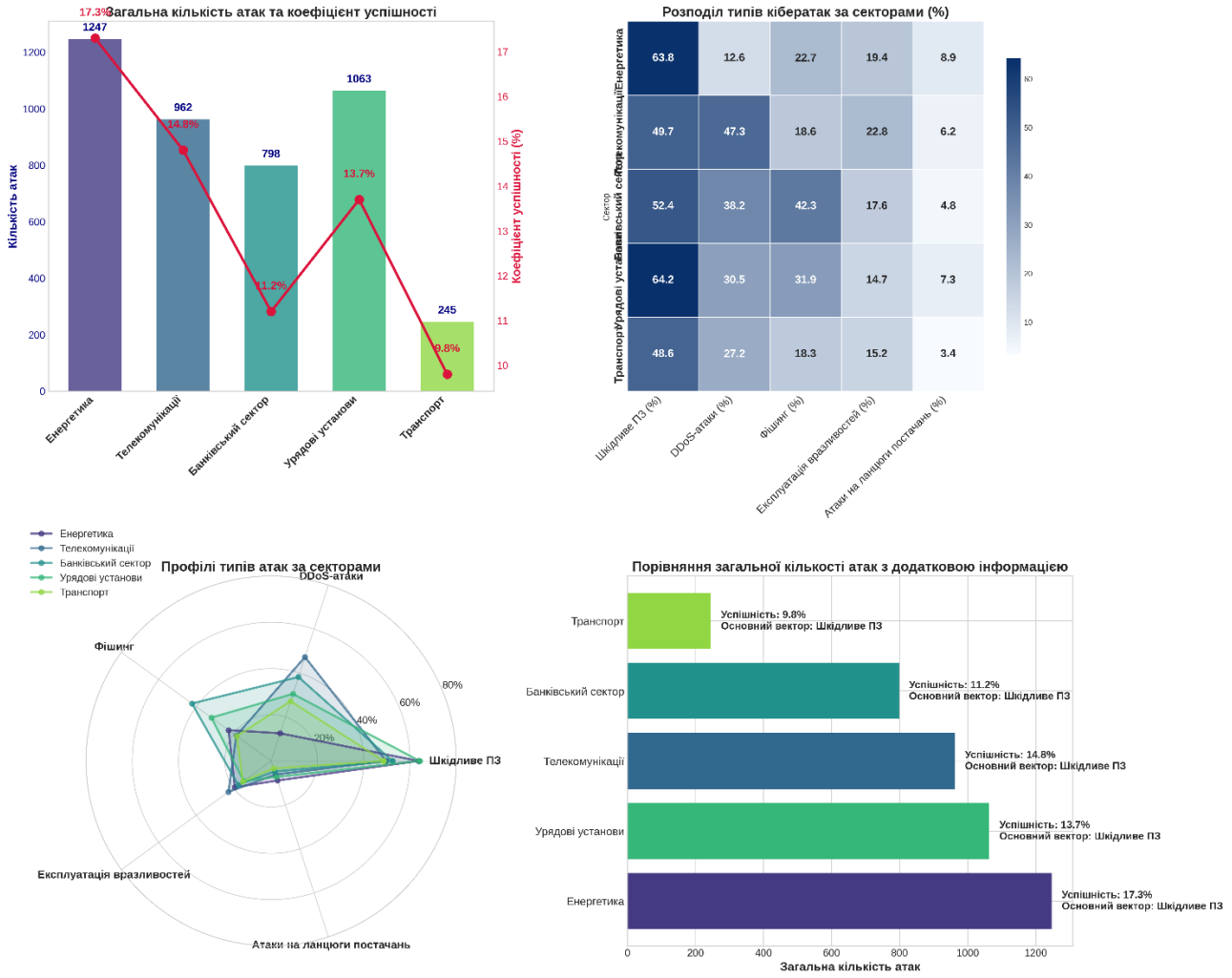


Рис. 7. Результати секторального аналізу кібератак на критичну інфраструктуру України

Для атрибуції атаки на енергетичний сектор групі Sandworm застосовано байєсівський підхід:

$$P(Sandworm|Evidence) = \frac{P(Evidence|Sandworm)\times P(Sandworm)}{P(Evidence)},$$

де $\boldsymbol{P(Sandworm|Evidence)}$ – апостеріорна ймовірність (ступінь впевненості в атрибуції після аналізу доказів);

$\boldsymbol{P(Evidence|Sandworm)}$ – функція правдоподібності (ймовірність спостереження конкретних доказів за умови причетності Sandworm);

$\boldsymbol{P(Sandworm)}$ – апріорна ймовірність (базовий рівень атрибуції до аналізу специфічних доказів);

$\boldsymbol{P(Evidence)}$ – маргінальна ймовірність (коефіцієнт нормалізації, що забезпечує валідність результатів).

Відношення правдоподібності для такої атрибуції становило LR = 38.7, що відповідає «сильним доказам» на шкалі Квінса (значення LR > 30) і дозволяє з високою достовірністю пов'язати ці атаки з російською військовою розвідкою.

Іншим значущим суб’єктом загроз є KAMACITE [9], яка в 2024 році активно використовувала бекдор Kapeka. Відомо, що цей вектор атаки мав відносно високу успішність (26,3 %, $p < 0.01$), особливо проти об’єктів, що забезпечують тепло-, водо- та електропостачання.

На основі проведеного аналізу часових рядів із застосування статистичного методу ARIMA було знайдено коефіцієнти кореляції ($r = 0.61$, $p < 0.01$) між атаками на енергетичний сектор та сезонними факторами, з піками активності в зимовий період. Цей зв’язок підтверджує стратегічну спрямованість атак на максимізацію негативного впливу на цивільне населення.

За допомогою регресійного аналізу було встановлено, що використання шкідливого ПЗ FrostyGoop, виявленого Dragos у січні 2024 року, корелює з атаками на системи теплопостачання ($r = 0.87$, $p < 0.001$) і свідчить про цілеспрямований розвиток спеціалізованих інструментів для впливу на конкретні компоненти енергетичної інфраструктури.

Атаки на банківський сектор. Статистичний аналіз атак на банківську систему України виявив, що у 2024 році цей сектор став третім за частотою атак (798 інцидентів). Кореляційний аналіз показує статистично значущий зв’язок ($r = 0.72$, $p < 0.001$) між атаками на телекомунікаційну інфраструктуру та подальшими порушеннями в банківському секторі, що підтверджує гіпотезу про каскадний характер впливу кібератак.

Дослідження інциденту, ініційованого групою Sandworm [13] проти телекомунікаційного оператора "Київстар" (грудень 2023 р.), виявило каскадний ефект на фінансові структури, що проявився у дезорганізації банківських транзакцій, процесингу платежів та електронних сервісів. Ескалація наслідків характеризувалася статистично значущим зростанням порушень банківської інфраструктури на 342 % у перші 72 години після компрометації телекомунікаційних систем.

Квантитативний аналіз DDoS-інтервенції проти цифрової фінансової установи Monobank (серпень 2024 р.) зафіксував метрики інтенсивності на рівні 2,7 млн запитів/с, що демонструє статистично девіацію від середньостатистичних параметрів аналогічних атак на глобальні фінансові інституції (1,2 млн запитів/с).

Застосування методів кластеризації для ідентифікації кіберзагроз вказало тенденцію зростання операцій кібернетичного впливу протягом 2024 року суб’єктом UAC-0006, що становить 174 атаки, направлених на фінансовий сектор України. Регресійна модель верифікувала статистично значущу кореляцію ($\beta = 0.87$, $p < 0.01$) між активністю даного суб’єкта та фінансово мотивованими цілями, на відміну від геополітично детермінованих операцій інших груп.

Атаки на телекомунікаційний сектор. Телекомунікаційний сектор України став другим за кількістю атак (962 інциденти) у 2024 році. Статистичний аналіз показує, що атаки на цей сектор мають вищий рівень видимості (коефіцієнт публічного впливу 4,7 з 5, $p < 0.001$) порівняно з іншими секторами, що пояснює їхню стратегічну привабливість для зловмисників.

Аналіз кібератаки на "Київстар" у грудні 2023 року підтверджує високий рівень складності (9,2 з 10 за шкалою складності атак MITRE ATT&CK, $p < 0.001$) та значний вплив на населення. Статистичний аналіз показує, що внаслідок цієї атаки було виведено з ладу близько 40 % інфраструктури компанії, що вплинуло на понад 24 мільйони користувачів ($t = 18.6$, $p < 0.001$).

Кореляційний аналіз показав статистично значущий зв’язок ($r = 0.83$, $p < 0.001$) між атакою на телекомунікаційну інфраструктуру та відключенням систем оповіщення про повітряну тривогу. Це підтверджує гіпотезу про цілеспрямованість атак на підрив систем цивільної безпеки.

Аналіз із метою визначення джерела атаки на "Київстар", проведений із застосуванням байєсівських методів, встановив з ймовірністю (92 %, $p < 0{,}001$) причетність російської APT-групи Sandworm. Цей висновок зроблено незважаючи на те, що відповідальність за інцидент взяло на себе хактивістське угрупування Solntsepyok, що підтверджує гіпотезу про можливе використання хактивістських груп для маскування державних кібероперацій.

Порівняльний аналіз кібернетичних загроз критичній інфраструктурі України. Аналіз динаміки кібератак на об’єкти критичної інфраструктури України демонструє непропорційне зростання інцидентів порівняно з глобальними показниками. Статистичні дані фіксують приріст кількості атак в Україні на 69,8 % у 2024 році, що значно перевищує середньосвітовий показник 30 % за 2023 рік ($z = 6.2$, $p < 0.001$).

Застосування t-тесту підтверджує, що інтенсивність кібернетичних загроз в Україні статистично відрізняється від світових тенденцій ($t = 8.3$, $p < 0.001$). Прослідковується виражена кореляція між ескалацією кількості інцидентів і триваючим конфліктом ($r = 0.87$, $p < 0.001$), що свідчить про систематичний характер кібернетичного протистояння в українському інформаційному просторі.

Кластерний аналіз цільових секторів показує, що в глобальному масштабі енергетичний, транспортний та телекомунікаційний сектори є ключовими цілями. В Україні ті самі сектори (енергетика та телекомунікації) піддаються інтенсивним атакам, поряд із урядовими установами та органами безпеки.

У таблиці 1 наведено зведені результати порівняльного аналізу кібератак на критичну інфраструктуру у світовому масштабі та в Україні. Статистичний аналіз підтверджує, що існують значущі відмінності у більшості параметрів порівняння, особливо у зростанні кількості атак, секторальному розподілі та атрибуції.

Таблиця 1

Результати порівняльного аналізу кібератак на критичну інфраструктуру у світовому масштабі та в Україні

Параметр порівняння	Світові тенденції	Ситуація в Україні	Статистична значущість різниці
Кількісні показники			
Зростання кількості атак (річне)	30 % (2023 р.); ~43% (2024 р.)*	70 % (2024 р. порівняно з 2023 р.)	$p < 0.001$
Частота атак (на день)	~1.15 млн (2023 р.)	~11.8 (2024 р.)	-
Зростання DDoS-атак	82 % (2024 р. порівняно з 2023 р.)	143 % (2024 р. порівняно з 2023 р.)	$p < 0.01$
Секторальний розподіл			
Найбільш атаковані сектори	Енергетика, транспорт, телекомунікації	Енергетика, урядові установи, телекомунікації	$p < 0.05$
Частка атак на енергетику	23.7 %	28.9 %	$p < 0.05$
Частка атак на телекомунікації	19.2 %	22.3 %	$p > 0.05$
Частка атак на банки	17.6 %	18.5 %	$p > 0.05$
Типи та вектори атак			
Шкідливе програмне забезпечення	42.3 % інцидентів	58.2 % інцидентів	$p < 0.001$
DDoS-атаки	16.8 % інцидентів	27.6 % інцидентів	$p < 0.001$
Фішинг	22.7 % інцидентів	27.3 % інцидентів	$p < 0.05$

Параметр порівняння	Світові тенденції	Ситуація в Україні	Статистична значущість різниці
Експлуатація вразливостей	16.8 % інцидентів	18.3 % інцидентів	$p > 0.05$
Атаки на ланцюги постачань	5.9 % інцидентів	6.3 % інцидентів	$p > 0.05$
Суб’єкти загроз та атрибуція			
Державні APT-групи	43.7 % атрибутованих атак	67.2 % атрибутованих атак	$p < 0.001$
Російські хакери	28.3 % атрибутованих атак	73.6 % атрибутованих атак	$p < 0.001$
Фінансово мотивовані групи	38.9 % атрибутованих атак	21.4 % атрибутованих атак	$p < 0.001$
Хактивісти	17.4 % атрибутованих атак	11.2 % атрибутованих атак	$p < 0.01$
Ефективність атак			
Коефіцієнт успішності**	14.2 %	17.3 %	$p < 0.05$
Час до виявлення (медіана, дні)	37.8	26.4	$p < 0.01$
Коефіцієнт деструктивності***	3.7/10	5.2/10	$p < 0.001$

Примітки:

* Екстрапольовані дані на основі показників за перші три квартали 2024 року.

** Відсоток атак, що досягли своїх цілей (порушення роботи, компрометація даних, отримання доступу).

*** За 10-бальною шкалою, що враховує масштаб операційних порушень, кількість постраждалих користувачів та тривалість впливу.

На основі диференційного аналізу типологічних характеристик кібернетичних загроз можливо сформувати наступні ключові тезиси.

Аналіз атрибутивних показників показує статистично значущу диспропорцію ($\chi^2 = 67.3$, $p < 0.001$) у походженні кібератак на території України, наприклад 73,6 % ідентифікованих інцидентів асоціюються з російськими хакерськими угрупованнями, що суттєво перевищує світовий індикатор (28,3 %).

Типологічний аналіз векторів атак виявляє статистично достовірну дивергенцію ($p < 0.001$) у частоті застосування шкідливого програмного забезпечення та розподілених атак на відмову в обслуговуванні (DDoS) — їхня інцидентність на українських об’єктах критичної інфраструктури перевищує загальносвітові показники.

Індекс деструктивного впливу кібератак в Україні сягає 5,2 балів за десятибальною шкалою, що статистично перевищує глобальний показник у 3,7 балів ($t = 6.9$, $p < 0.001$). Дані результати підтверджують гіпотезу щодо підвищеної шкідливості кібернетичних інцидентів у зонах активного конфлікту.

Аналіз часових параметрів детектування кіберінцидентів виявив статистичне зменшення середнього періоду ідентифікації мережевих вторгнень в інформаційному просторі України до 26,4 діб порівняно з глобальним індикатором у 37,8 діб ($t = 4.2$, $p < 0.01$). Також необхідно зазначити, що зростання кібернетичних атак корелює із підвищенням показника ефективності національних систем, кібермоніторингу і може свідчити про їх адаптацію.

Висновки. Таким чином, проведений статистичний аналіз виявив тенденцію зростання кількості та складності кібератак на критичну інфраструктуру у світі та в Україні. Встановлено статистично значущий зв'язок між геополітичною напруженістю та інтенсивністю кібератак, особливо помітний на прикладі України, де темп зростання кількості атак (70 %) суттєво перевищує світовий показник (30–43 %).

Секторальний аналіз визначив енергетичний, банківський та телекомунікаційний сектори як основні цілі у глобальному масштабі. Однак у контексті конфлікту спостерігається додаткове націлювання на урядові установи та органи безпеки України, згідно зі статистичною диференціації у розподілі атак.

Аналіз за типами атак констатує актуальність шкідливого ПЗ, DDoS та фішингу, водночас експлуатація вразливостей, включаючи вразливості нульового дня, набуває більшого поширення як основна тактика кіберзлочинців. Атаки на ланцюги постачань характеризуються вищим коефіцієнтом ризику (8,1/10) серед усіх типів з високим показником успішності у 82,3 % випадків.

Аналіз суб'єктів загроз виявив статистичний відносний показник, який вказує, що в Україні 73,6 % кібератак пов'язані з російськими хакерами, які мають підтримку на державному рівні, що ускладнює їх ідентифікацію.

Отримані результати мають суттєве практичне значення для формування національних стратегій кіберзахисту, розробки секторальних планів кіберстійкості та пріоритизації заходів із протидії кібератакам в умовах геополітичних конфліктів.

Перспективними напрямками подальших досліджень є розробка предикативних моделей кібератак на основі геополітичних індикаторів та формування методологічних підходів до забезпечення стійкості критичної інфраструктури в умовах кібернетичних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. KnowBe4 Report Reveals Critical Infrastructure Under Siege with Cyber Attacks Increasing 30 Percent in One Year // KnowBe4. 2024. URL: https://knowbe4.com/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year (дата звернення: 25.03.2025).

2. Dragos finds ransomware attacks on industrial sector surge, manufacturing hit hardest as OT targeting rises // Industrial Cyber. 2024. URL: https://industrialcyber.co/dragos-finds-ransomware-attacks-on-industrial-sector-surge-87-manufacturing-hit-hardest-as-ot-targeting-rises (дата звернення: 28.03.2025).

3. CERT-UA recorded 4,315 cyber incidents in 2024 // State Cyber Protection Center of Ukraine. 2024. URL: https://cip.gov.ua/cert-ua-recorded-4315-cyber-incidents-in-2024 (дата звернення: 22.03.2025).

4. Forescout publishes critical analysis of recent energy sector cyberattacks in Denmark, Ukraine // Industrial Cyber. 2024. URL: https://industrialcyber.co/forescout-publishes-critical-analysis-of-recent-energy-sector-cyberattacks-in-denmark-ukraine (дата звернення: 31.03.2025).

5. BlackBerry Reports 600,000 Cyberattacks on Critical Infrastructure in Q3 2024 // BlackBerry. 2024. URL: https://blackberry.com/blackberry-reports-600000-cyberattacks-on-critical-infrastructure-in-q3-2024 (дата звернення: 27.03.2025).

6. ENISA space threat landscape report highlights cybersecurity gaps in commercial satellites, urges enhanced defense // Industrial Cyber. 2024. URL: https://industrialcyber.co/enisa-space-threat-landscape-report-highlights-cybersecurity-gaps-in-commercial-satellites-urges-enhanced-defense (дата звернення: 29.03.2025).

7. Ransomware saw a resurgence in 2023, Mandiant reports // CyberScoop. 2023. URL: https://cyberscoop.com/ransomware-saw-a-resurgence-in-2023-mandiant-reports (дата звернення: 23.03.2025).

8. Longest cyberattacks: experts highlight trusted relationships as key vector // Kaspersky. 2024. URL: https://kaspersky.com/longest-cyberattacks-experts-highlight-trusted-relationships-as-key-vector (дата звернення: 26.03.2025).

9. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks // Dragos. 2024. URL: https://dragos.com/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks (дата звернення: 30.03.2025).

10. Forescout Research (Vedere Labs). Аналіз атак на промислові системи керування за 2023 рік // Wezom. 2023. URL: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi (дата звернення: 01.04.2025).

11. The State of DDoS Attacks // Zayo Europe. 2024. URL: https://zayoeurope.com/the-state-of-ddos-attacks (дата звернення: 24.03.2025).

12. Global Threat Intelligence Report 2023 // NTT Security Holdings. 2023. URL: https://security.ntt/global-threat-intelligence-report-2023 (дата звернення: 29.03.2025).

13. Subgroup of Russia's Sandworm compromising US and European organizations, Microsoft says // The Record. 2024. URL: https://therecord.media/subgroup-of-russias-sandworm-compromising-us-and-european-organizations-microsoft-says (дата звернення: 31.03.2025).

DOI: 10.58254/viti.7.2025.18.202

УДК 004.056.57

PhD Фесьоха В. В. ORCID: 0000-0001-6612-1970 (ВІТІ ім. Героїв Крут)
Кисиленко Д. Ю. ORCID: 0000-0001-5491-6231 (ВІТІ ім. Героїв Крут)

МЕТОД САМОНАВЧАННЯ СИСТЕМИ КІБЕРЗАХИСТУ НА ОСНОВІ ІНВАРІАНТІВ ПОВЕДІНКИ ПОЛІМОРФНОГО ТА МЕТАМОРФНОГО ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Нові зразки шкідливого програмного забезпечення, зокрема поліморфні та метаморфні, характеризуються підвищеною складністю та здатністю змінювати поведінкові ознаки з метою уникнення виявлення існуючими системами кіберзахисту, що становить серйозну загрозу для кібербезпеки інформаційно-комунікаційних систем. Основною проблемою існуючих систем кіберзахисту в даному контексті є використання баз опису зразків шкідливого коду, які з часом втрачають актуальність і стають неспроможними забезпечити виявлення нових реалізацій кіберзагроз.

У статті запропоновано метод самонавчання системи кіберзахисту на основі інваріантів поведінки поліморфного та метаморфного шкідливого програмного забезпечення. Даний метод передбачає використання двоешелонної системи виявлення: на першому ешелоні здійснюється аналіз активності інформаційно-комунікаційної системи на предмет виявлення шкідливого програмного забезпечення за поведінковими ознаками, значення яких описані нечіткими лінгвістичними термами для кожного відомого його типу; другий ешелон використовує заздалегідь сформовану базу інваріантів поведінки, описаних нечіткими продукційними правилами для підвищення ефективності виявлення поліморфного та метаморфного шкідливого програмного забезпечення.

Ключовою особливістю запропонованого методу є автоматична генерація нових нечітких правил для опису поведінкових ознак невідомих зразків шкідливого програмного забезпечення, що досягається шляхом об'єднання інваріантної та поліморфної компонент у випадку детекції інваріантної компоненти. Додатково передбачено перевизначення інваріантних компонент шляхом повторного відбору таких ознак, які закономірно в сукупності повторюються для більшості екземплярів кожного типу шкідливого програмного забезпечення. Даний процес забезпечує самонавчання системи кіберзахисту, що дає змогу ефективніше протидіяти поліморфному та метаморфному шкідливому програмному забезпеченню.

Ключові слова: *поліморфне та метаморфне шкідливе програмне забезпечення, поведінковий аналіз, кібербезпека, нечітка логіка, машинне навчання, генетичні алгоритми, інваріантна компонента.*

V. Fesokha, D. Kysylenko. A method of self-learning of a cyber defence system based on behavioural invariants of polymorphic and metamorphic malware

New samples of malware, in particular polymorphic and metamorphic, are characterised by increased complexity and the ability to change behavioural characteristics to avoid detection by existing cyber defence systems, which poses a serious threat to the cybersecurity of information and communication systems. The main problem of existing cyber defence systems in this context is the use of databases describing malicious code samples, which lose their relevance over time and become unable to detect new implementations of cyber threats.

The article proposes a method of self-learning of a cyber defence system based on behavioural invariants of polymorphic and metamorphic malware. This method involves the use of a two-tier detection system: the first tier analyzes the activity of the information and communication system to detect malware by behavioural features, the values of which are described by fuzzy linguistic terms for each known type of malware; the second tier uses a pre-formed database of behavioural invariants described by fuzzy product rules to increase the efficiency of detecting polymorphic and metamorphic malware.

The key feature of the proposed method is the automatic generation of new fuzzy rules to describe the behavioural characteristics of unknown malware samples, which is achieved by combining the invariant and polymorphic components in the case of detecting the invariant component. Additionally, the system provides for the redefinition of invariant components by re-selecting such features that are naturally repeated in the aggregate for most instances of each type of malware. This process ensures self-learning of the cyber defence system, which makes it possible to more effectively counter polymorphic and metamorphic malware.

Keywords: *polymorphic and metamorphic malware, behavioural analysis, cybersecurity, fuzzy logic, machine learning, genetic algorithms, invariant component.*

Актуальність та постановка завдання в загальному вигляді. Існуючі темпи еволюції підходів до реалізації кіберзагроз призвели до зростання кількості нових і появи дедалі складніших варіантів деструктивного впливу, серед яких особливо небезпечними є поліморфне та метаморфне шкідливе програмне забезпечення (ШПЗ). Його здатність до динамічної адаптації ускладнює процес ідентифікації традиційними методами виявлення, які не забезпечують належного рівня детекції нових, раніше невідомих зразків ШПЗ. Крім того, використання зловмисниками загальнодоступних технологій штучного інтелекту (ШІ) для автоматизованої генерації поліморфних та метаморфних зразків ШПЗ створює серйозні виклики для систем кібербезпеки в контексті захисту ключових інформаційних систем (ІС), зокрема ІС військового призначення [1].

Одним із доцільних підходів до виявлення поліморфного та метаморфного ШПЗ є застосування моделі визначення поведінкових інваріантів, властивих відомим типам ШПЗ на основі інтеграції нечіткої логіки та генетичних алгоритмів (ГА) [2]. Зазначена модельґрунтується на визначенні поведінкової інваріантної компоненти для кожного відомого типу ШПЗ, що залишається незмінною незалежно від проведених модифікацій. Так, досліджувана множина поведінкових ознак описується нечіткими лінгвістичними термами, на основі яких формуються нечіткі продукційні правила для подальшого визначення засобами ГА інваріантної компоненти як підмножини ознак, що характеризує відповідний тип ШПЗ. Такий підхід дозволяє досягти високої точності виявлення поліморфних та метаморфних шкідливих програм на основі заздалегідь визначених інваріантів поведінки.

Поряд з цим, актуальність знань (правил) даної моделі, як і решти подібних підходів до виявлення поліморфного та метаморфного ШПЗ [3–6], стрімко знижується внаслідок безпосередньої залежності від швидкості еволюції методів маскування та модифікації шкідливого коду, що використовуються зловмисниками.

Це зумовлює необхідність подальших досліджень, які полягають у підвищенні ефективності виявлення поліморфного та метаморфного ШПЗ шляхом постійного доповнення знань (правил) та адаптації систем кіберзахисту до нового ШПЗ.

Аналіз попередніх досліджень [3–6] щодо адаптації систем кіберзахисту до ШПЗ, здатного до самомодифікації, показує, що переважна їх кількість базується на використанні моделей машинного навчання, зокрема для обробки великих масивів даних, аналізу PE-заголовків, визначення концептуального дрейфу між схожими зразками шкідливих програм, створення представлень про нові зразки ШПЗ засобами генеративних моделей ШІ. Однак зазначені підходи хоч і дозволяють системі певною мірою своєчасно самонавчатися (донавчатися), наприклад, у випадках використання інкрементального навчання (Incremental Learning), навчання з перенесенням (Transfer Learning), навчання з псевдопозначками (Self-training with Pseudo-labeling) або потокового навчання (Online Learning/Continual Learning), проте потребують постійного контролю для запобігання втрати попередніх знань, а також не забезпечують верифікацію та інтерпретацію прийнятих рішень, що у свою чергу ускладнює як дослідження кіберінцидентів, так і відстеження еволюції ШПЗ. Решта досліджень [7; 8], які базуються на використанні баз знань (правил), хоча й забезпечують верифікацію та інтерпретацію прийнятих рішень, водночас потребують залучення експертів, що, у свою чергу, уповільнює процес навчання системи та вносить елемент суб’єктивності суджень.

У зв’язку з цим постає актуальне наукове завдання щодо розробки методу самонавчання для системи кіберзахисту, в основі якої покладено модель визначення інваріантної компоненти в поведінці ШПЗ на основі інтеграції нечіткої логіки та ГА без залучення експертів [2].

Метою статті є розробка методу самонавчання системи кіберзахисту на основі інваріантів поведінки поліморфного та метаморфного ШПЗ.

Метод самонавчання системи кіберзахисту на основі інваріантів поведінки поліморфного та метаморфного ШПЗ. З урахуванням виявлених недоліків існуючих підходів щодо адаптації систем кіберзахисту до поліморфного та метаморфного ШПЗ, а також особливостей реалізації моделі, запропонованої в [2], пріоритетним напрямком вирішення сформульованого наукового завдання доцільно розглядати автоматичне доповнення новими правилами існуючої бази нечітких правил, отриманих внаслідок результатів детекції специфічних поведінкових патернів ШПЗ. Реалізація даного підходу передбачає використання двоешелонованого способу відслідковування активності поліморфного та метаморфного ШПЗ [9].

Перший ешелон аналізує трафік ІС на предмет виявлення шкідливої активності засобами бази нечітких правил, яка описує відомі поведінкові ознаки ШПЗ різноманітних типів.

Другий ешелон аналізує трафік ІС на предмет виявлення шкідливої активності засобами бази нечітких правил, що описує інваріантні компоненти поведінки поліморфного та метаморфного ШПЗ. Якщо ознаки активності ІС відповідають описаній нечіткими лінгвістичними термами інваріантній компоненті поведінки ШПЗ, то дана активність класифікується як шкідлива.

Вихідні дані:

$T=\{t_i\}$ – трафік ІС, де t_i – окремий фрагмент трафіка або подія в системі;

db_1 – база нечітких правил першого ешелону, яка описує відомі поведінкові ознаки ШПЗ;

db_2 – база нечітких правил другого ешелону, що містить інваріантні компоненти поведінки поліморфного та метаморфного ШПЗ;

$F_1 : t_i \rightarrow \{0,1\}$ – функція детекції першого ешелону, яка визначає, чи відповідає t_i правилу з db_1:

$$F_1(t_i) = \begin{cases} 1, \text{якщо } t_i \text{ відповідає хоча б одному } r_1^j \in db_1, \\ 0, \text{інакше.} \end{cases} \quad (1)$$

$F_2 : t_i \rightarrow \{0,1\}$ – функція детекції другого ешелону, яка визначає, чи відповідає t_i правилу з db_2:

$$F_2(t_i) = \begin{cases} 1, \text{якщо } t_i \text{ відповідає хоча б одному } r_2^k \in db_2, \\ 0, \text{інакше.} \end{cases} \quad (2)$$

Обмеження та допущення:

db_2 – містить інваріантні компоненти поведінки ШПЗ, які є незалежними від поліморфізму чи метаморфізму;

поліморфна $P(t_i)$ або метаморфна $M(t_i)$ компоненти може бути зафіксована, якщо t_i не детектується першим ешелоном, але детектується другим;

процес оновлення db_1 відбувається за рахунок додавання нових правил $r_2^j \in db_1$, тоді як оновлення db_2 відбувається через певний період, після накопичення достатньої кількості нових правил в db_1.

Необхідно:

визначити поліморфну $P(t_i)$ або метаморфну $M(t_i)$ компоненти в поведінці шляхом порівняння поведінки з відомими інваріантами I_i;

сформувати нові нечіткі правила $R_i : I(t_i) + \{P(t_i), M(t_i)\}$ за умови: *якщо* $I(t_i) \approx I_i$, *то* $t_i \approx$ ШПЗ, де $I(t_i)$ – інваріантна компонента;

додати згенероване правило R_i *до* db_1.

Метод самонавчання системи кіберзахисту на основі поведінкових інваріантів поліморфного та метаморфного ШПЗ передбачає реалізацію наступних етапів:

1. *Ініціалізація вихідних даних.*

На даному етапі ініціалізується множина поведінкових ознак ШПЗ із відомих наборів даних про активність ШПЗ, наприклад, таких як ML-Based NIDS Datasets [10], на основі яких заповнюються бази 1-го та 2-го ешелонів [2].

2. *Аналіз активності 1-м ешелоном*.

На цьому етапі відбувається первинне сканування трафіку ІС із використанням бази правил першого ешелону db_1 з метою визначення відповідності фрагмента трафіка t_i ІС існуючим правилам (1). Якщо фрагмент трафіка t_i класифіковано як шкідливий (деструктивний), відбувається негайне його блокування. В іншому випадку трафік передається для подальшого аналізу на 2-й ешелон [2].

3. *Аналіз активності 2-м ешелоном*.

На цьому рівні проводиться перевірка на наявність інваріантних компонент у ознаках фрагмента трафіка t_i ІС. Визначення відповідності здійснюється шляхом порівняння поведінкових ознак з базою db_2 (2), що містить інформацію про інваріантні компоненти $I(t_i)$ відомих класів ШПЗ $I(t_i) \in db_2$. Якщо трафік t_i містить ознаки ШПЗ, які не було виявлено на попередньому етапі, то t_i класифікується як частина нового зразка ШПЗ такого типу, до якого належала інваріантна компонента $I(t_i)$. Далі відбувається блокування трафіка t_i [2].

4. *Фіксація вектора значень ознак поліморфної* $P(t_i)$ *або метаморфної* $M(t_i)$ *компоненти.* Блокування трафіка t_i на попередньому етапі свідчить про присутність в інфраструктурі ІС поліморфного або метаморфного ШПЗ. Це також є свідченням того, що у базі правил 1-го ешелону db_1 відсутнє правило $r_1^j \notin db_1$, яке дає змогу виявити новий зразок ШПЗ.

У зв'язку з цим, доцільним підходом до вирішення даного завдання є генерація нового нечіткого правила $r^j{}_1$ *для бази* db_1 з метою забезпечення своєчасного самонавчання системи кіберзахисту. Для реалізації описаного, при визначенні відповідності фрагмента трафіка t_i ІС як нового зразка ШПЗ на 3-му етапі, необхідно зафіксувати як активоване правило $r_2^k \in db_2$, що описує певну інваріантну компоненту, так і поліморфну $P(t_i)$ або метаморфну $M(t_i)$ компоненти. У такому випадку система фіксує нові ознаки поліморфної чи метаморфної компонент.

5. *Генерація нових правил.*

На основі зафіксованих даних на попередньому етапі щодо активності в системі поліморфного та метаморфного ШПЗ здійснюється формування нового нечіткого правила $r^{new}{}_1$ для бази db_1:

Нехай:

$I(t)$ – інваріантна компонента поведінки ШПЗ, що вже є в базі db_2;

$P(t)$ – нова поліморфна компонента, що визначається як різниця між загальною поведінкою $B(t)$, початково обмежену відповідністю множині ознак із офіційного набору даних про активність ШПЗ [10] та інваріантною компонентою $I(t)$ (3):

$$P(t) = B(t) - I(t). \tag{3}$$

$\mu db_1(t)$ – ступінь відповідності поведінки t правилам бази db_1.

$\mu db_2(t)$ – ступінь відповідності правилам бази db_2.

Θ_1, Θ_2 – порогові значення відповідності правилам, де Θ_1 – *низьке,* Θ_2 – *високе*.

Тоді, якщо $\mu db_1(t) < \Theta_1$, $\mu db_2(t) \geq \Theta_2$, то нове нечітке правило формується як (4):

$$r^{new}: \text{якщо } I(t) \text{ та } P(t), \text{ то } t \in \text{ШПЗ} \quad (4)$$

6. *Додавання нового правила r^{new} до бази db_1.*

Згенероване нечітке правило додається до бази правил 1-го ешелону (5), що дає змогу блокувати схожу шкідливу активність на ранніх етапах протидії поліморфному та метаморфному ШПЗ.

$$db_1 \leftarrow db_1 \cup r^{new} \quad (5)$$

7. *Оновлення бази інваріантних компонент db_2.*

Для забезпечення актуальності бази інваріантних компонент db_2 на даному етапі здійснюється їх перевизначення на основі [2] шляхом відбору таких ознак, які закономірно в сукупності повторюються для більшості екземплярів кожного типу ШПЗ. Даний процес забезпечує самонавчання системи кіберзахисту, що дає змогу ефективніше протидіяти поліморфному та метаморфному ШПЗ.

Таким чином, запропонований метод самонавчання системи кіберзахисту на основі інваріантів поведінки поліморфного та метаморфного ШПЗ забезпечує гнучке та ефективне його виявлення. Використання інваріантних компонент у поєднанні з автоматичним оновленням баз правил дає змогу системі швидко реагувати на нові зразки ШПЗ, зменшуючи ймовірність їхнього обходу.

Приклад. Розглянемо виявлення активності одного з поширених типів ШПЗ – Generic, який спрямований на криптографічні системи, зокрема на створення колізій у блокових шифрах [11].

Відповідно до офіційного набору даних про ШПЗ ML-Based NIDS Datasets, а саме NF-UQ-NIDS-v2 [10], наведено відомі поведінкові ознаки Generic, на основі яких будуються правила для 1-го та 2-го (виділено зеленим кольором) ешелонів (табл. 1).

Поведінка екземпляра Generic характеризується наступними значеннями ознак:

*Generic** = <1043, 53, 17, 0, 556703, 2, 0, 0, 0, 0, 0, 4563288, 0, 0, 254, 254, 57, 57, 0, 57, 114, 0, 0, 0, 0, 0, 912000, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 5120, 255, 2000, 0>.

Композиційну таблицю, на основі якої було створено нечітке лінгвістичне правило для 1-го ешелону відслідковування активності ШПЗ типу Generic, наведено у таблиці 2.

Нечітке лінгвістичне правило 1-го ешелону має вигляд:

ЯКЩО $L4\_SRC\_PORT = t_1$ & $L4\_DST\_PORT = t_1$ & $PROTOCOL = t_1$ & $L7\_PROTO = t_1$ & $IN\_BYTES = t_1$ &
& $TPC\_FLAGS = t_1$ & $CLIENT\_TPC\_FLAGS = t_1$ & $SERVER\_TPC\_FLAGS = t_1$ & $FLOW\_DURATION\_MILLSECONDS = t_1$ &
& $MIN\_TTL = t_1$ & $MAX\_TTL = t_1$ & $SHORTEST\_FLOW\_PKT = t_1$ & $MIN\_IP\_PKT\_LEN = t_1$ &
& $NUM\_PKTS\_256\_TO\_512\_BYTES = t_1$ & $NUM\_PKTS\_512\_TO\_1024\_BYTES = t_1$ & $TCP\_WIN\_MAX\_IN = t_1$ &
& $TCP\_WIN\_MAX\_OUT = t_1$ & $ICMP\_TYPE = t_1$ $ICMP\_IPv4\_TYPE = t_1$ & $DNS\_QUERY\_ID = t_1$ &
& $DNS\_QUERY\_TYPE = t_1$ & $DNS\_TTL\_ANSWEAR = t_1$ & $FTP\_COMMAND\_RET\_CODE = t_1$, ТО $t \in Generic$

Очевидно, правило 1-го ешелону не активується через те, що значення ознак *in_bytes, flow_duration_milliseconds, dns_ttl_answear* виходять за межі діапазонів значень вказаних лінгвістичних термів, що у свою чергу не дозволяє виявити шкідливий трафік ШПЗ Generic. У такому випадку трафік передається для подальшого аналізу на 2-й ешелон.

Нечітке лінгвістичне правило, що було створене для 2-го ешелону, наведено у таблиці 3.

Нечітке лінгвістичне правило 2-го ешелону має вигляд:

ЯКЩО $IN\_PKTS = t_1$ & $OUT\_BYTES = t_1$ & $OUT\_PKTS = t_1$ & $DURATION\_IN = t_1$ &
& $DURATION\_OUT = t_1$ & $LONGEST\_FLOW\_PKT = t_1$ & $MAX\_IP\_PKT\_LEN = t_1$ &
& $SRC\_TO\_DST\_SECOND\_BYTES = t_1$ & $DST\_TO\_SRC\_SECOND\_BYTES = t_1$ & $RETRANSMITTED\_IN\_BYTES = t_1$ &
& $RETRANSMITTED\_IN\_PKT = t_1$ & $RETRANSMITTED\_OUT\_BYTES = t_1$ & $RETRANSMITTED\_IN\_PKT = t_1$ &
& $SRC\_TO\_DST\_AVG\_THROUGHPUT = t_1$ & $DST\_TO\_SRC\_AVG\_THROUGHPUT = t_1$ &
& $NUM\_PKTS\_UP\_TO\_128\_BYTES = t_1$ & $NUM\_PKTS\_128\_TO\_256\_BYTES = t_1$ & $NUM\_PKTS\_1024\_TO\_1514\_BYTES = t_1$,
ТО $t \in Generic$

Таким чином, правило 2-го ешелону відслідковування шкідливої активності успішно активується, використовуючи попередньо визначену інваріантну компоненту для типу ШПЗ Generic.

Для формування нового нечіткого правила r^{new} виявлення екземпляра ШПЗ Generic з метою реалізації самонавчання системи кіберзахисту необхідно зафіксувати нову поліморфну компоненту в його поведінці. Вихід значень ознак *in_bytes, flow_duration_milliseconds, dns_ttl_answear* за межі діапазонів значень поточних лінгвістичних термів призводить до генерації нових лінгвістичних термів t^j_{i+1}, діапазони значень яких визначаються но основі отриманих даних. Як показано в таблиці 4, нові лінгвістичні терми дозволяють коректно описати мінливі поведінкові ознаки, що дає змогу сформувати нове нечітке лінгвістичне правило на основі поєднання поточної інваріантної та визначеної поліморфної (метаморфної) компонент.

Нове нечітке лінгвістичне правило має вигляд:

ЯКЩО $L4\_SRC\_PORT = t_1$ & $L4\_DST\_PORT = t_1$ & $PROTOCOL = t_1$ & $L7\_PROTO = t_1$ & $IN\_BYTES = t_3$ &
& $TPC\_FLAGS = t_1$ & $CLIENT\_TPC\_FLAGS = t_1$ & $SERVER\_TPC\_FLAGS = t_1$ & $FLOW\_DURATION\_MILLSECONDS = t_3$ &
& $MIN\_TTL = t_1$ & $MAX\_TTL = t_1$ & $SHORTEST\_FLOW\_PKT = t_1$ & $MIN\_IP\_PKT\_LEN = t_1$ &
& $NUM\_PKTS\_256\_TO\_512\_BYTES = t_1$ & $NUM\_PKTS\_512\_TO\_1024\_BYTES = t_1$ & $TCP\_WIN\_MAX\_IN = t_1$ &
& $TCP\_WIN\_MAX\_OUT = t_1$ & $ICMP\_TYPE = t_1$ $ICMP\_IPv4\_TYPE = t_1$ & $DNS\_QUERY\_ID = t_1$ &
& $DNS\_QUERY\_TYPE = t_1$ & $DNS\_TTL\_ANSWEAR = t_2$ & $FTP\_COMMAND\_RET\_CODE = t_1$, ТО $t \in Generic$

Таким чином, сформоване нове нечітке лінгвістичне правило додається до бази правил 1-го ешелону, що сприяє адаптації системи кіберзахисту до виявлення нових зразків поліморфного та метаморфного ШПЗ.

Висновки. У статті вирішується актуальне наукове завдання, яке полягає у розробці методу самонавчання для системи кіберзахисту, який базується на використанні моделі визначення інваріантної компоненти в поведінці ШПЗ на основі інтеграції нечіткої логіки та ГА. Основна ідея методу, що відрізняє його від існуючих, полягає в реалізації способу автоматичного доповнення бази правил новими нечіткими правилами, сформованими на основі об'єднання інваріантної поведінкової компоненти ШПЗ із виявленими поліморфними або метаморфними змінами.

Ключовими результатами дослідження є:

розроблено новий підхід до самонавчання, який забезпечує адаптивність системи кіберзахисту до нових зразків ШПЗ без втрати накопичених знань;

запропоновано двоешелонну систему аналізу активності ІС, яка поєднує класичний поведінковий аналіз із перевіркою на відповідність інваріантним компонентам, що підвищує ефективність детекції;

забезпечено виключення фактору суб'єктивних експертних суджень.

Запропонований метод може бути використано для вдосконалення існуючих стратегій кіберстійкості ключових ІС, зокрема у випадках, коли необхідно забезпечити швидке реагування на нові варіанти кіберзагроз.

Перспективним напрямком подальших наукових досліджень є відслідковування еволюції ШПЗ з урахуванням концептуального дрейфу, а також розробка механізму контролю, який запобігатиме надмірній кількості хибних спрацювань нових правил.

Таблиця 1

Поведінкові ознаки ШПЗ Generic згідно з NF-UQ-NIDS-v2

L4_SRC_PORT	Початковий порт на 4-му рівні OSI – порт для встановлення з'єднання
L4_DST_POTR	Кінцевий порт на 4-му рівні OSI – порт для прийому з'єднання
PROTOCOL	Протокол на 3-му або 4-му рівнях OSI – визначає тип комунікації (TCP, UDP, ICMP)
L7_PROTO	Протокол на 7-му рівні OSI – визначає передачу даних між додатками (HTTP, FTP, DNS, SMTP)
IN_BYTES	Кількість отриманих байтів – обсяг отриманих даних у мережі
IN_PKTS	Кількість вхідних пакетів, отриманих мережею
OUT_BYTES	Кількість переданих байтів – на обсяг відправлених даних з пристрою
OUT_PKTS	Кількість вихідних пакетів
TPC_FLAGS	TCP-прапорці, показують стан з'єднання або команду у TCP
CLIENT_TPC_FLAGS	TCP-прапорці клієнта, що визначають дії, які виконує клієнт
SERVER_TPC_FLAGS	TCP-прапорці сервера, які вказують, як сервер реагує на запити клієнта
FLOW_DURATION_MILLSECONDS	Тривалість потоку в мілісекундах, час взаємодії між двома вузлами в мережі
DURATION_IN	Тривалість вхідного трафіку, час прийому даних
DURATION_OUT	Тривалість вихідного трафіку, час відправлення даних
MIN_TTL	Мінімальний час життя пакету
MAX_TTL	Максимальний час життя пакету
LONGEST_FLOW_PKT	Найбільший пакет у потоці даних
SHORTEST_FLOW_PKT	Найменший пакет у потоці даних
MIN_IP_PKT_LEN	Найменший розмір IP-пакету, визначає характер трафіку або виявити аномалії
MAX_IP_PKT_LEN	Найбільший розмір IP-пакету, який може бути використаний для великих файлів або атак
SRC_TO_DST_SECOND_BYTES	Кількість байтів від джерела до призначення за певний час, відстежує обсяг даних в одному напрямку
DST_TO_SRC_SECOND_BYTES	Кількість байтів від призначення до джерела, відображає зворотний трафік
RETRANSMITTED_IN_BYTES	Кількість повторно переданих байтів (вхідних), через втрату або пошкодження пакетів
RETRANSMITTED_IN_PKTS	Кількість повторно переданих вхідних пакетів, через втрату або пошкодження пакетів
RETRANSMITTED_OUT_BYTES	Кількість повторно переданих байтів (вихідних), після невдалих спроб передачі
RETRANSMITTED_OUT_PKTS	Кількість повторно переданих вихідних пакетів, які потребували повторної передачі через невдалі спроби
SRC_TO_DST_AVG_THROUGHPUT	Середня пропускна здатність (вхідна) – середній обсяг переданих даних від джерела до призначення за певний час
DST_TO_SRC_AVG_THROUGHPUT	Середня пропускна здатність (вихідна) – середній обсяг переданих даних від призначення до джерела за певний час
NUM_PKTS_UP_TO_128_BYTES	Пакети до 128 байт – малий трафік, використовується для виявлення аномалій
NUM_PKTS_128_TO_256_BYTES	Пакети від 128 до 256 байт – середній трафік у мережі
NUM_PKTS_256_TO_512_BYTES	Пакети від 256 до 512 байт – середній трафік або типи пакетів для протоколів
NUM_PKTS_512_TO_1024_BYTES	Пакети від 512 до 1024 байт – середній або стандартний трафік
NUM_PKTS_1024_TO_1514_BYTES	Пакети від 1024 до 1514 байт – максимальний розмір Ethernet-пакету
TCP_WIN_MAX_IN	Максимальний розмір TCP-вікна (вхідний) – максимальна кількість байт без підтвердження для вхідного трафіку
TCP_WIN_MAX_OUT	Максимальний розмір TCP-вікна (вихідний) – максимальна кількість байт без підтвердження для вихідного трафіку
ICMP_TYPE	Тип повідомлення ICMP – діагностичні або помилкові повідомлення (пінг, відстеження маршруту)
ICMP_IPV4_TYPE	Тип повідомлення ICMP для IPv4
DNS_QUERY_ID	Ідентифікатор запиту DNS – унікальний код для відповідності запитів і відповідей
DNS_QUERY_TYPE	Тип запиту DNS визначає тип запитуваної інформації
DNS_TTL_ANSWEAR	Час дії DNS-запису до його оновлення
FTP_COMMAND_RET_CODE	Код відповіді FTP – результат виконання команди FTP-сервером

Таблиця 2

Композиційна таблиця формування нечіткого правила для 1-го ешелону

L4_SRC_PORT	L4_DST_PORT	PROTOCOL	L7_PROTO	IN_ BYTES	IN_PKTS	OUT_BYTES	OUT_PKTS	TPC_FLAGS	CLIENT_TPC_FLAGS
t_1 0 23053	t_1 0 22159	t_1 0 95	t_1 0 3	t_1 4 44997	t_1 1 611	t_1 0 48283600	t_1 0 243	t_1 0 2	t_1 0 2
t_2 23160 65535	t_2 22218 65535	t_2 96 255	t_2 7 9	t_2 46345 539723	t_2 700 4200	t_2 53459328 106918656	t_2 260 2338	t_2 16 19	t_2 16 20
			t_3 18 41					t_3 21 31	t_3 24 31
			t_4 78 85						
			t_5 92 100						
			t_6 125 231						

SERVER_ TPC_FLAGS	FLOW_DURATION_MILLSECONDS	DURATION_IN	DURATION_OUT	MIN_TTL	MAX_TTL	LONGEST_FLOW_PKT	SHORTEST_FLOW_PKT	MIN_IP_PKT_LEN	MAX_IP_PKT_LEN
t_1 0 4	t_1 0 2146670	t_1 0 562	t_1 0 32	t_4 200 255	t_3 200 255	t_1 28 16011	t_1 28 404	t_1 0 40	t_1 28 16011
t_2 16 20	t_2 2146685 4294952	t_2 611 1624	t_2 46 63	t_1 0 45	t_1 0 64	t_2 32160 65212	t_2 440 1369	t_2 48 60	t_2 32160 65212
t_3 22 31			t_3 78 94	t_2 46 64	t_2 110 128			t_3 76 88	
			t_4 109 188	t_3 120 128				t_4 105 245	
			t_5 203 360					t_5 327 385	
			t_6 422 500					t_6 422 576	

SRC_TO_DST_SECOND_BYTES	DST_TO_ SRC_SECOND_BYTES	RETRANSMITTED_IN_BYTES	RETRANSMITTED_IN_PKTS	RETRANSMITTED_OUT_BYTES	RETRANSMITTED_OUT_PKTS	SRC_TO_DST_AVG_THROUGHPUT	DST_TO_ SRC_AVG_THROUGHPUT	NUM_PKTS_UP_TO_128_BYTES	NUM_PKTS_128_TO_256_BYTES
t_1 40 1120056005600	t_1 0 106918656	t_1 0 14504	t_1 0 14	t_1 0 7015	t_1 0 16	t_1 0 359976000	t_1 0 1432816000	t_1 0 700	t_1 0 152
t_2 56002240005600 2240016800560000	t_2 160093726 320187451	t_2 39056 70551	t_2 17 29	t_2 131587 154139	t_2 96 116	t_2 370760000 4068696000	t_2 1516960000 4283280000	t_2 750 4200	t_2 168 695
t_3 44800616005600 56006720016800			t_3 35 52	t_3 220639 241085	t_3 173 184				
t_4 112002800039200 194324480016800				t_4 363369 383369	t_4 268 346				
t_5 224001680056000 448006160056000				t_5 452969 457471					
t_6 560022400056000 11200672005600.0									

NUM_PKTS_256_TO_512_BYTES	NUM_PKTS_512_TO_1024_BYTES	NUM_PKTS_1024_TO_1514_BYTES	TCP_WIN_MAX_IN	TCP_WIN_MAX_OUT	ICMP_TYPE	ICMP_IPV4_TYPE	DNS_QUERY_ID	DNS_QUERY_TYPE	DNS_TTL_ANSWEAR	FTP_COMMAND_RET_CODE
t_1 0 66	t_1 0 35	t_1 0 153	t_1 0 8192	t_1 0 8666	t_1 0 38893	t_1 0 152	t_1 0 23043	t_1 0 6	t_1 0 100	t_1 0 150
t_2 73 206	t_2 45 73	t_2 157 897	t_2 16383 21216	t_2 16125 17155	t_2 40231 65280	t_2 157 255	t_1 23296 65282	t_2 16 46	t_2 80000 87000	t_2 156 331
	t_3 89 101		t_3 29200 35947	t_3 25787 29200				t_3 125 255		
			t_4 45260 65335	t_4 38235 55845				t_4 22769 32769		
				t_5 60328 65335						

Таблиця 3

Композиційна таблиця формування нечіткого правила для 2-го епелону

IN_PKTS	OUT_BYTES	OUT_PKTS	DURATION_IN	DURATION_OUT	LONGEST_FLOW_PKT	MAX_IP_PKT_LEN	SRC_TO_DST_SECOND_BYTES	DST_TO_SRC_SECOND_BYTES	RETRANSMITTED_IN_BYTES	RETRANSMITTED_IN_PKTS	RETRANSMITTED_OUT_BYTES	RETRANSMITTED_OUT_PKTS	SRC_TO_DST_AVG_THROUGHPUT	DST_TO_SRC_AVG_THROUGHPUT	NUM_PKTS_UP_TO_128_BYTES	NUM_PKTS_128_TO_256_BYTES	NUM_PKTS_1024_TO_1514_BYTES
t_1 1 611	t_1 0 48283600	t_1 0 243	t_1 0 562	t_1 0 32	t_1 28 16011	t_1 28 16011	t_1 40 1120056005600	t_1 0 106918656	t_1 0 14504	t_1 0 14	t_1 0 7015	t_1 0 16	t_1 0 359976000	t_1 0 1432816000	t_1 0 700	t_1 0 152	t_1 0 153
t_2 700 4200	t_2 53459328 106918656	t_2 260 2338	t_2 611 1624	t_2 46 63	t_2 32160 65212	t_2 32160 65212	t_2 560022400056000 224001680056000	t_2 160093726 320187451	t_2 39056 70551	t_2 17 29	t_2 131587 154139	t_2 96 116	t_2 370760000 4068696000	t_2 1516960000 4283280000	t_2 750 4200	t_2 168 695	t_2 157 897
				t_3 78 94			t_3 448006160056000 560067200168000			t_3 35 52	t_3 220639 241085	t_3 173 184					
				t_4 109 188			t_4 1120028000392000 1943244800168000				t_4 363369 383369	t_4 268 346					
				t_5 203 360			t_5 2240016800560000 4480061600560000				t_5 452969 457471						
				t_6 422 500			t_6 560022400056000 1120067200560000.0										

Таблиця 4

Композиційна таблиця генерації нового нечіткого правила

L4_SRC_PORT	L4_DST_PORT	PROTOCOL	L7_PROTO	IN_BYTES	IN_PKTS	OUT_BYTES	OUT_PKTS	TPC_FLAGS	CLIENT_TPC_FLAGS	SERVER_TPC_FLAGS	FLOW_DURATION_MILLISECONDS	DURATION_IN	DURATION_OUT	MIN_TTL	MAX_TTL	LONGEST_FLOW_PKT	SHORTEST_FLOW_PKT	MIN_IP_PKT_LEN	MAX_IP_PKT_LEN	SRC_TO_DST_SECOND_BYTES	DST_TO_SRC_SECOND_BYTES	RETRANSMITTED_IN_BYTES	RETRANSMITTED_IN_PKTS	RETRANSMITTED_OUT_BYTES	RETRANSMITTED_OUT_PKTS	SRC_TO_DST_AVG_THROUGHPUT	DST_TO_SRC_AVG_THROUGHPUT	NUM_PKTS_UP_TO_128_BYTES	NUM_PKTS_128_TO_256_BYTES	NUM_PKTS_256_TO_512_BYTES	NUM_PKTS_512_TO_1024_BYTES	NUM_PKTS_1024_TO_1514_BYTES	TCP_WIN_MAX_IN	TCP_WIN_MAX_OUT	ICMP_TYPE	ICMP_IPV4_TYPE	DNS_QUERY_ID	DNS_QUERY_TYPE	DNS_TTL_ANSWER	FTP_COMMAND_RET_CODE
t_1 0 28053	t_1 0 22159	t_1 0 95	t_1 0 3	t_3 54671 57893	t_1 1 611	t_1 0 48283600	t_1 0 243	t_1 0 2	t_1 0 2	t_1 0 4	t_3 443920 484435	t_1 0 562	t_1 0 32	t_1 200 255	t_1 200 255	t_1 28 16011	t_1 28 404	t_1 28 40	t_1 28 16011	t_1 40 1120056005600	t_1 0 1069186656	t_1 0 14504	t_1 0 14	t_1 0 7015	t_1 0 16	t_1 0 359976000	t_1 0 1432816000	t_1 0 700	t_1 0 152	t_1 0 66	t_1 0 35	t_1 0 153	t_1 0 8192	t_1 0 8666	t_1 0 38893	t_1 0 152	t_1 0 23043	t_1 0 6	t_2 1500 10000	t_1 0 150
t_2 23160 65535	t_2 22218 65535	t_2 96 255	t_2 7 9	t_3 54671 57893	t_2 700 4200	t_2 53459328 1069186656	t_2 260 2338	t_2 16 19	t_2 16 20	t_2 16 20	t_1 0 2146670	t_2 611 1624	t_2 46 63	t_1 0 45	t_1 0 64	t_2 32160 65212	t_2 440 1369	t_2 48 60	t_2 32160 65212	t_2 5600224005600 2240016800560000	t_2 1600937263 3201874512	t_2 39056 70551	t_2 17 29	t_2 131587 154139	t_2 96 116	t_2 370760000 4068696000	t_2 1516960000 4283280000	t_2 168 695	t_2 73 206	t_2 45 73	t_2 157 897	t_2 16383 21216	t_2 40231 65280	t_2 157 255	t_2 23296 65282	t_2 16 46	t_1 0 100	t_1 0 156 331
t_3 18 41	t_3 0 3	t_3 0 95	t_3 0 3	t_2 46345 539723	t_3 1 611	t_3 0 48283600	t_3 0 243	t_3 0 2	t_3 0 2	t_3 0 4	t_2 2146685 4294952	t_3 0 562	t_3 0 32	t_3 0 64	t_3 0 64	t_3 28 16011	t_3 28 404	t_3 28 40	t_3 28 16011	t_3 4480061660560 5600672001680	t_3 2206391 2410851	t_3 35 52	t_3 0 14	t_3 220639 241085	t_3 0 16	t_3 173 184	t_3 0 359976000	t_3 0 700	t_3 0 152	t_3 0 66	t_3 0 35	t_3 0 153	t_3 0 8192	t_3 0 8666	t_3 0 38893	t_3 0 152	t_3 0 23043	t_3 0 6	t_3 125 255	t_3 0 150
t_4 78 85	t_4 22218 65535	t_4 96 255	t_4 7 9	t_4 4 44997	t_4 1 611	t_4 0 48283600	t_4 0 243	t_4 0 2	t_4 0 2	t_4 0 4	t_4 443920 484435	t_4 0 562	t_4 0 32	t_4 200 255	t_4 200 255	t_4 28 16011	t_4 28 404	t_4 28 40	t_4 28 16011	t_4 1120028000392200 1943244800168000	t_4 363369 383369	t_4 0 14504	t_4 0 14	t_4 0 7015	t_4 0 16	t_4 268 346	t_4 0 359976000	t_4 0 700	t_4 0 152	t_4 0 66	t_4 0 35	t_4 0 153	t_4 45260 65335	t_4 38235 55845	t_4 0 38893	t_4 0 152	t_4 22769 32769	t_4 0 6	t_4 0 100	t_4 0 150
t_5 92 100	t_5 0 92	t_5 0 92	t_5 0 92	t_3 54671 57893	t_3 1 611	t_3 0 48283600	t_3 0 243	t_3 0 2	t_3 0 2	t_3 0 4	t_3 443920 484435	t_3 0 562	t_3 0 32	t_3 0 64	t_3 0 64	t_3 28 16011	t_3 28 404	t_3 28 40	t_3 28 16011	t_5 2240016800560000 4480061660560	t_5 452969 457471	t_5 0 14504	t_5 0 14	t_5 0 7015	t_5 0 16	t_5 0 359976000	t_5 0 1432816000	t_5 0 700	t_5 0 152	t_5 0 66	t_5 0 35	t_5 0 153	t_5 60328 65335	t_5 0 8666	t_5 0 38893	t_5 0 152	t_5 0 23043	t_5 0 6	t_5 80000 87000	t_5 0 150
t_6 125 231	t_6 0 125	t_6 0 125	t_6 0 125	t_4 0 57893	t_4 1 611	t_4 0 48283600	t_4 0 243	t_4 0 2	t_4 0 2	t_4 0 4	t_4 443920 484435	t_4 0 562	t_4 0 32	t_4 0 64	t_4 0 64	t_4 28 16011	t_4 28 404	t_4 28 40	t_4 28 16011	t_6 5600224000560000 1120067200560000	t_6 0 1069186656	t_6 0 14504	t_6 0 14	t_6 0 7015	t_6 0 16	t_6 0 359976000	t_6 0 1432816000	t_6 0 700	t_6 0 152	t_6 0 66	t_6 0 35	t_6 0 153	t_6 0 8192	t_6 0 8666	t_6 0 38893	t_6 0 152	t_6 0 23043	t_6 0 6	t_6 0 100	t_6 0 150

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shimony E., Tsarfati O. Chatting our way into creating a polymorphic malware. *Identity Security and Access Management Leader. CyberArk*. URL:https://www.cyberark.com/resources/threat-research/chatting-our-way-into-creating-a-polymorphic-malware.

2. Фесьоха В., Кисиленко Д. Модель визначення інваріантної компоненти в поведінці шкідливого програмного забезпечення на основі інтеграції нечіткої логіки та генетичних алгоритмів. *Системи і технології зв’язку, інформатизації та кібербезпеки*. 2024. Vol. 1, no. 6. P. 232–242. URL: https://doi.org/10.58254/viti.6.2024.19.232.

3. Хандрос А. В., Ткач В. М. Застосування алгоритмів машинного навчання для детекції шкідливого програмного забезпечення через аналіз PE-заголовків. *Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених*. 2024. С. 179–181.

4. Domain adaptation-based deep learning framework for android malware detection across diverse distributions / S. Xiong et al. *Artificial intelligence advances*. 2024. Vol. 6, no. 1. P. 13–24. URL: https://doi.org/10.30564/aia.v6i1.6718.

5. MORPH: towards automated concept drift adaptation for malware detection / M. Alam et al. *ArXiv preprint arxiv:2401.12790*. 2024. URL: https://openreview.net/forum?id=Y5OSp4yq6X.

6. Varikuti H., Vatsavayi V. K. A hybrid malware detection framework with drift adaptation for timestamped data. *Journal of theoretical and applied information technology*. 2024. Vol. 102, no. 9. P. 4137–4144. URL: https://www.jatit.org/volumes/Vol102No9/35Vol102No9.pdf.

7. A lightweight malware detection model based on knowledge distillation / C. Miao et al. *Mathematics*. 2024. Vol. 12, no. 24. P. 4009. URL: https://doi.org/10.3390/math12244009 (date of access: 01.03.2025).

8. Semantic data representation for explainable windows malware detection models / P. Švec et al. 2024. URL: https://doi.org/10.13140/RG.2.2.29257.76648.

9. Фесьоха В. В., Кисиленко Д. Ю. Адаптивний підхід до виявлення шкідливого програмного забезпечення з властивістю самомодифікації. *IV Міжнародна науково-технічна конференція – ВІТІ імені Героїв Крут – 2024 «Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку»*. 2024. С. 143. URL: https://doi.org/10.61929/viti.mntk.4.2024.

10. ML-Based NIDS Datasets. *School of Information Technology and Electrical Engineering*. URL: https://staff.itee.uq.edu.au/marius/NIDS_datasets/#RA6.

11. Virus (Generic) | F-Secure Labs. *Schutz für digitale Momente | F-Secure*. URL: https://www.f-secure.com/v-descs/virus-w32-generic.shtml.

DOI: 10.58254/viti.7.2025.19.213

УДК 004.8

Фомкін Д. В. ORCID: 0000-0003-0128-9355 (ВІТІ ім. Героїв Крут)
Шемендюк О. В. ORCID: 0000-0002-5594-2973 (ВІТІ ім. Героїв Крут)
Ткач В. О. ORCID: 0000-0003-0013-7368 (ВІТІ ім. Героїв Крут)
Балан Д. Д. ORCID: 0000-0002-6714-8718 (ВІТІ ім. Героїв Крут)

АНАЛІЗ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО КОДУ В ФАЙЛАХ PDF: ВИБІР ОПТИМАЛЬНОЇ МОДЕЛІ

В останні роки спостерігається різке зростання складних кібератак із використанням зловмисно закодованих документів, оскільки збільшуються об'єми інформації, яка передається. Файли, які виконуються, прикріплені до електронних листів або вебсторінок, можуть бути небезпечними, про що відомо більшості користувачів Інтернету. Тим не менш, документи є корисним інструментом для розповсюдження шкідливого програмного забезпечення, оскільки люди не знають про них. Поширення зловмисно закодованих документів зі збільшенням кількості передачі інформації призвело до зростання кількості складних атак. Файли формату портативних документів (Portable Document Format, далі – PDF) стали основним вектором атаки шкідливого програмного коду завдяки їх адаптивності та широкому використанню. Виявлення шкідливого програмного коду у файлах PDF є складним завданням через його здатність включати різні шкідливі елементи, такі як вбудовані сценарії, експлойти та шкідливі URL-адреси. У цій статті проведено аналіз у підходах машинного навчання та представлено порівняльний аналіз методів машинного навчання (далі – ML), включаючи Naive Bayes (далі – NB), K-Near Neighbor (далі – KNN), Average One Dependency Estimator (далі – A1DE), Random Forest (далі – RF) та Support Vector Machine (далі – SVM) для виявлення шкідливих PDF-файлів. Це дослідження базується на різних типах критеріїв тестування, з відсотковим поділом та K-кратною перехресною перевіркою, для отримання більш об'єктивних результатів. Результати дослідження підкреслюють ефективність моделей машинного навчання у точному виявленні шкідливого програмного коду в PDF-файлах, визначать найбільш ефективні методи та надають уявлення про розробку надійних систем для захисту від зловмисних дій. Подальші напрямки досліджень в області виявлення шкідливих PDF-файлів повинні бути зосереджені на дослідженні методів глибокого навчання, що може підвищити продуктивність і точність моделей.

Ключові слова: *кібербезпека, шкідливий програмний код, PDF-файл, машинне навчання, JavaScript.*

D. Fomkin, O. Shemendyk, V. Tkach, D. Balan. Comparative analysis of machine learning models for malware detection in PDF: evaluation of training and testing criteria

In recent years, there has been a sharp increase in sophisticated cyberattacks using maliciously encrypted documents as the amount of information transmitted increases. Executable files attached to emails or web pages can be dangerous, as most internet users are aware of. Nevertheless, documents are a useful tool for spreading malware because people are unaware of them. The spread of maliciously encrypted documents with an increase in the number of information transfers has led to an increase in the number of sophisticated attacks. Portable Document Format (PDF) files have become the main attack vector of malicious code due to their adaptability and widespread use. Detecting malicious code in PDF files is challenging due to its ability to include various malicious elements, such as embedded scripts, exploits and malicious URLs. This article analyzes machine learning approaches and provides a comparative analysis of machine learning (ML) methods, including Naive Bayes (NB), K-Near Neighbor (KNN), Average One Dependency Estimator (A1DE), Random Forest (RF), and Support Vector Machine (SVM) to detect malicious PDF files. This study is based on different types of testing criteria, with percentage division and K-fold cross-validation, to obtain more objective results. The results of the study highlight the effectiveness of machine learning models in accurately detecting malicious code in PDF files, identify the most effective methods, and provide insight into the development of robust systems to protect against malicious activities. Further research in the field of detecting malicious PDF files should focus on investigating deep learning methods that can improve the performance and accuracy of models.

Keywords: *cybersecurity, malware, PDF, machine learning, JavaScript.*

Постановка задачі. В останні роки спостерігається різке зростання складних кібератак з використанням зловмисно закодованих документів, оскільки збільшуються об'єми передачі інформації. Основним вектором кібератак з використанням програмного коду, які були виявлені, є файли формату PDF, який легко адаптується порівняно з іншими форматами

документів. Шкідливі PDF-файли часто містять JavaScript або бінарні скрипти, які використовують слабкі сторони безпеки для виконання зловмисних дій [1]. Adobe Acrobat Reader виявив величезну кількість вразливостей в 2017 році. Кожне програмне забезпечення для читання має певні недоліки, і шкідливий PDF-файл може ними скористатися [2]. Поява більш сучасних технологій, що не виконуються, і методів атак на основі файлів зробила захист PDF більш складним, оскільки зловмисні PDF-файли зазвичай досліджують вектори зараження у ворожих обставинах [3; 4].

Вкрай важливе виявлення шкідливого програмного коду в PDF з кількох причин. По-перше, це допомагає захистити користувачів від несанкціонованого доступу або запуску небезпечних файлів, захищаючи їх від потенційної шкоди. По-друге, вразливості в програмному забезпеченні для читання PDF та інших програмах можуть бути використані за допомогою шкідливих PDF-файлів, що робить критично важливим виявлення та запобігання таких кібератак. По-третє, PDF-файли часто містять конфіденційну інформацію, яка може бути викрадена, що призводить до фінансових втрат, витоку даних або крадіжки особистих даних.

Отже, існує нагальна потреба у розробці ефективних методів захисту від складних атак з використанням шкідливого програмного коду у PDF-файлах.

Аналіз останніх досліджень і публікацій. Використовуючи різні моделі машинного навчання, було проведено кілька різновидів досліджень з метою виявлення шкідливого програмного забезпечення в PDF.

Ах Реум Канг та інші науковці описали використання PDF у 2019 році [5]. Вони дали ретельний аналіз структури та вмісту JavaScript у PDF-файлі з вбудованим XML. Потім були створені різноманітні функції, такі як методи кодування конфігурації матеріалу та змінних, таких як розмір файлу, ключові слова, версії та рядки, які можуть прочитати JavaScript.

Підходи до навчання стійких класифікаторів шкідливих програм PDF, що використовують спостережувальні функції стійкості, були описані Ю. Чен та іншими науковцями у 2019 році [6]. У роботі досліджено, що класифікатор повинен ідентифікувати шкідливий програмний код в PDF-файлі як шкідливий, вони демонструють, як точно оцінити найгіршу поведінку класифікатора шкідливого програмного коду щодо певних властивостей стійкості.

Наукові роботи Wepawet [7], Laskov та інші [8] були зосереджені на небезпечному JavaScript, який був представлений у шкідливому програмному забезпеченні формату Portable Document Format. Тут підходи машинного навчання були використані для розробки класифікаторів шкідливих програмних кодів у PDF.

Ес Джей Хітан та інші [9] запропонували атрибути, виходячи з лексичних особливостей скриптів JavaScript, а також функцій, констант, об'єктів, методів і ключових слів. Джей Занг та інші [10] об'єднали кількість об'єктів JavaScript, кількість сторінок та дані фільтрації потоку зі структурою PDF, характеристиками сутностей, інформацією метаданих та статистикою вмісту.

Після виявлення того, що шкідливий JavaScript функціонує інакше, ніж законний код JavaScript, Д. Лю, Х. Ван і А. Ставру [12] запропонували контекстно-залежний підхід. Цей підхід передбачає використання оригінального коду JavaScript як вхідних даних для функції "eval" для відкриття PDF-файлу, уважно відстежуючи будь-яку незвичайну поведінку на основі наведених інструкцій.

За даними Еррера-Сілва Я. А. й Ернандес-Альварес М. [13], кібератаки з використанням програм-вимагачів зросли за останні десять років, викликавши велике занепокоєння серед організацій.

Дхаларія М. і Гандотра Е. представили гібридний метод виявлення і класифікації шкідливих програм Android [14]. Запропонований метод поєднує методи статичного та

динамічного аналізу для ефективного виявлення шкідливих додатків та класифікації їх у різні сімейства шкідливих програм. Автори навчають моделі машинного навчання для виявлення шкідливих програм і класифікації сімейства, використовуючи функції, взяті як зі статичної, так і з динамічної поведінки додатків Android. Експериментальні результати демонструють ефективність гібридного підходу в точному виявленні та класифікації шкідливих програм Android, тим самим сприяючи сфері мобільної безпеки та допомагаючи запобігати шкідливим діям на пристроях Android.

Всі розглянуті вище дослідження мають один спільний недолік – обмеження сфери використання за типом загроз.

Таким чином, **основною метою** цього дослідження є розробка універсальної моделі виявлення шкідливого програмного коду, здатної захистити системи від шкідливих дій, спричинених шкідливими PDF-файлами, що необхідно для оперативного попередження та реагування на кіберінциденти в мережі, шляхом аналізу методів машинного навчання для виявлення шкідливого програмного коду в PDF-файлах.

Виклад основного матеріалу. У цьому дослідженні представлено аналіз деяких моделей машинного навчання, а саме: Average One Dependency Estimator (A1DE), K-Nearest Neighbor (KNN), Support Vector Machine (SVM) [15], Naive Bayes (NB) та Random Forest (RF) [16]. Це дослідження зосереджено на порівнянні різних моделей машинного навчання та критеріїв навчання моделей для пошуку кращого рішення для виявлення шкідливого програмного коду в PDF-файлах. Моделі машинного навчання включають A1DE, NB, KNN, RF та SVM, тоді як критерії навчання включають процентне розділення з 70 % та 30 % для навчання та тестування відповідно, а також 10-кратну перехресну перевірку. Загальна схема дослідження представлена на рисунку 1.

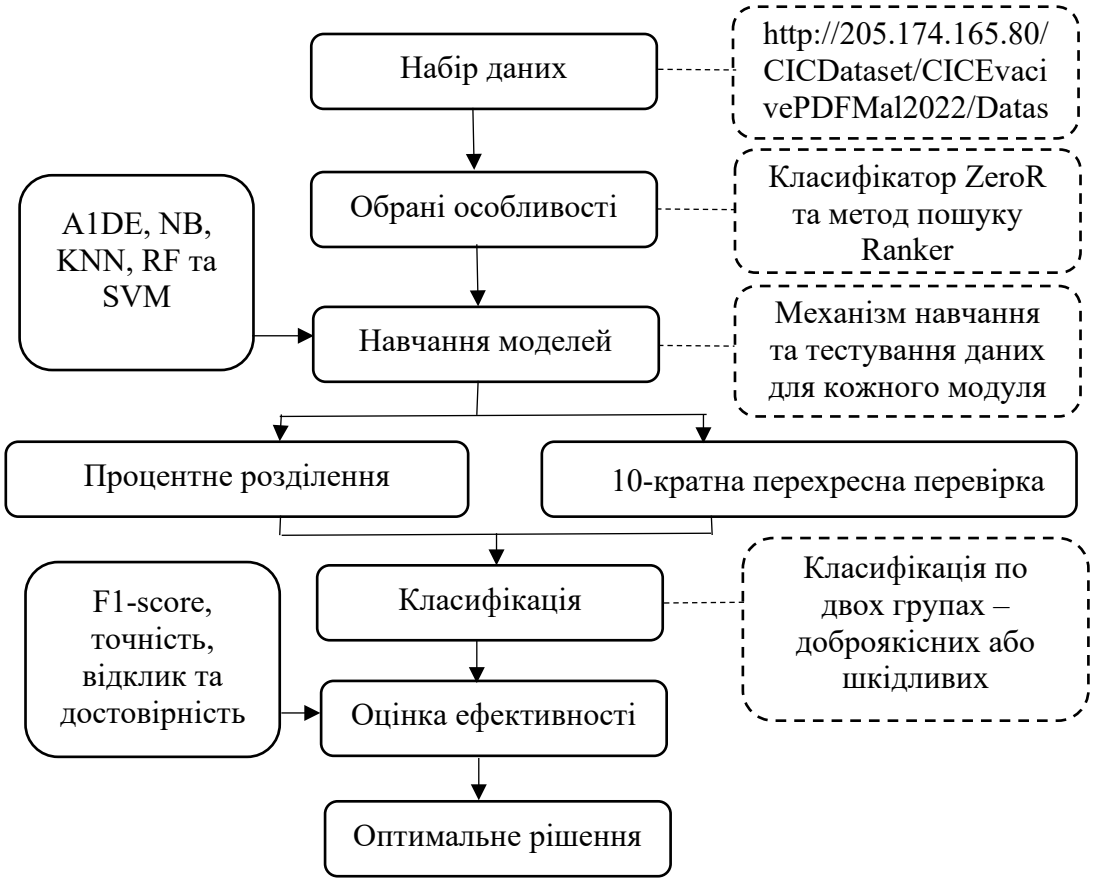


Рис. 1. Узагальнена схема дослідження

Пояснення набору даних та попередня обробка

Було взято набір даних про виявлення шкідливого програмного коду у файлах формату PDF від Канадського інституту кібербезпеки (https://www.unb.ca/cic/datasets/pdfmal-2022.html). Набір даних має 33 характеристики, 32 з яких є незалежними, а 1 з них – залежна. Перші 11 характеристик були усунені, оскільки вони не мали ефекту на етапі аналізу. Ці характеристики в сукупності називаються загальними ознаками, і вони містять наступну інформацію: шифрування, розмір метаданих, номер сторінки, заголовок, номер зображення, текст, номер об'єкта, шрифтові об'єкти, кількість вбудованих файлів та середній розмір усіх вбудованих носіїв – це всі фактори, які слід враховувати. Дані очищаються і не потребують подальшої попередньої обробки.

Для подальшого аналізу виникає необхідність вибрати деякі особливості, які найкращим чином підходять для аналізу. З цією метою ми вибираємо деякі особливості зі структурних особливостей, які визначають PDF-файл, з точки зору його структури, що вимагає більш ретельної обробки та розкриває інформацію про загальні рамки PDF-файлу.

Було використано методи Classifier Attribute Evaluator, що включають в себе класифікатор ZeroR та метод пошуку Ranker для отримання таких функцій. Для оцінки точності кількість складок, що використовуються, дорівнює 5. Вибрані функції ранжуються як вибрані атрибути: "21, 7, 8, 10, 6, 5, 4, 3, 2, 9, 11, 20, 18, 19, 12, 17, 16, 15, 14, 13, 1:21".

У такому порядку присутні такі атрибути: кольори, шифрування, JS, XFA startxref, трейлер, xref, кінцевий потік, потік, endobj, запуск, OpenAction, AA, EmbeddedFile, JBIG2Decode, Acroform, pageno, ObjStm, JavaScript, RichMedia та obj.

У таблиці 1 представлено обрані ознаки з їх описом.

Таблиця 1

№	Ознака	Опис
1	Xref	Розмір потоку, оскільки шкідливий код може бути прихований у потоках
2	Trailer	Number of trailers inside the PDF
3	Pageno	Кількість трейлерів у PDF-файлі. Шкідливі PDF-файли часто містять менше сторінок – часто лише одну порожню сторінку – тому, що їм байдуже, як представлено їхній матеріал
4	Stream	Це показує, скільки послідовностей двійкових даних міститься в PDF-файлі
5	Encrypt	Ця функція вказує на те, чи захищений PDF-файл паролем
6	Objstm	Потоки, які містять додаткові об'єкти
7	Endstream	Ключові слова, що означають припинення трансляції
8	JS	Декілька об'єктів, що охоплюють код JavaScript
9	Obj	Це може бути ознакою спроби заплутатися
10	JavaScript	Це показує, як багато речей включає код JavaScript, найпоширеніший тип характеристики
11	AA	Визначає конкретну дію при інциденті
12	OpenAction	При відкритті PDF-файлу ця властивість визначає, яку дію слід виконати. Більшість шкідливих PDF-файлів, які часто зустрічаються, використовують цю функцію в поєднанні з JavaScript
13	endobj	PDF-файли дозволяють використовувати широкий спектр методів обфускації, включаючи обфускацію рядків у шістнадцятковій, вісімковій тощо, які часто використовуються в стратегіях ухилення
14	Acroform	Поля форм у PDF-файлах, створених за допомогою Acrobat, містять сценарії, які хакери можуть використати проти вас
15	Startxref	Численні ключові слова, які включають "startxref", вказують на місце початку таблиці Xref
16	JBIG2Decode	JBig2Decode – популярний фільтр для кодування небезпечних даних. Які елементи мають найбільшу кількість вкладених фільтрів? Вкладені фільтри

		можуть перешкоджати декодуванню та пропонувати ухилення
17	Richmeddia	Кількість мультимедійних ключових слів показує кількість флеш-пам'яті та вбудованих медіафайлів
18	Launch	Слово "launch" стосується акту виконання команди або програми
19	EmbeddedFile	Файли PDF можуть вкладати або вбудовувати інші речі, такі як документи Word, фотографії тощо, які можна використовувати зловмисно
20	XFA	XFA, архітектура XML-форм, що дозволяє використовувати технології сценаріїв, що можуть використовувати зловмисники, можна знайти в деяких PDF-файлах
21	Color	У PDF-файлі використовується багато кольорових схем
22	Class	Віднесіть до категорії доброякісних або шкідливих

Завдяки своїй зручності, PDF став форматом документів, що найбільш часто використовується протягом усього часу. На жаль, розповсюдженість PDF-файлів та їх складні можливості дозволили зловмисникам використовувати їх різними способами. Зловмисник може скористатися кількома важливими властивостями PDF для поширення шкідливого корисного навантаження. Цей набір даних, який включає 10 019 записів, в яких 5551 шкідливий і 4468 є доброякісними, які схильні ухилятися від взаємно значущих ознак, виявлених у кожному класі, збирає ці шкідливі дані та інформацію.

Це дослідження зосереджено на двох різних типах аналізу тестування. Один заснований на відсотковому розщепленні набору даних, де ми використовували 70 % даних для навчання, а решта 30 % даних для тестування. Другий метод – K-кратна перехресна перевірка, в якій ми вибрали значення K як 10. У цьому дослідженні представлено порівняння цих методів тестування. Методи машинного навчання порівнюються за допомогою стандартних показників оцінки, таких як F1-score, точність, відгук та достовірність. Ці показники можна розрахувати за формулами (1)–(4):

$$\text{Точність} = \frac{TP}{TP+FP}; \tag{1}$$

$$\text{Чутливість} = \frac{TP}{TP+FN}; \tag{2}$$

$$F1 = \frac{2*\text{Точність}*\text{Чутливість}}{\text{Точність}+\text{Чутливість}}; \tag{3}$$

$$\text{Достовірність} = \frac{TP+TN}{TP+TN+FP+FN}, \tag{4}$$

де $F1$ – $F1$-score (ефективність прогнозування);

TP – істинні позитивні значення розрахунків (true positive);

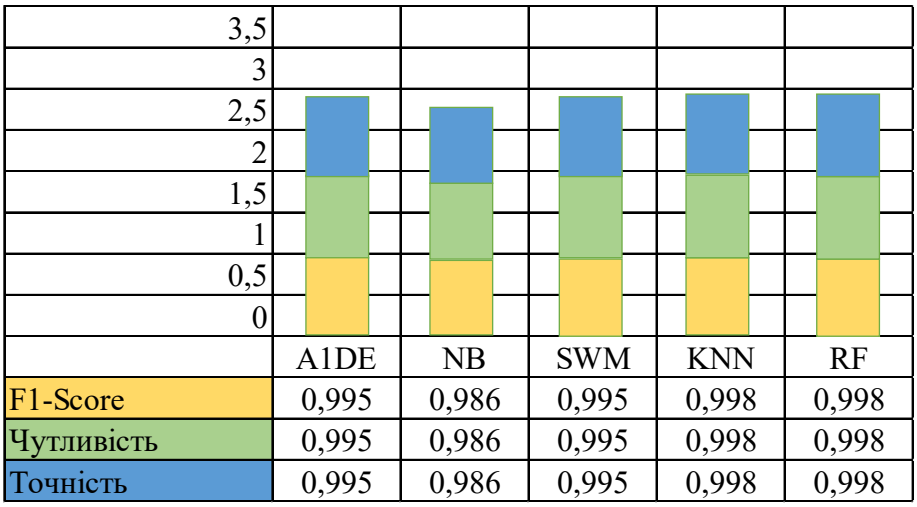
FP – помилкові позитивні значення розрахунків (false positive);

TN – істинно негативні розрахунків (true negative);

FN – помилково негативні значення розрахунків (false negative).

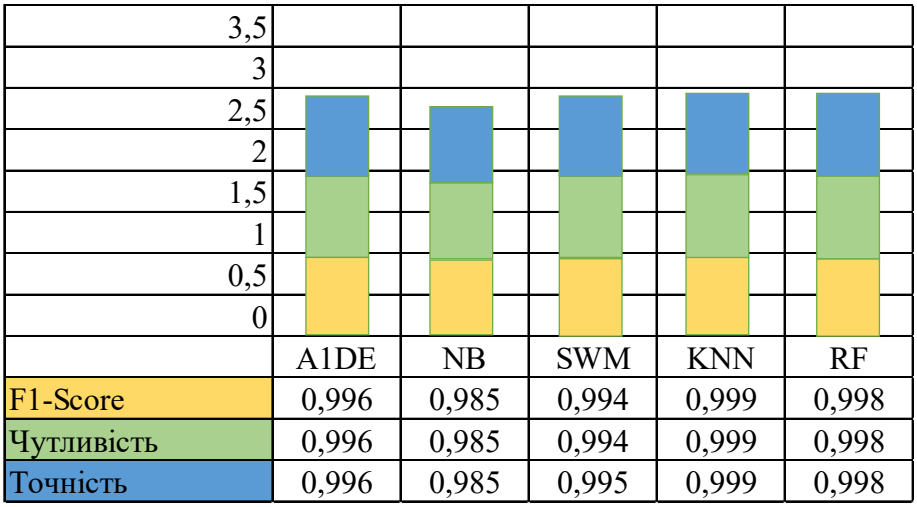
Аналіз результатів. Проведемо аналіз за допомогою вищезгаданих моделей машинного навчання, включаючи A1DE, NB, SVM, KNN та RF. Ці моделі оцінюються за допомогою F1-score (ефективність прогнозування), точності, чутливості та достовірності. Для відсоткового поділу було використано 70 % даних для навчання, а 30 % даних для тестування. У моделі K-кратної перевірки було обрано значення K як 10. Рисунок 2 представляє точність, чутливість та F1-score кожної техніки з використанням першого

критерію тестування, який становить 70 % та 30 % даних для навчання та тестування відповідно. На рисунку 3 представлено результати для 10-кратної перехресної перевірки.



	A1DE	NB	SWM	KNN	RF
F1-Score	0,995	0,986	0,995	0,998	0,998
Чутливість	0,995	0,986	0,995	0,998	0,998
Точність	0,995	0,986	0,995	0,998	0,998

Рис. 2. Аналіз точності, чутливості та F1-Score з використанням критерію розподілу відсотків



	A1DE	NB	SWM	KNN	RF
F1-Score	0,996	0,985	0,994	0,999	0,998
Чутливість	0,996	0,985	0,994	0,999	0,998
Точність	0,996	0,985	0,995	0,999	0,998

Рис. 3. Аналіз точності, чутливості та F1-Score за допомогою 10-кратної перехресної перевірки

Враховуючи критерії тестування, цей аналіз показує, що використовувати краще 10-кратну перехресну перевірку, а не поділ даних 70 % і 30 % для навчання та тестування. Крім того, KNN перевершує інші моделі, що використовуються за 10-кратною перехресною перевіркою. Використовуючи критерій відсоткового поділу, KNN і RF показують однакову продуктивність.

На рисунках 4 та 5 окремо представлений аналіз достовірності кожної моделі, що використовується з використанням обох критеріїв тестування, а саме з відсотковим поділом і K-кратною перехресною перевіркою.

В обох випадках KNN перевершує інші моделі з кращою точністю 99,8499 % за критеріями тестування відсоткового поділу та 99,8599 % за критеріями K-кратної перехресної перевірки. Цей аналіз показує, що в поточному сценарії K-кратна перехресна перевірка є кращими критеріями навчання та тестування для моделі навчання.

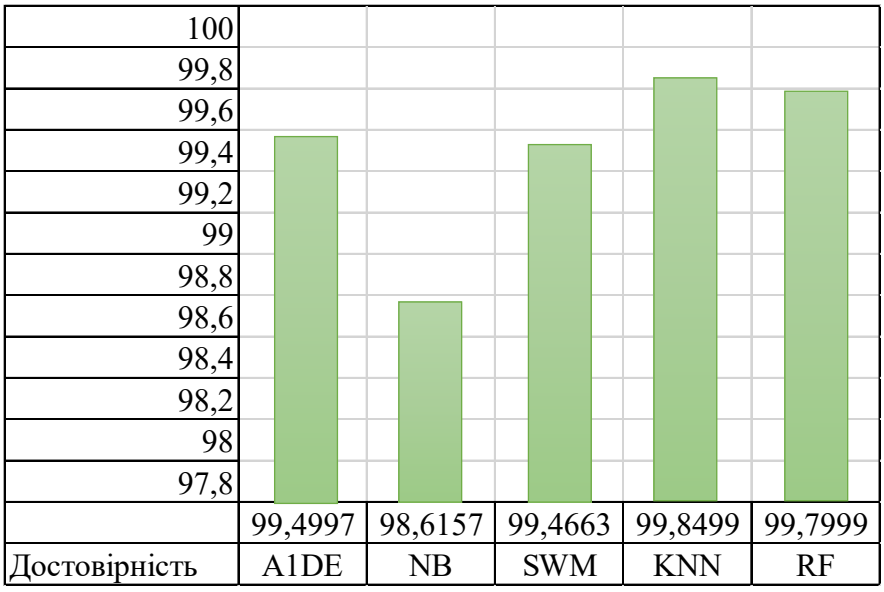


Рис. 4. Аналіз достовірності з використанням критеріїв тестування відсоткового поділу

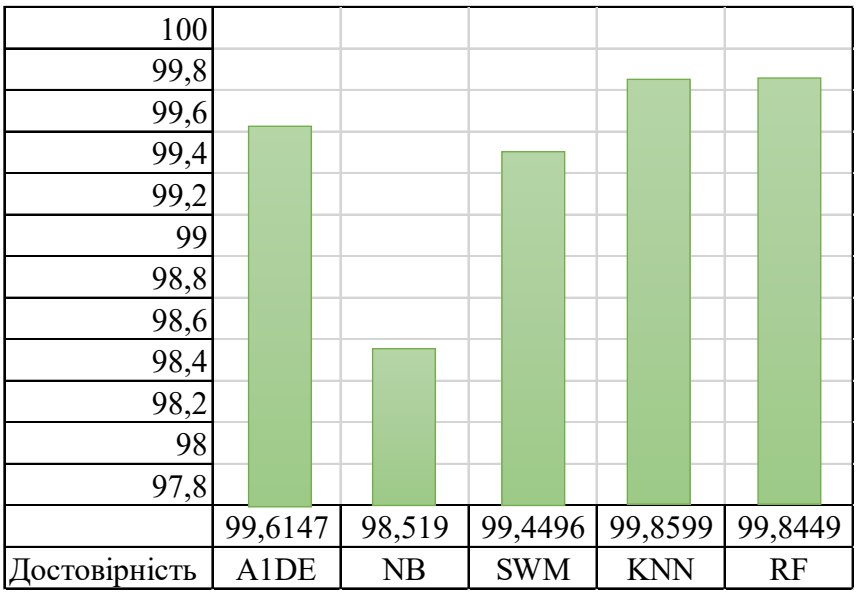


Рис. 5. 10-точковий аналіз з використанням 10-кратних критеріїв перехресної перевірки

На основі різноманітних вхідних значень, моделі машинного навчання прогнозують вихідні значення. Одним із найпростіших алгоритмів машинного навчання є KNN, який зазвичай використовується для класифікації. Він класифікує точку даних на основі того, як класифікуються її сусіди. Lazy Learner (навчання на основі екземплярів) – це інша назва KNN. Він нічого не вчиться протягом усього періоду навчання. Жодна дискримінаційна функція не генерується за допомогою навчальних даних. Іншими словами, ніякої підготовки не потрібно. Він лише черпає навчання зі збереженого набору навчальних даних для прогнозування в режимі реального часу. Техніка KNN набагато швидша, ніж інші розглянуті техніки, оскільки інші моделі вимагають навчання, тоді як техніка KNN не вимагає навчання раніше створення прогнозів, і свіжі дані можуть бути включені без зусиль, не впливаючи на точність методів.

В цілому, отримані результати показують, що моделі машинного навчання перевершують обидва методи оцінки, демонструючи їх ефективність у правильному

прогнозуванні цільової змінної. Оскільки розбиття даних на розділи та навчання моделі відрізняються в усіх двох методах, значення точності, отримані відсотковим поділом та 10-кратною перехресною перевіркою, різняться не суттєво. Однак відмінні рейтинги точності моделей демонструють їх потенціал для точних прогнозів у нинішній ситуації.

Результати роботи надають уявлення про ефективність моделей машинного навчання для виявлення шкідливих програм у PDF-файлах. Порівняльний аналіз та оцінка ефективності сприяють розробці надійних систем захисту від шкідливих дій, пов'язаних із шкідливим програмним забезпеченням PDF. Дослідження демонструє ефективність моделей машинного навчання у точному виявленні шкідливого програмного забезпечення PDF та надає уявлення про розробку надійних систем для захисту від шкідливих дій. Отримані дані свідчать про те, що KNN є перспективною моделлю для виявлення шкідливих програм PDF, але для перевірки та покращення результатів можуть знадобитися подальші дослідження та експерименти.

Висновки. У цій роботі було проведено порівняльний аналіз моделей машинного навчання для виявлення шкідливого коду в PDF-файлах, зосередивши увагу на моделях A1DE, NB, SVM, KNN та RF. При цьому використовувався набір даних, отриманий від Канадського інституту кібербезпеки та два критерії тестування: процентне ділення та 10-кратна перехресна перевірка. Оцінка базувалася на показниках точності, запам'ятовування, оцінки F1 та точності. Результати показали, що KNN перевершив інші моделі, досягнувши точності 99,8599 % за допомогою 10-кратної перехресної перевірки. Ці результати підкреслюють ефективність моделей машинного навчання у точному виявленні шкідливого програмного забезпечення PDF та надають уявлення про розробку надійних систем для захисту від шкідливих дій у файлах PDF. Дослідження сприяє посиленню заходів кібербезпеки, надаючи надійну модель для виявлення шкідливого програмного коду в PDF-файлах, яка може допомогти запобігти розповсюдженню витончених атак за допомогою зловмисно закодованих документів.

Подальші напрямки досліджень в області виявлення шкідливого програмного коду в PDF-файлах повинні бути зосереджені на декількох ключових областях, а саме дослідження методів глибокого навчання, таких як згорткові нейронні мережі (convolutional neural networks) та рекурентні нейронні мережі (recurrent neural networks) та можливості підвищення продуктивності і точності моделей. Включення методів обробки природної мови (natural language processing) для аналізу текстового вмісту в PDF-файлах, що може надати цінну інформацію для виявлення шкідливого програмного коду. Крім того, розробка систем, які можуть аналізувати PDF-файли в режимі реального часу та своєчасно виявляти нові загрози, була б дуже корисною.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Y. S. Jeong, J. Woo and A. R. Kang. Malware detection on byte streams of pdf files using convolutional neural networks // Security and Communication Networks. 2019. Vol. 2019. Pp. 144–152. DOI: 10.1155/2019/8485365.

2. A. Falah, S. R. Pokhrel, L. Pan and A. de Souza-Daw. Towards enhanced PDF maldocs detection with feature engineering: Design challenges // Multimedia Tools and Applications. 2022. Vol. 81, no. 28. Pp. 41103–41130. DOI: 10.1007/s11042-022-11960-x.

3. W. Xu, Y. Qi and D. Evans. "Automatically evading classifiers", in Proc. of the 23rd Annual Network and Distributed System Security Symp., San Diego, California, vol. 2016, no. February, pp. 21–24, 2016.

4. S. Sibi Chakkaravarthy, D. Sangeetha and V. Vaidehi. A survey on malware analysis and mitigation techniques. // Computer Science Review. 2019. Vol. 32. Pp. 1–23. DOI: 10.1016/j.cosrev.2019.01.002.

5. A. R. Kang, Y. S. Jeong, S. L. Kim and J. Woo. Malicious PDF detection model against adversarial attack built from benign PDF containing JavaScript // Applied Sciences. 2019. Vol. 9, no. 22. Pp. 4764. DOI: 10.3390/app9224764.

6. Y. Chen, S. Wang, D. She and S. Jana. "On training robust {PDF} malware classifiers," in 29th USENIX Security Symp. (USENIX Security 20), Boston, USA, pp. 2343–2360, 2020.

7. M. Cova, C. Kruegel and G. Vigna. "Detection and analysis of drive-by-download attacks and malicious JavaScript code", in Proc. of the 19th Int. Conf. on World Wide Web, North Carolina, USA, pp. 281–290, 2010.

8. P. Laskov and N. Srndic. "Static detection of malicious JavaScript-bearing PDF documents", in Proc. of the 27th Annual Computer Security Applications Conf., Orlando, Florida, USA, pp. 373–382, 2011.

9. S. J. Khitan, A. Hadi and J. Atoum. PDF forensic analysis system using YARA // International Journal of Computer Science and Network Security. 2017. Vol. 17, no. 5. Pp. 77–85.

10. J. Zhang. MLPdf: An effective machine learning based approach for PDF malware detection. 2018. Pp. 1–6.

11. S. S. Khan, M. Khan, S. Technology and R. Naseem. Challenges in opinion mining, comprehensive // A Science and Technology Journal, 2018. Vol. 33, no. 11. Pp. 123–135.

12. D. Liu, H. Wang and A. Stavrou. "Detecting malicious JavaScript in pdf through document instrumentation", in 2014 44th Annual IEEE/IFIP Int. Conf. on Dependable Systems and Networks, Atlanta, USA, pp. 100–111, 2014.

13. J. A. Herrera-Silva and M. Hernández-Álvarez. Dynamic feature dataset for ransomware detection using machine learning algorithms // Sensors. 2023. Vol. 23, no. 3. Pp. 1053. DOI: 10.3390/s23031053.

14. M. Dhalaria and E. Gandotra, "A hybrid approach for android malware detection and family classification," International Journal of Interactive Multimedia and Artificial Intelligence, vol. 6, no. 6, pp. 174–188, 2020. DOI:10.9781/ijimai.2020.09.001

15. M. Deore and U. Kulkarni. Mdfrcnn: Malware detection using faster region proposals convolution neural network // International Journal of Interactive Multimedia and Artificial Intelligence. 2022. Vol. 7, no. 4. Pp. 146–162.

16. T. Tsafrir, A. Cohen, E. Nir and N. Nissimю. Efficient feature extraction methodologies for unknown MP4-malware detection using machine learning algorithms // Expert Systems with Applications. 2023. Vol. 219. Pp. 119615. DOI: 10.1016/j.eswa.2023.119615.

DOI: 10.58254/viti.7.2025.20.222

УДК. 621.391

Хоменко П. В. ORCID: 0000-0002-8543-1971 (ВІТІ ім. Героїв Крут)
канд. техн. наук, професор Радзівілов Г. Д. ORCID: 0000-0002-6047-1897 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Ільїнов М. Д. ORCID: 0009-0008-6945-3354 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СУЧАСНИХ РАДІОЗАСОБІВ КЛАСУ MANET

У статті представлено результати комплексного дослідження функціональних можливостей, технічних характеристик та оперативних обмежень тактичних радіостанцій Silvus StreamCaster SC4400 у контексті їх застосування в умовах динамічного електромагнітного середовища. Проаналізовано вплив архітектурних особливостей системи (конфігурація MIMO 4×4) на її функціональні параметри, включаючи пропускну здатність, енергоефективність та стійкість до радіоелектронної протидії. Здійснено компаративний аналіз Silvus SC4400 з аналогічними системами (Persistent MPU5 та TrellisWare TSM) на основі репрезентативної методологічної бази, що інтегрує результати емпіричних випробувань та математичного моделювання.

Застосовано багатокритеріальний підхід до оцінювання ефективності тактичних систем зв’язку, ідентифіковано ключові переваги SC4400, зокрема: розширений частотний діапазон (300 МГц – 6 ГГц), високу пропускну здатність (до 100+ Мбіт/с) та низьку канальну затримку (7 мс на один хоп), що забезпечує оптимальні характеристики для передачі мультимедійного контенту в реальному часі. Водночас виявлено функціональні обмеження системи, включаючи відсутність інтегрованої обчислювальної платформи, недостатню стійкість до інтенсивної радіоелектронної протидії та суттєві обмеження антенних систем у контексті енергетичного потенціалу та адаптивності діаграми направленості. Науково обґрунтовано оптимальні сценарії застосування досліджуваних систем залежно від їх техніко-експлуатаційних характеристик та специфіки оперативного середовища. Запропоновано перспективні напрями вдосконалення Silvus SC4400 з урахуванням виявлених обмежень та сучасних тенденцій розвитку тактичних комунікаційних технологій.

Ключові слова: *тактичні системи зв’язку, MANET, Silvus StreamCaster SC4400, MIMO-технології, радіоелектронна боротьба, радіоелектронна розвідка, завадостійкість, пропускна здатність, діаграма направленості.*

P. Khomenko, H. Radzivilov, M. Ilinov. Analysis of the functionality of Manet tactical radio systems

This article presents the results of a comprehensive study on the functionality, technical specifications, and operational limitations of the Silvus StreamCaster SC4400 tactical radio, particularly concerning its application within dynamic electromagnetic environments. The impact of the system's architectural features (4x4 MIMO configuration) on its functional parameters, including throughput, energy efficiency, and resilience against electronic warfare (EW), is analyzed. A comparative analysis of the Silvus SC4400 with analogous systems (Persistent MPU5 and TrellisWare TSM) was performed using a representative methodological framework that integrates empirical testing results and mathematical modeling.

Employing a multi-criteria approach to evaluate tactical communication system effectiveness, key advantages of the SC4400 were identified, including: a wide frequency range (300 MHz – 6 GHz), high throughput (up to 100+ Mbps), and low hop latency (7 ms), ensuring optimal performance characteristics for real-time multimedia transmission. Concurrently, functional limitations of the system were identified, including the absence of an integrated computing platform, insufficient resilience against intensive electronic warfare (EW), and significant antenna system limitations concerning energy potential and directivity pattern adaptability. Optimal application scenarios for the systems under study are scientifically substantiated based on their technical and operational characteristics and the specifics of the operational environment. Prospective directions for enhancing the Silvus SC4400 are proposed, considering the identified limitations and current trends in tactical communication technology development.

Keywords: *tactical communication systems, MANET, Silvus StreamCaster SC4400, MIMO technology, Electronic Warfare (EW), Electronic Intelligence (ELINT), jam resistance, throughput, antenna pattern.*

Постановка задачі. Відомо, що сучасні військові операції суттєво залежать від надійних тактичних систем зв’язку, що забезпечують командування та управління, ситуаційну обізнаність і координацію між розосередженими підрозділами. Однак операційне середовище стає дедалі складнішим через наявність розвинених засобів радіоелектронної

боротьби (РЕБ) противника та складних фізичних ландшафтів, що створюють перешкоди для надійності, ефективності цих систем зв’язку для вирішення цільових задач. Здатність противника здійснювати радіоелектронну розвідку (РЕР) для виявлення, ідентифікації та визначення місцезнаходження ще більше підкреслює потребу в стійких технологіях зв’язку.

Так, радіостанції Silvus StreamCaster SC4400 класу мереж (MANET) розглядаються як перспективний напрям розвитку тактичних систем для інтеграції на мобільні базові станції, БпЛА-ретранслятор та інших напрямках.

Однак у сучасних наукових роботах недостатньо наведено інформації щодо спроможності та комплексного деталізованого дослідження функціонування засобів зв’язку Silvus, їхніх характеристик у складних динамічних умовах в різних сценаріях експлуатації.

Таким чином, виникає необхідність всебічного аналізу та порівняння з існуючими аналогами при різних сценаріях застосування.

Метою дослідження є проведення комплексного аналізу технічних характеристик, переваг та обмежень радіостанцій Silvus StreamCaster SC4400 в умовах динамічного середовища.

Аналіз останніх публікацій. Нижче наведено системний огляд наукових публікацій, присвячених дослідженню радіостанцій Silvus та аналогів, науково-технічні аспекти їх функціонування в умовах невизначеності.

Так, у технічних специфікаціях Silvus Technologies [1] представлено детальну інформацію характеристик радіостанцій SC4400, включаючи частотні діапазони, параметри випромінюваної потужності, а також топологічні характеристики MANET-мереж із підтримкою до 380 вузлів. Технологія 4×4 MIMO, згідно з наведеними даними, забезпечує теоретичну пропускну здатність понад 100 Мбіт/с. Необхідно зазначити, що технічні специфікації, надані виробником, відображають лабораторні умови експлуатації, які суттєво відрізняються від реальних польових сценаріїв, і не містять комплексного аналізу функціонування Silvus в умовах активної радіоелектронної боротьби та інтенсивного радіоперехоплення.

Експериментальні дослідження, проведені Colorado DOPS [2], представляють емпіричні результати польових випробувань Silvus SC3500 (попереднього покоління SC4400) з конкретними показниками дальності зв’язку та пропускної здатності в різних топографічних умовах. Однак методологія експериментальних досліджень не відображає комплексного впливу радіоелектронної протидії. Випробування здійснювалися переважно в цивільному середовищі, що не дозволяє екстраполювати отримані результати на застосування в умовах активних бойових дій.

Результати військових польових випробувань, представлені в [3], містять аналіз імплементації радіостанцій Silvus у 25-й піхотній дивізії США для забезпечення комунікаційної інфраструктури в умовах тропічних лісів та урбанізованого середовища. У дослідженні [3] зазначається мобільність системи та здатність функціонувати при відсутності прямої видимості (NLOS). Разом з тим, дослідження характеризується відсутністю представлених показників надійності зв’язку та ефективності функціонування в умовах електромагнітних завад, що обмежує можливості формування комплексної оцінки.

Інженерний аналіз протоколу MN-MIMO, представлений у роботі [4], містить деталізований опис запатентованого протоколу, що застосовується в SC4400. У дослідженні розглянуто алгоритми автоматичного уникнення завад (MAN-IA) та анулювання інтерференції (MAN-IC), а також представлено теоретичне обґрунтування їх ефективності. Необхідно зазначити, що аналіз ґрунтується переважно на теоретичних моделях, що потребують додаткової емпіричної верифікації. Питання енергоефективності та функціональних обмежень протоколу в умовах мультидіапазонної радіоелектронної протидії розглянуто недостатньо.

Порівняльний аналіз MANET-систем, представлений у дослідженні [5], містить науково обґрунтоване зіставлення характеристик Silvus SC4400, Persistent Systems MPU5 та TrellisWare TSM. Також у цьому дослідженні наведено об’єктивні дані щодо функціональних характеристик кожної системи, зокрема акцентується на широкому частотному діапазоні та підвищену пропускну здатність Silvus порівняно з альтернативними системами. Автори акцентують на суттєвій диференціації технічних характеристик досліджуваних систем. Водночас, дослідження не містить комплексного аналізу вразливостей до спрямованих завад різних типів, а також характеризується недостатньою увагою до тактичних аспектів застосування систем у реальних бойових умовах.

Аналіз наукових публікацій [1–5] демонструє відсутність цілісної методологічної бази для оцінювання ефективності радіостанцій Silvus SC4400 в контексті їх застосування в умовах високоінтенсивних бойових дій із використанням сучасних засобів радіоелектронної боротьби. Особливо актуальною є проблема недостатності емпіричних даних щодо функціонування системи під впливом динамічних факторів невизначеності, характерних для сучасного театру бойових дій.

Виклад основного матеріалу. Для проведення об’єктивного аналізу функціональних характеристик радіостанцій Silvus SC4400 у контексті динамічної невизначеності оперативного середовища необхідно здійснити науково обґрунтований вибір репрезентативних аналогів. Вибір конкретних комунікаційних систем для порівняльного аналізу будується за наступними критеріями:

1. **Функціональна еквівалентність** – обрані системи повинні належати до класу тактичних мобільних комунікаційних платформ із підтримкою технології MANET (Mobile Ad-hoc Network), що забезпечує методологічну коректність зіставлення.

2. **Цільове призначення** – всі досліджувані системи орієнтовані на забезпечення безперервної комунікаційної інфраструктури в умовах тактичних операцій з високим ступенем мобільності та мінливості середовища.

3. **Репрезентативність технологічних підходів** – обрані системи репрезентують різні технологічні концепції реалізації MANET-мереж, що дозволяє провести комплексний аналіз альтернативних підходів.

4. **Актуальність імплементації** – досліджувані системи активно використовуються в сучасних збройних конфліктах.

Відповідно до зазначених критеріїв, для аналізу вибрано три комунікаційні системи: Silvus SC4400, Persistent Systems MPU5 та TrellisWare TSM-950. Вище наведені комунікаційні системи характеризуються архітектурними та функціональними диференціаціями, що дозволяє проаналізувати їхню ефективність у широкому спектрі оперативних сценаріїв.

Радіостанція **Silvus SC4400** – конструктивно-технологічний підхід, що ґрунтується на максимізації пропускної здатності та експлуатаційній гнучкості комунікаційного каналу. Архітектурною особливістю **Silvus** є імплементація конфігурації 4×4 MIMO (Multiple Input Multiple Output), що забезпечує чотири незалежні просторові канали передачі даних для підвищення спектральної ефективності. В радіостанції **Silvus** застосовується пропрієтарний протокол MN-MIMO (Mesh Network Multiple Input Multiple Output), що інтегрує адаптивні алгоритми модуляції та кодування (AMC) з динамічною топологією мережі. Функціональною специфікою SC4400 є широкий частотний діапазон (300 МГц – 6 ГГц), що забезпечує високу адаптивність до електромагнітних умов оперативного середовища.

Комунікаційна система **Persistent Systems MPU5** застосовує концептуальний підхід, орієнтований на інтеграцію комунікаційних та обчислювальних функцій в єдиній апаратно-програмній платформі. Архітектурно система базується на конфігурації 3×3 MIMO, що забезпечує балансування між пропускною здатністю та енергоефективністю. Ключовою

диференціацією MPU5 є імплементація повноцінної обчислювальної підсистеми на базі операційної системи Android, що трансформує радіостанцію у мультифункціональний комунікаційно-обчислювальний вузол із можливістю локального виконання спеціалізованих програмних додатків (зокрема, ATAK – Android Tactical Assault Kit). Система базується на протоколі Wave Relay, що забезпечує криптографічний захист та оптимізацію маршрутизації в динамічних мережевих топологіях.

Радіосистема **TrellisWare TSM-950** інкорпорує технологічний підхід, орієнтований на максимізацію надійності комунікаційного каналу в умовах електромагнітної протидії. Архітектурно система використовує конфігурацію 2×2 MIMO, що потенційно обмежує пропускну здатність, однак оптимізує енергоефективність та спрощує програмно-апаратну імплементацію. Функціональною особливістю TSM-950 є імплементація спеціалізованого протоколу з хвильовою формою Katana, що інтегрує технології розширеного спектра з прямою послідовністю (Direct Sequence Spread Spectrum, DSSS) та адаптивного частотного стрибкоподібного переналаштування (Adaptive Frequency Hopping Spread Spectrum, AFHSS). Ключовою перевагою системи є здатність до масштабування мережі до понад 800 вузлів без деградації критичних показників латентності.

Архітектурні та функціональні диференціації досліджуваних систем створюють підґрунтя для детального аналізу їхніх експлуатаційних характеристик у контексті динамічної невизначеності оперативного середовища. Систематизація ключових параметрів функціонування радіосистем представлена в таблиці 1.

Таблиці 1

Систематизація ключових параметрів функціонування радіосистем

Параметр	Silvus SC4400	Persistent MPU5	TrellisWare TSM	Методологія оцінювання
Архітектура системи	Конфігурація MIMO: 4×4	Конфігурація MIMO: 3×3	Конфігурація MIMO: 2×2	Технічна документація [1; 9; 10]
Частотні діапазони	300 МГц – 6 ГГц (UHF, L, S, C, ISM)	500 МГц – 5 ГГц (обмежений набір)	225 МГц – 2,5 ГГц (UHF, L, S)	Специфікація обладнання [1; 9; 10]
Метод передачі	Широкосмуговий COFDM (5–20 МГц)	Широкосмуговий OFDM (5–20 МГц)	Вузькосмуговий DSSS (1,2–10 МГц)	Аналіз спектрограм [11]
Енергетичні показники	Вихідна потужність: до 20 Вт (80 Вт EIRP з формуванням променя)	Вихідна потужність: 3–6 Вт	Вихідна потужність: 5–10 Вт	Вимірювання спектроаналізатором [12]
Чутливість приймача	–102 дБм (BER 10^{-6}, смуга 5 МГц)	–97 дБм (BER 10^{-6}, смуга 5 МГц)	–110 дБм (BER 10^{-6}, смуга 3 МГц)	Лабораторні вимірювання [13]
Енергоспоживання	38–42 Вт при макс. потужності	28–34 Вт при макс. потужності	30–36 Вт при макс. потужності	Вимірювання при навантаженні [14]
Мережеві характеристики	Масштабованість мережі: до 380 вузлів	Масштабованість мережі: до 140 вузлів	Масштабованість мережі: до 820 вузлів	Результати випробувань [5; 15]
Канальна затримка	7 мс (один хоп)	10–12 мс (один хоп)	15–18 мс (один хоп)	Вимірювання методом "ping" [16]
Швидкість передачі	До 100+ Мбіт/с	До 80 Мбіт/с	До 8 Мбіт/с	Вимірювання при ідеальних умовах [17]

Параметр	Silvus SC4400	Persistent MPU5	TrellisWare TSM	Методологія оцінювання
Стійкість до протидії	Стійкість до завад (J/S): до 15 дБ	Стійкість до завад (J/S): до 13 дБ	Стійкість до завад (J/S): до 28 дБ (режим Katana)	Лабораторні випробування [18]
Механізми протидії РЕБ	MAN-IA, MAN-IC (просторова фільтрація)	QAM, Cognitive Wave Relay	Katana (frequency hopping, DSSS)	Аналіз технічної документації [1; 9; 10]
Додаткові особливості	Інтегрована обчислювальна платформа: відсутня	Інтегрована обчислювальна платформа: Android	Інтегрована обчислювальна платформа: обмежена	Технічна документація [1; 9; 10]
Маса	1,1 кг (без батареї)	1,2 кг (без батареї)	0,9 кг (без батареї)	Технічна документація [1; 9; 10]

Із таблиці видно результати комплексного порівняльного аналізу техніко-експлуатаційних характеристик трьох перспективних тактичних радіозасобів: Silvus SC4400, Persistent MPU5 та TrellisWare TSM. Дані демонструють суттєві архітектурні та функціональні відмінності, що визначають сфери оптимального застосування кожної системи.

Так, Silvus SC4400 характеризується використанням конфігурації MIMO 4×4, що перевищує можливості просторового мультиплексування Persistent MPU5 (MIMO 3×3) та TrellisWare TSM (MIMO 2×2). Зазначена архітектурна перевага корелює з діапазоном функціонування Silvus SC4400 (300 МГц – 6 ГГц), що охоплює ультрависокочастотний, L-, S-, C-діапазони та ISM-діапазони. Persistent MPU5 має обмеженіший частотний діапазон (500 МГц – 5 ГГц), а TrellisWare TSM функціонує в більш обмеженому спектрі (225 МГц – 2,5 ГГц). Порівняння частотних діапазонів систем наведено на графіку рисунка 1.

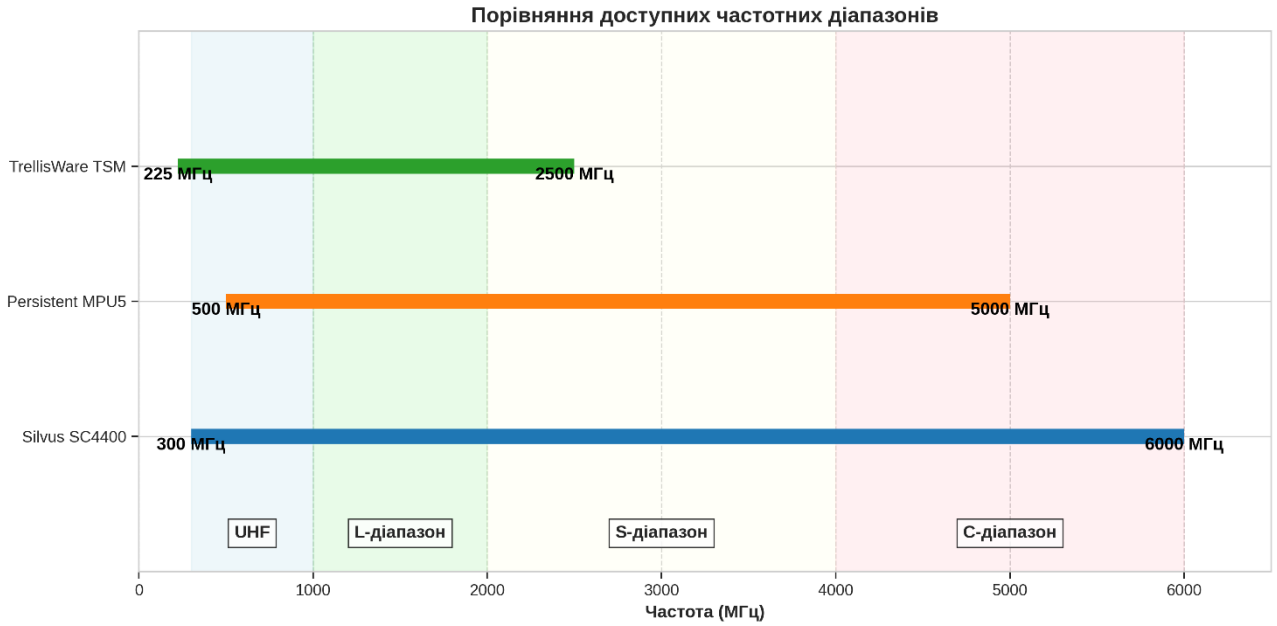


Рис. 1. Порівняння частотних діапазонів

Принципова відмінність між системами полягає в обраних методах передачі. Silvus SC4400 та Persistent MPU5 базуються на широкосмугових технологіях COFDM/OFDM із шириною каналу від 5 до 20 МГц, що дозволяє досягати високої швидкості передачі даних. Натомість TrellisWare TSM використовує вузькосмугову технологію DSSS із шириною каналу 1,2–10 МГц, що забезпечує підвищену завадостійкість за рахунок меншої швидкості.

Вихідна потужність Silvus SC4400 сягає 20 Вт (до 80 Вт EIRP із формуванням променя), що суттєво перевищує показники Persistent MPU5 (3–6 Вт) та TrellisWare TSM (5–10 Вт). Документовані польові випробування підтверджують, перевагу SC4400 (8 Вт) відносно дальності дії в умовах прямої видимості порівняно з MPU5. При цьому TrellisWare TSM забезпечує чутливість приймача –110 дБм (BER 10^{-6}, смуга 3 МГц), що перевищує аналогічні характеристики Silvus SC4400 (–102 дБм) та Persistent MPU5 (–97 дБм) (рис. 2). Таким чином, радіостанція TSM дозволяє підтримувати зв’язок при низьких співвідношеннях сигнал/шум.

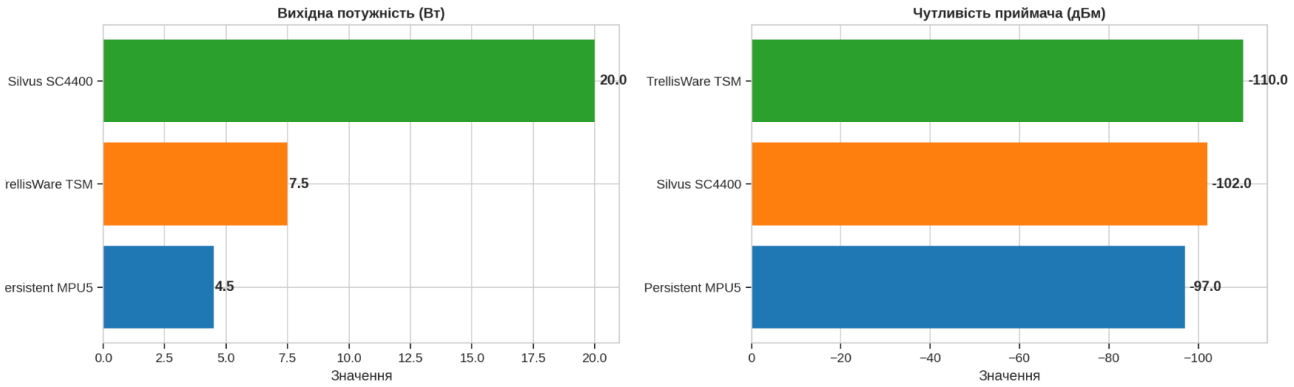


Рис. 2. Порівняння за вихідною потужністю та показником чутливості приймача

Масштабованість мережі TrellisWare TSM досягає 820 вузлів, цей показник перевищує можливості Silvus SC4400 (до 380 вузлів) та особливо Persistent MPU5 (до 140 вузлів), що представлено на рисунку 3. Однак за швидкістю передачі даних ситуація протилежна (рис. 4): Silvus SC4400 забезпечує до 100+ Мбіт/с, Persistent MPU5 – до 80 Мбіт/с, а TrellisWare TSM – до 8 Мбіт/с.

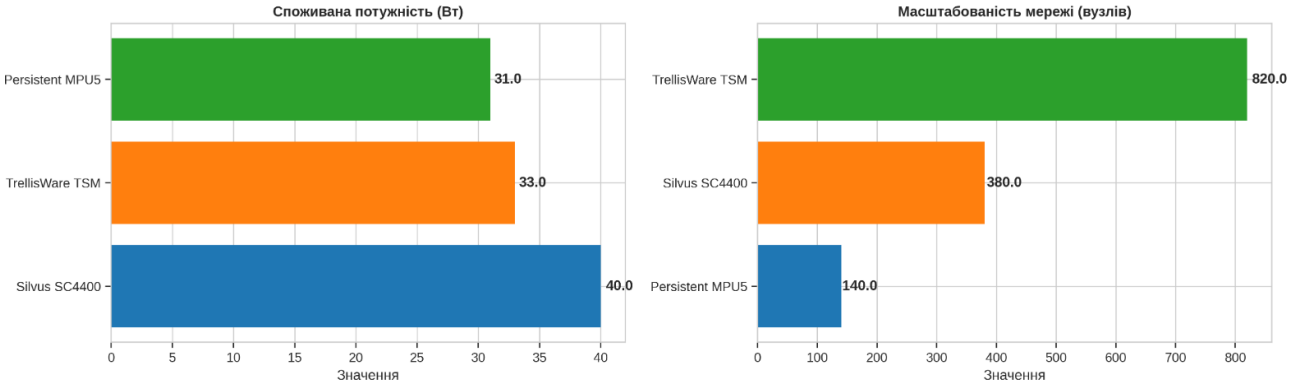


Рис. 3. Порівняння за показником енергоспоживанням радіостанцій та масштабованості приймача

TrellisWare TSM у режимі Katana демонструє стійкість до завад (J/S) до 28 дБ, що перевищує відповідні характеристики Silvus SC4400 (до 15 дБ) та Persistent MPU5 (до 13 дБ) (рис. 5). Режим Katana використовує технології частотних стрибків та розширення спектра

методом прямої послідовності, спеціально розроблені для екстремальних умов радіоелектронної боротьби.

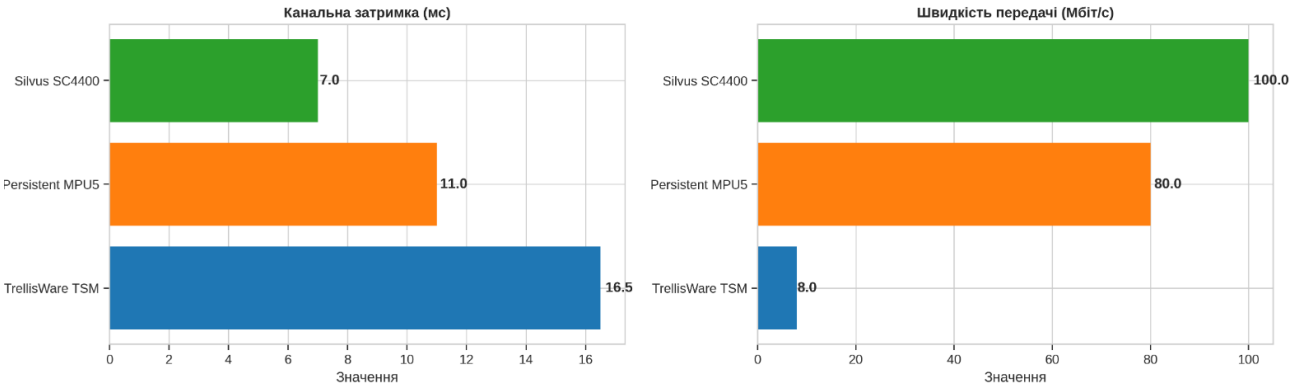


Рис. 4. Порівняння за показником швидкості передачі даних

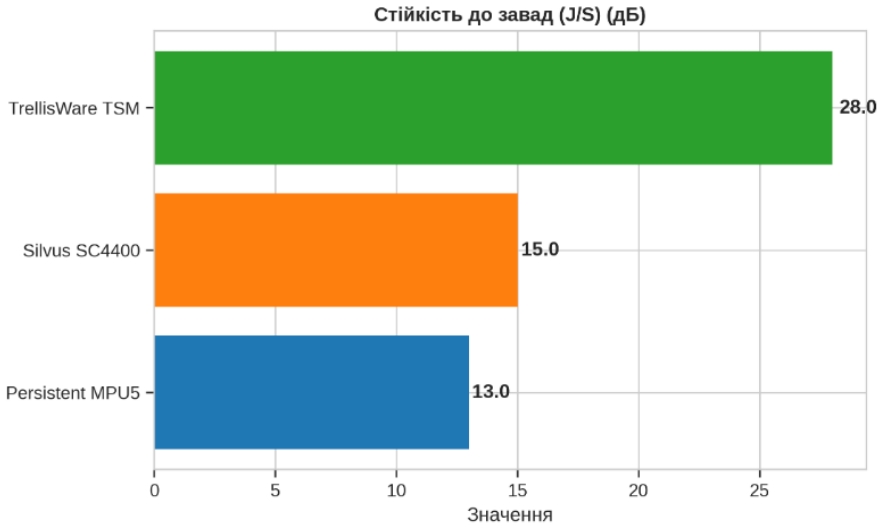


Рис. 5. Порівняння за показником стійкості до завад

Silvus SC4400 використовує технології MAN-IA та MAN-IC із просторовою фільтрацією для протидії завадам, тоді як Persistent MPU5 застосовує технології QAM та Cognitive Wave Relay. Необхідно зазначити, що Silvus активно розробляє методи ECCM, цільовою задачею є наблизити стійкість до рівня вузькосмугових рішень.

Канальна затримка Silvus SC4400 складає 7 мс на один хоп, що менше порівняно з Persistent MPU5 (10–12 мс) та TrellisWare TSM (15–18 мс) (рис. 6). Це забезпечує суттєву перевагу для застосувань, чутливих до латентності, особливо при передачі відеоконтенту.

Важливою відмінністю є наявність у Persistent MPU5 інтегрованої обчислювальної платформи на базі Android, що дозволяє запускати застосунки (наприклад, ATAK) безпосередньо на радіостанції. SC4400 такої можливості не має – для роботи з нею потрібен зовнішній пристрій (планшет або комп’ютер), що ускладнює інтеграцію в польових умовах.

Маса радіозасобів порівняння: Silvus SC4400 – 1,1 кг, Persistent MPU5 – 1,2 кг, TrellisWare TSM – 0,9 кг (без батарей), що забезпечує зручність транспортування у всіх випадках.

Таким чином, проведений комплексний аналіз демонструє, що архітектурно-технологічні характеристики Silvus SC4400 формують фундаментальні переваги в контексті просторового мультиплексування та пропускної здатності каналу завдяки імплементації

конфігурації MIMO 4×4. Частотно-спектральний діапазон системи (300 МГц – 6 ГГц) забезпечує підвищену адаптивність до динамічних електромагнітних умов, хоча використання широкосмугового методу передачі COFDM детермінує потенційну вразливість до спрямованих завад. Енергетичні показники SC4400 характеризуються вихідною потужністю до 20 Вт, що при застосуванні технології формування променя досягає EIRP до 80 Вт, збільшуючи радіус дії системи у 1,6–1,8 рази порівняно з конкурентними рішеннями при ідентичних параметрах антенних систем. Мережеві параметри демонструють масштабованість до 380 вузлів та оптимальну канальну затримку (7 мс на один хоп), що відповідає вимогам застосувань, чутливих до латентності.

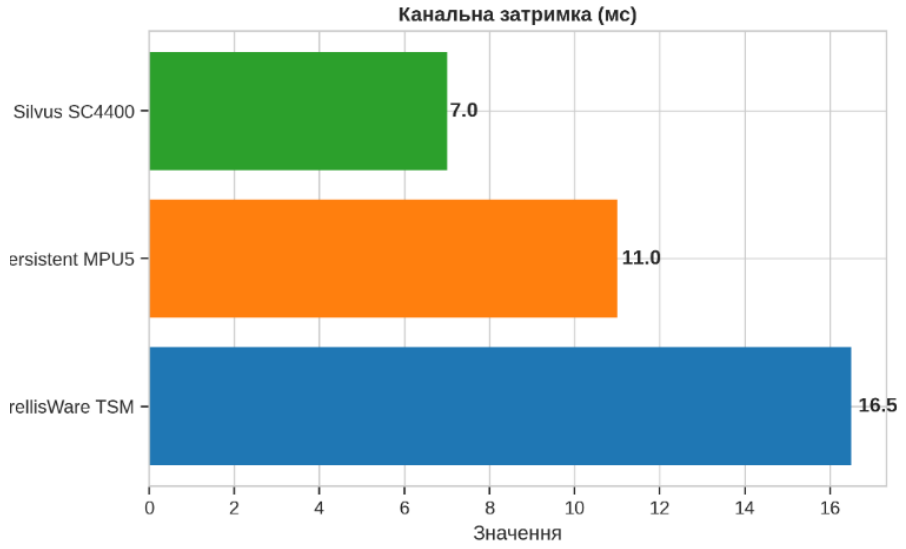


Рис. 6. Порівняння канальної затримки

Однак необхідно зазначити, що наявні дослідження функціонування радіостанцій Silvus SC4400 в умовах активної РЕР та РЕБ характеризуються недостатньою комплексністю та емпіричною верифікацією. Відсутність систематизованих експериментальних даних щодо стійкості системи до діяльності сучасних засобів радіоелектронної протидії суттєво обмежує можливості прогнозування її ефективності в умовах високоінтенсивних бойових дій. **Також окремого аналізу потребують** характеристики антенних систем, а саме процес передачі та прийому радіосигналів у складних електромагнітних умовах. На основі проведеного аналізу технічної документації та експериментальних даних [17–19] виявлено наступні кількісні показники обмежень існуючої антенної системи Silvus:

– Всеспрямовані антени, що використовуються в стандартній конфігурації SC4400, мають коефіцієнт спрямованої дії близько 2 дБі [20]. Тобто 63 % випромінюваної потужності розподіляється в напрямках, відмінних від напрямку на кореспондента, що суттєво обмежує енергетичний потенціал лінії зв’язку.

– Експериментальні дослідження показують, що при швидких змінах напрямку руху платформи (з кутовою швидкістю понад 15°/с) спостерігається зниження якості сигналу на 40–45 % [22]. Вище наведене пояснюється тим, що всеспрямовані антени не здатні адаптивно підсилювати сигнал у потрібному напрямку при зміні взаємного розташування абонентів.

– Аналіз функціонування SC4400 в умовах міської забудови показує, що глибина завмирань сигналу внаслідок інтерференції між прямим та відбитими сигналами може досягати 25–30 дБ [23], що призводить до суттєвого зниження стабільності зв’язку та збільшення частоти повторної передачі пакетів даних.

Висновки. Таким чином, проведений комплексний аналіз показав, що архітектурно-технологічні характеристики Silvus SC4400 формують фундаментальні переваги в контексті просторового мультиплексування та пропускної здатності каналу завдяки імплементації конфігурації MIMO 4×4. Частотно-спектральний діапазон системи забезпечує підвищену адаптивність до динамічних електромагнітних умов, однак використання широкосмугового методу передачі COFDM детермінує потенційну вразливість до спрямованих завад. Енергетичні показники SC4400 характеризуються вихідною потужністю до 20 Вт, що при застосуванні технології формування променя досягає EIRP до 80 Вт, збільшуючи радіус дії системи у 1,6–1,8 рази порівняно з конкурентними рішеннями при ідентичних параметрах антенних систем.

Однак встановлено, що антенні системи зі стандартною конфігурацією SC4400 характеризуються низьким коефіцієнтом спрямованої дії (близько 2 дБі), що призводить до нераціонального розподілу випромінюваної потужності та зниження енергетичного потенціалу лінії зв’язку. Емпірично підтверджено, що при швидких змінах напрямку руху платформи та в умовах складної електромагнітної обстановки (міська забудова) спостерігається значна деградація якості сигналу (до 40–45 %) внаслідок відсутності адаптивних механізмів формування діаграми направленості.

Додатковим функціональним обмеженням Silvus SC4400 є відсутність інтегрованої обчислювальної платформи, що ускладнює автономне функціонування та потребує зовнішніх пристроїв для повноцінної експлуатації. Оптимальними сферами застосування Silvus SC4400 є сценарії, що вимагають високої пропускної здатності при помірній щільності вузлів та середній інтенсивності радіоелектронної протидії.

Із урахуванням вищенаведеного, **перспективним напрямом подальших** досліджень є детальний аналіз та розробка математичних моделей функціонування системи Silvus SC4400 у різноманітних сценаріях експлуатації. Зокрема, актуальним є створення комплексних аналітичних моделей, що враховуватимуть нелінійні характеристики розповсюдження радіосигналу в умовах складної електромагнітної обстановки, динамічної топології мережі та активної радіоелектронної протидії. Формалізація стохастичних процесів у системах з адаптивними алгоритмами модуляції та кодування дозволить прогнозувати ефективність функціонування у критичних режимах експлуатації та оптимізувати параметри системи відповідно до специфічних вимог кожного сценарію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Spectrum Dominance: LPI/LPD and Anti-Jamming Capabilities // Silvus Technologies. URL: https://www.silvustechnologies.com.
2. Silvus SC3500 Field Test Findings // Colorado DOPS. URL: https://cdpsdocs.state.co.us.
3. Ball M. Silvus Adds Anti-Jamming Capabilities to MANET Radios // UST Magazine. 2019. URL: https://www.unmannedsystemstechnology.com.
4. Silvus SC4400 Data Sheet // Silvus Technologies. URL: https://www.silvustechnologies.com.
5. Silvus SC4400E Product Description // Unmanned Systems Source. URL: https://www.unmannedsystemssource.com.
6. Silvus radios in urban, mobile, high-scatter environments // Military & Aerospace Electronics. URL: https://www.militaryaerospace.com.
7. User review: Silvus vs Persistent MPU5 // Reddit r/QualityTacticalGear. URL: https://www.reddit.com.
8. TSM Waveform Datasheet // TrellisWare Technologies. URL: https://www.trellisware.com
9. Radio Modernization (Silvus in jungle ops) // U.S. Army. URL: https://www.army.mil.
10. Silvus range vs frequency observation // XXLSEC. URL: https://www.silvustechnologies.com.

11. Analysis and Synthetic Model of Adaptive Beamforming for Smart Antenna Systems in Wireless Communication // Journal of Communications. Vol. 13. No. 8, August 2018. URL: https://www.jocm.us/show-194-1241-1.html.

12. Jamming and Anti-jamming Techniques in Wireless Networks: A Survey // Scholarworks. URL: https://scholarworks.montana.edu/bitstreams/b1d9de32-0aa5-4aa9-b6e1-9dde2aee188c/download.

13. Measurement, data analysis and modeling of electromagnetic wave propagation gain in a typical vegetation environment // PMC. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9836301/.

14. A Deep Dive into GPS Anti-Jamming // TUALCOM. URL: https://www.tualcom.com/a-deep-dive-into-gps-anti-jamming/.

15. Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare // CEUR-WS.org. URL: https://ceur-ws.org/Vol-3654/paper24.pdf.

16. American Geosynchronous SIGINT Satellites // Space Policy Project. URL: https://spp.fas.org/military/program/sigint/androart.htm.

17. Electronic Warfare – The Early Years Part 1 // InfoAge Science and History Museums. URL: https://www.infoage.org/wp-content/uploads/2019/06/INL_V04_N02.pdf.

18. PS MPU5's viability in an adversarial environment // Reddit r/QualityTacticalGear. URL: https://www.reddit.com/r/QualityTacticalGear/comments/1d0rhu7/ps_mpu5s_viability_in_an_adversarial_environment/.

19. Effects of Hilly Terrain on UHF Band Radio Frequency Propagation // Index Copernicus. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/316194.

20. Dai H.-N. An Overview of Using Directional Antennas in Wireless Networks / H.-N. Dai, K.-W. Ng, M. Li, M.-Y. Wu // International Journal of Communication Systems. 2011. Vol. 00. P. 1–39. DOI: 10.1002/dac // Wiley InterScience. URL: www.interscience.wiley.com.

21. Ilie D. Avoiding Detection by Hostile Nodes in Airborne Tactical Networks / D. Ilie, H. Grahn, L. Lundberg, A. Westerhagen, B. Granbom, A. Höök // Future Internet. 2023. Vol. 15 (6). P. 204. DOI: https://doi.org/10.3390/fi15060204.

22. Radio wave propagation | Radio Station Management Class Notes // Fiveable. URL: https://library.fiveable.me/radio-station-management/unit-1/radio-wave-propagation/study-guide/YZ5sbBFLt8TpHfhf.

23. Impact of Mountains and Hills on Cell Signal and How to Boost It // My Signal Boosters. URL: https://mysignalboosters.com/blog/impact-of-mountains-and-hills-on-cell-signal-and-how-to-boost-it/.

DOI: 10.58254/viti.7.2025.21.232

УДК 681.35

канд. техн. наук Хусаінов П. В. ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
Черниш Ю. О. ORCID: 0000-0002-6626-5656 (ВІТІ ім. Героїв Крут)
Терещенко Т. П. ORCID: 0000-0002-9659-7897 (ВІТІ ім. Героїв Крут)

ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ ОЦІНКИ ЧАСУ КОМПРОМЕТАЦІЇ SERVER-SIDE WEB APPLICATION ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

На сучасному етапі розвитку методів і способів організації кіберзахисту об'єктів критичної інфраструктури одним із дієвих підходів залишається систематичний пошук вразливостей таких об'єктів у формі тестування на проникнення (penetration testing). Основною формою тестування на проникнення слід вважати практичне доведення можливості несанкціонованого та віддаленого нав'язування виконання демонстраційної шкідливої програми з авторизованими повноваженнями у складі одного з компонентів системи об'єкта критичної інфраструктури. Показником ефективності організації процесу тестування на проникнення запропоновано використовувати часові витрати досягнення тактичної цілі Compromise System.

Оцінка часових витрат досягнення тактичної цілі Compromise System в реальних умовах виконання практичних завдань тестування на проникнення знаходиться під впливом багатьох факторів невизначеності. Для зменшення впливу невизначеності пропонується два підходи. Перший підхід – шляхом впровадження методів теорії інформаційної підтримки прийняття рішень, на етапах досягнення тактичних цілей Reconnaissance та Resource Development. Другий – застосування критеріїв прийняття рішень в умовах невизначеності для обробки результатів експериментальних випробувань демонстраційних шкідливих програм, при проходженні казуального ланцюжка Initial Access – Execution. Обґрунтування сформульованих положень здійснено шляхом дослідження структурно-казуальних відношень предметної області на основі аналізу The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology та таксономій експертних знань Adversarial Tactics, Techniques & Common Knowledge.

Викладено змістовний опис методики оцінки зменшення невизначеності, оцінки часу компрометації компонентів Server-side Web Application при проходженні казуального ланцюжка Initial Access – Execution (у контексті етапу досягнення тактичної цілі Gaining Access тестування на проникнення) за способом Exploit Public-Facing Application на основі застосування критеріїв прийняття рішень в умовах невизначеності.

Ключові слова: *тестування на проникнення, прийняття рішень, оцінка часу.*

P. Khusainov, Y. Chernysh, T. Tereshchenko. Decreasing an indetermination of evaluation of time to compromise Server-Side Web Application of Industrial Control System

At the present stage of development of methods and ways of organizing cyber defense of critical infrastructure facilities, one of the effective approaches is the systematic search for vulnerabilities of such facilities in the form of penetration testing. The main form of penetration testing should be considered practical proof of the possibility of unauthorized and remote imposition of a demonstration malware program with authorized powers as part of one of the components of the critical infrastructure system. As an indicator of the effectiveness of organizing the penetration testing process, it is proposed to use the time spent on achieving the tactical goal of the Compromise System.

Estimating the time required to achieve the Compromise System tactical objective in real-world penetration testing is subject to many uncertainty factors. Two approaches are proposed to reduce the impact of uncertainty. The first is by implementing methods of decision support information theory at the stages of achieving the tactical goals of Reconnaissance and Resource Development. The second is the use of decision-making criteria under uncertainty to process the results of experimental tests of demonstration malware, when passing the casual chain Initial Access - Execution. The substantiation of the formulated provisions was carried out by studying the structural and casual relations of the subject area based on the analysis of The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology and the taxonomies of expert knowledge Adversarial Tactics, Techniques & Common Knowledge.

A substantial description of the methodology for assessing the reduction of uncertainty, estimating the time of compromise of Server-side Web Application components during the passage of the casual chain Initial Access - Execution (in the context of the stage of achieving the tactical goal of Gaining Access penetration testing) by the Exploit Public-Facing Application method based on the application of decision-making criteria under conditions of uncertainty is presented.

Keywords: *penetration test, decision making, assessment of time.*

Постановка завдання. Об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури (ОКІ), кібератака, яка безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Кіберзахист ОКІ забезпечується шляхом впровадження на ньому комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю. Власник/керівник ОКІ зобов'язаний проводити перевірку ефективності заходів щодо захисту об'єкта критичної інформаційної інфраструктури від несанкціонованого втручання (зовнішнього проникнення) шляхом періодичного виконання (не рідше одного разу на рік) тестування на проникнення. Тестування на проникнення (*penetration testing*) уособлює комплекс заходів оцінки захищеності об'єкта кіберзахисту від кіберзагроз шляхом доведення або заперечення твердження про можливість компрометації системи (об'єкта кіберзахисту) із застосуванням способів і засобів здійснення кібератак. Поняття "компрометація системи" уособлює факт будь-якого порушення сталого, надійного та штатного режимів функціонування системи (об'єкта кіберзахисту), яка підлягає спостереженню, та/або порушення конфіденційності, цілісності, доступності оброблюваної інформації [1–5].

Доведення можливості компрометації системи (об'єкта критичної інформаційної інфраструктури ОКІ) свідчить про її вразливість. Вразливість системи (об'єкта критичної інформаційної інфраструктури ОКІ) – властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режими функціонування системи (об'єкта критичної інформаційної інфраструктури ОКІ), здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів. Пошук та виявлення потенційної вразливості організовується Власником системи (об'єкта критичної інформаційної інфраструктури ОКІ) шляхом оголошення публічної пропозиції. Дослідник (фізична або юридична особа) потенційної вразливості надає відповідну послугу Власнику системи (об'єкта критичної інформаційної інфраструктури ОКІ) на основі договору. Зокрема, визначається величина граничного часу (директивного, обмеженого) протягом якого Дослідник повинен практично продемонструвати можливість компрометації системи (об'єкта критичної інформаційної інфраструктури ОКІ) шляхом здійснення віддаленої кібератаки у формі *penetration test* [6].

Аналіз публікацій. Сценарій здійснення Дослідником віддаленої кібератаки у формі *penetration test* розглядається як комбінація послідовності тактик (етапів досягнення тактичних цілей) та технік (способів, методів) відповідних експертних продуктів:

The Cyber Kill Chain – узагальнена односпрямована послідовність тактик кібератаки шляхом нав'язування виконання шкідливого програмного засобу [7];

The Unified Kill Chain – сукупність тактик у контексті здійснення трьох послідовних фаз (*In, Through, Out*) компрометації системи багатокомпонентного об'єкта (кіберзхисту) [8];

Ethical Hacking Methodology – взаємопов'язані етапи кібератаки за методологією *Certified Ethical Hacker (CEH)* [9];

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) – опис тактик (*tactics*), технік (*techniques*) кібератак, які здійснювалися проти комунікаційних, технологічних систем та персональних мобільних комунікаційних пристроїв [10].

Формулювання мети статті. Одним із перспективних напрямів діяльності Дослідника на етапі *Initial Access* (несанкціоноване набуття авторизованих повноважень) слід вважати техніку *Exploit Public-Facing Application* через: відсутність потреби у привілеях; відсутність фізичного доступу до апаратних компонентів системи; складність (неможливість) впливу на ланцюги постачання та використання способів соціальної інженерії стосовно легітимних користувачів системи. Адекватність вибору цього способу підкреслюється тим, що близько

20 % категорій дефектів програм (196 із 940) таксономії *Common Weakness Enumeration (CWE)* та більше ніж 20 % вразливостей (63 324 з 273 728) таксономії *Common Vulnerabilities and Exposures (CVE)* відносяться до *Server-side Web Application* [11; 12].

Метою статті є викладення (оприлюднення) змістового опису методики зменшення невизначеності оцінки часу компрометації компонентів *Server-side Web Application* системи (об’єкта критичної інформаційної інфраструктури ОКІ) при проходженні Дослідником казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application* на основі застосування критеріїв прийняття рішень в умовах невизначеності.

Основна частина. Поняття та відношення між ними, які утворюють єдину основу для одноманітного розуміння необхідної для рішення задачі інформації, прийнято називати предметною областю. Множина понять про об’єкти, факти, процеси, події уособлює екстенсіональне представлення предметної області, а множина обумовлених ними відношень зв’язків та залежностей понять – інтенсіональне. Розрізняють структурний, функціональний, казуальний та семантичний типи відношень інтенсіонального представлення предметної області. Структурні відношення застосовуються для визначення ієрархій або мереж понять, функціональні відношення – для порядку перетворення декларативної інформації, казуальні відношення – для причинно-наслідкових зв’язків, ланцюгів зв’язків. Семантичний тип уособлює всі інші можливі типи відношень.

При ієрархічному представленні множина структурних відношень понять є деревоподібним графом, при мережевому представленні – графом типу “мережа”. Семантична мережа – найбільш узагальнена модель представлення знань про предметну область із використанням різнотипних зв’язків. При однорідності типів зв’язків семантичної мережі відокремлюють мережі класифікації (відображення структури відношень понять предметної області), функціональні мережі (опис процедур визначення понять через інші поняття) та сценарії.

Сценарій – формалізований опис стандартної послідовності взаємозв’язаних фактів типової ситуації у предметній області, послідовності дій або процедур досягнення цілей, стереотипних знань. Під поняттям “стереотипні знання” розглядається такий опис ситуації у предметній області у формі послідовності фактів опису, який дозволяє передбачати та відновлювати значення пропущених фактів. За типами відношень розрізняють казуальні сценарії, дерева цілей та сценарії класифікації.

Казуальний сценарій є типовою послідовністю дій (процедур), що підлягає структуризації у формі казуального ланцюжка (сценарію), в якому кожна чергова дія створює умови для здійснення наступної. Дерево цілей є відображенням декомпозиції головної цілі в системі часткових цілей. Сценарії класифікації призначені для відображення результатів узагальнення структурованих знань про предметну область. Для структуризації знань у сценаріях класифікації найчастіше застосовуються відношення типу “причина – наслідок”, “ціль – підціль”, “частина – ціле”, “засіб – результат”, “інструмент – дія” і т. д. Під поняттям “узагальнення” розглядається процес здобуття нових знань, які пояснюють, класифікують вже відомі факти предметної області, а також можуть передбачувати нові. Узагальнення передбачає застосування моделей класифікації, формування понять, розпізнавання образів, виявлення закономірностей. Здатність людини до узагальнення є базисом будь-якого наукового дослідження, одержання нових знань.

Діяльність людини характеризується деревом цілей. Коренева вершина графу такого дерева асоціюється з головною ціллю, вузлові вершини – з проміжними цілями, кінцеві (термінальні) вершини є відображенням первинних (елементарних) цілей. Досягненню цілі відповідає значення певної оціночної функції. Лінійно впорядкована послідовність дій людини спрямована на досягнення головної цілі, будемо називати її траєкторією діяльності.

Траєкторія діяльності утворюється сукупністю структурованих казуальних відношень, що визначають просування до головної цілі від первинних (елементарних) через проміжні [13].

Типовим фрагментом траєкторії діяльності є частково-впорядкована послідовність дій досягнення (головної, проміжної, первинної) цілі з деякої фіксованої початкової ситуації. Під поняттям “ситуація” розглядається деякий узагальнений стан (актуальний опис середовища, визначений на певному часовому інтервалі), що змінюється за результатом виконання дій. Така частково-впорядкована послідовність дій розпочинається від перебування у відомому стані початкової ситуації, подібна казуальному сценарію та може розглядатися у контексті застосування стереотипних знань.

Предметна область процесу компрометації системи (об’єкта критичної інформаційної інфраструктури ОКІ) є семантичною мережею казуальних і структурних відношень між етапами (фазами, кроками) кібератаки. Казуальні відношення відображають існуючу повноту експертних знань про типові послідовності варіантів дій та процедур суб’єкта кібератаки (порушника, хакера) для компрометації системи цільового об’єкта, зокрема системи (об’єкта критичної інформаційної інфраструктури ОКІ) або компонентів її технологічних майданчиків (локацій). Структурні відношення визначають взаємозв’язок етапів досягнення тактичних цілей (тактик) для компрометації системи (*Compromise System*).

Основним акцентом доведення Дослідником можливості компрометації системи є авторизоване виконання демонстраційної шкідливої програми в обчислювальному середовищі одного з компонентів системи (об’єкта критичної інформаційної інфраструктури ОКІ) за визначений час. Під поняттям “демонстраційна шкідлива програма” розглядається спеціальна форма реалізації функцій шкідливої програми щодо несанкціонованого створення (нелегітимним користувачем) авторизованого обчислювального процесу (потоку) в одному з компонентів системи (об’єкта критичної інформаційної інфраструктури ОКІ), але без впровадження типової деструктивної частини алгоритму (*payload*) відомих шкідливих програм. Відповідно, під поняттям “шкідлива програма” розглядається одна з можливих форм реалізації алгоритму здійснення порушення режиму функціонування, безпеки та процедур обробки критичної технологічної інформації, який забезпечується шляхом несанкціонованого створення авторизованого обчислювального процесу (потоку) у певному компоненті системи. Несанкціоноване створення авторизованого обчислювального процесу (потоку) є результатом етапу досягнення тактичної цілі (рис. 1) *Gaining Access* (за методологією *CEH*) та/або *Initial Access* (за методологією *ATT&CK*).

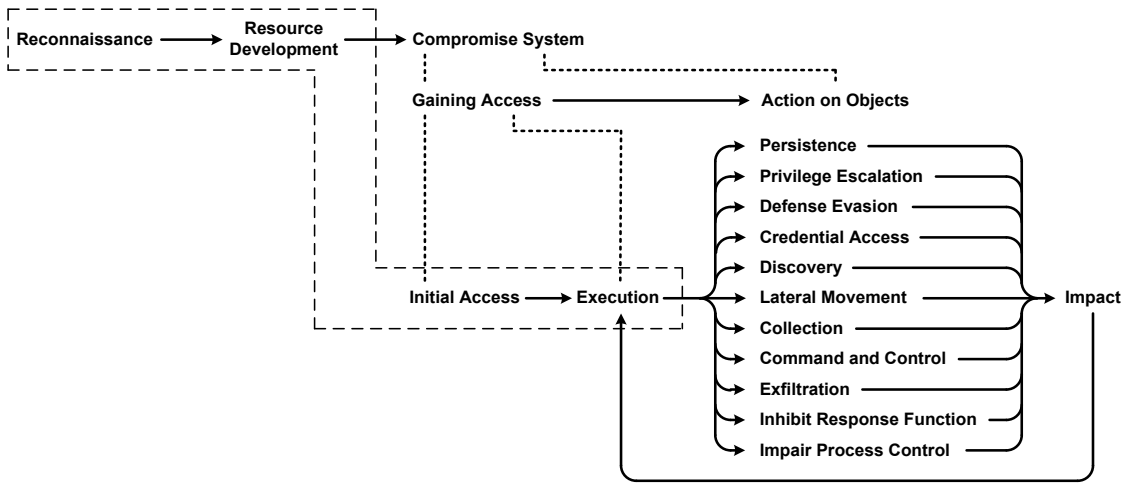


Рис. 1. Структурно-казуальна модель компрометації системи (об’єкта критичної інформаційної інфраструктури ОКІ) у контексті діяльності Дослідника

За методологією *CEH* успішний результат *Gaining Access* полягає у тому, що Дослідник одержав принципову можливість віддаленого (через комп'ютерну мережу) управління певним авторизованим обчислювальним процесом (потоком) демонстраційної шкідливої програми в одному з компонентів системи (об'єкта критичної інформаційної інфраструктури ОКІ) шляхом виконання (з повноваженнями авторизації) передбаченого набору команд деструктивного характеру на етапі досягнення тактичної цілі *Action on Objects* (за методологіями *The Cyber Kill Chain, The Unified Kill Chain*). Загальною недостатністю такого підходу є неврахування факторів невизначеності на оцінку часових витрат очікування успішного результату застосування демонстраційної шкідливої програми у контексті доведення Дослідником можливості компрометації системи (казуальне відношення *Gaining Access – Action on Objects*). Множина варіантів *Action on Objects* утворюється комбінуванням способів (технік) дій досягнення тактичних цілей (тактик) за методологією *ATT&CK*:

Persistence (забезпечення постійності набутих повноважень *Initial Access*);

Privilege Escalation (розширення/зміна набутих 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 у середовищі компонента системи за результатами *Discovery*, але поза контекстом *Initial Access*);

Collection (акумулювання критичної технологічної інформації системи як етап її подальшого витоку);

Command and Control (утворення прихованого каналу управління компонентом системи з повноваженнями авторизованого користувача);

Exfiltration (здійснення витоку критичної технологічної інформації системи);

Inhibit Response Function (блокування процедур реагування на небезпечні стани технологічного процесу);

Impair Process Control (модифікація процедур реагування на небезпечні стани технологічного процесу та обробки критичної технологічної інформації);

Impact (порушення функціонування системи об'єкта критичної інформаційної інфраструктури ОКІ та безпеки критичної технологічної інформації).

Успіх доведення Дослідником можливості компрометації системи (об'єкта критичної інформаційної інфраструктури ОКІ) за визначений час є функціоналом від:

якості прийняття рішення на етапі одержання/узагальнення/аналізу інформації для ідентифікації вразливості системи (як узагальнення етапів *Footprinting*, *Scanning*, *Enumeration*, *Vulnerability Analysis* за методологією *CEH*; етап *Reconnaissance* за методологіями *The Cyber Kill Chain, The Unified Kill Chain, ATT&CK*);

якості прийняття рішення на етапі здійснення вибору/підготовки/створення/придбання засобів експлуатації вразливості системи (етап *Weaponization* за методологіями *The Cyber Kill Chain, The Unified Kill Chain*; етап *Resource Development* за методологією *ATT&CK*);

застосування критеріїв прийняття рішень в умовах невизначеності або в умовах ризику при обґрунтуванні вибору (на основі експериментальних даних) демонстраційної шкідливої програми (експлойту) для компрометації системних компонентів *Server-side Web Application* (при проходженні казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application*).

Нагадаємо, що під поняттям "вразливість" (*vulnerability*) розглядається така властивість системи (об'єкта критичної інформаційної інфраструктури ОКІ), яка призводить до негативного технічного ефекту (*negative technical impact*). Нав'язування негативного

технічного ефекту базується на можливості непередбаченого використання (експлуатації) певного дефекту (*weakness*) програмних, апаратних, програмно-апаратних компонентів системи, які при певних умовах призводять до її вразливості.

Перші два аспекти відносяться до понятійного апарату теорії інформаційної підтримки прийняття рішень [14]. Прийняття рішень (ПР) Дослідником (у ролі особи, яка приймає рішення) є результатом складних психологічних процесів. Логіко-психологічний підхід базується на представленні процесів ПР у формі послідовності етапів, а саме: постановка задачі; здобуття та обробка інформації для ПР; аналіз та ідентифікація проблемної ситуації; вироблення множини альтернативних рішень; вибір рішення; реалізація рішення. Сукупність дій етапів ПР розглядається як композиція множин операцій інформаційної підготовки ПР, вибору та реалізації рішення (результат процесу ПР). Вибір рішення Дослідником принципово не може мати формального подання. Він керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями.

По-перше, розумова 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 мислення. 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 для ПР.

По-друге, прямий чи опосередкований вплив на вибір рішення ОПР можуть мати психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формуються) 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, перемикання, розподіл та об’єм).

Зокрема, невизначеність або неповна визначеність початкової ситуації для здійснення цілеспрямованої діяльності заперечує можливість застосування стереотипних знань. За такої умови постає необхідність пошуку можливих варіантів траєкторії діяльності та вибору одного з них за критеріями на основі значення оціночної функції. Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення можуть бути: неможливість точного передбачення наслідків рішень; неможливість повторення або експериментальної перевірки рішення; неможливість контролю всіх факторів; наявність множини альтернативних рішень та необхідність вибору одного з них; низка якість початкової інформації формулювання задачі та вибору рішення.

Розрізняють два широких класи задач вибору рішень при неповній інформації про задачу та проблемну ситуацію ПР. Перший клас задач відомий як “прийняття рішень в умовах ризику”, другий – “прийняття рішень в умовах невизначеності”. Неповнота інформації ПР в умовах ризику передбачає існування функцій розподілу ймовірностей для всіх досліджуваних величин, в умовах невизначеності – функції розподілу невідомі або не можуть бути визначені. На практиці невизначеність не означає повної відсутності інформації про задачу. Може бути відома деяка кінцева кількість значень кожної величини, але без відповідних функцій розподілу ймовірностей. Розгляд проблематики вирішення задач ПР в умовах ризику можливо при наявності експериментальних даних необхідного об’єму для визначення функцій розподілу кожної з досліджуваних величин.

Базові стратегії зменшення впливу невизначеності та суб'єктивізму при вирішенні задач ПР в умовах невизначеності реалізуються шляхом застосування критеріїв максиміну, Байеса-Лапласа та Севіджа. Хоча не існує загальних підходів для визначення придатності до застосування згадуваних критеріїв в тих чи інших ситуаціях, але все ж можна навести з цього приводу деякі евристичні правила: критерій максиміну спрямований на вибір найбільш обережного передбачуваного результату для всіх комбінацій умов експериментів до моменту необхідності обґрунтування кінцевого рішення; критерій Байєса-Лапласа заснований на більш оптимістичних передбаченнях ніж критерій максиміну, але є менш оптимістичним за критерій Севіджа. Згадувані критерії є базисом для усунення невизначеності, шляхом зменшення суб'єктивізму особистих міркувань та передбачень ОПР, а також протиріч, які їх обумовлюють. Практичне застосування критеріїв ПР в умовах невизначеності базується на обробці матриці рішень, яка сформована зі значень оціночної функції (без знання функції розподілу її величини) за результатами проведених експериментальних випробувань.

Розглянемо змістовний опис методики оцінки зменшення невизначеності, оцінки часу, компрометації компонентів *Server-side Web Application* системи (об'єкта критичної інформаційної інфраструктури ОКІ) при проходженні Дослідником казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application* на основі застосування критеріїв ПР в умовах невизначеності.

Досліджуваною величиною (значення оціночної функції) є експериментальне вимірювання (оцінка) часового інтервалу до настання успішного результату роботи демонстраційної шкідливої програми. Застосування демонстраційної шкідливої програми здійснюється у формі експлойта, який для компонентів *Server-side Web Application* виступає в ролі *Web*-клієнта легітимного користувача (рис. 2, *а*). Нагадаємо, що під поняттям "експлойт" (*exploit)* розглядається спеціальний програмний засіб, призначений для віддаленої (через комп'ютерну мережу) експлуатації дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application*, що призводить до їх вразливості (вразливого стану) та прояву негативного технічного ефекту демонстративної шкідливої програми. Основною функціональною рисою досягнення успішного результату демонстративної шкідливої програми шляхом застосування експлойта з існуючої колекції експлойтів (*expoloits*) Дослідника (рис. 2, *б*) є утворення прихованого каналу управління вразливим компонентом (*Gaining Access*) з авторизованими повноваженнями технічного персоналу *Server-side Web Application*, де T_{GA} – показник часового інтервалу, витрачений на досягнення тактичної цілі *Gaining Access*.

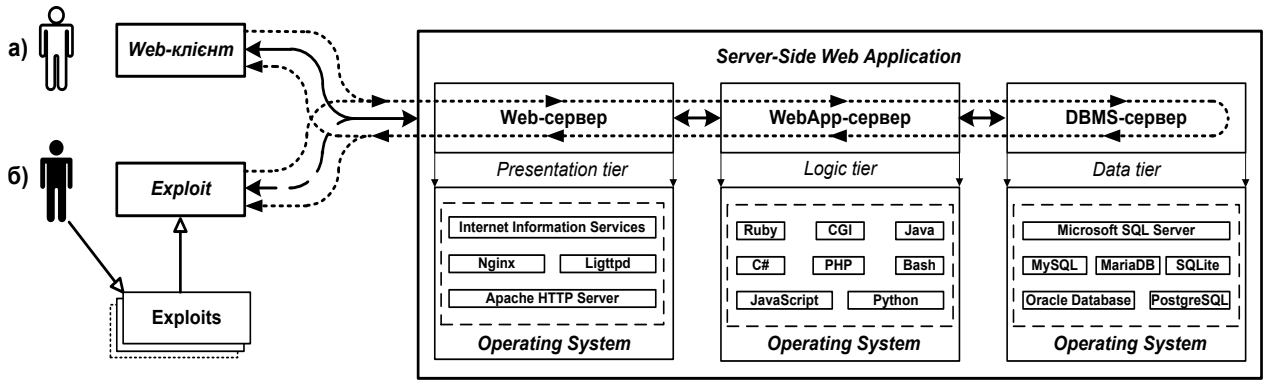


Рис. 2. Організація одержання експериментальних даних для оцінки часових витрат *Gaining Access* (*Initial Access – Execution*) за напрямом впливу *Exploit Public-Facing Application*

Розглянемо можливі інтерпретації T_{GA} за категоріями дефектів (проєктування, реалізації, налаштування) *Server-side Web Application* [15; 16]:

A01:2021 Broken Access Control – некоректна зміна повноважень (недотримання принципу найменших привілеїв), маркерів доступу (функцій інтерфейсу прикладного програмування, посилань на об'єкти), $T_{GA} = T_{A01}$, *Total CVEs* = 19013;

A02:2021 Cryptographic Failures – некоректна перевірка дійсності параметрів автентифікації, цифрових підписів програмних компонентів, запобігання надлишкової інформативності при обробці некоректних комбінацій криптографічних даних (ключів, векторів ініціалізації) при утворенні менш стійких захищених каналів комунікації, $T_{GA} = T_{A02}$, *Total CVEs* =3075;

A03:2021 Injection – передавання на обробку небезпечних (некоректних) вхідних даних (об'єктів), надлишкова інформативність при обробці некоректних (неправильних) запитів до системи керування базою даних, $T_{GA} = T_{A03}$, *Total CVEs* = 32078;

A04:2021 Insecure Design – недотримання порядку *OWASP Software Assurance Maturity Model (SAMM)* при розробці компонентів *Server-side Web Application* із застосуванням апробованих колекцій програмних компонентів, $T_{GA} = T_{A04}$, *Total CVEs* = 2691;

A05:2021 Security Misconfiguration – використання хмарних сервісів (облікових записів) з налаштуваннями за замовчанням, надлишкова інформативність при обробці некоректних запитів до компонентів *Server-side Web Application*, несистематичне застосування оновлень безпеки та аналізу ризиків, $T_{GA} = T_{A05}$, *Total CVEs* =789;

A06:2021 Vulnerable and Outdated Components – використання застарілих версій програмних компонентів *Server-side Web Application*, $T_{GA} = T_{A06}$, *Total CVEs* = 0;

A07:2021 Identification and Authentication Failures – можливість угадування (прогнозування) та повторного використання значень одноразових паролів (маркерів, ідентифікаторів), критичне порушення логіки двофакторної автентифікації (відновлення паролів), потрапляння незашифрованих (зашифрованих нестійкими криптографічними алгоритмами) значень паролів у діагностичні повідомлення (відповіді на некоректні запити до компонентів) *Server-side Web Application*, $T_{GA} = T_{A07}$, *Total CVEs =3897*;

A08:2021 Software and Data Integrity Failures – некоректна перевірка автентичності (цілісності, безпечності, дійсності) даних у складі серіалізованих об'єктів (конвеєрів обробки даних) компонентів *Server-side Web Application*, що інсталюються (оновлюються) з репозиторіїв (зовнішніх носіїв) за замовчанням, $T_{GA} = T_{A08}$, *Total CVEs* =1152;

A09:2021 Security Logging and Monitoring Failures – неузгодженість форматів повідомлень про події функціонування компонентів *Server-side Web Application,* потрапляння критичної технологічної інформації (ідентифікаторів, параметрів автентифікації) до вмісту повідомлень про події, $T_{GA} = T_{A09}$, *Total CVEs* = 242;

A10:2021 Server-Side Request Forgery – потрапляння запитів *Web*-клієнта у запити *Web*-сервера до інших компонентів *Server-side Web Application*, $T_{GA} = T_{A10}$, *Total CVEs* = 387.

Придатність наведених категорій дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application* до експлуатації визначається на основі обробки вмісту матриці рішень, де $T_{ij} = T_{GA}$:

$$\begin{array}{cccccc} & w_1 & \cdots & w_j & \cdots & w_m \\ d_1 & T_{11} & \cdots & T_{1j} & \cdots & T_{1m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ d_i & T_{i1} & \cdots & T_{ij} & \cdots & T_{im} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ d_n & T_{n1} & & T_{nj} & & T_{nm} \end{array} \quad (1)$$

Множина значень величини показника $T_{ij} = T_{GA}$, розташованих по елементах матриці рішень $\|T_{ij}\|$, залежно від умов експериментального випробування, характеризуються перетинами доданих означень множин комбінацій незалежних змінних $W = \{w_j\}$ (верхній рядок) та залежних змінних $D = \{d_i\}$ (крайній лівий стовпчик). Кожний елемент $w_j \in W$ уособлює одну з можливих комбінацій значень незалежних змінних, $j = \overline{1,m}$, а кожний елемент $d_i \in D$ – одну з можливих комбінацій залежних (контрольованих) змінних опису умов певної ітерації експериментального випробування, $i = \overline{1,n}$.

Результатом обробки матриці рішень (1) у термінах понятійного апарату теорії ПР в умовах невизначеності є вибір одного з можливих альтернативних рішень або альтернативи. Поняття альтернативного рішення (альтернативи) відповідає $\underline{i}$-му порядковому номеру елемента $d_i \in D$ (i-го рядка матриці рішень), а обґрунтування його вибору є результатом застосування критеріїв максиміну, Байєса-Лапласа та Севіджа з урахуванням особливостей постановки задачі. Вибір одного з альтернативних рішень уособлюється з вибором експлойту (з існуючої колекції експлойтів), який є найбільш придатним для компрометації одного з компонентів *Server-Side Web Application* системи (об'єкта критичної інформаційної інфраструктури ОКІ) при проходженні Дослідником казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application*.

Орієнтовна розмірність матриці рішень для кожної з категорії дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application* може бути оцінена на підставі відповідного значення *Total CVEs* – загальна кількість *CVE* в категорії *Top 10 Web Application Security Risks*. Необхідно зазначити, що значення *Total CVEs* = 0 у категорії *A06:2021 Vulnerable and Outdated Components* відображає практично несуттєву ймовірність успіху Дослідника для казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application.*

Застосування критерію максиміну базується на припущенні, що обране на його основі рішення не може бути гіршим за будь-яке інше з множини альтернатив. Правило вибору альтернативного рішення $d_i = min\ \ T_{ik}$, де $T_{ik} = \underset{j}{max} T_{ij}$, передбачає доповнення матриці $\|T_{ij}\|$ стовпчиком із найбільшими значеннями T_{ij} у кожному рядку. Рішенням є вибір j-го рядка $\|T_{ij}\|$, для якого $d_i = min\ \ \underset{j}{max} T_{ij}$.

За наявності статистично вичерпної вибірки результатів експериментальних випробувань наявної колекції експлойтів для кожної категорії дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application* доцільно розглянути застосування критерію Байеса-Лапласа. Правило вибору одного з альтернативних рішень $d_i = max\ \ \overline{T}_{ik}$, $\overline{T}_{ik} = \sum_{j=1}^{n} T_{ij} \cdot p_j$, $\sum_{j=1}^{n} p_j = 1$, де $\overline{T}_{ik}$– середні значення показника T_{ik}, p_j – ймовірність здійснення спроби експлуатації дефекту (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application,* яка відповідає умовам експерименту w_j. Ймовірності здійснення експерименту з умовами w_j відомі та не залежать від часу спостереження. Критерій Байеса-Лапласа передбачає доповнення матриці $\|T_{ij}\|$ стовпчиком із величиною математичного очікування величини значень $\overline{T}_{ik}$ у кожному рядку. Обирається j-й рядок $\|T_{ij}\|$, який відповідає альтернативі d_i, для якої величина T_{ij} (у додатковому стовпчику зі значеннями математичного очікування) є найменшою. Застосування критерію Байеса-Лапласа передбачає зростання достовірності результату при збільшенні множини результатів експериментів (теоретично до нескінченності) і ризику неправильного рішення при їх відносно невеликій кількості. Поява умов ризику для критерію Байеса-Лапласа доцільна

за принципом "недостатності обґрунтування" та на практиці має більш широке розповсюдження. За відсутності достатньо повної, великої та репрезентативної вибірки значень результатів експериментів замість математичного очікування величини $\overline{T}_{ik}$ пропонується використовувати середнє математичне $\hat{T}_{ik} = \frac{1}{n}\sum_{j=1}^{n} T_{ij}$.

Критерій Севіджа використовує поняття додаткової втрати при виборі альтернативи d_i для умов w_j, яка має відмінне від найкращого значення оціночної функції. Правило вибору одного з альтернативних рішень базується на використанні величини залишків $d_i = \min_i \max_j (\max_i T_{ij} - T_{ij})$. Обчислення залишків $\Delta T_{ij} = \max_i T_{ij} - T_{ij}$ здійснюється стовпцями $\|T_{ij}\|$ шляхом віднімання від максимального значення T_{ij} у стовпчику від значення кожного його елемента. Для зручності оперування значеннями залишків при виборі рішення утворюють матрицю залишків $\|\Delta T_{ij}\|$ всіх елементів $\|T_{ij}\|$. Критерій Севіджа передбачає доповнення $\|\Delta T_{ij}\|$ стовпчиком максимальних залишків у рядку $\max_j \Delta T_{ij}$. Далі обирається j-й рядок $\|T_{ij}\|$, який відповідає альтернативі d_i, для якої величина $\max_j \Delta T_{ij}$ (у додатковому стовпчику $\|\Delta T_{ij}\|$) є найменшою.

Висновки. Взагалі, вибір рішень із кількох можливих (на основі матриці рішень) не є однозначним, оскільки найкраще значення оціночного показника може спостерігатися у кількох альтернатив. Наявність лише однієї альтернативи притаманно, зазвичай, досить простим (елементарним) та детермінованим процедурам вибору рішення.

Подальші дослідження здійснюються за напрямком забезпечення розв'язання більш складних (структурованих, багатоетапних) задач діяльності Дослідника вразливості системи (об'єкта критичної інформаційної інфраструктури ОКІ), які досить органічно конструюються з елементарних процедур застосування критеріїв ПР в умовах невизначеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. С. 42. Ст. 403.

2. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX // Офіційний вісник України. 2021. № 98. С. 23. Ст. 6341.

3. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: постанова Каб. Міністрів України від 19.06.2019 № 518 // Офіційний вісник України. 2019. № 50. С. 53. Ст. 1697.

4. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

5. 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.

6. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: постанова Каб. Міністрів України від 16.052023 № 497 // Офіційний вісник України. 2023. № 52. С. 72. Ст. 2911.

7. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

8. The Unified Kill Chain. URL: https://www.unifiedkillchain.com.

9. Certified Ethical Hacker. URL: https://cert.eccouncil.org/certified-ethical-hacker.html.

10. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.

11. Common Weakness Enumeration. URL: https://cwe.mitre.org.

12. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org.

13. Герасимов Б. М., Камишин В. В. Організаційна ергономіка: методи і алгоритми дослідження та проектування. К.: Інфосистем, 2009. 212 с.

14. Герасимов Б. М., Локазюк В. М., Оксіюк О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень: навч. посіб. К.: Вид-во Європ. ун-ту, 2007. 335 с.

15. Терещенко Т. П., Остапчук В. М., Хусаінов П. В., Черниш Ю. О. Оцінка та запобігання прояву вразливості Server-Side Web Application // Системи і технології зв’язку, інформатизації та кібербезпеки. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2024. № 5. 240 с. DOI: 10.58254/viti.5.2024. С. 204–214.

16. Черниш Ю. О., Хусаінов П. В., Терещенко Т. П. Прийняття рішень в процесі пошуку вразливості Server-Side Web Application // Системи і технології зв’язку, інформатизації та кібербезпеки. Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2024. № 6. 280 с. DOI: 10.58254/viti.6.2024. С. 264–274.

DOI: 10.58254/viti.7.2025.22.243

УДК 519.718.2

канд. техн. наук, доцент Штаненко С. С. ORCID: 0000-0001-9776-4653 (ВІТІ ім. Героїв Крут)
д-р техн. наук, професор Толюпа С. В. ORCID: 0000-0002-1919-9174 (КНУ ім. Т. Шевченка)
д-р техн. наук, професор Самохвалов Ю. Я. ORCID: 0000-0001-5123-1288 (КНУ ім. Т. Шевченка)

ДІАГНОСТИЧНА МОДЕЛЬ РОЗПІЗНАВАННЯ ТЕХНІЧНОГО СТАНУ МІКРОПРОЦЕСОРНИХ СИСТЕМ З ЕЛЕМЕНТАМИ ШТУЧНОГО ІНТЕЛЕКТУ

У статті запропонована діагностична модель розпізнавання технічного стану мікропроцесорних систем, в основу якої покладено ідеї штучного інтелекту. Проведено аналіз існуючих моделей та методів розпізнавання технічного стану, наведено недоліки та переваги. Доведено, що найбільш ефективними є дискретні моделі, які реалізовані у вигляді нейронних ансамблів та являють собою нелінійні перетворювачі аналогової інформації, що задається набором певних статистичних і динамічних характеристик. При цьому формування ансамблів у нейронній мережі відповідає запам'ятовуванню образів, ознак, об'єктів тощо. Обґрунтовано, що опис технічного стану мікропроцесорних систем шляхом застосування дискретно-подійної моделі, в якій причинно-наслідкові зв'язки являють собою дискретні випадкові марківські ланцюги, в сукупності зі штучною нейронною мережею відкривають нові можливості щодо інтелектуалізації процедури розпізнавання технічного стану мікропроцесорних систем. Взагалі дана стаття належить до серії наукових робіт, які пов'язані з вирішенням основних задач технічної діагностики, а саме: оцінкою технічного стану мікропроцесорних систем, а також виявленням та локалізацією несправностей за умови, що мікропроцесорні системи реалізовані на програмованих логічних інтегральних схемах та функціонують в умовах деструктивних несприятливих впливів.

Ключові слова: *обчислювальна техніка, мікропроцесорна система, технічна діагностика, штучна нейронна мережа, нейроморфна система.*

S. Shtanenko, S. Toliupa, Y. Samokhvalov. Diagnostic model for identifying the technical condition of microprocessor systems with elements of artificial intelligence

The article proposes a diagnostic model for recognizing the technical condition of microprocessor systems, which is based on the ideas of artificial intelligence. An analysis of existing models and methods of recognizing the technical condition is carried out, the disadvantages and advantages are given. It has been proven that the most effective are discrete models, which are presented in the form of neural ensembles, and are nonlinear converters of analog information specified by a set of certain statistical and dynamic characteristics. At the same time, the formation of ensembles in the neural network corresponds to the memorization of images, signs, objects, etc. It is substantiated that the description of the technical state of microprocessor systems through the use of a discrete-event model, in which cause-and-effect viscous systems represent discrete random Markov chains in combination with an artificial neural network, opens up new opportunities for the intellectualization of the procedure for recognizing the technical state of microprocessor systems. In general, this article is a series of works related to the consideration of the main tasks of technical diagnostics, namely: assessment of the technical condition of microprocessor systems, as well as detection and localization of malfunctions, provided that the microprocessor systems are implemented on programmable logic integrated circuits and function in the conditions of internal and external adverse influences.

Keywords: *computer technology, microprocessor system, technical diagnostics, artificial neural network, neuromorphic system.*

Постановка завдання. Створення апаратних і програмних засобів обчислювальної техніки, їх широке застосування в різних галузях виробничої діяльності людини висували на передній план одну з найактуальніших задач – контроль і діагностування мікропроцесорних систем, які є основою побудови сучасної обчислювальної техніки. Забезпечення високих показників надійності обчислювальної техніки, а також контроль і діагностування мікропроцесорних систем на різних етапах їх життєвого циклу неможливо без інтенсивного

розвитку теорії технічної діагностики й ефективного впровадження її результатів у практику [1].

Контроль і діагностування апаратних та програмних складових мікропроцесорних систем є, мабуть, одним із найскладніших технологічних процесів. Його складність обумовлена необхідністю глибоких знань як апаратної, так і програмної складових. Враховуючи те, що сучасні мікропроцесорні системи побудовані на мікросхемах різного ступеня інтеграції, доступ до контрольних точок ускладнений, а в деяких випадках і зовсім неможливий. Крім цього мікропроцесорні системи можуть включати в себе системні та прикладні додатки на мовах кількох рівнів, що теж суттєво ускладнює процес їх контролю та діагностування [2]. Тому проблеми, які постають на різних етапах життєвого циклу сучасних мікропроцесорних систем, потребують подальшого розвитку методології їх контролю та діагностування з урахуванням сучасної елементної бази, а також можливістю накопичення раніше отриманого досвіду. Таким чином, **актуальним науковим завданням** є розробка діагностичної моделі розпізнавання технічного стану мікропроцесорних систем, в основу якої покладено ідеї штучного інтелекту.

Аналіз останніх публікацій. На сьогодні питанням контролю та діагностування мікропроцесорних систем присвячено велику кількість наукових праць.

Так, робота [3] присвячена питанням тестового комбінаційного тестування мікропроцесорів сучасних персональних комп’ютерів. У статті [4] представлено методику фізичного діагностування цифрових пристроїв об’єктів радіоелектронної техніки, основою якої є енергодинамічні, енергостатичні та електромагнітні методи діагностування. В роботі [5] представлено порівняльний аналіз методологій технічного діагностування радіоелектронної техніки та визначено напрямки подальших досліджень в галузі технічної діагностики, які пов’язані з автоматизацією системи технічної діагностики. Стаття [6] продовжує серію робіт з обґрунтування створення автоматизованої системи діагностування та контролю сучасних апаратно-програмних засобів шляхом включення до складу діагностичної системи набору програмних модулів (програм), що реалізують методи непрямого контролю. В роботах [7; 8] запропоновано для вирішення основних задач технічної діагностики, а саме оцінки технічного стану складних технічних систем та прогнозування, застосувати штучні нейронні мережі. Але особлива увага щодо інтелектуалізації процедури діагностування мікропроцесорних пристроїв та систем приділена в роботі [9], де розглянуто основні компоненти штучного інтелекту, наведено переваги та недоліки застосування тих або інших компонентів.

Однак поява сучасної елементної бази для проєктування мікропроцесорних систем, а також умови функціонування обчислювальної техніки при деструктивних впливах вимагають пошук нових методів контролю та діагностування з метою виявлення та локалізації несправностей, а також розробки діагностичних моделей розпізнавання технічного стану мікропроцесорних систем, реалізованих у базисі програмно-реконфігурованої логіки [10].

Зважаючи на сказане, **метою статті** є обґрунтування необхідності розробки діагностичної моделі розпізнавання технічного стану мікропроцесорних систем, в основу якої покладені ідеї штучного інтелекту.

Аналіз діагностичних моделей та методів. Під діагностичною моделлю розуміють формальний опис мікропроцесорної системи, що піддається діагностуванню та враховує можливі зміни її технічного стану [11]. Такі моделі можуть бути представлені в аналітичній, табличній, векторній, графічній та інших формах.

У свою чергу діагностичний процес розпізнає технічний стан мікропроцесорної системи відповідно до зовнішніх проявів (симптомів), які реєструються системою технічного діагностування (СТД). При цьому по відношенню до симптомів СТД постає як система обробки діагностичної інформації для прийняття рішення про технічний стан

мікропроцесорної системи. Тому для створення СТД необхідна модель, що містить у своєму складі мікропроцесорну систему (далі ОД – об’єкт діагностування), симптоми та безпосередньо саму СТД, яка в подальшому і буде основою для побудови системи розпізнавання технічного стану.

Всі діагностичні моделі ОД можна поділити на три основні групи: безперервні, дискретні та спеціальні. Розглянемо їх більш детально.

Так, безперервні моделі представляють ОД у тому випадку, коли процеси протікають у часі, що безперервно змінюється, та є аргументом відповідних функцій. Вони використовуються при розробці діагностичного забезпечення для окремих пристроїв та приладів, що входять до ОД й описуються диференційними лінійними та нелінійними рівняннями.

У свою чергу дискретні моделі (ДМ) визначають стан ОД лише послідовності дискретних значень незалежної змінної (часу), але не враховуючи характеру перебігу процесу у проміжках.

Якщо розглядати спеціальні моделі, то вони поділяються на три групи: інформаційні моделі, моделі характеристик об’єкта та функціональні моделі.

Інформаційні моделі описують інформаційні потоки, що циркулюють в ОД, які розглядаються як перетворювачі інформації, або подають інформаційну оцінку змін, що відбуваються у стані ОД.

Моделі показників можуть представляти як статичні, так і динамічні властивості ОД загалом чи його окремих елементів.

Функціональні моделі відображають операції, що виконуються ОД в режимах і можуть бути схемою зв’язків між окремими конструктивними блоками, або алгоритми виконання об’єктом або його частинами покладених на нього функцій.

Зазначимо, що будь-які з різновидів ДМ можуть використовуватися індивідуально або в комбінації відповідно до умов, в яких розробляється діагностичне забезпечення з урахуванням специфіки ОД.

Якщо розглядати методи, які використовуються при дослідженні діагностичних моделей, то вони поділяються на аналітичні, графічні та графо-аналітичні.

Аналітичні методи дозволяють застосовувати зручні способи оптимізації та отримати співвідношення, що характеризують об’єкт при зміні його стану.

До них належать методи малого параметра, теорії чутливості, математичної логіки, планування експерименту та розпізнавання образів. Аналітичні моделі досить ефективні при аналізі будь-якого ДМ, проте зі зростанням складності моделей рішення стає надто громіздким.

Графічні методи мають велику наочність і можуть служити як безпосередньо, так і для ілюстрації аналітичних методів. Серед графічних методів особливе місце посідають методи, засновані на теорії графів (орієнтованих та неорієнтованих).

Графо-аналітичні методи є різними комбінаціями графічних та аналітичних методів.

Так, при аналізі ДМ досить часто користуються апаратом математичної логіки, головним завданням якої є структурне моделювання об’єктів. За допомогою такого апарату може здійснюватись і аналіз спеціальних ДМ, що характеризуються кінцевим числом станів.

Однак відповідно до [12], найбільш перспективним напрямом у розробці ДМ є їх представлення у вигляді нейронних ансамблів. При цьому ансамбль може бути описаний як нелінійний перетворювач аналогової інформації, що задається набором певних статистичних і динамічних характеристик. Формування ансамблів у такій мережі відповідає запам’ятовуванню образів (ознак, об’єктів, подій, понять). Ансамблі формуються у процесі навчання під час подачі на мережу набору вхідних образів, тобто діагностичних портретів зовнішнього середовища.

Групи нейромереж, що мають зв’язок між собою і найбільш часто збуджуються одночасно, утворюють ядра ансамблів. У них накопичуються комбінації діагностичних ознак, що найчастіше зустрічаються в портретах, тому ядра можна розглядати як відображення образів діагнозів (класів) об’єктів, які об’єктивно існують у зовнішньому середовищі.

Більш рідкісні комбінації збуджених елементів нейромережі утворюють бахрому ансамблів, у якій фіксуються індивідуальні особливості об’єктів зовнішнього середовища. При подачі на навчену ансамблеву нейромережеву систему (НМС) деякого вхідного діагностичного портрета здійснюється відновлення найближчого до нього образу, з числа тих, що запам’ятовувалися в НМС (рис. 1).

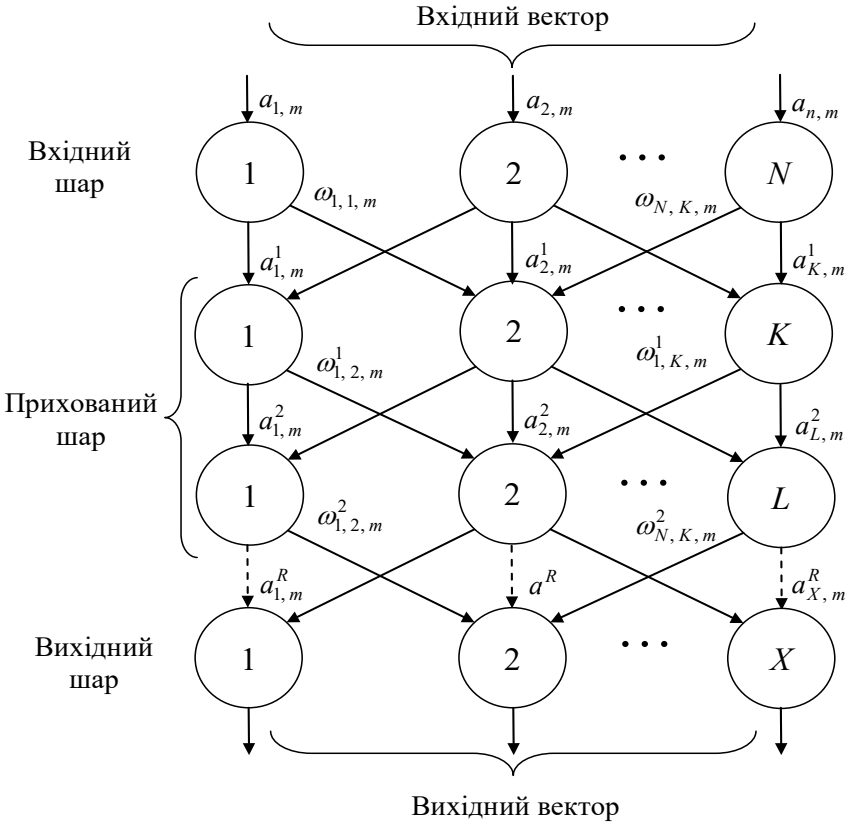


Рис. 1. Нейромережева система

Зазначимо, що при виборі ДМ необхідно виходити з того, що нейромережева система розпізнавання технічного стану (далі НМС РТС) повинна бути реалізована на основі прийнятої концепції комбінованих детермінованих самоорганізованих (адаптивних) систем. Ця вимога обумовлена тим, що СТД обов’язково повинна мати досить високу початкову структурну організацію. Крім того, НМС РТС має орієнтуватися на всю номенклатуру існуючого та перспективного парку ОД та на великий клас технічних станів, що функціонує в умовах апріорної статистичної невизначеності.

Крім цього, представлення ДМ у вигляді нейромережевих ансамблів обумовлено низкою унікальних властивостей нейромережі, а саме:

яскраво виражена паралельність поширення активності через мережу та обробка всієї інформації у вигляді локальних взаємодій між сусідніми вузлами, тобто паралельність обробки інформації у нейромережі;

агрегатна розподіленість – властивість, що визначає здатність зберігання фрагментів знань у кількох вузлах мережі, кожен із яких може разом з іншими елементами використовувати зберігання декількох фрагментів;

асоціативність, тобто здатність НМС РТС відновлювати інформацію, що зберігається в них, за наявною частковою (фрагментальною) інформацією;

здатність нейромережі до навчання та самонавчання, що є основною «інтелектуальною» властивістю, та здійснювати функціонування без жорстких зовнішніх програм. Ця властивість нейромережі визначає можливість її параметричної адаптації до задач, що розв’язуються;

надійність – відмінна властивість НМС РТС, вихід з ладу деякої частини її елементів не призводить до відмови у роботі всієї мережі.

Так, сукупність перерахованих властивостей нейромережі призводить до появи в ній здатності довільного виникнення інтелектуальних якостей, внаслідок чого вона об’єктивно може стати основою для побудови нового покоління високоефективних інтелектуальних діагностичних систем.

На підставі проведеного в роботах [12; 13] аналізу особливостей вирішення задачі діагностування МПС, а також виходячи з розглянутих загальних вимог до НМС РТС та на основі принципу її адекватності зовнішньому середовищу, сформулюємо загальні вимоги до діагностичної моделі.

1. Діагностична модель має бути дискретною, лінійною, стаціонарною системою, якій властива безперервність та дискретність зміни стану у часі.

2. Модель має бути ймовірнісною, тому що технічний стан ОД є ланцюжком ймовірнісних подій.

3. Модель має бути динамічною, здатною описувати поведінку ОД у часі, оскільки значна частина діагностичної інформації з’являється саме у процесі перемикання, у перехідному режимі, на малих інтервалах часу.

4. Модель повинна бути зв’язковою (коннекціоністською), оскільки фізично ОД є мережевою структурою, яка (виходячи з принципу адекватності) і повинна бути покладена в основу моделі.

На сьогодні згідно з [14] переліченим вимогам задовольняє детерміновано-стохастична діагностична модель, яка може бути представлена у графо-аналітичному вигляді. Причому ступінь її детермінізму визначається, з одного боку, необхідністю задоволення всього різноманіття ОД і, з іншого боку, – застосовністю дискретно-подійного методу синтезу структури НМС РТС. При цьому дискретно-подійний синтез здійснюється адекватним відображенням детермінованої частини діагностичної моделі на структуру та параметри детермінованої частини НМС РТС. Стохастична частина діагностичної моделі відображається на структуру індетермінованої частини НМС РТС у процесі структурної та параметричної самоорганізації.

Слід зазначити, що графо-аналітичний підхід до діагностичної моделі має на увазі коннекціоністську (пов’язану) модель (рис. 2) переходу з технічного стану A_i в стан A_j із щільністю ймовірності переходу a_{ij}.

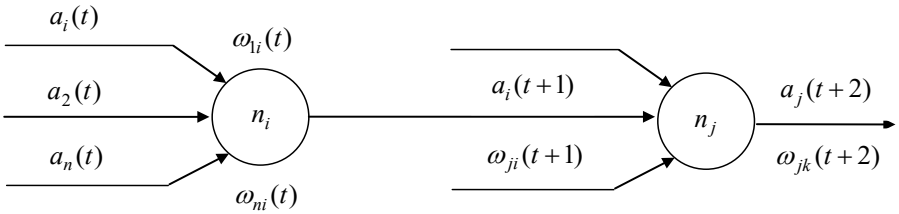


Рис. 2. Коннекціоністська модель переходу з одного технічного стану в інший

Імовірності переходу можна знайти у загальному вигляді шляхом розв'язання диференціального рівняння (1):

$$dP_i(t) \Big/ dt = \sum_{j=1}^{n} \alpha_{ij} P_j(t) - P_i(t) \sum_{i=1}^{m} \alpha_{ij} \,, \tag{1}$$

де m, n – розмірність простору технічного стану ОД.

У загальному вигляді закон, який описує можливість перебування ОД у стані A_i, невідомий. Однак діагностична модель може бути представлена сукупністю переходів ОД із стану в стан, що підпорядковуються пуассонівському потоку подій. Під подіями розуміються зміни технічного стану у дискретні моменти часу ОД, які підлягають розпізнаванню. Зміни технічного стану ідеалізуються як миттєві, а еволюційні зміни, які відбуваються, не беруться до уваги. Так як динаміка технічного стану ОД розвивається від події до події, то фазова траєкторія такої динамічної дискретно-подійної системи описується кусковою лінією. Відрізки такої кусково-ламаної лінії відображають послідовність технічних станів ОД, а їх тривалість відображає час перебування у відповідному стані. Між переходами A_i та A_j існує причинно-наслідковий зв'язок, тобто стани є зв'язаними (коннекціоністськими). Як випливає з виразу (1), еволюція дискретно-подійних систем, що розпізнають, в просторі технічних станів ймовірно визначена.

Основою коннекціоністської діагностичної моделі є реалізація причинно-наслідкового зв'язку між подіями: здійснення першої події є достатньою підставою для очікування того, що станеться друга подія, потім третя і так далі по всій фазовій траєкторії. Причинно-наслідкові зв'язки у всьому просторі технічних станів ОД описуються операторами, які складаються з операторних компонентів і описують перехід із одного технічного стану до іншого. Поділ та об'єднання причинно-наслідкових зв'язків створює можливість ієрархічної структуризації та аналізу технічного стану ОД на будь-якому рівні деталізації.

Поняття зв'язності технічних станів дискретно-подійної діагностичної моделі можна сформулювати наступним чином. Дві події A_i та A_j у просторі технічних станів ОД будуть зв'язаними, якщо існує процес (оператор) L, що дозволяє спостерігати (виявляти) існуючий зв'язок. Прояв (реєстрація) існуючого зв'язку може відбуватися безпосередньо (за явними діагностичними ознаками дефекту) або опосередковано (через симптоми дефекту). Крім цього, зв'язок між подіями повинен бути ймовірно визначений, а процес (оператор) – реалізований у часі (2):

$$\exists L\left[P_i(t)(f : R_i(A_i, X))\right] \to (R_j(A_j, X)) \,. \tag{2}$$

Зв'язаність проявляється як між подіями A_i, A_j, так і в середині події (між символами і станом) через предикати зв'язку $R_i(A_i, X)$, $R_j(A_j, X)$, тобто зв'язність схильна до ієрархічної структуризації. Вираз (2) свідчить про таке: для того щоб пов'язати події – необхідні обставини прояву зв'язку. Події, які мають наслідки, повинні бути узгоджені з обставинами зв'язку у часі. Оскільки еволюція технічних станів ОД у часі представляється фазовою траєкторією у просторі технічного стану, має сенс говорити про зв'язок не лише двох подій, а про зв'язок множини подій. Це означає, що оператор зв'язку (2) необхідно застосувати багаторазово.

Таким чином, розпізнавання події в просторі технічних станів можна уявити полем (ланцюгом) причинно-наслідкових зв'язків, що беруть початок на операторах, які їх

формують. При цьому будь-які події у просторі технічних станів можуть вважатися зв'язковими, якщо перше має змінене поле, що досягає другої події. Такі дискретно-подійні системи можуть у подальшому бути представлені у вигляді дискретних діагностичних моделей.

Марківська модель системи технічного діагностування. Діагностичний процес, що протікає в СТД, розпізнає технічний стан у більшості випадків опосередковано (зовнішніми проявами, симптомами дефекту). Явні діагностичні ознаки призводять до тривіальних рішень у процесі розпізнавання технічного стану та практичного інтересу не становлять. Симптоми дефекту, як елемент дискретно-подійного процесу, пов'язані з технічним станом предикатів зв'язку. Фізично симптоми у СТД видаються стаціонарними діагностичними ознаками (портретами). По відношенню до діагностичних ознак СТД виступає як система обробки діагностичної інформації для прийняття рішення про технічний стан ОД.

Діагностична система, що складається з ОД, в кожен довільний момент часу $t_k, t_k \in T$ може перебувати в одному зі станів $S_i, ..., S_\alpha, ..., S_r, S_\alpha \in S$. У дискретні моменти часу система зазнає змін стану відповідно до ймовірнісного правила (2). При цьому як стан системи загалом, так і ОД, однозначно визначають сукупність діагностичних ознак (портретів):

$$A_2 = \bigcup_{\mu=1}^{N} A_\mu \,, \tag{3}$$

де (A_1) – стан правильного функціонування ОД;

(A_2) – стан неправильного функціонування ОД;

$|N|$ – потужність простору технічного стану мікропроцесорної системи.

Таким чином, повний детерміновано-стохастичний опис такої дискретно-подійної системи μ, $\mu = 1, ..., M$ вимагає визначення початкового стану системи $S_\alpha \in S$ в момент часу $t = 0$ і ймовірнісного опису поточного стану q_t в момент часу t.

При описі процесу переходу СТД зі стану S_i до стану S_j необхідно зберегти марківську властивість еволюції технічного стану ОД в якості фазової траєкторії у просторі технічного стану.

Поле причинно-наслідкових зв'язків у дискретно-подійній діагностичній моделі є дискретним випадковим марківським полем (ланцюгом), тому що необхідно лише ймовірно визначати поточний та попередній стани, а для інтервалів $t = t_j - t_i$, $t_{i(j)} \in T$ ймовірність збереження попереднього стану значно перевищує ймовірність зміни стану.

Перехідна ймовірність при цьому не залежить від часу t, а залежить лише від номера спостереження стану (4):

$$\alpha_{i,j} = P(qt = S_i / q_t - 1)\,,\ i, j = 1, 2, ..., k\,. \tag{4}$$

Вона має наступні властивості:

$$\alpha_{i,j} > 0 \text{ і } \sum_{j=1}^{k} \alpha_{i,j} = 1,$$

оскільки задовольняє звичайним ймовірнісним обмеженням. Це марківська модель, яка спостерігається, тому що в кожен момент часу спостерігається поточний технічний стан, який пов'язаний із конкретним діагностичним портретом. Однак при діагностуванні поряд із контролем технічного стану проводиться пошук дефекту, який здійснюється послідовністю

спостережень (перевірок). Імовірність виявлення дефекту через d спостережень $0 = \{S_{i1}, S_{i2}, ..., S_{id}, S_{i(d+1)} \neq S_i\}$ при рівноймовірних переходах, отримаємо

$$P_i(d) = (\alpha_{i,j})^{d-1}(1-\alpha_{i,j}). \quad (5)$$

Ця експоненційна функція є характеристикою тривалості даного стану в ланцюзі Маркова. Використовуючи $P_i(d)$, можна обчислити очікувану кількість повторень стану (6):

$$d_i = \sum_{d=1}^{\infty} d_{pi}(d) = \sum_{d=1}^{\infty} d(\alpha_{i,j})(1-\alpha_{i,j}) = 1/1-\alpha_{i,j}. \quad (6)$$

Зазначимо, що при розпізнаванні технічного стану ОД доводиться мати справу зі складним стохастичним процесом, що складається з кількох випадкових процесів, один із яких є основним і не спостерігається, тобто є прихованим (про нього можна лише судити за допомогою іншого випадкового процесу). Прихований дефект виявляється стохастичними методами, наприклад, подачею шумоподібних тестів, орієнтованих не на конкретний дефект, а на отримання реакцій від цього дефекту, а також ланцюжком послідовних спостережень діагностичних портретів, кількість яких визначається на підставі виразу (6). А це вже є прихований марківський процес, для опису якого необхідно задавати наступні елементи моделі, а саме:

1. Число прихованих станів у моделі – M. Воно визначається числом можливих дефектів структурних елементів ОД та їхньою комбінацією, оскільки будь-який із цих елементів може бути дефектним. Це число класів технічних станів A_μ, що розпізнаються, $\mu = 1, ..., M$ – алфавіт діагностичних ознак (класів).

2. Число різних знаків спостереження N, які можуть народжуватися моделлю, тобто розмір дискретного алфавіту, який визначається числом символів у діагностичному портреті $X = \{x_i, ..., x_n\}$.

3. Розподіл ймовірностей переходів між станами, матрицю перехідних ймовірностей $A = \{\alpha_{i,j}\}$. Тут $\alpha_{i,j} = P(S_j | S_{j-1}, ..., S_i)$ – ймовірність події у дискретно-подійній моделі.

Вона визначає той факт, що в момент часу t_i стан СТД буде S_j за умови, що відбулися переходи $S_{\alpha 1} \wedge S_{\alpha 2} \wedge ... \wedge S_i$. Простір станів $S_\alpha \in S$ є зв'язаний, тому що ймовірність події в момент t_j залежить від стану системи в момент часу t_i.

4. Розподіл ймовірностей появи символів спостереження в стані j:

$$B = \{b(k)\},\ b(k) = P(X_k | q_t = S_j),\ j = 1, ...,\ M,\ k = 1, ...,\ N.$$

5. Початковий розподіл ймовірностей станів:

$$\Pi = \{\Pi_i\},\ \Pi_i = P(q_1 = S_i) = P(S_1, ..., S_{\nu-1}),$$

де ν – число, що визначає складність станів.

Таким чином, процедура побудови прихованої марківської моделі (ПММ) полягає в наступному:

1. Вибирається початковий стан $q_1 = S_i$ відповідно до розподілу та зв'язності Π.

2. Встановлюється початковий час $t = 1\ (t = t_1)$.

3. Вибирається X відповідно до розподілу ймовірностей появи символів алфавіту в стані S_i, тобто відповідно до $d_i(k)$.

4. Здійснюється перехід до нового стану $q_{t+1} = S_i$ відповідно до перехідних ймовірностей α_{ij}.

5. Встановлюється значення $t = t + 1$ і, якщо $t < T$, здійснюється перехід до кроку 3, інакше процедура закінчується.

Так, згідно з [15] еволюція технічного стану ОД в просторі станів, що мають конфігурацію $\Omega = S^T$, може бути описана із застосуванням дискретно-подійної моделі СТД у вигляді ПММ.

Для цього передбачається завдання двох параметрів моделі N і M, множини допустимих символів спостереження, а також трьох ймовірнісних заходів A, B, Π, тобто $L(A, B, \Pi)$.

Оптимальний вибір параметрів моделі $L(A, B, \Pi)$ здійснюється під час її створення, коли вона найкраще відповідає наявним спостереженням.

При цьому має існувати послідовність спостережень, яка використовується для створення моделі. Ця послідовність спостережень є стохастичною частиною моделі, яка навчається. Процес навчання дуже важливий, оскільки під час навчання відбувається параметрична самоорганізація системи за даними спостереження, внаслідок чого створюється модель СТД, що найкраще відповідає реальному стану.

Наведена ПММ використовується для синтезу структури класифікатора, що розпізнає невідомий технічний стан.

При цьому класифікатор на заданій послідовності спостережень $0 = 0_1, 0_2, ..., 0_T$ обчислює ймовірність появи даної послідовності для конкретної моделі $P(O/L)$.

Далі для технічного стану, що розпізнається, вибирається такий стан, для моделі якого ця ймовірність найбільша, тобто проводиться оцінка методом максимальної правдоподібності.

Дискретно-подійна модель СТД в якості ПММ є вихідною при синтезі структури НМС РТС. Послідовність спостережень технічних станів ОД сприйматиметься матрицею рецепторів, синтезованою з урахуванням розподілу ймовірностей спостереження стану $B = \{b(k)\}$.

Якщо кількість помітних символів спостереження становить N, то марківське інформаційне поле технічних станів може бути ототожнено з вершинами N-мірного куба.

Задача матриці ймовірностей появи символів спостереження полягає в редукції марківських полів, при цьому простір технічних станів може бути представлений як n-мірний евклідів простір.

Висуваються $(M + 1)$ гіпотези $H_1, H_2, ..., H_\mu, H_{N,M}$ про належність спостережуваних станів S_n – класу технічних станів.

Таким чином, задача розпізнавання технічного стану полягає в тому, щоб за результатами спостереження прийняти одну з гіпотез H_M про стан неправильного або правильного функціонування H_{M+1} та відхилити інші.

Для цього в n-мірному евклідовому просторі станів необхідно побудувати замкнуту поверхню, що поділяє ситуацію A_1 і A_2.

Ситуація A_2 при цьому не задовольняє гіпотезі компактності. Навчальна послідовність свідомо не міститиме достатньої для якісної моделі числа спостережень. Рішення про прийняття гіпотези ґрунтується на вектор-відношенні правдоподібності, що несе всю інформацію про гіпотези, що перевіряються. Обчислювані в класифікаторі компоненти $(M + 1)$-мірного вектора відносин правдоподібності є критерієм, який дозволить побудувати нелінійну поверхню, що розділяється. Тоді вирішальне правило можна записати:

$$S_\alpha \in A_1, \text{ якщо } f(A_1/S) > P_\mu P(X/H_\mu);\ S_\alpha \in A_2, \text{ якщо } f(A_2/S) > P_\mu P(X/H_\mu), \qquad (7)$$

де $f(A_2/S)$ – функція ймовірності приналежності ситуації S_α до A_1 або A_2, яка задовольняє умову

$$f(A_2/S_0) = P_0 P(X/H_0) \text{ при } f(A_1/S) = P_0 P(X/H_0).$$

Процедура розпізнавання технічного стану полягає в обчисленні функції $f(A_1/S)$ та виборі раціональної поверхні, яка розділяється $f(A_1/S) - P_\mu P(X/H_\mu) = 0$.

Її реалізація полягає у виконанні ітеративної процедури

$$\|S_\alpha\|_{r+1}^{-1} = \|S_\alpha\|_r^{-1} + \Gamma(Z)\|A_m\|_r \left\|S_\alpha^*\right\|_r^{-1},$$

де $\|S_\alpha\|_{r+1}$ – матриця ситуацій розмірності $(r+1)$;

Z – розмірність простору станів на $(r+1)$ кроці, $Z \in M$;

$\|A_m\|_r$ – неузгодженість ситуацій;

$\left\|S_\alpha^*\right\|$ – правильне значення станів, що визначається під час спостережень.

Зазначимо, що процес розпізнавання буде ітеративним, оскільки НМС РТС необхідно постійно донавчати. У цьому ситуація $S_\alpha \in S$ описується діагностичним портретом, виходячи з символів спостереження та матриці $B = \{b(h)\}$, а зв'язок станів у матриці ситуацій $\|S_\alpha\|_{r+1}^{-1}$ розмірності $(r+1)$ – матрицею перехідних ймовірностей $A = \|\alpha_{ij}\|$ ПММ.

Крім цього якість діагностичної інформації однозначно пов'язана з кількістю діагностичних параметрів і кількістю контрольних точок. Очевидно, що для збільшення кількості діагностичної інформації $I = \log N$ необхідно збільшити кількість символів спостережень N у дискретному алфавіті ПММ. Оскільки спостереження здійснюються за допомогою зняття діагностичних портретів при фіксованому алфавіті (числі контрольних точок ОД), то для збільшення кількості діагностичної інформації необхідно збільшувати відносну ентропію діагностичного портрета:

$$H = -\sum_{i=1}^{k} b_i \log b_i, \tag{8}$$

де k – число контрольних точок;

b_i – ймовірність появи символів спостереження з матриці $\|B\|$ у структурі ПММ.

При цьому діагностичний портрет повинен із більшим чи меншим ступенем достовірності відображати технічний стан ОД. В ідеальному випадку є можливість визначити технічний стан по одному діагностичному портрету та одному спостереженню.

Теоретично це можливо, оскільки ймовірності появи символів спостереження b_i не рівні, отже можуть існувати такі діагностичні параметри підвищеної якості, які у одному повідомленні (діагностичному портреті) несуть всю (чи майже всю) інформацію про технічний стан ОД.

Діагностичні параметри підвищеної якості однозначно (з імовірністю близькою до одиниці) пов'язані з технічним станом. Має сенс говорити про умовну ентропію появи спостереження $0_i, i = 1, ..., N$ при технічному стані $S_i, i = 1, ..., M$, оскільки в структурі ПММ спостерігаються два стохастичні процеси. Ця умовна ентропія на підставі формули Шеннона запишеться наступним чином:

$$H(S_i 0_j) = \sum_{i=1}^{M}\sum_{j=1}^{N} P(S_i 0_j)\log P(S_i 0_j) = -\sum_{i=1}^{M}\sum_{j=1}^{N} P(S_i)\, P_{S_i}(0_j)\log\left[P(S_i)\, P_{S_i}(0_j)\right] =$$

$$= -\sum_{i=1}^{M} P(S_i)\log P(S_i)\sum_{j=1}^{N} P_{S_i}(0_j) - \sum_{i=1}^{M} P(S_i)\sum_{j=1}^{N} P_{S_i}(0_j)\log P_{S_i}(0_j),$$

де $P(S_i 0_j) = P(S_i, 0_j)$ $P_{S_i}(0_j)$ – ймовірність появи спостереження 0_j, $j = 1, ..., M$ при технічному стані S_i, $j = 1, ..., M$;

$P_{S_i}(0_j)$ – умовна ймовірність появи символів спостереження, що визначається b_i;

$P(S_i)$ – ймовірність технічного стану S_i.

З виразу (6) витікає, що для підвищення умовної ентропії (інформативності) спостережень необхідні неповторювані спостереження. У діагностичному портреті інформативність за деяким дефектом сприймається як визначення технічного стану, виявлене за допомогою симптомів цього дефекту. Очевидно, що максимальна інформативність матиме діагностичні портрети, зняті з максимальної кількості конкретних точок, що значно збільшує розмірність простору технічних станів. Мінімальна інформативність матиме діагностичні портрети, зняті в одній контрольній точці, проте при цьому важко приймати рішення про технічний стан (важко локалізувати місце дефекту через брак інформації про технічний стан).

Таким чином, діагностичні моделі, представлені ПММ, задовольняють концепції дискретних ланцюгів Маркова і є їх розвитком на випадок розпізнавання технічного стану. Отже, з великою ймовірністю можна використовувати математичний апарат ПММ для опису самообробних (нейроморфних) мереж, що представляють простір технічних станів ОД.

Нейромережева система розпізнавання технічного стану. Як вже було раніше зазначено, розпізнавання технічного стану визначається як комплекс задач, пов'язаних із перетворенням та обробкою вхідної інформації у вихідну. Вхідною інформацією служать портрети об'єкта контролю та діагностування (сигнали, параметри, ознаки об'єктів розпізнавання), а вихідною – прийняте рішення про віднесення об'єктів (образів), що розпізнаються, до деякого класу (діагнозу простору технічного стану). Також відомо, що розпізнавання базується на математичному апараті теорії прийняття рішення про технічний стан об'єкта контролю та діагностування, і задача розпізнавання є дискретним аналогом задачі пошуку оптимальних рішень. При цьому задача розпізнавання технічного стану може бути представлена у вигляді етапів її розв'язання (рис. 3).

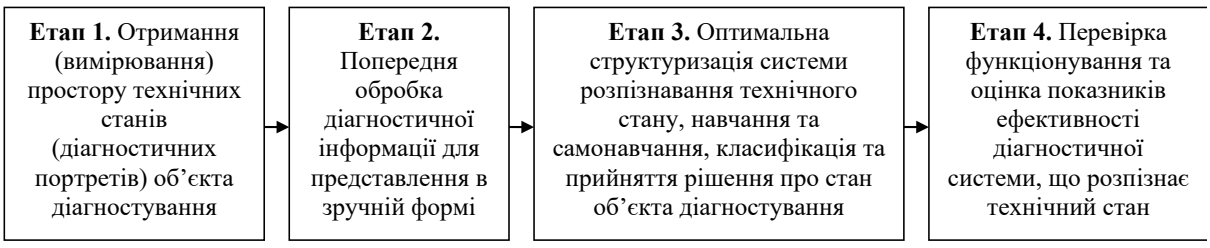


Рис. 3. Етапи вирішення задачі розпізнавання технічного стану

Так, враховуючи складність розпізнавання технічного стану мікропроцесорних систем, в технічній діагностиці вже певний час чітко проявляється тенденція щодо використання елементів та компонентів штучного інтелекту як діагностичних систем, а саме штучних нейронних мереж.

Штучні нейронні мережі – це універсальний апроксиматор [16], що складається зі взаємопов’язаної сукупності простих обчислювальних елементів – нейронів. В результаті аналізу роботи нейронних механізмів мозку може бути відбудована множина моделей, які відрізняються одна від одної вихідними концепціями, рівнем узагальнень, запропонованих спрощень тощо.

Так, згідно з [17; 18] новим витком розвитку та застосування штучних нейронних мереж стала поява ПЛІС, які своєю організацією дозволили не лише проєктувати адаптивні мікропроцесорні системи, а й апаратно-програмним шляхом реалізувати нейрони, об’єднуючи їх у мережу. Крім цього, архітектура ПЛІС дозволила за допомогою мов опису апаратури синтезувати нейронні процесори, а також реалізувати метод Built-Inself-Test (самодіагностування), шляхом розміщення нейронної мережі разом із мікропроцесорною системою на одному кристалі ПЛІС (рис. 4).

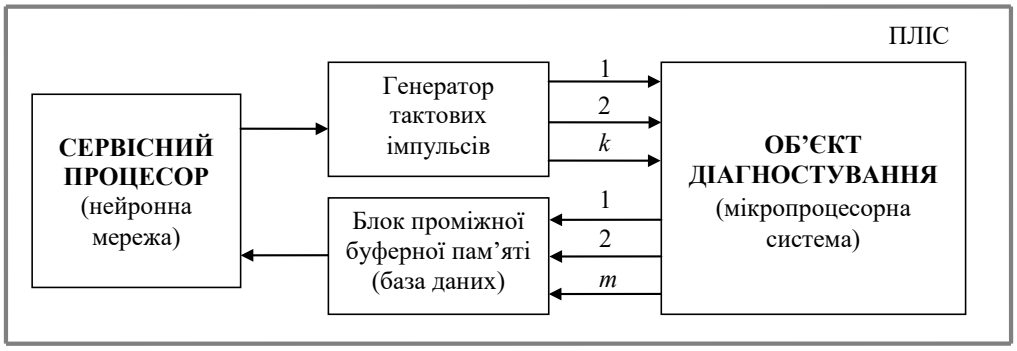


Рис. 4. Структурна схема системи самодіагностування

Зазначимо, що до складу системи самодіагностування мікропроцесорної системи входять: сервісний процесор, який формує блок тест-векторів і записує їх у генератор тактових імпульсів; блок проміжної буферної пам’яті для запам’ятовування відповідних реакцій; об’єкт діагностування. Принцип дії системи самодіагностування можемо інтерпретувати наступним чином. Генератор тактових імпульсів за сигналом сервісного процесора на основі записаного блоку тест-векторів формує тестові впливи, які через паралельні незалежні канали подаються на об’єкт діагностування. При подачі на об’єкт діагностування тестових впливів на його виходах з’являються сигнали відповідних реакцій, які в подальшому через канали фіксуються в блоці проміжної буферної пам’яті (база даних) та зчитуються сервісним процесором у вигляді векторів відповідних реакцій для подальшого аналізу. Так, у роботі [16] в якості сервісного процесору запропоновано використовувати нейронну мережу Хопфілда, фрагмент якої представлено на рисунку 5.

Таким чином, реалізована на ПЛІС система самодіагностування мікропроцесорної системи, в основі якої лежить штучна нейронна мережа, являє собою НМС РТС, принцип дії якої можемо інтерпретувати наступним чином.

У процесі розпізнавання технічного стану на вхід НМС РТС надходить діагностична інформація у вигляді набору симптомів (діагностичного портрета), що призводить до збудження нейронів. При цьому рівень збудження залежить від ймовірності зв’язку передачі збудження та визначається вагою $G_\alpha(K)$. І, як наслідок, на виходах нейроподібних елементів створюється відображення діагностичної інформації у вигляді розподілу збуджень. Залежно від рівня збудження (ваги) збуджується певний синаптичний зв’язок, який передає збудження з вагою $G_\alpha(K)$, що є ефективністю синапсу.

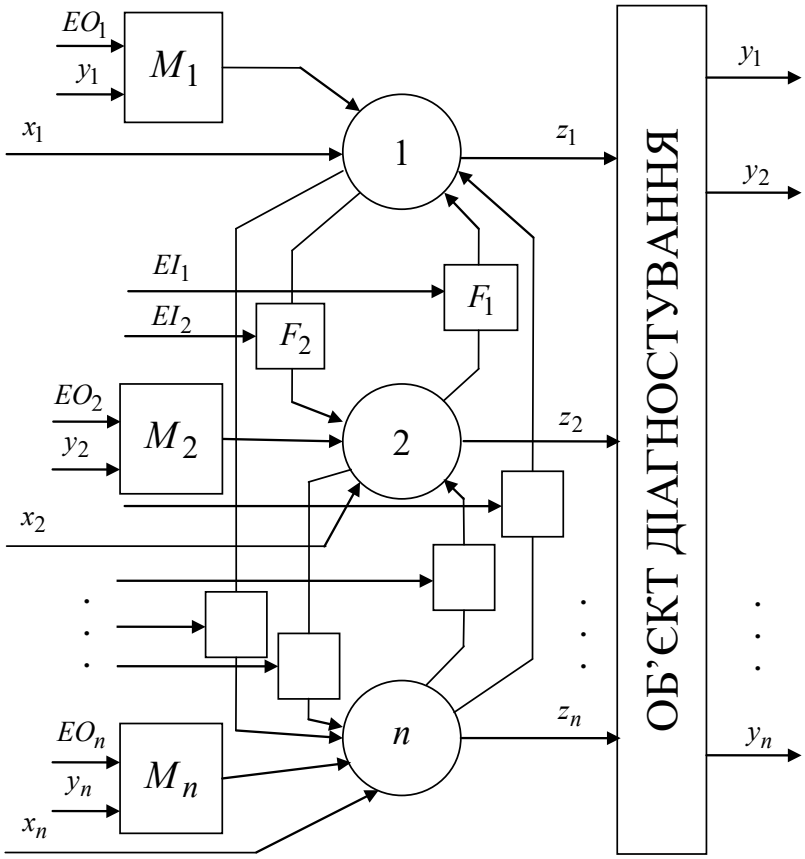


Рис. 5. Фрагмент структури генератора тактових імпульсів
на нейронній мережі Хопфілда

Реакція нейрона в алгоритмі розпізнавання технічного стану визначається добутком попарних оцінок ймовірностей з виходів рецепторів та відповідних ваг синаптичних зв'язків і має вигляд:

$$g_i(K) = \prod_{\alpha=1}^{r} G_\alpha(K)\, d_\alpha(K),$$

де $d_\alpha(K) = \begin{cases} 1, \textit{при } X_\alpha = U_\alpha, \\ 0, \textit{при } X_\alpha \neq U_\alpha, \end{cases}$ – індикатор рівня збудження нейрона;

$G_\alpha(K)$ – величина ефективності синаптичного зв'язку α -входу нейрона;

U_α – еталонне значення α -симптомів.

При цьому $\sum_{k=1}^{r} d_\alpha(K) = 1$. В результаті на виході нейронного ансамблю формується сигнал

$$\Lambda_i(x) = \prod_{k=0}^{n} \prod_{\alpha=1}^{r} g_i(K).$$

Такі діагностичні нейронні мережі є спрощеною просторово-часовою моделлю, оскільки не враховують її нелінійність. Однак вони мають асоціативні властивості, які нагадують властивості біологічних систем. Інформація про технічний стан ОД представляється мережею пов'язаних станів-вузлів та впорядкованим поширенням активності через мережу. Це мережа одночасно активних елементів, які обробляються (станів та переходів-асоціацій), локальні взаємодії яких у часі визначають поведінку

діагностичної системи. Таку НМС РТС зручно розглядати як систему, що містить три основні частини: мережу або просторово-пов'язані стани, правила активації (збудження мережі) та правила навчання (переоцінки параметрів).

Запропонована НМС РТС складатиметься зі станів-вузлів, з'єднаних спрямованими зв'язками-асоціаціями. Діагностична модель представляється коннекціоністською моделлю, яка має справу з діагностичною інформацією та втілює ідею нейроморфного моделювання. Кожен вузол такої мережі є конкретним станом S_i з простору спостережуваних станів $S_1, S_2, ..., S_n$. Він має певний рівень активності, що відповідає цьому вузлу на момент часу t.

Рівень активності вузла в коннекціоністській моделі відображає ступінь відповідності стану S_i послідовності спостережень O і є імовірнісною характеристикою $P(O/L)$, отриманою із ПММ $L(A, B, \Pi)$. Ця активність у кожний момент часу передається сусіднім вузлам згідно з правилом активації. Сумарна вхідна активність $(i-1)\,N_{i-1}(t)$, яку вузол N у кожний момент отримує від сусідніх вузлів, змінює власний рівень активності, що фіксується індикатором рівня збудження $d_\alpha(K)$. Зв'язкам у такій діагностичній моделі приписані певні характеристики їхньої сили, які використовуються при обчисленні оновлених значень активності вузлів.

Всі зв'язки від вузла N_i до вузла N_j є вагами синаптичного зв'язку $G_\alpha(K)$, отриманого на основі ймовірності переходів із ПММ – $A = \{a_{ij}\}$. Якщо активність вузла N_i прагне збільшити активність сусіднього вузла N_j, то з'єднання, що йде від вузла N_i до N_j вузла, є збуджуючим зв'язком $d_\alpha(K) = 1$. І навпаки, якщо активність вузла N_i прагне зменшити чи змінює активність в N_j, то зв'язок гальмує, і відповідає $d_\alpha(K) = 0$.

Правило активації є процедурою, за якою рівень активності кожного вузла змінюється залежно від впливів з боку сусідніх вузлів. Тут проявляється яскраво виражена паралельність поширення збудження по мережі та обробка всієї діагностичної інформації у вигляді локальних взаємодій між сусідніми вузлами.

Так, перші дві компоненти (мережа і правило активації) є класифікатором, третій компонент – НМС РТС – це правила навчання. Під навчанням НМС РТС розуміють всяку зміну поведінки мережі в результаті подій, що відбулися. У діагностичних моделях правила навчання зазвичай представляють процедуру параметричної самоорганізації, яка описує закономірність зміни ваги зв'язків $G_\alpha(K)$ залежно від спостережень.

У загальному вигляді структуру НМС РТС та алгоритм синтезу можемо описати виразом (9) за умови, що маємо m класів технічних станів.

$$\Lambda^{(0)} = \left\| \Lambda_i(X) = \prod_{k=1}^{m} \left[\prod_{k=1}^{n} \prod_{\alpha=1}^{\kappa} G_\alpha(K) \right] \right\| \tag{9}$$

Відповідно до (9) структура НМС РТС складатиметься з m нейронних ансамблів (мереж), кожна з яких містить $(n-1)$ нейронів, що має r зв'язків, кількість яких змінюється в процесі навчання.

Кінцевою метою НМС є розпізнавання технічного стану мікропроцесорної системи, який закінчується при ітераційному повторенні сталого стану нейронної мережі. При збіганні стану нейронної мережі зі станом для еталонної мікропроцесорної системи – мікропроцесорна система, яка діагностується, вважається справною, в іншому випадку вважається несправною. При цьому аналіз розбіжностей еталонного стану та стану

мікропроцесорної системи, яка діагностується, дає інформацію про тип і місце прояву несправності.

Таким чином, розглянутий підхід до розпізнавання технічного стану, в основі якого лежить принцип самодіагностування в сукупності з нейронною мережею, значно підвищує ефективність процесу контролю і діагностування мікропроцесорної системи та відкриває нові можливості щодо автоматизації операції знаходження місця прояву несправностей, поповнення бази даних про несправності та прийняття рішення на відновлення функціонування мікропроцесорної системи.

Висновки. Представлено підхід до вирішення проблеми розпізнавання технічного стану та розробки діагностичних моделей мікропроцесорної системи на основі їх нейронного уявлення, що поєднує приховані марківські та коннекціоністські моделі діагностування. Зазначено, що об’єднання мережевих діагностичних моделей з методами теорії штучного інтелекту дозволить розглядати множину альтернатив інтерпретації діагностичного експерименту, множину спільних симптомів, сформувати метод розпізнавання первинних симптомів (розпізнати дефект), і, зрештою, завдяки виділенню найімовірніших рішень, підвищити ефективність процедури діагностування. Запропоновано формальний метод представлення технічного стану мікропроцесорної системи, який базується на його описі у вигляді ланцюга причинно-наслідкових зв’язків. Такі ланцюги, які реалізовані у вигляді дискретної діагностичної моделі, є втіленням розробленого дискретно-подійного методу, що допускає детерміновано-стохастичну постановку задачі розпізнавання технічного стану мікропроцесорної системи.

Подальшим напрямом наукових досліджень є проєктування в базисі ПЛІС відмовостійких мікропроцесорних систем із вбудованою системою контролю та діагностування з елементами штучного інтелекту, реалізуючи при цьому концепцію «Embedded System – вбудована система та System on Chip – система на кристалі».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Локазюк В. М., Поморова О. В., Домінов А. О. Інтелектуальне діагностування мікропроцесорних пристроїв та систем: навч. посіб. для вузів. К.: «Такі справи», 2001. 286 с.

2. Shtanenko S., Samokhvalov Y., Iohov O., Maliuk V. Microprocessor systems based on programmable logic devices as an object of diagnostics // Advanced Information Systems. 2022. № 6 (1). P. 81–87. URL: https://doi.org/10.20998/2522-9052.2022.1.14.

3. Локазюк В. М. Тестове комбіноване діагностування персональних комп’ютерів / В. М. Локазюк, О. М. Заєць // Вимірювальна та обчислювальна техніка в технологічних процесах: Зб. наук. пр. Хмельницький: ТУП, 2000. С. 160–163.

4. Сакович Л. М., Глухов С. І., Бабій О. С., Гальоса А. О. Методика фізичного діагностування цифрових пристроїв об’єктів радіоелектронної техніки // Системи озброєння і військова техніка. 2020. № 2 (62). С. 93–101.

5. Глухов С. І. Порівняльний аналіз методологій технічного діагностування радіоелектронної техніки / С. І. Глухов, Л. М. Сакович, О. С. Бабій, А. О. Гальоса // Scientific Collection «InterConf», (128): 13th International Scientific and Practical Conference «Science and Practice: Implementation to Modern Society», Manchester, Great Britain, 16-18 October 2022: proceedings. Manchester: Peal Press Ltd., 2022. P. 229–234.

6. Кузавков В., Янковський О., Болотюк Ю. Обґрунтування вибору показників оцінки ефективності функціонування автоматизованої системи контролю // Сучасні інформаційні технології у сфері безпеки та оборони. 2022. № 44. С. 21–27. URL: https://doi.org/10.33099/2311-7249/2022-44-2-21-27.

7. Бабокин Г. И., Шпрехер Д. М. Применение нейронных сетей для диагностики электромеханических систем // Горный информационно-аналитический бюллетень (научно-технический журнал). 2011. № S4. С. 132–139.

8. Горева Т. И., Портнягин Н. Н., Пюкке Г. А. Нейросетевые модели диагностики технических систем // Вестник КРАУНЦ. Физ.-мат. науки. 2012. Вып. 1 (4). С. 31–43. DOI: http://dx.doi.org/10.18454/2079-6641-2012-4-1-31-43.

9. Герасимов Б. М. Інтелектуальні системи підтримки прийняття рішень / Б. М. Герасимов, В. М. Локазюк, О. Г. Оксіюк, О. В. Поморова. К: Вид-во Європ. ун-ту, 2007. 335 с.

10. Shtanenko S., Samokhvalov Y., Toliupa S., Silko O. An Approach to Restore the Proper Functioning of Embedded Systems Due to Adverse Effects. In: Luntovskyy A., Klymash M., Melnyk I., Beshley M., Schill A. (eds) Digital Ecosystems: Interconnecting Advanced Networks with AI Applications. TCSET 2024. Lecture Notes in Electrical Engineering, vol 1198. Springer, Cham. URL: https://doi.org/10.1007/978-3-031-61221-3_28.

11. Mubaraali L., Kuppuswamy N., Muthukumar R. Intelligent fault diagnosis in microprocessor systems for vibration analysis in roller bearings in whirlpool turbine generators real time processor applications // Microprocessors and Microsystems. 2020. Vol. 76. ISSN 0141-9331. URL: https://doi.org/10.1016/j.micpro.2020.103079.

12. Штаненко С. С., Самохвалов Ю. Я., Толюпа С. В. Підхід до визначення технічного стану мікропроцесорних систем реалізованих на програмно-реконфігураційній логіці // Збірник наукових праць ВІТІ «Системи і технології зв’язку, інформатизації та кібербезпеки». 2023. № 4. С. 110–123.

13. Лукова-Чуйко Н. В. Методи інтелектуального розподілу даних в системах виявлення мережевих вторгнень та функціональна стійкість інформаційних систем до кібератак / Н. В. Лукова-Чуйко, С. В. Толюпа, В. С. Наконечний, М. М. Браіловський: монографія. К.: Формат, 2021. 370 с.

14. Toliupa S., Shtanenko S., Silko O., Khusainov P., Kulko A. An Approach to Restore the Proper Functioning of Embedded Systems Due to Cyber Threats. 2023. CEUR Workshop Proceedings, 3624. P. 301–316.

15. Theodor Freiheit. A discrete state Markov chain model and decomposition solution method for the transient behaviour of buffered long serial transfer lines // Journal of Manufacturing Systems. 2023. Vol. 68. P. 493–507. ISSN 0278-6125. URL: https://doi.org/10.1016/j.jmsy.2023.05.010.

16. Герасимов Б. М. Інтелектуальні системи підтримки прийняття рішень: навч. посіб. для студ. вищ. техн. навч. закл. / Б. М. Герасимов [та ін.]; Європейський ун-т. К.: Вид-во ЄУ, 2007. 335 с.

17. Палагин А. В. Особенности проектирования компьютерных систем на кристалле ПЛИС / А. В. Палагин, Ю. С. Яковлев // Науковий журнал «Математичні машини і системи». 2017. № 2. С. 3–14. ISSN 1028-9763.

18. Samokhvalov Y., Toliupa S., Buchyk S., Shtanenko S. Design of Robotic Systems in the Basis of CAD Intel Quartus Prime. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT). Kyiv, Ukraine, 2021. P. 179–183. DOI: 10.1109/ATIT54053.2021.9678857.

19. Толюпа С., Самохвалов Ю., Хусаінов П., Штаненко С. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. № 2 (22). С. 134–147.

АВТОРИ НОМЕРА

1. *Балан Дмитро Дмитрович* – викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

2. *Бернацький Андрій Петрович* – доктор філософії, старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

3. *Бондаренко Дмитро Михайлович* – начальник центру Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, м. Київ, Україна.

4. *Волошин Василь Вікторович* – молодший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

5. *Данилюк Ігор Андрійович* – кандидат технічних наук, доцент, головний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

6. *Думітраш Ольга Вячеславівна* – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

7. *Здоренко Юрій Миколайович* – кандидат технічних наук, доцент, доцент кафедри Національного університету «Полтавська політехніка ім. Юрія Кондратюка», м. Полтава, Україна.

8. *Зінченко Михайло Олександрович* – начальник науково-дослідного управління Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

9. *Ільїнов Михайло Дмитрович* – кандидат технічних наук, доцент, доцент кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

10. *Кисиленко Дар’я Юріївна* – ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

11. *Коваленко Олексій Олександрович* – начальник Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

12. *Ковальчук Богдан Петрович* – кандидат фізико-математичних наук, молодший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

13. *Колтовсков Дмитро Геннадійович* – доктор філософії, старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

14. *Комаров Володимир Олександрович* – кандидат технічних наук, провідний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

15. *Кондратюк Андрій Георгійович* – старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

16. *Корольов Андрій Павлович* – кандидат технічних наук, доцент, доцент кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

17. *Креденцер Борис Петрович* – доктор технічних наук, професор, головний науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

18. *Кузавков Василій Вікторович* – доктор технічних наук, професор, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

19. *Куцаєв Володимир Вікторович* – молодший науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

20. ***Лазута Роман Григорович*** – старший науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

21. ***Ланко Антон Вікторович*** – заступник начальника факультету телекомунікаційних систем Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

22. ***Липський Олександр Анатолійович*** – кандидат технічних наук, доцент, головний науковий співробітник Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, м. Київ, Україна.

23. ***Любарський Сергій Володимирович*** **–** кандидат технічних наук, доцент, доцент кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

24. ***Макаренко Олександр Олексійович*** – старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

25. ***Макарчук Василь Іванович*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

26. ***Масесов Микола Олександрович*** **–** кандидат технічних наук, старший науковий співробітник, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

27. ***Мацаєнко Андрій Миколайович*** **–** кандидат технічних наук, старший викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

28. ***Нестеренко Ігор Костянтинович*** **–** кандидат технічних наук, старший науковий співробітник, доцент кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

29. ***Остапчук Віктор Миколайович*** – кандидат технічних наук, начальник Головного управління зв’язку та кібербезпеки Генерального штабу Збройних Сил України, м. Київ, Україна.

30. ***Панченко Ігор В’ячеславович*** – кандидат технічних наук, начальник кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

31. ***Плугова Ольга Богданівна*** **–** науковий співробітник науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

32. ***Радзівілов Григорій Данилович*** – кандидат технічних наук, професор, заступник начальника Військового інституту телекомунікацій та інформатизації ім. Героїв Крут з наукової роботи, м. Київ, Україна.

33. ***Роскошний Дмитро Володимирович*** – старший викладач кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ, Україна.

34. ***Руденко Володимир Іванович*** **–** старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

35. ***Савченко Віталій Анатолійович*** **–** доктор технічних наук, професор кафедри управління кібербезпекою та захистом інформації Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.

36. ***Сайко Володимир Григорович*** **–** доктор технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

37. ***Самохвалов Юрій Якович*** – доктор технічних наук, професор, професор кафедри інтелектуальних технологій Київського національного університету ім. Тараса Шевченка, м. Київ, Україна.

38. ***Станілога Олександр Олександрович*** **–** ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

39. ***Стефанишин Ярослав Іванович*** – науковий співробітник Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, м. Київ, Україна.

40. ***Терещенко Тетяна Павлівна*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

41. ***Ткач Володимир Олександрович*** **–** старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

42. ***Толюпа Сергій Васильович*** **–** доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченка, м. Київ, Україна.

43. ***Тлустий Андрій Олександрович*** **–** ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

44. ***Унтілова Олена Олексіївна*** **–** ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

45. ***Ушаков Віктор Дмитрович*** – директор, фізична особа – підприємець «Ушаков Віктор Дмитрович», м. Київ, Україна.

46. ***Фесенко Олексій Дмитрович*** **–** доктор філософії, доцент кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

47. ***Фесьоха Віталій Вікторович*** **–** доктор філософії, докторант науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

48. ***Фомкін Денис Валентинович*** **–** науковий співробітник науково-організаційного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

49. ***Хавер Анюта Вячеславівна*** **–** аспірант Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна.

50. ***Хоменко Павло Володимирович*** **–** ад’юнкт науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

51. ***Хусаінов Павло Валентинович*** – кандидат технічних наук, професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

52. ***Цимбал Ірина Володимирівна*** **–** науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

53. ***Черниш Юлія Олександрівна*** – старший науковий співробітник Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

54. ***Шаповал Віталій Михайлович*** **–** начальник науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

55. ***Шарнін Сергій Анатолійович*** **–** викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

56. ***Шемендюк Олександр Віталійович*** – начальник науково-дослідного відділу Наукового центру зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

57. ***Штаненко Сергій Станіславович*** – кандидат технічних наук, доцент, викладач кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

58. ***Яковчук Олександр Вікторович*** **–** начальник науково-дослідного відділу – заступник начальника науково-дослідного управління Військового інституту телекомунікацій та інформатизації ім. 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.